[SCENARIO-DOMAIN-TRUSTS]: Domain Trust Scenarios

Tools. This protocol documentation is intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it. A protocol specification does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them.

Table of Contents

1 Introduction

This document describes state diagrams and protocol usage scenarios for management of Active Directory trust accounts.

1.1 References

1.1.1 Normative References

[C706] The Open Group, "DCE 1.1: Remote Procedure Call"

[MS-ADA1] Microsoft Corporation, "Active Directory Schema Attributes A-L"

[MS-ADA2] Microsoft Corporation, "Active Directory Schema Attributes M"

[MS-ADA3] Microsoft Corporation, Active Directory Schema Attributes N-Z

[MS-APDS] Microsoft Corporation, "Authentication Protocol Domain Support Specification"

[MS-DRSR] Microsoft Corporation, "Directory Replication Service (DRS) Remote Protocol Specification"

[MS-KILE] Microsoft Corporation, "Kerberos Protocol Extensions"

[MS-LSAD] Microsoft Corporation, "Local Security Authority (Domain Policy) Remote Protocol Specification"

[MS-LSAT] Microsoft Corporation, Local Security Authority (Translation Methods) Remote Protocol Specification

[MS-NLMP] Microsoft Corporation, "NT LAN Manager (NTLM) Authentication Protocol Specification"

[MS-NRPC] Microsoft Corporation, "Netlogon Remote Protocol Specification"

[MS-RPCE] Microsoft Corporation, "Remote Procedure Call Protocol Extensions"

[MS-SMB] Microsoft Corporation, "Server Message Block (SMB) Protocol Specification"

[MS-SMB2] Microsoft Corporation, "Server Message Block (SMB) Version 2.0 Protocol Specification"

[RFC2254] T. Howes, The String Representation of LDAP Search Filters, RFC 2254, December 1997, http://www.ietf.org/rfc/rfc2254.txt

1.1.2 Informative References

[HowTrustsWork] "Technet: How Domain and Forest Trusts Work"

[LogonAuthTechnologies] "Technet: Logon and Authentication Technologies"

[ManagingForestTrusts] "Technet: Managing Forest Trusts"

[ManagingTrusts] "Technet: Managing Trusts"

[ManagingTrustedDomainInfo] "Managing Trusted Domain Information"

[TrustTechnologies] "Technet: Trust Technologies"

[Understanding2008Trusts] "Technet: Windows Server 2008: Understanding Trusts"

[UnderstandingADTrusts] "Technet: Active Directory Concepts: Understanding Trusts"

2 Overview

A domain controller (DC) is said to have a *trust account* with a DC in another domain when a Trusted Domain Object (TDO) (and a down-level trust account, if applicable) exists for the other domain. Creation of a trust account is carried out using the lsarpc RPC interface ([MS-LSAD]).

Users in a *trusted* domain can access resources in a *trusting* domain, but users in a *trusting* domain cannot access resources in a *trusted* domain.

An *outgoing* trust is from a *trusting* domain (DomainA) to a *trusted* domain (DomainB). Users in the *trusted* domain (DomainB) can access resources in the *trusting* domain (DomainA), but users in the *trusting* (DomainA) domain cannot access resources in the *trusted* domain (DomainB).

An *incoming* trust is from a *trusted* (DomainA) domain to a *trusting* domain (DomainB). Users in the *trusted* domain (DomainA) can access resources in the *trusting* domain (DomainB), but users in the *trusting* (DomainB) domain cannot access resources in the *trusted* domain (DomainA).

2.1 Trust Accounts

By default, down-level trust accounts are kept in the following Active Directory container:

CN=Users,DC=domain

The trust accounts are named after the NETBIOS domain name of the *trusting* domain with a dollar sign ($) appended and special flags set. They are hidden by Active Directory Users and Computers, but they are visible when you use ADSI Editor (ADSIEdit.msc) or the LDP (ldp.exe) tool.

Netlogon RPC can return any RID as long as that instance of Netlogon RPC is consistently returning the same value for the same secure channel.

The Microsoft implementation uses the RID of the User object; therefore it must be present whenever a trustedDomain object for an inbound or bidirectional trust is present. Hence, when replicating a trustedDomain object to AD, the associated User object must also be replicated.

2.1.1 Outgoing Trust Creation

When creating an *outgoing* trust with another domain, the local (*trusted*) domain will create a TDO, and the remote (*trusting*) domain will create both a trust account and a TDO.

If the local end of the trust only is created, the administrator will be required to provide a trust password.

If both ends of the trust are created, the administrator will not be required to provide a trust password, but will need to provide an account and password for the remote (*trusting*) domain, which will have a trust account and TDO for the local (*trusted*) domain after this operation is completed.

All outgoing external trusts have SID Filtering enabled by default.

2.1.2 Incoming Trust Creation

When creating an *incoming* trust with another domain, the local (*trusting*) domain will create both a trust account and a TDO.

If the local end of the trust only is created, the administrator will be required to provide a trust password.

If both ends of the trust are created, the administrator will not need to provide a trust password, but will need to provide an account and password for the remote (*trusted*) domain, which will have a TDO for the local (*trusting*) domain after this operation is completed.

2.1.3 Sample Trust Account

The following sample TDO comprises an incoming (*trusting*) trust from '2008DOMAIN1.COM' to '2008DOMAIN2.COM'

```
Dn: CN=2008DOMAIN2$,CN=Users,DC=2008DOMAIN1,DC=COM
accountExpires: 9223372036854775807 (never);
badPasswordTime: 0 (never);
badPwdCount: 0;
cn: 2008DOMAIN2$;
codePage: 0;
countryCode: 0;
distinguishedName: CN=2008DOMAIN2$,CN=Users,DC=2008DOMAIN1,DC=COM;
dSCorePropagationData: 0x0 = (  );
```

```
instanceType: 0x4 = ( WRITE );
isCriticalSystemObject: TRUE;
lastLogoff: 0 (never);
lastLogon: 0 (never);
logonCount: 0;
name: 2008DOMAIN2$;
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=2008DOMAIN1,DC=COM;
objectClass (4): top; person; organizationalPerson; user;
objectGUID: 6e70e511-1edb-4b9f-acd5-1209c738b5da;
objectSid: S-1-5-21-2074671935-2981103931-2886920652-1105;
primaryGroupID: 513 = ( GROUP_RID_USERS );
pwdLastSet: 9/12/2008 10:29:56 AM Pacific Daylight Time;
sAMAccountName: 2008DOMAIN2$;
sAMAccountType: 805306370 = ( TRUST_ACCOUNT );
userAccountControl: 0x820 = ( PASSWD_NOTREQD | INTERDOMAIN_TRUST_ACCOUNT );
uSNChanged: 32800;
uSNCreated: 32797;
whenChanged: 9/12/2008 10:29:56 AM Pacific Daylight Time;
whenCreated: 9/12/2008 10:29:56 AM Pacific Daylight Time;
```

2.2 Trusted Domain Objects (TDO)

Trusted domain objects are located in the following Active Directory container:

CN=system,DC=domain

2.2.1 Sample Trusted Domain Objects (TDO)

2.2.1.1 Sample outgoing (*trusted*) TDO

The following sample TDO comprises an outgoing (*trusted*) trust from '2008DOMAIN1.COM' to '2008DOMAIN2.COM':

```
Dn: CN=2008DOMAIN2.COM,CN=System,DC=2008DOMAIN1,DC=COM
cn: 2008DOMAIN2.COM;
distinguishedName: CN=2008DOMAIN2.COM,CN=System,DC=2008DOMAIN1,DC=COM;
dSCorePropagationData: 0x0 = (  );
instanceType: 0x4 = ( WRITE );
isCriticalSystemObject: TRUE;
name: 2008DOMAIN2;
objectCategory: CN=Trusted-Domain,CN=Schema,CN=Configuration,DC=2008DOMAIN1,DC=COM;
objectClass (3): top; leaf; trustedDomain;
objectGUID: 36bf3015-f63d-48fa-927f-192655beeaf9;
securityIdentifier: <ldp: Binary blob 24 bytes>;
showInAdvancedViewOnly: TRUE;
trustAttributes: 0x8 = ( FOREST_TRANSITIVE );
trustDirection: 2 = ( OUTGOING );
trustPartner: 2008DOMAIN2.COM;
trustPosixOffset: -2147483648;
trustType: 2 = ( UPLEVEL );
uSNChanged: 16417;
```

```
uSNCreated: 16416;
whenChanged: 9/5/2008 5:42:27 AM Pacific Daylight Time;
whenCreated: 9/5/2008 5:42:27 AM Pacific Daylight Time;
```

2.2.1.2 Sample incoming (*trusting*) TDO

The following sample TDO comprises an incoming (*trusting*) trust from '2008DOMAIN1.COM' to '2008DOMAIN2.COM':

```
Dn: CN=2008DOMAIN2.COM,CN=System,DC=2008DOMAIN1,DC=COM
cn: 2008DOMAIN2.COM;
distinguishedName: CN=2008DOMAIN2.COM,CN=System,DC=2008DOMAIN1,DC=COM;
flatName: 2008DOMAIN2;
dSCorePropagationData: 0x0 = (  );
instanceType: 0x4 = ( WRITE );
isCriticalSystemObject: TRUE;
name: 2008DOMAIN2;
objectCategory: CN=Trusted-Domain,CN=Schema,CN=Configuration,DC=2008DOMAIN1,DC=COM;
objectClass (3): top; leaf; trustedDomain;
objectGUID: 7a55d3d1-a05f-49e3-9ab4-72dae26e3326;;
securityIdentifier: <ldp: Binary blob 24 bytes>;
showInAdvancedViewOnly: TRUE;
trustAttributes: 0x0 = (   );
trustDirection: 1 = ( INBOUND );
trustPartner: 2008DOMAIN2.COM;
trustPosixOffset: 0;
trustType: 2 = ( UPLEVEL );
uSNChanged: 90138;
uSNCreated: 90130;
whenChanged: 10/2/2008 9:38:14 AM Eastern Daylight Time;
```

whenCreated: 10/2/2008 9:35:57 AM Eastern Daylight Time;

2.3 Trust Passwords

Both domains in a trust relationship share a password, which is stored in the TDO object in Active Directory. As part of the account maintenance process, every thirty days, the trusting domain controller changes the password stored in the TDO. Because all two-way trusts are actually two one-way trusts going in opposite directions, the process occurs twice for two-way trusts. To change a password, domain controllers in domains on each side of the trust complete the following process:

1. The primary domain controller (PDC) emulator in the *trusting* domain creates a new password. A domain controller in the *trusted* domain never initiates the password change; it is always initiated by the *trusting* domain PDC emulator.

2. The domain controller in the *trusting* domain sets the OldPassword field of the TDO object to the previous NewPassword field.

3. The domain controller in the *trusting* domain sets the NewPassword field of the TDO object to the new password.

4. Keeping a copy of the previous password makes it possible to revert to the old password if the domain controller in the *trusted* domain fails to receive the change, or if the change is not replicated before a request is made that uses the new trust password.

5. The domain controller in the *trustin*g domain makes remote call to a domain controller in the *trusted* domain asking it to set the password on the trust account to the new password.

a. The domain controller in the *trusted* domain changes the trust password to the new password.

b. The password is now changed on both domain controllers. Normal replication distributes the TDO objects to the other domain controllers in the domain. However, is possible for the domain controller in the *trusting* domain to change the password without successfully updating a domain controller in the *trusted* domain. This might occur because a secured channel, which is required to process the password change, could not be established. It is also possible that the domain controller in the *trusted* domain might be unavailable at some point during the process and might not receive the updated password.

c. To deal with situations in which the password change is not successfully communicated, the domain controller in the *trusting* domain never changes the new password unless it has successfully authenticated (set up a secured channel) using the new password. This is why both the old and new passwords are kept in the TDO object of the *trusting* domain. Because a password change is not finalized until authentication using the password succeeds, the old, stored password can be used over the secured channel until the domain controller in the *trusted* domain receives the new password, thus enabling uninterrupted service.

d. If authentication using the new password fails because the password is invalid, the *trusting* domain controller tries to authenticate using the old password. If it authenticates successfully with the old password, it resumes the password change process within 15 minutes.

e. Most trust passwords propagate to all domain controllers within a day. Trust passwords have a default lifetime of 30 days, by which time all domain controllers will have received the new password.

The key version number of the trust password for a trust object is set by invoking LsarSetTrustedDomainInfoByName when the trust is created. It is incremented by 1 each time the trust password is changed. The key version number can be determined at any time by making an LsarQueryTrustedDomainInfoByName request or parsing the trustAuthInfoIncoming / trustAuthInfoOutgoing attributes using the information provided in [MS-ADTS] trustAuthInfo Attributes, and looking for an LSAPR_AUTH_INFORMATION structure with AuthType equal to TRUST_AUTH_TYPE_VERSION (3).

Please refer to [MS-ADTS] Trust Objects for additional information.

2.4 Verifying a Trust

A *trusting* domain verifies the status of the secure channel to a *trusted* domain DC using NetrLogonControl2Ex (NETLOGON_INFO_2). On Windows Server 2003 and later, NETLOGON_CONTROL_TC_VERIFY (0x0000000A) verifies the current status of the specified trusted domain secure channel.

This operation is equivalent to the following:

```
DWORD My NetrLogonControl2Ex(
                             LOGONSRV_HANDLE  ServerName,
                             PNETLOGON_INFO_2 pNetlogonInfo2,
                             wchar_t*         TrustedDomainName)
{
     return NetrLogonControl2Ex(
          ServerName,                 // RPC Binding Handles for Netlogon Methods
          NETLOGON_CONTROL_TC_VERIFY, // 0x0000000A
          NETLOGON_INFO_2,            // 0x00000002
          (PNETLOGON_CONTROL_DATA_INFORMATION)TrustedDomainName,
          (PNETLOGON_CONTROL_QUERY_INFORMATION)pNetlogonInfo2);
}
```

3 Managing Trust Accounts

3.1 Create a Trust - State Changes

3.1.1 Outgoing Trust - State Changes

The following state changes occur as a part of creating an *outgoing* trust operation:

Initial State

Server (DC)	Server (DC)
PrimaryDomain.DomainName = "2008DOMAIN1.COM"	PrimaryDomain.DomainName = "2008DOMAIN2.COM"
CN-System TDO = {null}, CN=Users account = {null}	CN-System TDO = {null}, CN=Users account = {null}

Final State

Server (DC)	Server (DC)
PrimaryDomain.DomainName = "2008DOMAIN1.COM"	PrimaryDomain.DomainName = "2008DOMAIN2.COM"
CN-System TDO = {2.2.1.1 Sample outgoing (trusted) TDO}, CN=Users account = {null}	CN-System TDO = {0 Sample TDO}, CN=Users account = {2.1.2 Sample Trust Account}

3.1.2 Incoming Trust - State Changes

The following state changes occur as a part of creating an *incoming* trust operation:

Initial State

Server (DC)	Server (DC)
PrimaryDomain.DomainName = "2008DOMAIN1.COM"	PrimaryDomain.DomainName = "2008DOMAIN2.COM"

Server (DC)	Server (DC)
CN-System TDO = {null}, CN=Users account = {null}	CN-System TDO = {null}, CN=Users account = {null}

Final State

Server (DC)	Server (DC)
PrimaryDomain.DomainName = "2008DOMAIN1.COM"	PrimaryDomain.DomainName = "2008DOMAIN2.COM"
CN-System TDO = {2.2.1.2 Sample incoming (trusting) TDO}, CN=Users account = {2.1.2 Sample Trust Account}	CN-System TDO = {null}, CN=Users account = {null}

4 Message Sequencing

4.1 Summary

4.2 Protocol Specification Reference Table

The following table lists the protocol documents that correspond to the operations shown in this document.

Protocol message	Protocol specification title	Details
Locate a domain controller.	[MS-ADTS]: Active Directory Technical Specification	Locating a domain controller: LDAP (CLDAP) "Ping"
Connection management.	[MS-SMB]: Server Message Block (SMB) Protocol Specification [MS-SMB2]: Server Message Block (SMB) Version 2.0 Protocol Specification	SMB_COM_NEGOTIATE SMB2 CLOSE SMB2 CREATE SMB2 LOGOFF SMB2 NEGOTIATE

Protocol message	Protocol specification title	Details
		SMB2 SESSION_SETUP SMB2 TREE_CONNECT SMB2 TREE_DISCONNECT
Policy object methods, trusted domain object methods and common object methods.	[MS-LSAD]: Local Security Authority (Domain Policy) Remote Protocol Specification	LsarClose LsarCreateTrustedDomainEx2 LsarDeleteObject LsarLookupNames4 LsarOpenPolicy2 LsarOpenTrustedDomainByName LsarQueryInformationPolicy2 LsarQueryTrustedDomainInfo LsarQueryTrustedDomainInfoByName LsarSetTrustedDomainInfoByName
Secure channel establishment methods and maintenance and domain trust methods.	[MS-NRPC]: Netlogon Remote Protocol Specification	DsrEnumerateDomainTrusts NetrLogonControl2Ex NetrLogonSamLogonWithFlags

Protocol message	Protocol specification title	Details
		NetrServerAuthenticate3 NetrServerGetTrustInfo NetrServerReqChallenge
Look up each of a set of objects in the directory and return it to the caller in the requested format.	[MS-DRSR]: Directory Replication Service (DRS) Remote Protocol Specification	IDLDRSBind (IDL_DRSBind) IDLDRSCrackNames (IDL_DRSCrackNames) IDLDRSUnbind (IDL_DRSUnbind)

4.3 *Protocol Action Descriptions and References*

All network traces in this document were produced using Microsoft Network Monitor 3.2.

1. 5.1 LDAP (CLDAP) "Ping"

   This is used to verify the aliveness of a domain controller as described in LDAP "Ping", and to check the Netlogon attribute (see NetrLogonSamLogonEx). This is an LDAP *rootDSE* search ([MS-ADTS] rootDSE Attributes) that retrieves the nonexistent attribute "NetLogon". The LDAP search filter [RFC2254] included in the SearchRequest is a one-level AND of equality tests of the following elements: DnsDomain, Host, NtVer.

   Example:

DnsDomain=2008DOMAIN2.COM)(Host=2008DOMAIN1DC1)(NtVer==\04\04\16\00\00\01))

This operation is equivalent to invoking the Win32 API 'DsGetDcName' function, as shown below:

```
DWORD MyDsGetDcName(
                    LPCTSTR                  DomainName,
                    PDOMAIN_CONTROLLER_INFO* ppdci)
{
   return ::DsGetDcName(
                        NULL,
                        DomainName,
                        NULL,
                        NULL,
                        DS_RETURN_DNS_NAME,
                        ppdci);
}
```

2000 Functional Level: NtVer==\04\04\16\00\00\01
2003 Functional Level: NtVer==\04\04\16\00\00\01
2008 Functional Level: NtVer==

2. 5.2 Name Resolution (DNS)

If necessary, this operation is part of the '5.2.2 SMB: Session Control' operation.

   a. 5.2.1 DNS: 2008DOMAIN1.COM Queries for 2008DOMAIN2.COM
   b. 5.2.2 DNS: 2008DOMAIN2.COM Queries for 2008DOMAIN1.COM

3. 5.2.2 SMB: Session Control ([SMB2] Message Processing Events and Sequencing Rules)
   a. 5.3.1 SMB -> SMB2: Session Control ([SMB2] Connecting to a Share by Using a Multi-Protocol Negotiate)
      i. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE
      ii. 5.3.1.2 SMB2: SMB2 SESSION_SETUP
      iii. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (IPC$)
      iv. 5.3.1.4 SMB2: SMB2 TREE_DISCONNECT
      v. 5.3.1.5 SMB2: SMB2 LOGOFF

   b. 5.3.2 SMB2 Session Control ([SMB2] Connecting to a Share by Using an SMB2 Negotiate)
      i. 5.3.2.1 SMB2: SMB2 NEGOTIATE
      ii. 5.3.2.2 SMB2: SMB2 SESSION_SETUP
      iii. 5.3.2.3 SMB2: SMB2 TREE_CONNECT (IPC$)
4. 5.4 lsarpc ([MS-LSAD]: Local Security Authority (Domain Policy) Remote Protocol Specification)
   a. 5.4.1 SMB2 / RPC : lsarpc Session Control
      i. 5.4.1.1 SMB2: SMB2 CREATE lsarpc
      ii. 5.4.1.2 RPC: Bind to lsarpc ([C706])
      iii. 5.4.1.3 lsarpc: LsarClose
      iv. 5.4.1.4 SMB2: SMB2 CLOSE
      v. 5.4.1.5 SMB2: SMB2 LOGOFF
   b. 5.4.2 TCP / RPC: lsarpc Session Control
   c. 5.4.3 lsarpc: Procedure Calls

4. 5.5.1.1.4 SMB2: SMB2 TREE_DISCONNECT
5. 5.5.1.1.5 SMB2: SMB2 LOGOFF

ii. 5.5.1.2 Netlogonr: Session Control (EPT) ([C706])

1. 5.5.1.2.1 RPC: c/o Bind (EPT) ([C311])
2. 5.5.1.2.2 Epm: Request: ept_map (Netlogonr) ([C706])
3. 5.5.1.2.3 RPC: Bind to Netlogonr ([C706])
4. 5.5.1.2.4 RPC: Alter Context (security context) ([C706])

b. 5.5.2 Netlogonr: Procedure Calls ([MS-NRPC] Message Processing Events and Sequencing Rules)

i. 5.5.2.1 Netlogonr: DsrEnumerateDomainTrusts
ii. 5.5.2.2 Netlogonr: NetrLogonControl2Ex
iii. 5.5.2.3 Netlogonr: NetrServerReqChallenge
iv. 5.5.2.4 Netlogonr: NetrServerAuthenticate3

NetrServerAuthenticate3 queries the trusted domain object using the value in the accountName field.

AccountName: A null-terminated Unicode string that identifies the name of the account that contains the secret key (password) that is shared between the client and the server. If there is a period (".") at the end of the account name, that is ignored during processing.

As the documentation states for NetrServerAuthenticate3, SecureChannelType indicates the type of secure channel being established. TrustedDnsDomainSecureChannel: A secure channel between two DCs, connected through a trust relationship created between two Windows 2000 Server or Windows Server 2003 domains. A Trusted Domain Object (TDO) is used in this type of channel. See 7.1.6.7 "Essential Attributes of a Trusted Domain Object" in [MS-ADTS] for information about TDO.

        v. 5.5.2.5 Netlogonr: NetrServerGetTrustInfo (Get the Trust Password)
        vi. 5.5.2.6 Netlogonr: NetrLogonSamLogonWithFlags

6. 5.6 DRSUAPI [MS-DRSR]: Directory Replication Service (DRS) Remote Protocol Specification
    a. 5.6.1 DRSUAPI: Session Control
        i. 5.6.1.1 RPC Bind to ept ([C706])
        ii. 5.6.1.2 ept_map to DRSUAPI ([C706])
        iii. 5.6.1.3 RPC: c/o Bind to DRSUAPI ([C706])
        iv. 5.6.1.4 RPC: c/o Alter Cont (update security context) ([C706])
    b. 5.6.2 DRSUAPI: Procedure calls
        i. 5.6.2.1 DRSUAPI: IDLDRSBind (IDL_DRSBind)
        ii. 5.6.2.2 DRSUAPI: IDLDRSCrackNames (IDL_DRSCrackNames)

This is equivalent to the call shown below:

```
ULONG MyCrackCanonicalNameToFQDN(
                                 DRS_HANDLE       hDrs,
                                 LPCWSTR          pwzDomainName,
                                 PDS_NAME_RESULT *ppNameResult)
{
   DS_NAME_RESULT      NameResult;
   DRS_MSG_CRACKREQ_V1 Request;
   DRS_MSG_CRACKREPLY  Reply;
   DWORD               dwOutVersion = 1;
   DWORD               dwResult     = NO_ERROR;

   Request.V1.CodePage      = ::GetACP();
   Request.V1.LocaleId      = ::GetUserDefaultLCID();
   Request.V1.dwFlags       = DS_NAME_NO_FLAGS;
   Request.V1.formatOffered = DS_CANONICAL_NAME;
   Request.V1.formatDesired = DS_FQDN_1779_NAME;
   Request.V1.cNames        = sizeof(DS_NAME_RESULT_ITEMW);
   Request.V1.rpNames       = (WCHAR **)&pwzDomainName;
   ::SecureZeroMemory(
                         (PVOID)&Reply,
                         (SIZE_T)sizeof(Reply));
   dwResult = ::IDL_DRSCrackNames(
                                    hDrs,
                                    1,
                                    &Request,
                                    &dwOutVersion,
                                    &Reply);
   if (NO_ERROR == dwResult) {
      *ppNameResult = Reply.V1.pResult;
   }
   return Result;
}
```

iii. 5.6.2.3 DRSUAPI: IDLDRSUnbind (IDL_DRSUnbind)

7. 5.7 Kerberos [MS-KILE]: Kerberos Protocol Extensions
    a. 5.7.1 Kerberos: AS Request Sname: krbtgt/ (KDC_ERR_PREAUTH_REQUIRED)
    b. 5.7.2 Kerberos: AS Request Sname: krbtgt/ (Success)
    c. 5.7.3 Kerberos: TGS Request Realm: Sname: cifs/
    d. 5.7.4 Kerberos: TGS Request Sname: krbtgt/2008DOMAIN2.COM
    e. 5.7.5 Kerberos: TGS Request Realm: Sname: LDAP/
8. 5.8 LDAP ([MS-ADTS]: Active Directory Technical Specification : LDAP)
    a. 5.8.1 LDAP: Search Request
    b. 5.8.2 LDAP: Bind Request

4.4 Creating Trusts

The following list enumerates the various operations carried out for trust creation and deletion.

4.4.1 Creating An Outgoing Trust

1. Locate a Domain Controller
    a. 5.1 LDAP (CLDAP) "Ping"
    b. 5.2.1 DNS: 2008DOMAIN1.COM Queries for 2008DOMAIN2.COM
2. Check Domain Policy
    a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE (Socket 1)
    b. 5.3.1.2 SMB2: SMB2 SESSION_SETUP (Socket 1)
    c. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (Socket 1)
    d. 5.4.1.1 SMB2: SMB2 CREATE lsarpc (Socket 1)
    e. 5.4.1.2 RPC: Bind to lsarpc ([C706]) (Socket 1)
    f. 5.4.3.1.1 lsarpc: LsarOpenPolicy2 (ViewLocalInformation) (Socket 1)
    g. 5.4.3.2 lsarpc: LsarQueryInformationPolicy2 (PolicyDnsDomainInformation) (Socket 1)
    h. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE (Socket 2)
    i. 5.3.2.2 SMB2: SMB2 SESSION_SETUP (Socket 2)

   j. 5.3.2.3 SMB2: SMB2 TREE_CONNECT (IPC$) (Socket 2)
   k. 5.4.1.3 lsarpc: LsarClose (Socket 1)

3. Create the TDO on the Remote Domain
   a. 5.7.1 Kerberos: AS Request Sname: krbtgt/ (KDC_ERR_PREAUTH_REQUIRED) (For Socket 2)
   b. 5.7.2 Kerberos: AS Request Sname: krbtgt/ (Success) (For Socket 2)
   c. 5.7.3 Kerberos: TGS Request Realm: Sname: cifs/ (For Socket 2)
   d. 5.7.4 Kerberos: TGS Request Sname: krbtgt/2008DOMAIN2.COM (For Socket 2)
   e. 5.4.1.1 SMB2: SMB2 CREATE lsarpc (Socket 2)
   f. 5.4.1.2 RPC: Bind to lsarpc ([C706]) (Socket 2)
   g. 5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret) (Socket 2)
   h. 5.4.3.4 lsarpc: LsarQueryTrustedDomainInfoByName (TrustedDomainFullInformation) (Socket 2)
   i. 5.4.3.5.1 lsarpc: LsarCreateTrustedDomainEx2 (Outgoing) (Socket 2)
   j. 5.4.1.3 lsarpc: LsarClose (Socket 2)
   k. 5.4.1.4 SMB2: SMB2 CLOSE (Socket 2)

4. Get the Trust Password (Verify)
   a. 5.5.1.2.1 RPC: c/o Bind (EPT) ([C706]) (Socket 3)
   b. 5.5.1.2.2 Epm: Request: ept_map (Netlogonr) ([C706]) (Socket 3)
   c. 5.5.1.2.3 RPC: Bind to Netlogonr ([C706]) (Socket 3)
   d. 5.5.2.3 Netlogonr: NetrServerReqChallenge (Socket 3)
   e. 5.5.2.4 Netlogonr: NetrServerAuthenticate3 (Socket 3)
   f. 5.5.1.2.4 RPC: Alter Context (security context) ([C706]) (Socket 3)
   g. 5.5.2.5 Netlogonr: NetrServerGetTrustInfo (Socket 3)

5. Cleanup
   a. 5.4.1.4 SMB2: SMB2 CLOSE (Socket 2)

    b. 5.4.1.4 SMB2: SMB2 CLOSE (Socket 1)

4.4.2 Creating An Incoming Trust

1. Locate a Domain Controller
    a. 5.1 LDAP (CLDAP) "Ping"
    b. 5.2.1 DNS: 2008DOMAIN1.COM Queries for 2008DOMAIN2.COM
2. Check Domain Policy (Socket 1)
    a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE (Socket 1)
    b. 5.3.1.2 SMB2: SMB2 SESSION_SETUP (Socket 1)
    c. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (Socket 1)
    d. 5.4.1.1 SMB2: SMB2 CREATE (Socket 1)
    e. 5.4.1.2 RPC: Bind to lsarpc (Socket 1) ([C706])
    f. 5.4.3.1.1 lsarpc: LsarOpenPolicy2 (ViewLocalInformation) (Socket 1)
    g. 5.4.3.2 lsarpc: LsarQueryInformationPolicy2 (PolicyDnsDomainInformation) (Socket 1)
    h. 5.4.1.3 lsarpc: LsarClose (Socket 1)
3. Create the TDO on the Remote Domain
    a. 5.7.1 Kerberos: AS Request Sname: krbtgt/ (KDC_ERR_PREAUTH_REQUIRED) (For Socket 2)
    b. 5.7.2 Kerberos: AS Request Sname: krbtgt/ (Success) (For Socket 2)
    c. 5.7.3 Kerberos: TGS Request Realm: Sname: cifs/ (For Socket 2)
    d. 5.7.4 Kerberos: TGS Request Sname: krbtgt/2008DOMAIN2.COM (For Socket 2)

e. 5.3.2.1 SMB2: SMB2 NEGOTIATE (Socket 2)
f. 5.3.2.2 SMB2: SMB2 SESSION_SETUP (Socket 2)
g. 5.3.2.3 SMB2: SMB2 TREE_CONNECT (IPC$)
h. 5.4.1.2 RPC: Bind to lsarpc ([C706]) (Socket 2)
i. 5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret) (Socket 2)
j. 5.4.3.4 lsarpc: LsarQueryTrustedDomainInfoByName (TrustedDomainFullInformation) (Socket 2)
k. 5.4.1.3 lsarpc: LsarClose (Socket 2)
l. 5.4.3.5.2 lsarpc: LsarCreateTrustedDomainEx2 (Incoming) (Socket 2)
m. 5.4.1.3 lsarpc: LsarClose (Socket 2)
n. 5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret) (Socket 1)
o. 5.4.1.3 lsarpc: LsarClose (Socket 1)
p. 5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret) (Socket 2)
q. 5.4.1.3 lsarpc: LsarClose (Socket 2)

4. Verify the Local End of the Trust

   a. 5.5.1.1.1 SMB2: SMB2 CREATE NETLOGON (Socket 2)
   b. 5.5.1.1.2 RPC: Bind to Netlogonr ([C706]) (Socket 2)
   c. 5.5.2.1 Netlogonr: DsrEnumerateDomainTrusts (Socket 2)
   d. 5.5.1.1.3 SMB2: SMB2 CLOSE (Socket 2)
   e. 5.5.1.1.1 SMB2: SMB2 CREATE NETLOGON (Socket 2)
   f. 5.5.1.1.2 RPC: Bind to Netlogonr ([C706]) (Socket 2)
   g. 5.5.2.2 Netlogonr: NetrLogonControl2Ex (Socket 2)

5. Authenticate with and Get the Trust Information

   a. DRSUAPI

      i. 5.6.1.1 RPC Bind to ept ([C706]) (For Socket 3)

ii. 5.6.1.2 ept_map to DRSUAPI ([C706]) (For Socket 3)
iii. 5.7.5 Kerberos: TGS Request Realm: Sname: LDAP/ (Socket 3)
iv. 5.6.1.3 RPC: c/o Bind to DRSUAPI ([C706]) (Socket 3)
v. 5.6.1.4 RPC: c/o Alter Cont (update security context) ([C706]) (Socket 3)
vi. 5.6.2.1 DRSUAPI: IDLDRSBind (IDL_DRSBind) (Socket 3)
vii. 5.6.2.2 DRSUAPI: IDLDRSCrackNames (IDL_DRSCrackNames) (Socket 3)
viii. 5.6.2.3 DRSUAPI: IDLDRSUnbind (IDL_DRSUnbind) (Socket 3)
ix. 5.8.1 LDAP: Search Request (Socket 3)
x. 5.8.2 LDAP: Bind Request (Socket 3)

b. Get the Trust Password

i. 5.5.1.2.1 RPC: c/o Bind (EPT) ([C706]) (For Socket 4)
ii. 5.5.1.2.2 Epm: Request: ept_map (Netlogonr) ([C706]) (For Socket 4)
iii. 5.5.1.2.3 RPC: Bind to Netlogonr (Socket 4) ([C706])
iv. 5.5.2.3 Netlogonr: NetrServerReqChallenge (Socket 4)
v. 5.5.2.4 Netlogonr: NetrServerAuthenticate3 (Socket 4)
vi. 5.5.1.2.4 RPC: Alter Context (security context) ([C706]) (Socket 4)
vii. 5.5.2.5 Netlogonr: NetrServerGetTrustInfo (Get the Trust Password) (Socket 4)

6. Cleanup

a. 5.4.1.3 lsarpc: LsarClose (Socket 2)
b. 5.5.1.1.3 SMB2: SMB2 CLOSE (Socket 2)
c. 5.4.1.4 SMB2: SMB2 CLOSE (Socket 1)

4.4.3 Creating a 2-Way Trust

1. Locate a Domain Controller
    a. 5.1 LDAP (CLDAP) "Ping"
    b. 5.2.1 DNS: 2008DOMAIN1.COM Queries for 2008DOMAIN2.COM
2. Check Domain Policy (Socket 1)
    a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE (Socket 1)
    b. 5.3.1.2 SMB2: SMB2 SESSION_SETUP (Socket 1)
    c. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (Socket 1)
    d. 5.4.1.1 SMB2: SMB2 CREATE lsarpc (Socket 1)
    e. 5.4.1.2 RPC: Bind to lsarpc (Socket 1) ([C706])
    f. 5.4.3.1.1 lsarpc: LsarOpenPolicy2 (ViewLocalInformation) (Socket 1)
    g. 5.4.3.2 lsarpc: LsarQueryInformationPolicy2 (PolicyDnsDomainInformation) (Socket 1)
    h. 5.4.1.3 lsarpc: LsarClose (Socket 1)
3. Create the TDO on the Remote Domain
    a. 5.7.1 Kerberos: AS Request Sname: krbtgt/ (KDC_ERR_PREAUTH_REQUIRED) (For Socket 2)
    b. 5.7.2 Kerberos: AS Request Sname: krbtgt/ (Success) (For Socket 2)
    c. 5.7.3 Kerberos: TGS Request Realm: Sname: cifs/ (For Socket 2)
    d. 5.7.4 Kerberos: TGS Request Sname: krbtgt/2008DOMAIN2.COM (For Socket 2)
    e. 5.3.2.1 SMB2: SMB2 NEGOTIATE (Socket 2)
    f. 5.3.2.2 SMB2: SMB2 SESSION_SETUP (Socket 2)
    g. 5.3.2.3 SMB2: SMB2 TREE_CONNECT (IPC$) (Socket 2)

   h. 5.4.1.1 SMB2: SMB2 CREATE lsarpc (Socket 2)
   i. 5.4.1.2 RPC: Bind to lsarpc (Socket 2) ([C706])
   j. 5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret) (Socket 2)
   k. 5.4.3.4 lsarpc: LsarQueryTrustedDomainInfoByName (TrustedDomainFullInformation) (Socket 2)
   l. 5.4.1.3 lsarpc: LsarClose (Socket 2)
   m. 5.4.3.5.3 lsarpc: LsarCreateTrustedDomainEx2 (2-way trust) (Socket 2)
   n. 5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret) (Socket 2)
   o. 5.4.1.3 lsarpc: LsarClose (Socket 2)
4. Verify the Local End of the Trust
   a. 5.5.1.1.1 SMB2: SMB2 CREATE NETLOGON (Socket 3)
   b. 5.5.1.1.2 RPC: Bind to Netlogonr ([C706]) (Socket 3)
   c. 5.5.1.2.1 RPC: c/o Bind (EPT) ([C706]) (Socket 3)
   d. 5.5.1.2.2 Epm: Request: ept_map (Netlogonr) ([C706]) (Socket 3)
   e. 5.5.1.2.3 RPC: Bind to Netlogonr ([C706]) (Socket 3)
   f. 5.5.2.1 Netlogonr: DsrEnumerateDomainTrusts (Socket 3)
   g. 5.5.1.1.3 SMB2: SMB2 CLOSE (Socket 3)
   h. 5.5.1.1.1 SMB2: SMB2 CREATE NETLOGON (Socket 3)
   i. 5.5.1.1.2 RPC: Bind to Netlogonr([C706]) (Socket 3)
   j. 5.5.2.2 Netlogonr: NetrLogonControl2Ex (Socket 3)
   k. 5.5.1.1.3 SMB2: SMB2 CLOSE (Socket 3)
5. Get the Trust Password
   a. 5.5.1.2.1 RPC: c/o Bind (EPT) (For Socket 4) ([C706])
   b. 5.5.1.2.2 Epm: Request: ept_map (Netlogonr) ([C706]) (For Socket 4)
   c. 5.5.1.2.3 RPC: Bind to Netlogonr (Socket 4) ([C706])

    d. 5.5.2.3 Netlogonr: NetrServerReqChallenge (Socket 4)
    e. 5.5.2.4 Netlogonr: NetrServerAuthenticate3 (Socket 4)
    f. 5.5.1.2.4 RPC: Alter Context (security context) (Socket 4)
    g. 5.5.2.5 Netlogonr: NetrServerGetTrustInfo (Get the Trust Password) (Socket 4)

6. Cleanup
    a. 5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret) (Socket 1)
    b. 5.4.1.3 lsarpc: LsarClose (Socket 1)

4.5 Deleting Trusts

4.5.1 Deleting an Outgoing Trust

1. Check Domain Policy
    a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE (Socket 1)
    b. 5.3.1.2 SMB2: SMB2 SESSION_SETUP (Socket 1)
    c. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (Socket 1)
    d. 5.4.1.1 SMB2: SMB2 CREATE lsarpc (Socket 1)
    e. 5.4.1.2 RPC: Bind to lsarpc ([C706]) (Socket 1)
    f. 5.4.3.1.1 lsarpc: LsarOpenPolicy2 (ViewLocalInformation) (Socket 1)

g. 5.4.1.3 lsarpc: LsarClose (Socket 1)
h. 5.3.1.4 SMB2: SMB2 TREE_DISCONNECT (Socket 1)
i. 5.3.1.5 SMB2: SMB2 LOGOFF (Socket 1)

2. Delete the Trust Account
   a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE (Socket 2)
   b. 5.7.1 Kerberos: AS Request Sname: krbtgt/ (KDC_ERR_PREAUTH_REQUIRED) (For Socket 2)
   c. 5.7.2 Kerberos: AS Request Sname: krbtgt/ (Success) (For Socket 2)
   d. 5.7.3 Kerberos: TGS Request Realm: Sname: cifs/ (For Socket 2)
   e. 5.7.4 Kerberos: TGS Request Sname: krbtgt/2008DOMAIN2.COM (For Socket 2)
   f. 5.3.1.2 SMB2: SMB2 SESSION_SETUP (Socket 2)
   g. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (Socket 2)
   h. 5.4.1.1 SMB2: SMB2 CREATE lsarpc (Socket 2)
   i. 5.4.1.2 RPC: Bind to lsarpc ([C706]) (Socket 2)
   j. 5.4.3.1.3 lsarpc: LsarOpenPolicy2 (CreateSecret) (Socket 2)
   k. 5.4.3.6.1 lsarpc: LsarDeleteObject (Outgoing trust) (Socket 2)
3. Cleanup
   a. 5.4.1.3 lsarpc: LsarClose (Socket 2)
   b. 5.4.1.4 SMB2: SMB2 CLOSE (Socket 2)

4.5.2 Deleting an Incoming Trust

1. Check Domain Policy
    a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE (Socket 1)
    b. 5.3.1.2 SMB2: SMB2 SESSION_SETUP (Socket 1)
    c. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (Socket 1)
    d. 5.4.3.1.1 SMB2: SMB2 CREATE lsarpc (Socket 1)
    e. 5.4.1.2 RPC: Bind to lsarpc ([C706]) (Socket 1)
    f. 5.4.3.1.1 lsarpc: LsarOpenPolicy2 (ViewLocalInformation) (Socket 1)
    g. 5.4.1.3 lsarpc: LsarClose (Socket 1)
2. Delete the Trust Account
    a. 5.3.1.1 SMB-> SMB2 SMB_COM_NEGOTIATE (Socket 2)
    b. 5.7.1 Kerberos: AS Request Sname: krbtgt/ (KDC_ERR_PREAUTH_REQUIRED) (For Socket 2)
    c. 5.7.2 Kerberos: AS Request Sname: krbtgt/ (Success) (For Socket 2)
    d. 5.7.3 Kerberos: TGS Request Realm: Sname: cifs/ (For Socket 2)
    e. 5.7.4 Kerberos: TGS Request Sname: krbtgt/2008DOMAIN2.COM (For Socket 2)
    f. 5.3.1.2 SMB2 SMB2 SESSION_SETUP (Socket 2)
    g. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (Socket 2)
    h. 5.4.3.1.1 SMB2: SMB2 CREATE lsarpc (Socket 2)
    i. 5.4.1.2 RPC: Bind to lsarpc ([C706]) (Socket 2)
    j. 5.4.3.1.3 lsarpc: LsarOpenPolicy2 (CreateSecret) (Socket 2)
    k. 5.4.3.4 lsarpc: LsarQueryTrustedDomainInfoByName (TrustedDomainFullInformation) (Socket 2)
    l. 5.4.3.6.2 lsarpc: LsarDeleteObject (Incoming trust) (Socket 2)
3. Cleanup
    a. 5.4.1.3 lsarpc: LsarClose (Socket 2)
    b. 5.4.1.4 SMB2: SMB2 CLOSE (Socket 2)

4.5.3 Deleting a 2-Way Trust

1. Check Domain Policy
    a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE (Socket 1)
    b. 5.3.1.2 SMB2: SMB2 SESSION_SETUP (Socket 1)
    c. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (Socket 1)
    d. 5.4.1.1 SMB2: SMB2 CREATE lsarpc (Socket 1)
    e. 5.4.1.2 RPC: Bind to lsarpc ([C706]) (Socket 1)
    f. 5.4.3.1.1 lsarpc: LsarOpenPolicy2 (ViewLocalInformation) (Socket 1)
    g. 5.4.1.3 lsarpc: LsarClose (Socket 1)
    h. 5.3.1.4 SMB2: SMB2 TREE_DISCONNECT (Socket 1)
    i. 5.3.1.5 SMB2: SMB2 LOGOFF (Socket 1)
4. Delete the Trust
    a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE (Socket 2)
    b. 5.7.1 Kerberos: AS Request Sname: krbtgt/ (KDC_ERR_PREAUTH_REQUIRED) (For Socket 2)
    c. 5.7.2 Kerberos: AS Request Sname: krbtgt/ (Success) (For Socket 2)
    d. 5.7.3 Kerberos: TGS Request Realm: Sname: cifs/ (For Socket 2)
    e. 5.7.4 Kerberos: TGS Request Sname: krbtgt/2008DOMAIN2.COM (For Socket 2)
    f. 5.3.2.2 SMB2: SMB2 SESSION_SETUP (Socket 2)
    g. 5.3.2.3 SMB2: SMB2 TREE_CONNECT (IPC$) (Socket 2)
    h. 5.4.1.1 SMB2: SMB2 CREATE lsarpc (Socket 2)

    i. 5.4.1.2 RPC: Bind to lsarpc ([C706]) (Socket 2)
    j. 5.4.3.1.3 lsarpc: LsarOpenPolicy2 (CreateSecret) (Socket 2)
    k. 5.4.3.9 LsarOpenTrustedDomainByName (Socket 2)
    l. 5.4.3.6.3 lsarpc: LsarDeleteObject (2-Way trust) (Socket 2)
2. Cleanup
    a. 5.4.1.3 lsarpc: LsarClose (Socket 2)
    b. 5.4.1.4 SMB2: SMB2 CLOSE (Socket 2)

4.6 Establishing A Secure Channel

4.6.1 Establishing an Outgoing Trust Secure Channel

1. 5.2.2 DNS: 2008DOMAIN2.COM Queries for 2008DOMAIN1.COM
2. Authenticate
    a. 5.5.1.2.2 Epm: Request: ept_map (Netlogonr) ([C706]) (For Socket 1)
    b. 5.5.1.2.3 RPC: Bind to Netlogonr ([C706]) (Socket 1)
    c. 5.5.2.3 Netlogonr: NetrServerReqChallenge (Socket 1)
    d. 5.5.2.4 Netlogonr: NetrServerAuthenticate3 (Socket 1)
3. Lookup the Account Name

    a. 5.4.2 TCP / RPC: lsarpc Session Control ([C706]) (For Socket 2)
    b. 5.5.1.1.2 RPC: c/o Bind (EPT) ([C706]) (Socket 2)
    c. 5.4.3.7 lsarpc: LsarLookupNames4 (Socket 2)

4.6.2 Establishing an Incoming Trust Secure Channel

Note that the referenced packets should be interpreted as originating on 2008DOMAIN2.COM, instead of 2008DOMAIN1.COM; the 'NetrLogonSamLogonWithFlags' packets are in proper form.

1. 5.2.1 DNS: 2008DOMAIN1.COM Queries for 2008DOMAIN2.COM
2. Authenticate and Connect
    a. 5.5.1.2.2 Epm: Request: ept_map (Netlogonr) ([C706])
    b. 5.5.1.2.3 RPC: Bind to Netlogonr ([C706])
    c. 5.5.2.3 Netlogonr: NetrServerReqChallenge
    d. 5.5.2.4 Netlogonr: NetrServerAuthenticate3
    e. 5.5.1.2.4 RPC: Alter Context (security context) ([C706])
    f. 5.5.2.6 Netlogonr:NetrLogonSamLogonWithFlags

4.7 Trust Password Reset Operations

4.7.1 Trust Password Reset (Outgoing)

1. Session Setup
   a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE
   b. 5.7.1 Kerberos: AS Request Sname: krbtgt/ (KDC_ERR_PREAUTH_REQUIRED)
   c. 5.7.2 Kerberos: AS Request Sname: krbtgt/ (Success)
   d. 5.7.3 Kerberos: TGS Request Realm: Sname: cifs/
   e. 5.7.4 Kerberos: TGS Request Sname: krbtgt/2008DOMAIN2.COM
   f. 5.3.2.2 SMB2: SMB2 SESSION_SETUP
   g. 5.3.2.3 SMB2: SMB2 TREE_CONNECT (IPC$)
   h. 5.4.1.1 SMB2: SMB2 CREATE lsarpc
   i. 5.4.1.2 RPC: Bind to lsarpc ([C706])
2. Reset Trust Password
   a. 5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret)
   b. 5.4.3.2 lsarpc: LsarQueryInformationPolicy2 (PolicyDnsDomainInformation)
   c. 5.4.3.3 lsarpc: LsarQueryTrustedDomainInfo (TrustedDomainFullInformation)
   d. 5.4.3.8 LsarSetTrustedDomainInfoByName
3. Cleanup
   a. 5.4.1.3 lsarpc: LsarClose
   b. 5.4.1.4 SMB2: SMB2 CLOSE

4.7.2 Trust Password Reset (Incoming)

1. Session Setup
    a. 5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE
    b. 5.3.1.2 SMB2: SMB2 SESSION_SETUP
    c. 5.3.1.3 SMB2: SMB2 TREE_CONNECT (IPC$)
    d. 5.4.1.1 SMB2: SMB2 CREATE lsarpc
    e. 5.4.1.2 RPC: Bind to lsarpc ([C706])
2. Reset Trust Password
    a. 5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret)
    b. 5.4.3.2 lsarpc: LsarQueryInformationPolicy2 (PolicyDnsDomainInformation)
    c. 5.4.3.3 lsarpc: LsarQueryTrustedDomainInfo (TrustedDomainFullInformation)
    d. 5.4.3.8 LsarSetTrustedDomainInfoByName
    e. 5.5.1.1.1 SMB2: SMB2 CREATE NETLOGON
    f. 5.5.1.1.2 RPC: Bind to Netlogonr ([C706])
    g. 5.5.2.2 Netlogonr: NetrLogonControl2Ex
3. Cleanup
    a. 5.5.1.1.3 SMB2: SMB2 CLOSE
    b. 5.4.1.3 lsarpc: LsarClose
    c. 5.4.1.4 SMB2: SMB2 CLOSE

5 Protocol Details

The protocol packet details in this section are intended as examples only. Please note that they were collected from a number of network traces. Hence, not all socket numbers, SMB/SMB2 sequencing values and so on do not precisely match the order specified in section 4 (Message Sequencing).

5.1 LDAP (CLDAP) "Ping"

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Udp: SrcPort = 61082, DstPort = LDAP(389), Length = 143
- LDAP (CLDAP): (LDAP (CLDAP))Search Request, MessageID: 5, BaseObject: NULL, SearchScope: base Object,
                                              SearchAlias: neverDerefAliases
  - Parser: Search Request, MessageID: 5
   + ParserHeader:
   + MessageID: 5
   - OperationHeader: Search Request, 3(0x3)
    + AsnId: Application Constructed Tag (3)
    + AsnLen: Length = 120, LengthOfLength = 4
   - SearchRequest: BaseDN: NULL, SearchScope: base Object, SearchAlias: neverDerefAliases
    + BaseObject: NULL
    + Scope: base Object
    + Alias: neverDerefAliases
    + SizeLimit: No Limit
    + TimeLimit: No Limit
    + TypesOnly: False
    - Filter: (&(DnsDomain=2008DOMAIN2.COM)(Host=2008DOMAIN1DC1)(NtVer==\04\04\16\00\00\01))
     + Operator: And, 0(0x00)
     + Length: 81
     + filter: (DnsDomain=2008DOMAIN2.COM)
     + filter: (Host=2008DOMAIN1DC1)
     + filter: (NtVer==\04\04\16\00\00\01)
    - Attributes: ( Netlogon )
     + AttributeSelectionHeader:
     + Attribute: Netlogon

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Udp: SrcPort = LDAP(389), DstPort = 61082
- LDAP (CLDAP): (LDAP (CLDAP))Search Result Entry, MessageID: 5, Status: Success
  - Parser: Search Result Entry, MessageID: 5
   - ParserHeader:
    + AsnId: Sequence and SequenceOf types (Universal 16)
    + AsnLen: Length = 166, LengthOfLength = 4
   + MessageID: 5
   - OperationHeader: Search Result Entry, 4(0x4)
    + AsnId: Application Constructed Tag (4)
    + AsnLen: Length = 157, LengthOfLength = 4
   + SearchResultEntry: NULL
  - Parser: search Result Done, MessageID: 5
   - ParserHeader:
    + AsnId: Sequence and SequenceOf types (Universal 16)
    + AsnLen: Length = 16, LengthOfLength = 4
   + MessageID: 5
   - OperationHeader: search Result Done, 5(0x5)
    + AsnId: Application Constructed Tag (5)
    + AsnLen: Length = 7, LengthOfLength = 4
   + SearchResultDone: Status: Success, MatchedDN: NULL, ErrorMessage: NULL
- NetlogonAttribute: LogonSAMLogonResponseEX (SAM Response to SAM logon request): 23 (0x17)
  - SamLogonResponseEx: 2008DOMAIN2DC1.2008DOMAIN2.COM
     Opcode: LogonSAMLogonResponseEX
     Sbz: 0 (0x0)
```

```
- Flags: 0x000013FD
   DSPDCFLAG:           (...............................1) DC is a PDC of Domain.
   Reserved1:           (..............................0.)
   DSGCFlag:            (.............................1..) DC is a GC of forest.
   DSLDAPFlag:          (............................1...) Server supports an LDAP server.
   DSDSFlag:            (...........................1....) DC supports a DS and is a Domain Controller.
   DSKDCFlag:           (..........................1.....) DC is running KDC service.
   DSTimeServFlag:      (.........................1......) DC is running time service.
   DSClosestFlag:       (........................1.......) DC is in closest site to client.
   DSWritableFlag:      (.......................1........) DC has a writable DS.
   DSGoodTimeServFlag:  (......................1.........) DC is running time service (has clock hardware).
   DSNDNCFlag:          (.....................0..........) DomainName is a non-domain NC serviced by the LDAP
                                                           server.
   Reserved:            (...000000000000000010...........)
   DSDNSControllerFlag: (..0.............................) DomainControllerName is not a DNS name.
   DSDNSDomainFlag:     (.0..............................) DomainName is not a DNS name.
   DSDNSForestFlag:     (0...............................) DnsForestName is not a DNS name.
  DomainGuid: {591D8D94-3CCA-43CF-AA17-49B6C72F44AB}
  DnsForestName: 2008DOMAIN2.COM
  DnsDomainName: 2008DOMAIN2.COM
  DnsHostName: 2008DOMAIN2DC1.2008DOMAIN2.COM
  NetbiosDomainName: 2008DOMAIN2
  NetbiosComputerName: 2008DOMAIN2DC1
  UserName:
  DcSiteName: Default-First-Site-Name
  ClientSiteName: Default-First-Site-Name
- Version: 0x00000005 NT Version 5 Client
   NetLogonNTVersion1:            (...............................1) NT Version 4
   NetLogonNTVersion5:            (..............................0.) NT Version 5
   NetLogonNTVersion5EX:          (.............................1..) Request for LogonResponseEX.
   NetLogonNTVersion5EXWithIP:    (............................0...) Not requesting responding DC IP address.
   Reserved:                      (........00000000000000000000....)
   NetLogonNTVersionAvoidNT4EMul: (.......0........................) Caller doesn't care about NT4.0 emulation.
   Reserved3:                     (....000.........................)
   NetlogonNTVersionPDC:          (...0............................) Not a query for a PDC.
```

```
      NetlogonNTVersionIP:           (..0.............................) Not a query for a DC running IP.
      NetlogonNTVersionLocal:        (.0..............................) Caller is a remote system.
      NetlogonNTVersionGC:           (0...............................) Not a query for a GC.
   - LmNtToken: Windows NT Networking: 0xFFFF
      NtTokenByte1: LMNT_TOKENBYTE: 255 (0xFF)
      NtTokenByte2: LMNT_TOKENBYTE: 255 (0xFF)
   - Lm20Token: OS/2 LAN Manager 2.0 (or later) Networking: 0xFFFF
      LmTokenByte1: LM20_TOKENBYTE: 255 0xFF
      LmTokenByte2: LM20_TOKENBYTE: 255 0xFF
```

5.2 Name Resolution (DNS)

5.2.1 DNS: 2008DOMAIN1.COM Queries for 2008DOMAIN2.COM

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Udp: SrcPort = 59449, DstPort = DNS(53), Length = 56
- Dns: QueryId = 0x905C, QUERY (Standard query), Query  for 2008DOMAIN2DC1.2008DOMAIN2.COM of type Host Addr on class
                                                 Internet
    QueryIdentifier: 36956 (0x905C)
  - Flags:  Query, Opcode - QUERY (Standard query), RD, Rcode - Success
     QR:                (0...............) Query
     Opcode:            (.0000...........) QUERY (Standard query) 0
     AA:                (.....0..........) Not authoritative
     TC:                (......0.........) Not truncated
     RD:                (.......1........) Recursion desired
     RA:                (........0.......) Recursive query support not available
     Zero:              (.........0......) 0
     AuthenticatedData: (..........0.....) Not AuthenticatedData
     CheckingDisabled:  (...........0....) Not CheckingDisabled
     Rcode:             (............0000) Success 0
    QuestionCount: 1 (0x1)
    AnswerCount: 0 (0x0)
    NameServerCount: 0 (0x0)
    AdditionalCount: 0 (0x0)
  - QRecord: 2008DOMAIN2DC1.2008DOMAIN2.COM of type Host Addr on class Internet
     QuestionName: 2008DOMAIN2DC1.2008DOMAIN2.COM
     QuestionType: A, IPv4 address, 1(0x1)
     QuestionClass: Internet, 1(0x1)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Udp: SrcPort = DNS(53), DstPort = 59449, Length = 72
- Dns: QueryId = 0x905C, QUERY (Standard query), Response - Success, 10.237.0.22
    QueryIdentifier: 36956 (0x905C)
  - Flags:  Response, Opcode - QUERY (Standard query), AA, RD, RA, Rcode - Success
     QR:                (1...............) Response
     Opcode:            (.0000...........) QUERY (Standard query) 0
     AA:                (.....1..........) Is authoritative
     TC:                (......0.........) Not truncated
     RD:                (.......1........) Recursion desired
     RA:                (........1.......) Recursive query support available
     Zero:              (.........0......) 0
     AuthenticatedData: (..........0.....) Not AuthenticatedData
     CheckingDisabled:  (...........0....) Not CheckingDisabled
     Rcode:             (............0000) Success 0
    QuestionCount: 1 (0x1)
    AnswerCount: 1 (0x1)
    NameServerCount: 0 (0x0)
    AdditionalCount: 0 (0x0)
  - QRecord: 2008DOMAIN2DC1.2008DOMAIN2.COM of type Host Addr on class Internet
     QuestionName: 2008DOMAIN2DC1.2008DOMAIN2.COM
     QuestionType: A, IPv4 address, 1(0x1)
     QuestionClass: Internet, 1(0x1)
  - ARecord: 2008DOMAIN2DC1.2008DOMAIN2.COM of type Host Addr on class Internet: 10.237.0.22
     ResourceName: 2008DOMAIN2DC1.2008DOMAIN2.COM
     ResourceType: A, IPv4 address, 1(0x1)
     ResourceClass: Internet, 1(0x1)
     TimeToLive: 3600 (0xE10)
     ResourceDataLength: 4 (0x4)
     IPAddress: 10.237.0.22
```

5.2.2 DNS: 2008DOMAIN2.COM Queries for 2008DOMAIN1.COM

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Udp: SrcPort = 50773, DstPort = DNS(53), Length = 56
- Dns: QueryId = 0xF9A8, QUERY (Standard query), Query  for 2008DOMAIN2DC1.2008DOMAIN2.COM of type Host Addr on class
                                                 Internet
    QueryIdentifier: 63912 (0xF9A8)
  - Flags:  Query, Opcode - QUERY (Standard query), RD, Rcode - Success
     QR:                (0...............) Query
     Opcode:            (.0000...........) QUERY (Standard query) 0
     AA:                (.....0..........) Not authoritative
     TC:                (......0.........) Not truncated
     RD:                (.......1........) Recursion desired
     RA:                (........0.......) Recursive query support not available
     Zero:              (.........0......) 0
     AuthenticatedData: (..........0.....) Not AuthenticatedData
     CheckingDisabled:  (...........0....) Not CheckingDisabled
     Rcode:             (............0000) Success 0
    QuestionCount: 1 (0x1)
    AnswerCount: 0 (0x0)
    NameServerCount: 0 (0x0)
    AdditionalCount: 0 (0x0)
  - QRecord: 2008DOMAIN2DC1.2008DOMAIN2.COM of type Host Addr on class Internet
     QuestionName: 2008DOMAIN2DC1.2008DOMAIN2.COM
     QuestionType: A, IPv4 address, 1(0x1)
     QuestionClass: Internet, 1(0x1)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Udp: SrcPort = DNS(53), DstPort = 50773, Length = 72
- Dns: QueryId = 0xF9A8, QUERY (Standard query), Response - Success, 10.237.0.22
    QueryIdentifier: 63912 (0xF9A8)
  - Flags:  Response, Opcode - QUERY (Standard query), AA, RD, RA, Rcode - Success
     QR:                (1...............) Response
     Opcode:            (.0000...........) QUERY (Standard query) 0
     AA:                (.....1..........) Is authoritative
     TC:                (......0.........) Not truncated
     RD:                (.......1........) Recursion desired
     RA:                (........1.......) Recursive query support available
     Zero:              (.........0......) 0
     AuthenticatedData: (..........0.....) Not AuthenticatedData
     CheckingDisabled:  (...........0....) Not CheckingDisabled
     Rcode:             (............0000) Success 0
    QuestionCount: 1 (0x1)
    AnswerCount: 1 (0x1)
    NameServerCount: 0 (0x0)
    AdditionalCount: 0 (0x0)
  - QRecord: 2008DOMAIN2DC1.2008DOMAIN2.COM of type Host Addr on class Internet
     QuestionName: 2008DOMAIN2DC1.2008DOMAIN2.COM
     QuestionType: A, IPv4 address, 1(0x1)
     QuestionClass: Internet, 1(0x1)
  - ARecord: 2008DOMAIN2DC1.2008DOMAIN2.COM of type Host Addr on class Internet: 10.237.0.22
     ResourceName: 2008DOMAIN2DC1.2008DOMAIN2.COM
     ResourceType: A, IPv4 address, 1(0x1)
     ResourceClass: Internet, 1(0x1)
     TimeToLive: 1200 (0x4B0)
     ResourceDataLength: 4 (0x4)
```

```
      IPAddress: 10.237.0.22
```

5.3 SMB: Session Control

5.3.1 SMB -> SMB2: Session Control

5.3.1.1 SMB-> SMB2: SMB_COM_NEGOTIATE

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =144
- Smb: C; Negotiate
    Protocol: SMB
    Command: Negotiate 114(0x72)
  + NTStatus: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
  - SMBHeader: Command, TID: 0xFFFF, PID: 0xFEFF, UID: 0x0000, MID: 0x0000
   - Flags: 24 (0x18)
      LockAndRead:     (.......0) LOCK_AND_READ and WRITE_AND_UNLOCK NOT supported (Obsolete) (SMB_FLAGS_LOCK_AND_READ_OK)
      NoAck:           (......0.) An ACK response is needed (SMB_FLAGS_SEND_NO_ACK[only applicable when SMB transport is NetBIOS over
                                  IPX])
      Reserved_bit2:   (.....0..) Reserved (Must Be Zero)
      CaseInsensitive: (....1...) SMB paths are case-insensitive (SMB_FLAGS_CASE_INSENSITIVE)
      Canonicalized:   (...1....) Canonicalized File and pathnames (Obsolete) (SMB_FLAGS_CANONICALIZED_PATHS)
      Oplock:          (..0.....) Oplocks NOT supported for OPEN, CREATE & CREATE_NEW (Obsolete) (SMB_FLAGS_OPLOCK)
      OplockNotify:    (.0......) Notifications NOT supported for OPEN, CREATE & CREATE_NEW (Obsolete) (SMB_FLAGS_OPLOCK_NOTIFY_ANY)
      FromServer:      (0.......) Command - SMB is being sent from the client (SMB_FLAGS_SERVER_TO_REDIR)
   - Flags2: 51283 (0xC853)
      KnowsLongFiles:   (...............1) Understands Long File Names (SMB_FLAGS2_KNOWS_LONG_NAMES)
      ExtendedAttribs:  (..............1.) Understands extended attributes (SMB_FLAGS2_KNOWS_EAS)
      SignEnabled:      (.............0..) Security signatures NOT enabled (SMB_FLAGS2_SMB_SECURITY_SIGNATURE)
      Compressed:       (............0...) Compression Disabled for REQ_NT_WRITE_ANDX and RESP_READ_ANDX (SMB_FLAGS2_COMPRESSED)
      SignRequired:     (...........1....) Security Signatures are required (SMB_FLAGS2_SMB_SECURITY_SIGNATURE_REQUIRED)
      Reserved_bit5:    (..........0.....) Reserved (Must Be Zero)
      LongFileNames:    (.........1......) Use Long File Names (SMB_FLAGS2_IS_LONG_NAME)
      Reserved_bits7_9: (......000.......) Reserved (Must Be Zero)
      ReparsePath:      (.....0..........) NOT a Reparse path (SMB_FLAGS2_REPARSE_PATH)
      ExtSecurity:      (....1...........) Aware of extended security (SMB_FLAGS2_EXTENDED_SECURITY)
      Dfs:              (...0............) NO DFS namespace (SMB_FLAGS2_DFS)
      Paging:           (..0.............) Read operation will NOT be permitted unless user has permission (NO Paging IO)
                                           (SMB_FLAGS2_PAGING_IO)
      StatusCodes:      (.1..............) Using 32-bit NT status error codes (SMB_FLAGS2_NT_STATUS)
      Unicode:          (1...............) Using UNICODE strings (SMB_FLAGS2_UNICODE)
     PIDHigh: 0 (0x0)
     SecuritySignature: 0x0
     Reserved: 0 (0x0)
     TreeID: 65535 (0xFFFF)
     ProcessID: 65279 (0xFEFF)
     UserID: 0 (0x0)
     MultiplexID: 0 (0x0)
  - CNegotiate:
     WordCount: 0 (0x0)
     ByteCount: 109 (0x6D)
   - Dialect: PC NETWORK PROGRAM 1.0
      BufferFormat: Dialect 2(0x2)
      DialectName: PC NETWORK PROGRAM 1.0
   - Dialect: LANMAN1.0
      BufferFormat: Dialect 2(0x2)
      DialectName: LANMAN1.0
   - Dialect: Windows for Workgroups 3.1a
      BufferFormat: Dialect 2(0x2)
      DialectName: Windows for Workgroups 3.1a
   - Dialect: LM1.2X002
      BufferFormat: Dialect 2(0x2)
      DialectName: LM1.2X002
   - Dialect: LANMAN2.1
      BufferFormat: Dialect 2(0x2)
      DialectName: LANMAN2.1
   - Dialect: NT LM 0.12
      BufferFormat: Dialect 2(0x2)
      DialectName: NT LM 0.12
   - Dialect: SMB 2.002
      BufferFormat: Dialect 2(0x2)
      DialectName: SMB 2.002

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =236
- Smb2: R  NEGOTIATE (0x0), GUID={535674CC-5BE2-3AB4-40C2-ED1535D79C69}, Mid = 0
    SMBIdentifier: SMB
  - SMB2Header: R NEGOTIATE (0x0)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: NEGOTIATE (0x0)
     Credits: 1 (0x1)
   - Flags: 0x1
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................0...) Packet is not signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 0 (0x0)
     ProcessId: 0 (0x0)
     TreeId: 0 (0x0)
     SessionId: 0 (0x0)
     Sig: Binary Large Object (16 Bytes)
  - RNegotiate:
     Size: 65 (0x41)
     SecurityMode: Unknown (0x3)
     DialectRevision: 514 (0x202)
     Reserved: 0 (0x0)
     Guid: {535674CC-5BE2-3AB4-40C2-ED1535D79C69}
   - Capabilities: 0x1
      DFS:               (...............................1) DFS available
      Reserved_bits1_31: (0000000000000000000000000000000.) Reserved
     MaxTransactSize: 65536 (0x10000)
     MaxReadSize: 65536 (0x10000)
     MaxWriteSize: 65536 (0x10000)
     SystemTime: 09/15/2008, 03:44:06 PM
     SystemStartTime: 09/15/2008, 02:06:39 PM
     SecurityBufferOffset: 128 (0x80)
     SecurityBufferLength: 108 (0x6C)
     Reserved2: 541936672 (0x204D4C20)
   - securityBlob:
    - GssApi:
     + ApplicationHeader:
     + ThisMech: SpnegoToken (1.3.6.1.5.5.2)
     - InnerContextToken: 0x1
      - SpnegoToken: 0x1
       + Tag0:
       - NegTokenInit: 0x1
        + SequenceHeader:
        + Tag0:
        + MechTypes:
        + Tag3:
        - MechListMic:  &$not_defined_in_RFC4178@please_ignore
         + AsnOctetStringHeader:
           OctetStream:  &$not_defined_in_RFC4178@please_ignore

+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =162
- Smb2: C  SESSION SETUP (0x1), Mid = 1
    SMBIdentifier: SMB
  - SMB2Header: C SESSION SETUP (0x1)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   - Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: SESSION SETUP (0x1)
     Credits: 8 (0x8)
   - Flags: 0x0
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................0...) Packet is not signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 1 (0x1)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 0 (0x0)
     Sig: Binary Large Object (16 Bytes)
  - CSessionSetup:
     Size: 25 (0x19)
     VcNumber: 0 (0x0)
     SecurityMode: Signing Required (0x2)
   - Capabilities: 0x1
      DFS:               (...............................1) DFS available
      Reserved_bits1_31: (0000000000000000000000000000000.) Reserved
     Channel: 0 (0x0)
     SecurityBufferOffset: 88 (0x58)
     SecurityBufferLength: 74 (0x4A)
     PreviousSessionId: 0 (0x0)
   - securityBlob: 0x1
    - GssApi:
     + ApplicationHeader:
     + ThisMech: SpnegoToken (1.3.6.1.5.5.2)
     - InnerContextToken: 0x1
      - SpnegoToken: 0x1
       + Tag0:
       - NegTokenInit: 0x1
        + SequenceHeader:
        + Tag0:
        + MechTypes:
```

```
+ Tag2:
+ OctetStringHeader:
- MechToken: NTLM NEGOTIATE MESSAGE
 - NLMP: NTLM NEGOTIATE MESSAGE
    Signature: NTLMSSP
    MessageType: Negotiate Message (0x00000001)
  - NegotiateFlags: 0xE2088297 (NTLM v2128-bit encryption, Always Sign)
     NegotiateUnicode:                 (...............................1) The choice of character set encoding MUST be
                                                                          UNICODE.
     NegotiateOEM:                     (..............................1.) The choice of character set MUST be OEM
     RequestTarget:                    (.............................1..) TargetName MUST be supplied.
     Reserved1:                        (............................0...)
     NegotiateSign:                    (...........................1....) Requests session key negotiation for message
                                                                          signatures.
     NegotiateSeal:                    (..........................0.....) Does NOT request session key negotiation for message
                                                                          confidentiality.
     NegotiateDatagram:                (.........................0......) Does NOT request datagram-oriented (connectionless)
                                                                          authentication.
     NegotiateLMKey:                   (........................1.......) Requests LAN Manager (LM) session key computation.
     Reserved2:                        (.......................0........)
     NegotiateNTLM:                    (......................1.........) Requests usage of the NTLM v1 session security
                                                                          protocol.
     NegotiateNTOnly:                  (.....................0..........) LM authentication is allowed
     Reserved3:                        (....................0...........)
     NegotiateOEMDomainSupplied:       (...................0............) The domain name is NOT provided.
     NegotiateOEMWorkstationSupplied:  (..................0.............) The Workstation field is NOT present.
     Reserved4:                        (.................0..............)
     NegotiateAlwaysSign:              (................1...............) Requests the presence of a signature block on all
                                                                          messages.
     TargetTypeDomain:                 (...............0................) TargetName is NOT a domain name.
     TargetTypeServer:                 (..............0.................) TargetName is NOT a server name
     TargetTypeShare:                  (.............0..................) TargetName is NOT a share name
     NegotiateNTLM2:                   (............1...................) Requests usage of the NTLM v2 session security.
     NegotiateIdentify:                (...........0....................) Does NOT request an identify level token.
     Reserved5:                        (..........0.....................)
     RequestNonNTSessionKey:           (.........0......................) Does NOT request the usage of the LMOWF.
     NegotiateTargetInfo:              (........0.......................) Does NOT request extended information.
     Reserved6:                        (.......0........................)
     NegotiateVersion:                 (......1.........................) Requests the protocol version number.
```

```
             Reserved7:                         (.....0..........................)
             Reserved8:                         (....0...........................)
             Reserved9:                         (...0............................)
             Negotiate128:                      (..1.............................) Requests 128-bit session key negotiation.
             NegotiateKeyExch:                  (.1..............................) Requests an explicit key exchange.
             Negotiate56:                       (1...............................) Requesting 56-bit encryption
          + WorkstationDomainHeader: Length: 0, Offset: 0
          + WorkstationNameHeader: Length: 0, Offset: 0
          - Version: Windows 6.0 Build 28951 NLMPv15
             ProductMajorVersion: 6 (0x6)
             ProductMinorVersion: 0 (0x0)
             ProductBuild: 28951 (0x7117)
             Reserved: 0 (0x0)
             NTLMRevisionCurrent: 15 (0xF)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =391
- Smb2: R  SESSION SETUP (0x1) ,SessionFlags=0x0, Mid = 1 - NT Status: System - Error, Code = (22) STATUS_MORE_PROCESSING_REQUIRED
    SMBIdentifier: SMB
  - SMB2Header: R SESSION SETUP (0x1)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   - Status: 0xC0000016, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_ERROR, Code = (22) STATUS_MORE_PROCESSING_REQUIRED
     Command: SESSION SETUP (0x1)
     Credits: 8 (0x8)
   - Flags: 0x1
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................0...) Packet is not signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 1 (0x1)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RSessionSetup:
     Size: 9 (0x9)
   - SessionFlags: 0x0
      GU:                (...............0) NOT a guest user
      NU:                (..............0.) NOT a NULL user
      Reserved_bits2_15: (00000000000000..) Reserved
     SecurityBufferOffset: 72 (0x48)
     SecurityBufferLength: 319 (0x13F)
   - securityBlob: 0x1
    - ResponseToken:
     + Tag1:
     - NegTokenResp: 0x1
      + SequenceHeader:
      + Tag0:
      + NegState: accept-incomplete (1)
      + Tag1:
      + SupportedMech: NLMP (1.3.6.1.4.1.311.2.2.10)
      + Tag2:
      - ResponseToken:
       + OctetStringHeader:
       - SecurityBlob: NTLM CHALLENGE MESSAGE
        - NLMP: NTLM CHALLENGE MESSAGE
           Signature: NTLMSSP
           MessageType: Challenge Message (0x00000002)
         + TargetName: Length: 22, Offset: 56
         - ChallengeFlags: 0xE2898215 (NTLM v2128-bit encryption, Always Sign)
            NegotiateUnicode:                 (...............................1) The choice of character set encoding MUST be UNICODE.
            NegotiateOEM:                     (..............................0.) The choice of character set is NOT OEM
            RequestTarget:                    (.............................1..) TargetName MUST be supplied.
            Reserved1:                        (............................0...)
            NegotiateSign:                    (...........................1....) Requests session key negotiation for message
                                                                                 signatures.
            NegotiateSeal:                    (..........................0.....) Does NOT request session key negotiation for message
                                                                                 confidentiality.
            NegotiateDatagram:                (.........................0......) Does NOT request datagram-oriented (connectionless)
                                                                                 authentication.
            NegotiateLMKey:                   (........................0.......) Does NOT request LAN Manager (LM) session key
                                                                                 computation.
            Reserved2:                        (.......................0........)
            NegotiateNTLM:                    (......................1.........) Requests usage of the NTLM v1 session security
                                                                                 protocol.
            NegotiateNTOnly:                  (.....................0..........) LM authentication is allowed
            Reserved3:                        (....................0...........)
            NegotiateOEMDomainSupplied:       (...................0............) The domain name is NOT provided.
            NegotiateOEMWorkstationSupplied:  (..................0.............) The Workstation field is NOT present.
            Reserved4:                        (.................0..............)
            NegotiateAlwaysSign:              (................1...............) Requests the presence of a signature block on all
                                                                                 messages.
            TargetTypeDomain:                 (...............1................) TargetName MUST be a domain name.
            TargetTypeServer:                 (..............0.................) TargetName is NOT a server name
            TargetTypeShare:                  (.............0..................) TargetName is NOT a share name
            NegotiateNTLM2:                   (............1...................) Requests usage of the NTLM v2 session security.
            NegotiateIdentify:                (...........0....................) Does NOT request an identify level token.
            Reserved5:                        (..........0.....................)
            RequestNonNTSessionKey:           (.........0......................) Does NOT request the usage of the LMOWF.
            NegotiateTargetInfo:              (........1.......................) Requests extended information about the server
                                                                                 authentication realm to be sent as AV_PAIR in the
                                                                                 TargetInfo payload
            Reserved6:                        (.......0........................)
            NegotiateVersion:                 (......1.........................) Requests the protocol version number.
            Reserved7:                        (.....0..........................)
            Reserved8:                        (....0...........................)
            Reserved9:                        (...0............................)
            Negotiate128:                     (..1.............................) Requests 128-bit session key negotiation.
            NegotiateKeyExch:                 (.1..............................) Requests an explicit key exchange.
            Negotiate56:                      (1...............................) Requesting 56-bit encryption
         + Challenge: 82F59827B4078158
           Reserved: Binary Large Object (8 Bytes)
         + TargetInfoFields: Length: 206, Offset: 78
         - Version: Windows 6.0 Build 28951 NLMPv15
            ProductMajorVersion: 6 (0x6)
            ProductMinorVersion: 0 (0x0)
            ProductBuild: 28951 (0x7117)
            Reserved: 0 (0x0)
            NTLMRevisionCurrent: 15 (0xF)
           TargetNameString: 2008DOMAIN2
         - AvPairs: 0x1
- AvPair: 2008DOMAIN2 (Server NetBIOS domain name)
   AvId: 0x0002 MsvAvNbDomainName - Server NetBIOS domain name
   AvLen: 22 (0x16)
   UnicodeValue: 2008DOMAIN2
- AvPair: 2008DOMAIN2DC1 (Server NetBIOS computer name)
   AvId: 0x0001 MsvAvNbComputerName - Server NetBIOS computer name
   AvLen: 28 (0x1C)
   UnicodeValue: 2008DOMAIN2DC1
- AvPair: 2008DOMAIN2.COM (Server Microsoft Active Directory (AD) DNS domain name.)
   AvId: 0x0004 MsvAvDnsDomainName - Server Microsoft Active Directory (AD) DNS domain name.
   AvLen: 30 (0x1E)
   UnicodeValue: 2008DOMAIN2.COM
- AvPair: 2008DOMAIN2DC1.2008DOMAIN2.COM (Server Microsoft Active Directory (AD) DNS computer name.)
   AvId: 0x0003 MsvAvDnsComputerName - Server Microsoft Active Directory (AD) DNS computer name.
   AvLen: 60 (0x3C)
   UnicodeValue: 2008DOMAIN2DC1.2008DOMAIN2.COM
- AvPair: 2008DOMAIN2.COM (Microsoft Active Directory (AD) DNS forest tree name.)
   AvId: 0x0005 MsvAvDnsTreeName - Microsoft Active Directory (AD) DNS forest tree name.
   AvLen: 30 (0x1E)
   UnicodeValue: 2008DOMAIN2.COM
- AvPair: 3:44:06 PM 9/15/2008 (Server local time)
   AvId: 0x0007 MsvAvTimestamp - Server local time
   AvLen: 8 (0x8)
   ServerTime: 09/15/2008, 03:44:06 PM
- AvPair: NULL
   AvId: 0x0000 MsvAvEOL - End of list
   AvLen: 0 (0x0)
```

5.3.1.2 SMB2: SMB2 SESSION_SETUP

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =651
- Smb2: C  SESSION SETUP (0x1), Mid = 2
    SMBIdentifier: SMB
  - SMB2Header: C SESSION SETUP (0x1)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   - Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: SESSION SETUP (0x1)
     Credits: 1 (0x1)
   - Flags: 0x0
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................0...) Packet is not signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 2 (0x2)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - CSessionSetup:
     Size: 25 (0x19)
     VcNumber: 0 (0x0)
     SecurityMode: Signing Required (0x2)
   - Capabilities: 0x1
      DFS:               (...............................1) DFS available
      Reserved_bits1_31: (0000000000000000000000000000000.) Reserved
     Channel: 0 (0x0)
     SecurityBufferOffset: 88 (0x58)
     SecurityBufferLength: 563 (0x233)
     PreviousSessionId: 0 (0x0)
   - securityBlob: 0x1
    - ResponseToken:
     + Tag1:
     - NegTokenResp: 0x1
      + SequenceHeader:
      + Tag0:
      + NegState: accept-incomplete (1)
      + Tag2:
      - ResponseToken:
       + OctetStringHeader:
       - NLMPSecurityBlob: NTLM AUTHENTICATE MESSAGE, Domain: 2008DOMAIN1, User: Administrator, Workstation:
                           2008DOMAIN1DC1
          Signature: NTLMSSP
          MessageType: Authenticate Message (0x00000003)
        + LmChallengeResponse: Length: 24, Offset: 164
        + NtChallengeResponse: Length: 318, Offset: 188
        + DomainName: Length: 22, Offset: 88
        + UserName: Length: 26, Offset: 110
        + Workstation: Length: 28, Offset: 136
        + SessionKey: Length: 16, Offset: 506
        - AuthenticateFlags: 0xE2888215 (NTLM v2128-bit encryption, Always Sign)
           NegotiateUnicode:                 (..............................1) The choice of character set encoding
                                                                        MUST be UNICODE.
           NegotiateOEM:                     (.............................0.) The choice of character set is NOT OEM
           RequestTarget:                    (............................1..) TargetName MUST be supplied.
           Reserved1:                        (...........................0...)
           NegotiateSign:                    (..........................1....) Requests session key negotiation for
                                                                                message signatures.
           NegotiateSeal:                    (.........................0.....) Does NOT request session key
                                                                                negotiation for message
                                                                                confidentiality.
           NegotiateDatagram:                (........................0......) Does NOT request datagram-oriented
                                                                                (connectionless) authentication.
           NegotiateLMKey:                   (.......................0.......) Does NOT request LAN Manager (LM)
                                                                                session key computation.
           Reserved2:                        (......................0........)
           NegotiateNTLM:                    (......................1.........) Requests usage of the NTLM v1 session
                                                                                security protocol.
           NegotiateNTOnly:                  (.....................0..........) LM authentication is allowed
           Reserved3:                        (....................0...........)
           NegotiateOEMDomainSupplied:       (...................0............) The domain name is NOT provided.
           NegotiateOEMWorkstationSupplied:  (..................0.............) The Workstation field is NOT present.
           Reserved4:                        (.................0..............)
           NegotiateAlwaysSign:              (................1...............) Requests the presence of a signature
                                                                                block on all messages.
           TargetTypeDomain:                 (...............0................) TargetName is NOT a domain name.
           TargetTypeServer:                 (..............0.................) TargetName is NOT a server name
           TargetTypeShare:                  (.............0..................) TargetName is NOT a share name
           NegotiateNTLM2:                   (............1...................) Requests usage of the NTLM v2 session
                                                                                security.
           NegotiateIdentify:                (...........0....................) Does NOT request an identify level
                                                                                token.
           Reserved5:                        (..........0.....................)
           RequestNonNTSessionKey:           (.........0......................) Does NOT request the usage of the
                                                                                LMOWF.
           NegotiateTargetInfo:              (........1.......................) Requests extended information about the
                                                                                server authentication realm to be sent
                                                                                as AV_PAIR in the TargetInfo payload
           Reserved6:                        (.......0........................)
           NegotiateVersion:                 (......1.........................) Requests the protocol version number.
           Reserved7:                        (.....0..........................)
           Reserved8:                        (....0...........................)
           Reserved9:                        (...0............................)
           Negotiate128:                     (..1.............................) Requests 128-bit session key
                                                                                negotiation.
           NegotiateKeyExch:                 (.1..............................) Requests an explicit key exchange.
           Negotiate56:                      (1...............................) Requesting 56-bit encryption
        - Version: Windows 6.0 Build 28951 NLMPv15
           ProductMajorVersion: 6 (0x6)
           ProductMinorVersion: 0 (0x0)
           ProductBuild: 28951 (0x7117)
```

```
           Reserved: 0 (0x0)
           NTLMRevisionCurrent: 15 (0xF)
        + Pad:
          DomainNameString: 2008DOMAIN1
          UserNameString: Administrator
          WorkstationString: 2008DOMAIN1DC1
        + LmChallengeResponseStruct: 000000000000000000000000000000000000000000000000
        + NTLMV2ChallengeResponse: 4CCC6E3D22A957C5E25B3B90C3E813970101000000000000
        + Pad:
        + SessionKeyString: AF1D86DC358895E102F4D5E1123C06DC
      + Tag3:
      + MechListMic:

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =101
- Smb2: R  SESSION SETUP (0x1) ,SessionFlags=0x0, Mid = 2
    SMBIdentifier: SMB
  - SMB2Header: R SESSION SETUP (0x1)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   - Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: SESSION SETUP (0x1)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 2 (0x2)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RSessionSetup:
     Size: 9 (0x9)
   - SessionFlags: 0x0
      GU:               (...............0) NOT a guest user
      NU:               (..............0.) NOT a NULL user
      Reserved_bits2_15: (00000000000000..) Reserved
     SecurityBufferOffset: 72 (0x48)
     SecurityBufferLength: 29 (0x1D)
   - securityBlob: 0x1
    - ResponseToken:
     + Tag1:
     - NegTokenResp: 0x1
      + SequenceHeader:
      + Tag0:
      + NegState: accept-completed (0)
      + Tag3:
      - MechListMic:
       + OctetStringHeader:
         OctetStream: Binary Large Object (16 Bytes)
```

5.3.1.3 SMB2: SMB2 TREE_CONNECT

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =146
- Smb2: C  TREE CONNECT (0x3), Path=\\2008DOMAIN2DC1.2008DOMAIN2.COM\IPC$, Mid = 3
```

```
    SMBIdentifier: SMB
  - SMB2Header: C TREE CONNECT (0x3)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: TREE CONNECT (0x3)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 3 (0x3)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - CTreeConnect:
     Size: 9 (0x9)
     Reserved: 0 (0x0)
     PathOffset: 72 (0x48)
     PathLength: 74 (0x4A)
     Path: \\2008DOMAIN2DC1.2008DOMAIN2.COM\IPC$

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =80
- Smb2: R  TREE CONNECT (0x3), TID=0x1, Mid = 3
    SMBIdentifier: SMB
  - SMB2Header: R TREE CONNECT (0x3)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: TREE CONNECT (0x3)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 3 (0x3)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RTreeConnect: 0x1
     Size: 16 (0x10)
     ShareType: Pipe (0x2)
     Reserved: 0 (0x0)
   - ShareFlags: 48 (0x30)
      SHI1005_FLAGS_DFS:                          (...............................0) The specified share is not present
                                                                                    in a Distributed File System (DFS)
                                                                                    tree structure
      SHI1005_FLAGS_DFS_ROOT:                     (..............................0.) The specified share is not the root
                                                                                    volume in a DFS tree structure
      Reserved_bits3_4:                           (............................00..)
      SHAREFLAGS_CACHING_TYPE:                    (........................0011....) Unknown (0x3)
      SHI1005_FLAGS_RESTRICT_EXCLUSIVE_OPENS:     (.......................0........) The specified share allows
                                                                                    exclusive file opens that deny
                                                                                    reads to an open file
      SHI1005_FLAGS_FORCE_SHARED_DELETE:          (......................0.........) Shared files in the specified share
                                                                                    can't be forcibly deleted
```

```
      SHI1005_FLAGS_ALLOW_NAMESPACE_CACHING:     (.....................0..........) Clients aren't allowed to cache the
                                                                                    namespace of the specified share
      SHI1005_FLAGS_ACCESS_BASED_DIRECTORY_ENUM: (....................0...........) The server will not filter
                                                                                    directory entries based on the
                                                                                    access permissions of the client
      Reserved_bits13_32:                        (00000000000000000000............)
   - Capabilities: 0x0
      DFS:                     (...............................0) DFS unavailable
      Reserved_bits1_31:       (0000000000000000000000000000000.) Reserved
   - MaximalAccess: 0x1F01FF
      ReadData:             (...............................1) Set FILE_READ_DATA (file & named pipe),
                                                               FILE_LIST_DIRECTORY (directory)
      WriteData:            (..............................1.) Set FILE_WRITE_DATA (file & named pipe), FILE_ADD_FILE
                                                               (directory
      AppendData:           (.............................1..) Set FILE_APPEND_DATA (file), FILE_ADD_SUBDIRECTORY
                                                               (directory), FILE_CREATE_PIPE_INSTANCE (named pipe)
      ReadEA:               (............................1...) Set FILE_READ_EA (file & directory)
      WriteEA:              (...........................1....) Set FILE_WRITE_EA (file & directory)
      Execute:              (..........................1.....) Set FILE_EXECUTE (file), FILE_TRAVERSE (directory)
      Reserved_bit6:        (.........................1......) Reserved
      ReadAttributes:       (........................1.......) Set FILE_READ_ATTRIBUTES (all)
      WriteAttributes:      (.......................1........) Set FILE_WRITE_ATTRIBUTES (all)
      Reserved_bits9_15:    (................0000000.........) Reserved
      Delete:               (...............1................) Set DELETE (the right to delete the object)
      ReadControl:          (..............1.................) Set READ_CONTROL (read the object's security descriptor
                                                               NOT including SACL)
      WriteDAC:             (.............1..................) Set WRITE_DAC (modify the DACL in the object's security
                                                               descriptor)
      WriteOwner:           (............1...................) Set WRITE_OWNER (change the owner in the object's
                                                               security descriptor)
      Synchronize:          (...........1....................) Set SYNCHRONIZE (use the object for synchronization)
      Reserved_bits21_23:   (........000.....................) Reserved
      AccessSystemSecurity: (.......0........................) NOT Set ACCESS_SYSTEM_SECURITY (get or set the SACL in
                                                               an object's security descriptor)
      MaximumAllowed:       (......0.........................) NOT Set MAXIMUM_ALLOWED (all access rights valid for the
                                                               caller)
      Reserved_bits26_27:   (....00..........................) Reserved
      GenericAll:           (...0............................) NOT Set GENERIC_ALL
      GenericExecute:       (..0.............................) NOT Set GENERIC_EXECUTE
      GenericWrite:         (.0..............................) NOT Set GENERIC_WRITE
      GenericRead:          (0...............................) NOT Set GENERIC_READ
```

5.3.1.4 SMB2: SMB2 TREE_DISCONNECT

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: C  TREE DISCONNECT (0x4), TID=0x1, Mid = 18
    SMBIdentifier: SMB
  - SMB2Header: C TREE DISCONNECT (0x4)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: TREE DISCONNECT (0x4)
     Credits: 2 (0x2)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 18 (0x12)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - CTreeDisconnect: 0x1
     Size: 4 (0x4)
     Reserved: 0 (0x0)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: R  TREE DISCONNECT (0x4), Mid = 18
    SMBIdentifier: SMB
  - SMB2Header: R TREE DISCONNECT (0x4)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: TREE DISCONNECT (0x4)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 18 (0x12)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RTreeDisconnect:
     Size: 4 (0x4)
     Reserved: 0 (0x0)
```

5.3.1.5 SMB2: SMB2 LOGOFF

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: C  LOGOFF (0x2), Mid = 19
    SMBIdentifier: SMB
  - SMB2Header: C LOGOFF (0x2)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: LOGOFF (0x2)
     Credits: 4 (0x4)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 19 (0x13)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - CLogoff:
     Size: 4 (0x4)
     Reserved: 0 (0x0)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: R  LOGOFF (0x2), Mid = 19
    SMBIdentifier: SMB
  - SMB2Header: R LOGOFF (0x2)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: LOGOFF (0x2)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 19 (0x13)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RLogoff:
     Size: 4 (0x4)
     Reserved: 0 (0x0)
```

5.3.2 SMB2 Session Control

5.3.2.1 SMB2: SMB2 NEGOTIATE

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =102
- Smb2: C  NEGOTIATE (0x0), GUID={00000000-0000-0000-0000-000000000000}, Mid = 0
    SMBIdentifier: SMB
  - SMB2Header: C NEGOTIATE (0x0)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: NEGOTIATE (0x0)
     Credits: 0 (0x0)
   - Flags: 0x0
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................0...) Packet is not signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 0 (0x0)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 0 (0x0)
     Sig: Binary Large Object (16 Bytes)
  - CNegotiate:
     Size: 36 (0x24)
     DialectCount: 1 (0x1)
     SecurityMode: Signing Enabled (0x1)
     Reserved: 0 (0x0)
   - Capabilities: 0x0
      DFS:               (...............................0) DFS unavailable
      Reserved_bits1_31: (0000000000000000000000000000000.) Reserved
     Guid: {00000000-0000-0000-0000-000000000000}
     StartTime: No Time Specified (0)
   - Dialects:
      Dialects: 514 (0x202)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =236
- Smb2: R  NEGOTIATE (0x0), GUID={535674CC-5BE2-3AB4-40C2-ED1535D79C69}, Mid = 0
    SMBIdentifier: SMB
  - SMB2Header: R NEGOTIATE (0x0)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: NEGOTIATE (0x0)
     Credits: 1 (0x1)
   - Flags: 0x1
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................0...) Packet is not signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 0 (0x0)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 0 (0x0)
     Sig: Binary Large Object (16 Bytes)
  - RNegotiate:
     Size: 65 (0x41)
     SecurityMode: Unknown (0x3)
     DialectRevision: 514 (0x202)
     Reserved: 0 (0x0)
     Guid: {535674CC-5BE2-3AB4-40C2-ED1535D79C69}
   - Capabilities: 0x1
      DFS:               (...............................1) DFS available
      Reserved_bits1_31: (0000000000000000000000000000000.) Reserved
     MaxTransactSize: 65536 (0x10000)
     MaxReadSize: 65536 (0x10000)
     MaxWriteSize: 65536 (0x10000)
     SystemTime: 09/15/2008, 03:43:10 PM
     SystemStartTime: 09/15/2008, 02:06:39 PM
     SecurityBufferOffset: 128 (0x80)
     SecurityBufferLength: 108 (0x6C)
     Reserved2: 7471201 (0x720061)
   - securityBlob:
    - GssApi:
     + ApplicationHeader:
     + ThisMech: SpnegoToken (1.3.6.1.5.5.2)
     - InnerContextToken: 0x1
      - SpnegoToken: 0x1
       + Tag0:
       - NegTokenInit: 0x1
        + SequenceHeader:
        + Tag0:
        + MechTypes:
        + Tag3:
```

```
        + MechListMic:  &$not_defined_in_RFC4178@please_ignore
```

5.3.2.2 SMB2: SMB2 SESSION_SETUP

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...A...., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =3127
- Smb2: C  SESSION SETUP (0x1), Mid = 1
    SMBIdentifier: SMB
  - SMB2Header: C SESSION SETUP (0x1)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: SESSION SETUP (0x1)
     Credits: 8 (0x8)
   + Flags: 0x0
     NextCommand: 0 (0x0)
     MessageId: 1 (0x1)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 0 (0x0)
     Sig: Binary Large Object (16 Bytes)
  - CSessionSetup:
     Size: 25 (0x19)
     VcNumber: 0 (0x0)
     SecurityMode: Signing Required (0x2)
   - Capabilities: 0x1
      DFS:               (...............................1) DFS available
      Reserved_bits1_31: (0000000000000000000000000000000.) Reserved
     Channel: 0 (0x0)
     SecurityBufferOffset: 88 (0x58)
     SecurityBufferLength: 3039 (0xBDF)
     PreviousSessionId: 0 (0x0)
   - securityBlob: 0x1
    - GssApi:
     + ApplicationHeader:
     + ThisMech: SpnegoToken (1.3.6.1.5.5.2)
     - InnerContextToken: 0x1
      - SpnegoToken: 0x1
       + Tag0:
       - NegTokenInit: 0x1
        + SequenceHeader:
        + Tag0:
        + MechTypes:
        + Tag2:
        + OctetStringHeader:
        - MechToken: 0x1
         - MsKerberosToken: 0x1
          - GssApi:
           + ApplicationHeader:
           + ThisMech: KerberosToken (1.2.840.113554.1.2.2)
           - InnerContextToken: 0x1
            - KerberosToken: 0x1
               Krb5tokId: Krb5ApReq (0x100)
             - ApReq: KRB_AP_REQ (14)
              + ApplicationTag:
              + SequenceHeader:
              + Tag0:
              + PvNo: 5
              + Tag1:
              + MsgType: KRB_AP_REQ (14)
              + Tag2: 0x1
              - ApOptions:
               + KerberosFlagsHeader:
               + Padding:
               - KrbFlags: 0x20000000
                  Reserved:       (0...............................)
                  UseSessionKey:  (.0..............................)
                  MutualRequired: (..1.............................)
                  Unused:         (...00000000000000000000000000000)
              + Tag3:
              - Ticket: Realm: 2008DOMAIN2.COM, Sname: cifs/2008DOMAIN2DC1.2008DOMAIN2.COM
               + ApplicationTag:
               + SequenceHeader:
               + Tag0:
               + TktVno: 5
               + Tag1:
               + Realm: 2008DOMAIN2.COM
               + Tag2: 0x1
               + Sname: cifs/2008DOMAIN2DC1.2008DOMAIN2.COM
               + Tag3: 0x1
               + EncPart:
              + Tag4:

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =257
- Smb2: R  SESSION SETUP (0x1) ,SessionFlags=0x0, Mid = 1
    SMBIdentifier: SMB
  - SMB2Header: R SESSION SETUP (0x1)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: SESSION SETUP (0x1)
     Credits: 8 (0x8)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 1 (0x1)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - RSessionSetup:
     Size: 9 (0x9)
   - SessionFlags: 0x0
      GU:               (...............0) NOT a guest user
      NU:               (..............0.) NOT a NULL user
      Reserved_bits2_15: (00000000000000..) Reserved
     SecurityBufferOffset: 72 (0x48)
     SecurityBufferLength: 185 (0xB9)
   - securityBlob: 0x1
    - ResponseToken:
     + Tag1:
     - NegTokenResp: 0x1
      + SequenceHeader:
      + Tag0:
      + NegState: accept-completed (0)
      + Tag1:
      + SupportedMech: MsKerberosToken (1.2.840.48018.1.2.2)
      + Tag2:
      - ResponseToken:
       + OctetStringHeader:
       - SecurityBlob: 0x1
        - MsKerberosToken: 0x1
         - GssApi:
          + ApplicationHeader:
```

```
+ ThisMech: KerberosToken (1.2.840.113554.1.2.2)
- InnerContextToken: 0x1
 - KerberosToken: 0x1
    Krb5tokId: Krb5ApRep (0x200)
  - ApRep: KRB_AP_REP (15)
   + ApplicationTag:
   + SequenceHeader:
   + Tag0:
   + PvNo: 5
   + Tag1:
   + MsgType: KRB_AP_REP (15)
   + Tag2: 0x1
   - AuthorizationData:
    + SequenceHeader:
    + Tag0:
    + EType: aes256-cts-hmac-sha1-96 (18)
    + Tag2:
    + Cipher: ...
```

5.3.2.3 SMB2: SMB2 TREE_CONNECT (IPC$)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =146
- Smb2: C  TREE CONNECT (0x3), Path=\\2008DOMAIN2DC1.2008DOMAIN2.COM\IPC$, Mid = 2
    SMBIdentifier: SMB
  - SMB2Header: C TREE CONNECT (0x3)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
```

```
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: TREE CONNECT (0x3)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 2 (0x2)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CTreeConnect:
     Size: 9 (0x9)
     Reserved: 0 (0x0)
     PathOffset: 72 (0x48)
     PathLength: 74 (0x4A)
     Path: \\2008DOMAIN2DC1.2008DOMAIN2.COM\IPC$

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =80
- Smb2: R  TREE CONNECT (0x3), TID=0x1, Mid = 2
    SMBIdentifier: SMB
  - SMB2Header: R TREE CONNECT (0x3)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: TREE CONNECT (0x3)
     Credits: 1 (0x1)
```

```
 - Flags: 0x9
    ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
    AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
    Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
    Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
    Reserved4_27:  (....000000000000000000000000....)
    DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
    Reserved29_31: (000.............................)
   NextCommand: 0 (0x0)
   MessageId: 2 (0x2)
   ProcessId: 65279 (0xFEFF)
   TreeId: 1 (0x1)
   SessionId: 4398247837773 (0x4000C00004D)
   Sig: Binary Large Object (16 Bytes)
- RTreeConnect: 0x1
   Size: 16 (0x10)
   ShareType: Pipe (0x2)
   Reserved: 0 (0x0)
 - ShareFlags: 48 (0x30)
    SHI1005_FLAGS_DFS:                         (...............................0) The specified share is not present
                                                                                  in a Distributed File System (DFS)
                                                                                  tree structure
    SHI1005_FLAGS_DFS_ROOT:                    (..............................0.) The specified share is not the root
                                                                                  volume in a DFS tree structure
    Reserved_bits3_4:                          (............................00..)
    SHAREFLAGS_CACHING_TYPE:                   (........................0011....) Unknown (0x3)
    SHI1005_FLAGS_RESTRICT_EXCLUSIVE_OPENS:    (.......................0........) The specified share allows
                                                                                  exclusive file opens that deny
                                                                                  reads to an open file
    SHI1005_FLAGS_FORCE_SHARED_DELETE:         (......................0.........) Shared files in the specified share
                                                                                  can't be forcibly deleted
    SHI1005_FLAGS_ALLOW_NAMESPACE_CACHING:     (.....................0..........) Clients aren't allowed to cache the
                                                                                  namespace of the specified share
    SHI1005_FLAGS_ACCESS_BASED_DIRECTORY_ENUM: (....................0...........) The server will not filter
                                                                                  directory entries based on the
```

```
                                                                                   access permissions of the client
     Reserved_bits13_32:                        (00000000000000000000............)
  - Capabilities: 0x0
     DFS:                     (...............................0) DFS unavailable
     Reserved_bits1_31:       (0000000000000000000000000000000.) Reserved
  - MaximalAccess: 0x1F01FF
     ReadData:             (...............................1) Set FILE_READ_DATA (file & named pipe),
                                                             FILE_LIST_DIRECTORY (directory)
     WriteData:            (..............................1.) Set FILE_WRITE_DATA (file & named pipe), FILE_ADD_FILE
                                                             (directory)
     AppendData:           (.............................1..) Set FILE_APPEND_DATA (file), FILE_ADD_SUBDIRECTORY
                                                             (directory), FILE_CREATE_PIPE_INSTANCE (named pipe)
     ReadEA:               (............................1...) Set FILE_READ_EA (file & directory)
     WriteEA:              (...........................1....) Set FILE_WRITE_EA (file & directory)
     Execute:              (..........................1.....) Set FILE_EXECUTE (file), FILE_TRAVERSE (directory)
     Reserved_bit6:        (.........................1......) Reserved
     ReadAttributes:       (........................1.......) Set FILE_READ_ATTRIBUTES (all)
     WriteAttributes:      (.......................1........) Set FILE_WRITE_ATTRIBUTES (all)
     Reserved_bits9_15:    (................0000000.........) Reserved
     Delete:               (...............1................) Set DELETE (the right to delete the object)
     ReadControl:          (..............1.................) Set READ_CONTROL (read the object's security descriptor
                                                             NOT including SACL)
     WriteDAC:             (.............1..................) Set WRITE_DAC (modify the DACL in the object's security
                                                             descriptor)
     WriteOwner:           (............1...................) Set WRITE_OWNER (change the owner in the object's
                                                             security descriptor)
     Synchronize:          (...........1....................) Set SYNCHRONIZE (use the object for synchronization)
     Reserved_bits21_23:   (........000.....................) Reserved
     AccessSystemSecurity: (.......0........................) NOT Set ACCESS_SYSTEM_SECURITY (get or set the SACL in
                                                             an object's security descriptor)
     MaximumAllowed:       (......0.........................) NOT Set MAXIMUM_ALLOWED (all access rights valid for the
                                                             caller)
     Reserved_bits26_27:   (....00..........................) Reserved
     GenericAll:           (...0............................) NOT Set GENERIC_ALL
     GenericExecute:       (..0.............................) NOT Set GENERIC_EXECUTE
```

```
      GenericWrite:         (.0..............................) NOT Set GENERIC_WRITE
      GenericRead:          (0...............................) NOT Set GENERIC_READ
```

5.4 lsarpc

5.4.1 SMB2 / RPC : lsarpc Session Control

5.4.1.1 SMB2: SMB2 CREATE lsarpc

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =132
- Smb2: C  CREATE (0x5), Name=lsarpc@#17, Mid = 4
    SMBIdentifier: SMB
  - SMB2Header: C CREATE (0x5)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: CREATE (0x5)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 4 (0x4)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - CCreate:
     Size: 57 (0x39)
   - SecurityFlags: 0x00000000
      DynamicTrakcing:  (.......0) Security tracking mode is not dynamic.
      EffectiveOnly:    (......0.) Not Only the enabled aspects of the client security context are available to the
                                   server.
      Reserved_bits2_7: (000000..) UnUsed
     RequestedOplockLevel: SMB2_OPLOCK_LEVEL_NONE - No oplock is granted.
     ImpersonationLevel: Impersonation - The server can impersonate the client's security context while acting on
                         behalf of the client.
     SmbCreateFlags: 0 (0x0)
     Reserved: 0 (0x0)
   - DesiredAccess: 0x12019F
      ReadData:             (...............................1) Set FILE_READ_DATA (file & named pipe),
                                                               FILE_LIST_DIRECTORY (directory)
      WriteData:            (..............................1.) Set FILE_WRITE_DATA (file & named pipe), FILE_ADD_FILE
                                                               (directory
      AppendData:           (.............................1..) Set FILE_APPEND_DATA (file), FILE_ADD_SUBDIRECTORY
                                                               (directory), FILE_CREATE_PIPE_INSTANCE (named pipe)
      ReadEA:               (............................1...) Set FILE_READ_EA (file & directory)
      WriteEA:              (...........................1....) Set FILE_WRITE_EA (file & directory)
      Execute:              (..........................0.....) NOT Set FILE_EXECUTE (file), FILE_TRAVERSE (directory)
      Reserved_bit6:        (.........................0......) Reserved
      ReadAttributes:       (........................1.......) Set FILE_READ_ATTRIBUTES (all)
      WriteAttributes:      (.......................1........) Set FILE_WRITE_ATTRIBUTES (all)
      Reserved_bits9_15:    (................0000000.........) Reserved
      Delete:               (...............0................) NOT Set DELETE (the right to delete the object)
      ReadControl:          (..............1.................) Set READ_CONTROL (read the object's security descriptor
                                                               NOT including SACL)
      WriteDAC:             (.............0..................) NOT Set WRITE_DAC (modify the DACL in the object's
                                                               security descriptor)
      WriteOwner:           (............0...................) NOT Set WRITE_OWNER (change the owner in the object's
                                                               security descriptor)
      Synchronize:          (...........1....................) Set SYNCHRONIZE (use the object for synchronization)
      Reserved_bits21_23:   (........000.....................) Reserved
      AccessSystemSecurity: (.......0........................) NOT Set ACCESS_SYSTEM_SECURITY (get or set the SACL in
                                                               an object's security descriptor)
      MaximumAllowed:       (......0.........................) NOT Set MAXIMUM_ALLOWED (all access rights valid for the
                                                               caller)
      Reserved_bits26_27:   (....00..........................) Reserved
      GenericAll:           (...0............................) NOT Set GENERIC_ALL
      GenericExecute:       (..0.............................) NOT Set GENERIC_EXECUTE
      GenericWrite:         (.0..............................) NOT Set GENERIC_WRITE
      GenericRead:          (0...............................) NOT Set GENERIC_READ
   - FileAttributes:
    - FSCCFileAttribute: 0 (0x0)
       ReadOnly:           (...............................0) Read/Write
       Hidden:             (..............................0.) Not Hidden
       System:             (.............................0..) Not System
       Reserved_bits3:     (............................0...) Reserved
       Directory:          (...........................0....) File
       Archive:            (..........................0.....) Not Archive
       Device:             (.........................0......) Not Device
       Normal:             (........................0.......) Not Normal
       Temporary:          (.......................0........) Permanent
       Sparse:             (......................0.........) Not Sparse
       Reparse:            (.....................0..........) Not Reparse Point
       Compressed:         (....................0...........) Uncompressed
       Offline:            (...................0............) Online
       NotIndexed:         (..................0.............) Content indexed
       Encrypted:          (.................0..............) Unencrypted
       Reserved_bits15_31: (00000000000000000...............) Reserved
     ShareAccess: Shared for Read/Write (0x00000003)
     CreateDisposition: Opened (0x00000001)
   - CreateOptions: 0x40
      FILE_DIRECTORY_FILE:            (...............................0) non-directory
      FILE_WRITE_THROUGH:             (..............................0.) non-write through
      FILE_SEQUENTIAL_ONLY:           (.............................0..) non-sequentially writing allowed
      FILE_NO_INTERMEDIATE_BUFFERING: (............................0...) intermediate buffering allowed
      Reserved_bits4_5:               (..........................00....) NOT ignored by the server
      FILE_NON_DIRECTORY_FILE:        (.........................1......) NOT be a directory file or this call MUST be
                                                                         failed
      Reserved_bits7_8:               (.......................00.......) Reserved
      FILE_NO_EA_KNOWLEDGE:           (......................0.........) no EA knowledge bit is not set
      Reserved_bits10:                (.....................0..........) Reserved
      FILE_RANDOM_ACCESS:             (....................0...........) accesses to the file can NOT be random
      FILE_DELETE_ON_CLOSE:           (...................0............) the DesiredAccess field MUST NOT include the
                                                                         DELETE flag
      Reserved_bits13:                (..................0.............) Reserved
      FILE_OPEN_FOR_BACKUP_INTENT:    (.................0..............) the file is not being opened for backup intent
      FILE_NO_COMPRESSION:            (................0...............) the file can be compressed
      Reserved_bits16_20:             (............0000................) Reserved
      FILE_RESERVE_OPFILTER:          (...........0....................) Reserved. The client SHOULD set this bit to 0
      FILE_OPEN_REPARSE_POINT:        (..........0.....................) open the reparse the target that the reparse
                                                                         point references
      FILE_OPEN_NO_RECALL:            (.........0......................) the file should be recalled from tertiary
                                                                         storage such as tape
      FILE_OPEN_FOR_FREE_SPACE_QUERY: (........0.......................) No file open to query for free space
      Reserved_bits23_31:             (00000000........................) Reserved
     NameOffset: 120 (0x78)
     NameLength: 12 (0xC)
     CreateContextsOffset: 0 (0x0)
     CreateContextsLength: 0 (0x0)
```

```
     Name: lsarpc

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =152
- Smb2: R  CREATE (0x5), FID=0xFFFFFFFF00000001, Mid = 4
    SMBIdentifier: SMB
  - SMB2Header: R CREATE (0x5)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: CREATE (0x5)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 4 (0x4)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RCreate: 0x1
     Size: 89 (0x59)
     OplockLevel: SMB2_OPLOCK_LEVEL_NONE - No oplock is granted.
     Reserved: 0 (0x0)
     CreateAction: Opened (0x00000001)
     CreationTime: No Time Specified (0)
     LastAccessTime: No Time Specified (0)
     LastWriteTime: No Time Specified (0)
     LastChangeTime: No Time Specified (0)
     AllocationSize: 4096 (0x1000)
     EndOfFile: 0 (0x0)
   - FileAttributes:
    - FSCCFileAttribute: 128 (0x80)
       ReadOnly:           (...............................0) Read/Write
       Hidden:             (..............................0.) Not Hidden
       System:             (.............................0..) Not System
       Reserved_bits3:     (............................0...) Reserved
       Directory:          (...........................0....) File
       Archive:            (..........................0.....) Not Archive
       Device:             (.........................0......) Not Device
       Normal:             (........................1.......) Normal
       Temporary:          (.......................0........) Permanent
       Sparse:             (......................0.........) Not Sparse
       Reparse:            (.....................0..........) Not Reparse Point
       Compressed:         (....................0...........) Uncompressed
       Offline:            (...................0............) Online
       NotIndexed:         (..................0.............) Content indexed
       Encrypted:          (.................0..............) Unencrypted
       Reserved_bits15_31: (00000000000000000...............) Reserved
     Reserved2: 7471201 (0x720061)
   + Fid: Persistent: 0x1000000099, Volatile: 0xFFFFFFFF00000001
     CreateContextsOffset: 0 (0x0)
     CreateContextsLength: 0 (0x0)
```

5.4.1.2 RPC: Bind to lsarpc ([C706])

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =228
- Smb2: C  WRITE (0x9), FID=0xFFFFFFFF00000001, 0x74 bytes at offset 0 (0x0), Mid = 5
    SMBIdentifier: SMB
  - SMB2Header: C WRITE (0x9)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: WRITE (0x9)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 5 (0x5)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - CWrite: 0x1
     Size: 49 (0x31)
     DataOffset: 112 (0x70)
     DataLength: 116 (0x74)
     Offset: 0 (0x0)
   + Fid: Persistent: 0x1000000099, Volatile: 0xFFFFFFFF00000001
     Channel: 0 (0x0)
     RemainingBytes: 0 (0x0)
     WriteChannelInfoOffset: 0 (0x0)
     WriteChannelInfoLength: 0 (0x0)
     Flags: 0 (0x0)
```

```
- msrpc: c/o Bind:  UUID{12345778-1234-ABCD-EF00-0123456789AB} LSARpc  Call=0x1  Assoc Grp=0x0  Xmit=0x10B8
Recv=0x10B8
  - Bind: {12345778-1234-ABCD-EF00-0123456789AB} LSARpc
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0B - Bind
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 116 (0x74)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 4280 (0x10B8)
     MaxRecvFrag: 4280 (0x10B8)
     AssocGroupId: 0 (0x0)
   - PContextElem:
      NContextElem: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PContElem: 0x1
       PContId: 0 (0x0)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     - AbstractSyntax: {12345778-1234-ABCD-EF00-0123456789AB} LSARpc
```

```
      + IfUuid: {12345778-1234-ABCD-EF00-0123456789AB}
        IfVersion: 0 (0x0)
     - TransferSyntaxes: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
      + IfUuid: {8A885D04-1CEB-11C9-9FE8-08002B104860}
        IfVersion: 2 (0x2)
    - PContElem: 0x1
       PContId: 1 (0x1)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {12345778-1234-ABCD-EF00-0123456789AB} LSARpc
     + TransferSyntaxes: {6CB71C2C-9812-4540-0300000000000000} BTFN - Security Context Multiplexing Supported
     AuthVerifier: 0x1

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =80
- Smb2: R  WRITE (0x9), 0x74 bytes written, Mid = 5
    SMBIdentifier: SMB
  - SMB2Header: R WRITE (0x9)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: WRITE (0x9)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 5 (0x5)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RWrite: 0x1
     Size: 17 (0x11)
     Reserved: 0 (0x0)
     DataLength: 116 (0x74)
     Remaining: 0 (0x0)
     WriteChannelInfoOffset: 0 (0x0)
     WriteChannelInfoLength: 0 (0x0)

+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =113
- Smb2: C  READ (0x8), FID=0xFFFFFFFF00000001, 0x400 bytes from offset 0 (0x0), Mid = 6
    SMBIdentifier: SMB
  - SMB2Header: C READ (0x8)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: READ (0x8)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 6 (0x6)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - CRead: 0x1
     Size: 49 (0x31)
     Padding: 80 (0x50)
     Reserved: 0 (0x0)
     DataLength: 1024 (0x400)
     Offset: 0 (0x0)
   + Fid: Persistent: 0x1000000099, Volatile: 0xFFFFFFFF00000001
     MinimumCount: 0 (0x0)
     Channel: 0 (0x0)
     RemainingBytes: 0 (0x0)
     ReadChannelInfoOffset: 0 (0x0)
     ReadChannelInfoLength: 0 (0x0)
     Buffer: 0 (0x0)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =172
- Smb2: R  READ (0x8), 0x5c bytes read, Mid = 6
    SMBIdentifier: SMB
  - SMB2Header: R READ (0x8)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: READ (0x8)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 6 (0x6)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RRead: 0x1
     Size: 17 (0x11)
     DataOffset: 80 (0x50)
     Reserved: 0 (0x0)
     DataLength: 92 (0x5C)
     DataRemaining: 0 (0x0)
     Reserved2: 0 (0x0)
- msrpc: c/o Bind Ack:  Call=0x1  Assoc Grp=0xC6DE  Xmit=0x10B8  Recv=0x10B8
  - BindAck:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0C - Bind Ack
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 92 (0x5C)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 4280 (0x10B8)
     MaxRecvFrag: 4280 (0x10B8)
     AssocGroupId: 50910 (0xC6DE)
   - SecAddr: \pipe\lsass
      Length: 12 (0xC)
      PortSpec: \pipe\lsass
   + Pad2: 0x1
   - PResultList:
      NResults: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PResults: Acceptance, Reason=n/a
       Result: Acceptance
       Reason: n/a
     - TransferSyntax: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
      + IfUuid: {8A885D04-1CEB-11C9-9FE8-08002B104860}
        IfVersion: 2 (0x2)
    - PResults: Negotiate Ack, Security Context Multiplexing Supported
       Result: Negotiate Ack
     - bitmask: Security Context Multiplexing Supported
        BitMask: 3 (0x3)
        Unused: 0 (0x0)
     - TransferSyntax: {00000000-0000-0000-0000-000000000000} unknown
      + IfUuid: {00000000-0000-0000-0000-000000000000}
        IfVersion: 0 (0x0)
     AuthVerifier:
```

5.4.1.3 lsarpc: LsarClose

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =164
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 9
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 9 (0x9)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  + CIoCtl:
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Opnum=0x0  Context=0x0  Hint=0x14
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 44 (0x2C)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 20 (0x14)
     PContId: 0 (0x0)
     Opnum: 0 (0x0)
   - StubData: 20 bytes
      StubData: 0x1
- Lsad: LsarClose Request, Object Handle: {00000000-6316935A-2844-A840-A335-987AD568A050}
    ObjectHandle: {00000000-6316935A-2844-A840-A335-987AD568A050}

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =208
- Smb2: R  IOCTL (0xb), Mid = 9
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   + Flags: 0x9
     NextCommand: 0 (0x0)
     MessageId: 9 (0x9)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RIoCtl:
     Size: 49 (0x31)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x1000000099, Volatile: 0xFFFFFFFF00000001
     InputOffset: 112 (0x70)
     InputCount: 44 (0x2C)
     OutputOffset: 160 (0xA0)
     OutputCount: 48 (0x30)
     Flags: 0 (0x0)
     Reserved2: 0 (0x0)
     InputData: Binary Large Object (44 Bytes)
     OutputPadding: Binary Large Object (4 Bytes)
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Context=0x0  Hint=0x18  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   - StubData: 24 bytes
      StubData: 0x1
- Lsad: LsarClose Response, Handle Closed: {00000000-00000000-0000-0000-0000-000000000000},
                            Status = 0x00000000 - STATUS_SUCCESS
    ObjectHandle: {00000000-00000000-0000-0000-0000-000000000000}
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.1.4 SMB2: SMB2 CLOSE

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =88
- Smb2: C  CLOSE (0x6), FID=0xFFFFFFFF00000009, Mid = 10
    SMBIdentifier: SMB
  - SMB2Header: C CLOSE (0x6)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: CLOSE (0x6)
     Credits: 27 (0x1B)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 24 (0x18)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CClose: 0x1
     Size: 24 (0x18)
   - Flags: Not Contain additional fields in response packet
      POSTQUERY:         (...............0) NOT use the values returned in the response
      Reserved_bits1_15: (000000000000000.) Reserved
     Reserved: 0 (0x0)
   + Fid: Persistent: 0x1000000095, Volatile: 0xFFFFFFFF00000009

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21, Next Protocol = TCP, Packet ID = 11430, Total IP Length = 168
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =124
- Smb2: R  CLOSE (0x6), Mid = 10
    SMBIdentifier: SMB
  - SMB2Header: R CLOSE (0x6)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: CLOSE (0x6)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 24 (0x18)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - RClose:
     Size: 60 (0x3C)
     Flags: 0 (0x0)
     Reserved: 0 (0x0)
     CreationTime: No Time Specified (0)
     LastAccessTime: No Time Specified (0)
     LastWriteTime: No Time Specified (0)
     LastChangeTime: No Time Specified (0)
     AllocationSize: 0 (0x0)
     EndOfFile: 0 (0x0)
   - FileAttributes:
    - FSCCFileAttribute: 0 (0x0)
       ReadOnly:           (...............................0) Read/Write
       Hidden:             (..............................0.) Not Hidden
       System:             (.............................0..) Not System
       Reserved_bits3:     (............................0...) Reserved
       Directory:          (...........................0....) File
       Archive:            (..........................0.....) Not Archive
       Device:             (.........................0......) Not Device
       Normal:             (........................0.......) Not Normal
       Temporary:          (.......................0........) Permanent
       Sparse:             (......................0.........) Not Sparse
       Reparse:            (.....................0..........) Not Reparse Point
       Compressed:         (....................0...........) Uncompressed
       Offline:            (...................0............) Online
       NotIndexed:         (.................0..............) Content indexed
       Encrypted:          (................0...............) Unencrypted
       Reserved_bits15_31: (00000000000000000...............) Reserved
```

5.4.1.5 SMB2: SMB2 LOGOFF

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: C  LOGOFF (0x2), Mid = 11
    SMBIdentifier: SMB
  - SMB2Header: C LOGOFF (0x2)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: LOGOFF (0x2)
     Credits: 4 (0x4)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 19 (0x13)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - CLogoff:
     Size: 4 (0x4)
     Reserved: 0 (0x0)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: R  LOGOFF (0x2), Mid = 11
    SMBIdentifier: SMB
  - SMB2Header: R LOGOFF (0x2)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: LOGOFF (0x2)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 19 (0x13)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837777 (0x4000C000051)
     Sig: Binary Large Object (16 Bytes)
  - RLogoff:
     Size: 4 (0x4)
     Reserved: 0 (0x0)
```

5.4.2 TCP / RPC: lsarpc Session Control

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=49188, DstPort=49157
- RPC: c/o Bind:  UUID{12345778-1234-ABCD-EF00-0123456789AB} LSARpc  Call=0x1  Assoc Grp=0x0  Xmit=0x16D0  Recv=0x16D0
  - Bind: {12345778-1234-ABCD-EF00-0123456789AB} LSARpc
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0B - Bind
   - PfcFlags: 7 (0x7)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....1.. PFC_SUPPORT_HEADER_SIGN - SET, Header Sign was supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 192 (0xC0)
     AuthLength: 68 (0x44)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 0 (0x0)
   - PContextElem:
      NContextElem: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PContElem: 0x1
       PContId: 0 (0x0)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {12345778-1234-ABCD-EF00-0123456789AB} LSARpc
     + TransferSyntaxes: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PContElem: 0x1
       PContId: 1 (0x1)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {12345778-1234-ABCD-EF00-0123456789AB} LSARpc
     + TransferSyntaxes: {6CB71C2C-9812-4540-0300000000000000} BTFN - Security Context Multiplexing Supported
   - AuthVerifier: 0x1
      AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 0 (0x0)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - NetlogonMessage:
        MessageType: 0x0, Negotiate Message
      - Flags: 23 (0x17)
         NLAuthNetbiosDomainName:        (...............................1) Buffer contains NetBIOS domain name as an
                                                                            OEM string
         NLAuthNetbiosComputerName:      (..............................1.) Buffer contains NetBIOS computer name as an
                                                                            OEM string
         NLAuthDNSDomainName:            (.............................1..) Buffer contains DNS domain name as UTF-8
                                                                            string
         NLAuthDNSHostName:              (............................0...) Buffer does not contain DNS host name
         NLAuthUTF8NetbiosComputerName:  (...........................1....) Buffer contains computer name as UTF-8
                                                                            string
        NetBiosDomainName: 2008DOMAIN2
```

```
        NetBiosComputerName: 2008DOMAIN1DC1
        DNSDomainName: 2008DOMAIN2.COM
        UTF8NetBiosComputerName: 2008DOMAIN1DC1

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=49157, DstPort=49188
- RPC: c/o Bind Ack:  Call=0x1  Assoc Grp=0x15DFB  Xmit=0x16D0  Recv=0x16D0
  - BindAck:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0C - Bind Ack
   - PfcFlags: 7 (0x7)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....1.. PFC_SUPPORT_HEADER_SIGN - SET, Header Sign was supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 104 (0x68)
     AuthLength: 12 (0xC)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 89595 (0x15DFB)
   + SecAddr: 49157
     Pad2: 0x1
   - PResultList:
      NResults: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PResults: Acceptance, Reason=n/a
       Result: Acceptance
       Reason: n/a
     + TransferSyntax: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PResults: Negotiate Ack, Security Context Multiplexing Supported
       Result: Negotiate Ack
     + bitmask: Security Context Multiplexing Supported
     + TransferSyntax: {00000000-0000-0000-0000-000000000000} unknown
   - AuthVerifier:
      AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 0 (0x0)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - NetlogonMessage:
        MessageType: 0x1, Negotiate Response Message
      - Flags: 0 (0x0)
         NLAuthNetbiosDomainName:        (...............................0) Buffer does not contain NetBIOS domain name
         NLAuthNetbiosComputerName:      (..............................0.) Buffer does not contain NetBIOS computer
                                                                            name
         NLAuthDNSDomainName:            (.............................0..) Buffer does not contain DNS domain name
         NLAuthDNSHostName:              (............................0...) Buffer does not contain DNS host name
         NLAuthUTF8NetbiosComputerName:  (...........................0....) Buffer does not contain computer name
        Buffer: Binary Large Object (4 Bytes)
```

5.4.3 lsarpc: Procedure Calls

5.4.3.1 lsarpc: LsarOpenPolicy2

5.4.3.1.1 lsarpc: LsarOpenPolicy2 (ViewLocalInformation)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59967, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =256
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 7
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 7 (0x7)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837769 (0x4000C000049)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x1000000089, Volatile: 0xFFFFFFFF00000001
     InputOffset: 120 (0x78)
     InputCount: 136 (0x88)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x1  Opnum=0x2C  Context=0x0  Hint=0x70
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 136 (0x88)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 112 (0x70)
     PContId: 0 (0x0)
     Opnum: 44 (0x2C)
   + StubData: 112 bytes
- Lsad: LsarOpenPolicy2 Request, Target Computer: \\2008DOMAIN2DC1.2008DOMAIN2.COM, DesiredAccess: 0x00000001,
  + SystemName: \\2008DOMAIN2DC1.2008DOMAIN2.COM
  - ObjectAttributes:
   + padding: 2 Bytes
     Length: 0 (0x0)
   + RootDirectoryPointer: Pointer To NULL
   + ObjectNamePointer: Pointer To NULL
   + Attributes: 0x00000000
   + SecurityDescriptorPointer: Pointer To NULL
   + SecurityQualityofServicePointer: Pointer To NULL
    Pad: 0 Bytes
  - DesiredAccess: 0x00000001
   - SpecificRights: 0x0001
      PolicyViewLocalInformation:   (...............1) Allow viewing of local information such as the primary domain or
                                                       account
      PolicyViewAuditInformation:   (..............0.) Do NOT allow viewing of audit configuration information
      PolicyGetPrivateInformation:  (.............0..) Do NOT allow viewing of private information on the local
                                                       computer
      PolicyTrustAdmin:             (............0...) Do NOT allow administration of trusted domains
      PolicyCreateAccount:          (...........0....) Do NOT allow creation of Local Security Authority (LSAD) account
                                                       objects
      PolicyCreateSecret:           (..........0.....) Do NOT allow creation of Local Security Authority (LSAD) secret
                                                       objects
      PolicyCreatePrivilege:        (.........0......) This constant is not used
      PolicySetDefaultQuotaLimits:  (........0.......) Do NOT allow setting of default quota limits
      PolicySetAuditRequirements:   (.......0........) Do NOT allow configuration of different audit categories
      PolicyAuditLogAdmin:          (......0.........) Do NOT allow setting of audit configuration information
      PolicyServerAdmin:            (.....0..........) Do NOT allow administration of the local computer
      PolicyLookupNames:            (....0...........) Do NOT allow the lookup of names
      PolicyNotification:           (...0............) Do NOT allow requesting the notification of policy changes
      Reserved:                     (000.............)
   + AccessRights: 0x0000

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59967
+ Nbtss: SESSION MESSAGE, Length =296
- Smb2: R  IOCTL (0xb), Mid = 7
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   - Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
      Code:     (................0000000000000000) (0) STATUS_SUCCESS
      Facility: (...0000000000000................) FACILITY_SYSTEM
      Customer: (..0.............................) NOT Customer Defined
      Severity: (00..............................) STATUS_SEVERITY_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 7 (0x7)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837769 (0x4000C000049)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl:
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x1  Context=0x0  Hint=0x18  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
- Lsad: LsarOpenPolicy2 Response, PolicyHandle: {00000000-2C67EAF8-F712-1B49-831B-73C97D9770AE},
                                  Status = 0x00000000 - STATUS_SUCCESS
    PolicyHandle: {00000000-2C67EAF8-F712-1B49-831B-73C97D9770AE}
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.3.1.2 lsarpc: LsarOpenPolicy2 (ViewLocalInformation, TrustAdmin, CreateSecret)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =256
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 6
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 6 (0x6)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x100000008D, Volatile: 0xFFFFFFFF00000001
     InputOffset: 120 (0x78)
     InputCount: 136 (0x88)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Opnum=0x2C  Context=0x0  Hint=0x70
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 136 (0x88)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 112 (0x70)
     PContId: 0 (0x0)
     Opnum: 44 (0x2C)
   + StubData: 112 bytes
- Lsad: LsarOpenPolicy2 Request, Target Computer: \\2008DOMAIN2DC1.2008DOMAIN2.COM, DesiredAccess: 0x00000029,
  + SystemName: \\2008DOMAIN2DC1.2008DOMAIN2.COM
  - ObjectAttributes:
   + padding: 2 Bytes
     Length: 0 (0x0)
   + RootDirectoryPointer: Pointer To NULL
   + ObjectNamePointer: Pointer To NULL
   - Attributes: 0x00000000
      Reserved1:            (...............................0)
      ObjInherit:           (..............................0.) The handle can NOT be inherited by child processes of
                                                               the current process
      Reserved2:            (............................00..)
      ObjPermanent:         (...........................0....) The object is deleted when all open handles are closed
      ObjExclusive:         (..........................0.....) Any number of handles can be open for this object or
                                                               NONE of them are opened
      ObjCaseInsensitive:   (.........................0......) A default system settings are used when matching the
                                                               ObjectName value against the names of existing objects
      ObjOpenif:            (........................0.......) If the object already exists, a collision occurs
      ObjOpenlink:          (.......................0........) The object is NOT opened as a symbolic link
      ObjKernelHandle:      (......................0.........) The handle can NOT be accessed only in kernel mode
      ObjForceAccessCheck:  (.....................0..........) NO access checks for the object should be enforced
      Reserved:             (00000000000000000000............)
   + SecurityDescriptorPointer: Pointer To NULL
   + SecurityQualityofServicePointer: Pointer To NULL
    Pad: 0 Bytes
  - DesiredAccess: 0x00000029
   - SpecificRights: 0x0029
      PolicyViewLocalInformation:   (...............1) Allow viewing of local information such as the primary domain or
                                                       account
      PolicyViewAuditInformation:   (..............0.) Do NOT allow viewing of audit configuration information
      PolicyGetPrivateInformation:  (.............0..) Do NOT allow viewing of private information on the local
                                                       computer
      PolicyTrustAdmin:             (............1...) Allow administration of trusted domains
      PolicyCreateAccount:          (...........0....) Do NOT allow creation of Local Security Authority (LSAD) account
                                                       objects
      PolicyCreateSecret:           (..........1.....) Allow creation of Local Security Authority (LSAD) secret objects
      PolicyCreatePrivilege:        (.........0......) This constant is not used
      PolicySetDefaultQuotaLimits:  (........0.......) Do NOT allow setting of default quota limits
      PolicySetAuditRequirements:   (.......0........) Do NOT allow configuration of different audit categories
      PolicyAuditLogAdmin:          (......0.........) Do NOT allow setting of audit configuration information
      PolicyServerAdmin:            (.....0..........) Do NOT allow administration of the local computer
      PolicyLookupNames:            (....0...........) Do NOT allow the lookup of names
      PolicyNotification:           (...0............) Do NOT allow requesting the notification of policy changes
      Reserved:                     (000.............)
   + AccessRights: 0x0000

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =296
- Smb2: R  IOCTL (0xb), Mid = 6
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 6 (0x6)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl:
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Context=0x0  Hint=0x18  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
- Lsad: LsarOpenPolicy2 Response, PolicyHandle: {00000000-89508E53-C759-F642-B87D-3EBB144D7FB3},
                                  Status = 0x00000000 - STATUS_SUCCESS
    PolicyHandle: {00000000-89508E53-C759-F642-B87D-3EBB144D7FB3}
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.3.1.3 lsarpc: LsarOpenPolicy2 (CreateSecret)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59361, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =256
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 6
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   - Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 6 (0x6)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398046511157 (0x40000000035)
     Sig: Binary Large Object (16 Bytes)
  + CIoCtl:
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x1  Opnum=0x2C  Context=0x0  Hint=0x70
```

```
  + Request:
- Lsad: LsarOpenPolicy2 Request, Target Computer: \\2008DOMAIN2DC1.2008DOMAIN2.COM, DesiredAccess: 0x00000020,
  + SystemName: \\2008DOMAIN2DC1.2008DOMAIN2.COM
  + ObjectAttributes:
    Pad: 0 Bytes
  - DesiredAccess: 0x00000020
   - SpecificRights: 0x0020
      PolicyViewLocalInformation:   (...............0) Do NOT allow viewing of local information
      PolicyViewAuditInformation:   (..............0.) Do NOT allow viewing of audit configuration information
      PolicyGetPrivateInformation:  (.............0..) Do NOT allow viewing of private information on the local
                                                       computer
      PolicyTrustAdmin:             (............0...) Do NOT allow administration of trusted domains
      PolicyCreateAccount:          (...........0....) Do NOT allow creation of Local Security Authority (LSAD) account
                                                       objects
      PolicyCreateSecret:           (..........1.....) Allow creation of Local Security Authority (LSAD) secret objects
      PolicyCreatePrivilege:        (.........0......) This constant is not used
      PolicySetDefaultQuotaLimits:  (........0.......) Do NOT allow setting of default quota limits
      PolicySetAuditRequirements:   (.......0........) Do NOT allow configuration of different audit categories
      PolicyAuditLogAdmin:          (......0.........) Do NOT allow setting of audit configuration information
      PolicyServerAdmin:            (.....0..........) Do NOT allow administration of the local computer
      PolicyLookupNames:            (....0...........) Do NOT allow the lookup of names
      PolicyNotification:           (...0............) Do NOT allow requesting the notification of policy changes
      Reserved:                     (000.............)
   + AccessRights: 0x0000

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59361
+ Nbtss: SESSION MESSAGE, Length =296
- Smb2: R  IOCTL (0xb), Mid = 6
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 6 (0x6)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398046511157 (0x40000000035)
     Sig: Binary Large Object (16 Bytes)
  - RIoCtl:
     Size: 49 (0x31)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x5D, Volatile: 0xFFFFFFFF00000001
     InputOffset: 112 (0x70)
     InputCount: 136 (0x88)
     OutputOffset: 248 (0xF8)
     OutputCount: 48 (0x30)
     Flags: 0 (0x0)
     Reserved2: 0 (0x0)
     InputData: Binary Large Object (136 Bytes)
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x1  Context=0x0  Hint=0x18  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
- Lsad: LsarOpenPolicy2 Response, PolicyHandle: {00000000-844E503A-7C76-1E49-90F8-6E0D21371333},
                                  Status = 0x00000000 - STATUS_SUCCESS
    PolicyHandle: {00000000-844E503A-7C76-1E49-90F8-6E0D21371333}
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.3.2 lsarpc: LsarQueryInformationPolicy2 (PolicyDnsDomainInformation)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59350, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =166
```

```
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 7
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 7 (0x7)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x51, Volatile: 0xFFFFFFFF00000001
     InputOffset: 120 (0x78)
     InputCount: 46 (0x2E)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
```

```
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x2  Opnum=0x2E  Context=0x0  Hint=0x16
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 46 (0x2E)
     AuthLength: 0 (0x0)
     CallId: 4 (0x4)
     AllocHint: 22 (0x16)
     PContId: 0 (0x0)
     Opnum: 46 (0x2E)
   + StubData: 22 bytes
- Lsad: LsarQueryInformationPolicy2 Request, InfoClass: PolicyDnsDomainInformation (0x0C),
                                             Policy Handle: {00000000-89508E53-C759-F642-B87D-3EBB144D7FB3}
    PolicyHandle: {00000000-86FA3F2E-63FC-5E42-9938-F6B65744ADF7}
    InformationClass: PolicyDnsDomainInformation (0x0C) Dns domain information

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59350
+ Nbtss: SESSION MESSAGE, Length =392
- Smb2: R  IOCTL (0xb), Mid = 7
```

```
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   - Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
      Code:     (................0000000000000000) (0) STATUS_SUCCESS
      Facility: (...0000000000000................) FACILITY_SYSTEM
      Customer: (..0.............................) NOT Customer Defined
      Severity: (00..............................) STATUS_SEVERITY_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 7 (0x7)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl:
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x2  Context=0x0  Hint=0xD0  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 232 (0xE8)
     AuthLength: 0 (0x0)
     CallId: 4 (0x4)
     AllocHint: 208 (0xD0)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 208 bytes
- Lsad: LsarQueryInformationPolicy2 Response, PolicyDnsDomainInformation (0x0C),
                                              Name: 2008DOMAIN2, DNSDomainName: 2008DOMAIN2.COM,
                                              DNSForestName: 2008DOMAIN2.COM,
                                              SID: S-1-5-21-3252065517-4011377361-1377730089 Unknown SID,
                                              Status = 0x00000000 - STATUS_SUCCESS
  - PolicyInformation: PolicyDnsDomainInformation (0x0C) , Name: 2008DOMAIN2, DNSDomainName: 2008DOMAIN2.COM,
                                              DNSForestName: 2008DOMAIN2.COM,
                                              SID: S-1-5-21-3252065517-4011377361-1377730089 Unknown SID
   + Pointer: Pointer To 0x00020000
   + PolicyInformation: PolicyDnsDomainInformation (0x0C)
    pad: 0 Bytes
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.3.3 lsarpc: LsarQueryTrustedDomainInfo (TrustedDomainFullInformation)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=55615, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =194
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398046511177 (0x40000000049)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x81, Volatile: 0xFFFFFFFF00000001
```

```
     InputOffset: 120 (0x78)
     InputCount: 74 (0x4A)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Opnum=0x27  Context=0x0  Hint=0x32
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 74 (0x4A)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 50 (0x32)
     PContId: 0 (0x0)
     Opnum: 39 (0x27)
   + StubData: 50 bytes
```

```
- Lsad: LsarQueryTrustedDomainInfo Request, InfoClass: TrustedDomainFullInformation (0x08) , TrustedDomainSid: S-1-5-
21-2074671935-2981103931-2886920652 Unknown SID, PolicyHandle: {00000000-579A5F4A-0A56-294A-9A3A-CA26A7E360DA}
    PolicyHandle: {00000000-579A5F4A-0A56-294A-9A3A-CA26A7E360DA}
  - TrustedDomainSid: S-1-5-21-2074671935-2981103931-2886920652 Unknown SID
   + SubAuthoritySize: 4 Elements
     Revision: 1 (0x1)
     SubAuthorityCount: 4 (0x4)
   + IdentifierAuthority: {0,0,0,0,0,5} (0x5) [NT_AUTHORITY]
   - SubAuthority: 4 Sub-Authorities
      SubAuthorityValueF: 21 (0x15)
      SubAuthorityValue: 2074671935 (0x7BA8FB3F)
      SubAuthorityValue: 2981103931 (0xB1B0093B)
      SubAuthorityValue: 2886920652 (0xAC12E9CC)
    InformationClass: TrustedDomainFullInformation (0x08) Query complete information for a trusted domain

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=55615
+ Nbtss: SESSION MESSAGE, Length =396
- Smb2: R  IOCTL (0xb), Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398046511177 (0x40000000049)
     Sig: Binary Large Object (16 Bytes)
  - RIoCtl:
     Size: 49 (0x31)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x81, Volatile: 0xFFFFFFFF00000001
     InputOffset: 112 (0x70)
     InputCount: 74 (0x4A)
     OutputOffset: 192 (0xC0)
     OutputCount: 204 (0xCC)
     Flags: 0 (0x0)
     Reserved2: 0 (0x0)
     InputData: Binary Large Object (74 Bytes)
     OutputPadding: Binary Large Object (6 Bytes)
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Context=0x0  Hint=0xB4  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 204 (0xCC)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 180 (0xB4)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 180 bytes
- Lsad: LsarQueryTrustedDomainInfo Response, Status = 0x00000000 - STATUS_SUCCESS
  + TrustedDomainInformation:
    padding: 0 Bytes
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.3.4 lsarpc: LsarQueryTrustedDomainInfoByName (TrustedDomainFullInformation)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =216
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
```

```
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x100000008D, Volatile: 0xFFFFFFFF00000001
     InputOffset: 120 (0x78)
     InputCount: 96 (0x60)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x6  Opnum=0x30  Context=0x0  Hint=0x48
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 96 (0x60)
     AuthLength: 0 (0x0)
     CallId: 6 (0x6)
     AllocHint: 72 (0x48)
     PContId: 0 (0x0)
     Opnum: 48 (0x30)
   + StubData: 72 bytes
- Lsad: LsarQueryTrustedDomainInfoByName Request, TrustedDomainName: 2008DOMAIN1.COM  InfoClass: 
TrustedDomainFullInformation (0x08)
    PolicyHandle: {00000000-50255EFB-9E81-9846-BDB6-30CC9FCE95ED}
  + TrustedDomainName: 2008DOMAIN1.COM
    InformationClass: TrustedDomainFullInformation (0x08) Query complete information for a trusted domain

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =240
- Smb2: R  IOCTL (0xb), Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x9
```

```
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - RIoCtl:
     Size: 49 (0x31)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x100000008D, Volatile: 0xFFFFFFFF00000001
     InputOffset: 112 (0x70)
     InputCount: 96 (0x60)
     OutputOffset: 208 (0xD0)
     OutputCount: 32 (0x20)
     Flags: 0 (0x0)
     Reserved2: 0 (0x0)
     InputData: Binary Large Object (96 Bytes)
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x6  Context=0x0  Hint=0x8  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 32 (0x20)
     AuthLength: 0 (0x0)
     CallId: 6 (0x6)
     AllocHint: 8 (0x8)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 8 bytes
- Lsad: LsarQueryTrustedDomainInfoByName Response, 0x1, Status = 0xC0000034 - STATUS_OBJECT_NAME_NOT_FOUND
  + TrustedDomainInformation: 0x1
    pad: 0 Bytes
    ReturnValue: 0xC0000034 - STATUS_OBJECT_NAME_NOT_FOUND
```

5.4.3.5 lsarpc: LsarCreateTrustedDomainEx2

5.4.3.5.1 lsarpc: LsarCreateTrustedDomainEx2 (Outgoing)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59351, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =908
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 11
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 11 (0xB)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398046511149 (0x4000000002D)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x55, Volatile: 0xFFFFFFFF00000001
     InputOffset: 120 (0x78)
     InputCount: 788 (0x314)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x9  Opnum=0x3B  Context=0x0  Hint=0x2FC
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 788 (0x314)
     AuthLength: 0 (0x0)
     CallId: 9 (0x9)
     AllocHint: 764 (0x2FC)
     PContId: 0 (0x0)
     Opnum: 59 (0x3B)
   + StubData: 764 bytes
- Lsad: LsarCreateTrustedDomainEx2 Request, 0x1, DesiredAccess: 0x00000000, PolicyHandle:
                                            {00000000-C746E218-977B-2E4B-9AEC-0685F9100123}
    PolicyHandle: {00000000-C746E218-977B-2E4B-9AEC-0685F9100123}
  - TrustedDomainInformation: 0x1
   + InformationHeader:
   + Information: 2008DOMAIN1.COM, 2008DOMAIN1, S-1-5-21-2074671935-2981103931-2886920652 Unknown SID
  - AuthenticationInformation: 
   + Header: 
   - Data: 
    + MaxCount: 588 Elements
      AuthBlob: Binary Large Object (588 Bytes)
    Pad: 0 Bytes
  - DesiredAccess: 0x00000000
   + SpecificRights: 0x0000
   + AccessRights: 0x0000

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59351
+ Nbtss: SESSION MESSAGE, Length =952
- Smb2: R  IOCTL (0xb), Mid = 11
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 11 (0xB)
     AsyncId: 33 (0x21)
     SessionId: 4398046511149 (0x4000000002D)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl: 
```

```
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x9  Context=0x0  Hint=0x18  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 9 (0x9)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
- Lsad: LsarCreateTrustedDomainEx2 Response, TrustedDomainHandle: {87A9C1B2-27F01146-A918-40AD-677C-D37E00000000},
                                             Status = 0x00000000 - STATUS_SUCCESS
  + Pointer: Pointer To NULL
    TrustedDomainHandle: {87A9C1B2-27F01146-A918-40AD-677C-D37E00000000}
```

5.4.3.5.2 lsarpc: LsarCreateTrustedDomainEx2 (Incoming)

Create TDO on other domain

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60324, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =908
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 11
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 112 (0x70)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 11 (0xB)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398382055525 (0x40014000065)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x200000002D, Volatile: 0xFFFFFFFF00000001
```

```
     InputOffset: 120 (0x78)
     InputCount: 788 (0x314)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x9  Opnum=0x3B  Context=0x0  Hint=0x2FC
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 788 (0x314)
     AuthLength: 0 (0x0)
     CallId: 9 (0x9)
     AllocHint: 764 (0x2FC)
     PContId: 0 (0x0)
     Opnum: 59 (0x3B)
   + StubData: 764 bytes
- Lsad: LsarCreateTrustedDomainEx2 Request, 0x1, DesiredAccess: 0x00000000, PolicyHandle:
```

```
                                             {00000000-BD0DA5D2-7CF7-6944-9797-B29C9383CC0F}
    PolicyHandle: {00000000-BD0DA5D2-7CF7-6944-9797-B29C9383CC0F}
  - TrustedDomainInformation: 0x1
   + InformationHeader:
   + Information: 2008DOMAIN1.COM, 2008DOMAIN1, S-1-5-21-2074671935-2981103931-2886920652 Unknown SID
  - AuthenticationInformation:
   + Header:
   - Data:
    + MaxCount: 588 Elements
      AuthBlob: Binary Large Object (588 Bytes)
    Pad: 0 Bytes
  - DesiredAccess: 0x00000000
   + SpecificRights: 0x0000
   + AccessRights: 0x0000


+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=60324
+ Nbtss: SESSION MESSAGE, Length =952
- Smb2: R  IOCTL (0xb), Mid = 11
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   - Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
      Code:     (................0000000000000000) (0) STATUS_SUCCESS
      Facility: (...0000000000000................) FACILITY_SYSTEM
      Customer: (..0.............................) NOT Customer Defined
      Severity: (00..............................) STATUS_SEVERITY_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (...........................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 11 (0xB)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398382055525 (0x40014000065)
     Sig: Binary Large Object (16 Bytes)
  - RIoCtl:
     Size: 49 (0x31)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x200000002D, Volatile: 0xFFFFFFFF00000001
     InputOffset: 112 (0x70)
     InputCount: 788 (0x314)
     OutputOffset: 904 (0x388)
     OutputCount: 48 (0x30)
     Flags: 0 (0x0)
     Reserved2: 0 (0x0)
     InputData: Binary Large Object (788 Bytes)
     OutputPadding: Binary Large Object (4 Bytes)
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x9  Context=0x0  Hint=0x18  Cancels=0x0
  + Response:
- Lsad: LsarCreateTrustedDomainEx2 Response, TrustedDomainHandle: {D7D8A456-3215DF43-B4F9-49BB-AB0C-132500000000},
                                             Status = 0x00000000 - STATUS_SUCCESS
  + Pointer: Pointer To NULL
    TrustedDomainHandle: {D7D8A456-3215DF43-B4F9-49BB-AB0C-132500000000}
```

5.4.3.5.3 lsarpc: LsarCreateTrustedDomainEx2 (2-way trust)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =952
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 11
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 11 (0xB)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x100000008D, Volatile: 0xFFFFFFFF00000001
```

```
     InputOffset: 120 (0x78)
     InputCount: 832 (0x340)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x9  Opnum=0x3B  Context=0x0  Hint=0x328
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 832 (0x340)
     AuthLength: 0 (0x0)
     CallId: 9 (0x9)
     AllocHint: 808 (0x328)
     PContId: 0 (0x0)
     Opnum: 59 (0x3B)
   + StubData: 808 bytes
- Lsad: LsarCreateTrustedDomainEx2 Request, 0x1, DesiredAccess: 0x00000000,
                                                 PolicyHandle: {00000000-50255EFB-9E81-9846-BDB6-30CC9FCE95ED}
    PolicyHandle: {00000000-50255EFB-9E81-9846-BDB6-30CC9FCE95ED}
  - TrustedDomainInformation: 0x1
   + InformationHeader:
   - Information: 2008DOMAIN1.COM, 2008DOMAIN1, S-1-5-21-2074671935-2981103931-2886920652 Unknown SID
    + Name: 2008DOMAIN1.COM
    + FlatName: 2008DOMAIN1
    + Sid: S-1-5-21-2074671935-2981103931-2886920652 Unknown SID
  - AuthenticationInformation:
   + Header:
   - Data:
    + MaxCount: 632 Elements
      AuthBlob: Binary Large Object (632 Bytes)
    Pad: 0 Bytes
  - DesiredAccess: 0x00000000
   - SpecificRights: 0x0000
      TrustedQueryDomainName:  (...............0) Do NOT allow querying of the trusted domain name, attributes,
                                                  security identifier, or direction information
      TrustedQueryControllers: (..............0.) Do NOT allow querying the domain controller (DC) names in the trusted
                                                  domain
      TrustedSetControllers:   (.............0..) Do NOT allow setting of DC names in the trusted domain
      TrustedQueryPosix:       (............0...) Do NOT allow querying for the trusted domain's posix number
      TrustedSetPosix:         (...........0....) Do NOT allow setting of the trusted domain's posix number
      TrustedSetAuth:          (..........0.....) Do NOT allow setting of the trusted domain's authentication
                                                  information
      TrustedQueryAuth:        (.........0......) Do NOT allow querying of the trusted domain's authentication
                                                  information
      Reserved:                (000000000.......)
   + AccessRights: 0x0000

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =992
- Smb2: R  IOCTL (0xb), Mid = 11
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 11 (0xB)
     AsyncId: 33 (0x21)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl:
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x9  Context=0x0  Hint=0x18  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
```

```
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 9 (0x9)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
- Lsad: LsarCreateTrustedDomainEx2 Response, TrustedDomainHandle: {385333C5-9DBB4542-9D78-5CD2-808A-17D300000000},
                                                                  Status = 0x00000000 - STATUS_SUCCESS
  + Pointer: Pointer To NULL
    TrustedDomainHandle: {385333C5-9DBB4542-9D78-5CD2-808A-17D300000000}
```

5.4.3.6 lsarpc: LsarDeleteObject

5.4.3.6.1 lsarpc: LsarDeleteObject (Outgoing trust)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59361, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =164
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 8
    SMBIdentifier: SMB
```

```
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398046511157 (0x40000000035)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x5D, Volatile: 0xFFFFFFFF00000001
     InputOffset: 120 (0x78)
     InputCount: 44 (0x2C)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Opnum=0x22  Context=0x0  Hint=0x14
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 44 (0x2C)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 20 (0x14)
     PContId: 0 (0x0)
     Opnum: 34 (0x22)
   + StubData: 20 bytes
- Lsad: LsarDeleteObject Request, Object Handle: {00000000-F574515E-F4B3-E64E-A79E-16D0161549BC}
    ObjectHandle: {00000000-F574515E-F4B3-E64E-A79E-16D0161549BC}

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59361
+ Nbtss: SESSION MESSAGE, Length =73
- Smb2: R  Interim Response, Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x103, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (259) STATUS_PENDING
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     AsyncId: 21 (0x15)
     SessionId: 4398046511157 (0x40000000035)
     Sig: Binary Large Object (16 Bytes)
  - ErrorMessage: 0x1
     Size: 9 (0x9)
     Reserved: 0 (0x0)
     ByteCount: 0 (0x0)
     ErrorMessage: 93 (0x5D)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59361
+ Nbtss: SESSION MESSAGE, Length =208
- Smb2: R  IOCTL (0xb), Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     AsyncId: 21 (0x15)
     SessionId: 4398046511157 (0x40000000035)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl:
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Context=0x0  Hint=0x18  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
- Lsad: LsarDeleteObject Response, Status = 0x00000000 - STATUS_SUCCESS
    ObjectHandle: {00000000-00000000-0000-0000-0000-000000000000}
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.3.6.2 lsarpc: LsarDeleteObject (Incoming trust)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59579, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =164
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398113620045 (0x4000400004D)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x139, Volatile: 0xFFFFFFFF00000001
     InputOffset: 120 (0x78)
     InputCount: 44 (0x2C)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Opnum=0x22  Context=0x0  Hint=0x14
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 44 (0x2C)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 20 (0x14)
     PContId: 0 (0x0)
     Opnum: 34 (0x22)
   + StubData: 20 bytes
- Lsad: LsarDeleteObject Request, Object Handle: {00000000-2BD64DE0-996F-0C43-93EE-9A9675F5B5F3}
    ObjectHandle: {00000000-2BD64DE0-996F-0C43-93EE-9A9675F5B5F3}

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59579
+ Nbtss: SESSION MESSAGE, Length =73
- Smb2: R  Interim Response, Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x103, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (259) STATUS_PENDING
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     AsyncId: 21 (0x15)
     SessionId: 4398113620045 (0x4000400004D)
     Sig: Binary Large Object (16 Bytes)
  - ErrorMessage: 0x1
     Size: 9 (0x9)
     Reserved: 0 (0x0)
     ByteCount: 0 (0x0)
     ErrorMessage: 57 (0x39)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59579
+ Nbtss: SESSION MESSAGE, Length =208
- Smb2: R  IOCTL (0xb), Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     AsyncId: 21 (0x15)
     SessionId: 4398113620045 (0x4000400004D)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl:
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Context=0x0  Hint=0x18  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
- Lsad: LsarDeleteObject Response, Status = 0x00000000 - STATUS_SUCCESS
    ObjectHandle: {00000000-00000000-0000-0000-0000-000000000000}
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.3.6.3 lsarpc: LsarDeleteObject (2-Way trust)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59579, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =164
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398113620045 (0x4000400004D)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x139, Volatile: 0xFFFFFFFF00000001
```

```
     InputOffset: 120 (0x78)
     InputCount: 44 (0x2C)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Opnum=0x22  Context=0x0  Hint=0x14
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   + PackedDrep: 0x10
     FragLength: 44 (0x2C)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 20 (0x14)
     PContId: 0 (0x0)
     Opnum: 34 (0x22)
   + StubData: 20 bytes
- Lsad: LsarDeleteObject Request, Object Handle: {00000000-2BD64DE0-996F-0C43-93EE-9A9675F5B5F3}
    ObjectHandle: {00000000-2BD64DE0-996F-0C43-93EE-9A9675F5B5F3}

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =208
- Smb2: R  IOCTL (0xb), Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     AsyncId: 21 (0x15)
     SessionId: 4398113620045 (0x4000400004D)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl:
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Context=0x0  Hint=0x18  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   + PackedDrep: 0x10
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
- Lsad: LsarDeleteObject Response, Status = 0x00000000 - STATUS_SUCCESS
    ObjectHandle: {00000000-00000000-0000-0000-0000-000000000000}
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.3.7 lsarpc: LsarLookupNames4

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=49188, DstPort=49157
- RPC: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x1  Opnum=0x4D  Context=0x0  Hint=0x7C
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 192 (0xC0)
     AuthLength: 32 (0x20)
     CallId: 1 (0x1)
     AllocHint: 124 (0x7C)
     PContId: 0 (0x0)
     Opnum: 77 (0x4D)
   + StubData: 124 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (4 Bytes)
      AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 4 (0x4)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - NetlogonSignature:
        SignatureAlgorithm: 0x77 KERB_CHECKSUM_MD5_HMAC - The packet is signed using MD5-HMAC-64
        SealAlgorithm: 0x7A KERB_ETYPE_RC4_PLAIN_OLD - The packet is enrypted using RC4
        Pad: 65535 (0xFFFF)
        Flags: 0x0 No flags defined, must be 0
        SequenceNumber: Binary Large Object (8 Bytes)
        Checksum: Binary Large Object (8 Bytes)
        Confounder: Binary Large Object (8 Bytes)
```

```
- Lsat: LsarLookupNames4 Request, *Encrypted*
    EncryptedData: Binary Large Object (124 Bytes)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=49157, DstPort=49188, PayloadLen=128, Seq=2342297529 - 2342297657, Ack=2966781541,
Win=255 (scale factor 0x8) = 65280
- RPC: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x1  Context=0x0  Hint=0x34  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 128 (0x80)
     AuthLength: 32 (0x20)
     CallId: 1 (0x1)
     AllocHint: 52 (0x34)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 52 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (12 Bytes)
      AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 12 (0xC)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - NetlogonSignature:
        SignatureAlgorithm: 0x77 KERB_CHECKSUM_MD5_HMAC - The packet is signed using MD5-HMAC-64
        SealAlgorithm: 0x7A KERB_ETYPE_RC4_PLAIN_OLD - The packet is enrypted using RC4
        Pad: 65535 (0xFFFF)
        Flags: 0x0 No flags defined, must be 0
        SequenceNumber: Binary Large Object (8 Bytes)
        Checksum: Binary Large Object (8 Bytes)
        Confounder: Binary Large Object (8 Bytes)
- Lsat: LsarLookupNames4 Response, *Encrypted*
    EncryptedData: Binary Large Object (52 Bytes)
```

5.4.3.8 lsarpc: LsarSetTrustedDomainInfoByName

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59968, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =920
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000001, Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
```

```
   - Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
      Code:     (................0000000000000000) (0) STATUS_SUCCESS
      Facility: (...0000000000000................) FACILITY_SYSTEM
      Customer: (..0.............................) NOT Customer Defined
      Severity: (00..............................) STATUS_SEVERITY_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837781 (0x4000C000055)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x10000000A1, Volatile: 0xFFFFFFFF00000001
     InputOffset: 120 (0x78)
     InputCount: 800 (0x320)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Opnum=0x31  Context=0x0  Hint=0x308
```

```
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   + PfcFlags: 3 (0x3)
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 800 (0x320)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 776 (0x308)
     PContId: 0 (0x0)
     Opnum: 49 (0x31)
   + StubData: 776 bytes
- Lsad: LsarSetTrustedDomainInfoByName Request, TrustedDomainName: 2008DOMAIN1.COM,
                                                InfoClass: TrustedDomainFullInformationInternal (0x0A)
    PolicyHandle: {00000000-A420818E-848A-F049-8417-3E8EE1006084}
  + TrustedDomainName: 2008DOMAIN1.COM
    pad: 0 Bytes
    InformationClass: TrustedDomainFullInformationInternal (0x0A) It is used internally only
  - TrustedDomainInformation: TrustedDomainFullInformationInternal (0x0A)
   + padding1: 0 Bytes
     DomainInfoType: TrustedDomainFullInformationInternal (0x0A) It is used internally only
   + padding2: 2 Bytes
   - TrustedFullInfoInternal: 0x1
    - TrustedDomainInformation: 0x1
     + Pad: 0 Bytes
     + NameHeader:
     + FlatNameHeader:
     + PtrSid: Pointer To 0x0002000C
     + TrustDirection: 0x00000002
       TrustType: 0x00000002 - TRUST_TYPE_UPLEVEL - Trust is for Windows 2000 and Windows Server 2003
     - TrustAttributes: 0x00000004
      - TrustAttributes: 0x00000004
         NonTransitive:      (...............................0) Trust link allows transitivity
         UplevelOnly:        (..............................0.) Trust link is NOT valid only for uplevel clients
         QuarantinedDomain:  (.............................1..) Allow quarantined domains
         ForestTransitive:   (............................0...) Trust link does NOT contain forest trust information
         CrossOrganization:  (...........................0....) Trust is for a domain or forest that is part of the
                                                                enterprise
         WithinForest:       (..........................0.....) Trust is external to this forest
         TreatAsExternal:    (.........................0......) Trust is treated as internal for trust boundary
                                                                purposes
         Reserved:           (0000000000000000000000000.......)
    + PosixOffset:
    - AuthInformation:
     - AuthBlob:
      + padding: 0 Bytes
        AuthSize: 544 (0x220)
      + Pointer: Pointer To 0x00020010
    - Information: 2008DOMAIN1.COM, 2008DOMAIN1, S-1-5-21-2074671935-2981103931-2886920652 Unknown SID
     + Name: 2008DOMAIN1.COM
     + FlatName: 2008DOMAIN1
     + Sid: S-1-5-21-2074671935-2981103931-2886920652 Unknown SID
    - Data:
     + MaxCount: 544 Elements
       AuthBlob: Binary Large Object (544 Bytes)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59968
+ Nbtss: SESSION MESSAGE, Length =940
- Smb2: R  IOCTL (0xb), Mid = 8
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
```

```
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 8 (0x8)
     AsyncId: 21 (0x15)
     SessionId: 4398247837781 (0x4000C000055)
     Sig: Binary Large Object (16 Bytes)
  - RIoCtl:
     Size: 49 (0x31)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x10000000A1, Volatile: 0xFFFFFFFF00000001
     InputOffset: 112 (0x70)
     InputCount: 800 (0x320)
     OutputOffset: 912 (0x390)
     OutputCount: 28 (0x1C)
     Flags: 0 (0x0)
     Reserved2: 0 (0x0)
     InputData: Binary Large Object (800 Bytes)
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x3  Context=0x0  Hint=0x4  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 28 (0x1C)
     AuthLength: 0 (0x0)
     CallId: 3 (0x3)
     AllocHint: 4 (0x4)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 4 bytes
- Lsad: LsarSetTrustedDomainInfoByName Response, Status = 0x00000000 - STATUS_SUCCESS
    ReturnValue: 0x00000000 - STATUS_SUCCESS
```

5.4.3.9 lsarpc: LsarOpenTrustedDomainByName

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59968, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =220
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000005, Mid = 15
    SMBIdentifier: SMB
```

```
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 15 (0xF)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837781 (0x4000C000055)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x10000000A9, Volatile: 0xFFFFFFFF00000005
     InputOffset: 120 (0x78)
     InputCount: 100 (0x64)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x2  Opnum=0x37  Context=0x0  Hint=0x4C
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 100 (0x64)
     AuthLength: 0 (0x0)
     CallId: 2 (0x2)
     AllocHint: 76 (0x4C)
     PContId: 0 (0x0)
     Opnum: 55 (0x37)
   + StubData: 76 bytes
- Lsad: LsarOpenTrustedDomainByName Request, TrustedDomainName: 2008DOMAIN1.COM, DesiredAccess: 0x00010000,
                                             Policy Handle: {00000000-D52B0444-2498-E34E-93CD-2E4E881B5F73}
    PolicyHandle: {00000000-D52B0444-2498-E34E-93CD-2E4E881B5F73}
  + TrustedDomainName: 2008DOMAIN1.COM
  + pad: 2 Bytes
  - DesiredAccess: 0x00010000
   - SpecificRights: 0x0000
      TrustedQueryDomainName:  (...............0) Do NOT allow querying of the trusted domain name, attributes,
                                                  security identifier, or direction information
      TrustedQueryControllers: (..............0.) Do NOT allow querying the domain controller (DC) names in the trusted
                                                  domain
      TrustedSetControllers:   (.............0..) Do NOT allow setting of DC names in the trusted domain
      TrustedQueryPosix:       (............0...) Do NOT allow querying for the trusted domain's posix number
      TrustedSetPosix:         (...........0....) Do NOT allow setting of the trusted domain's posix number
      TrustedSetAuth:          (..........0.....) Do NOT allow setting of the trusted domain's authentication
                                                  information
      TrustedQueryAuth:        (.........0......) Do NOT allow querying of the trusted domain's authentication
                                                  information
      Reserved:                (000000000.......)
   - AccessRights: 0x0001
    - StandardRights: 0x01
       Delete:           (.......1) Right to delete the object
       ReadWriteExecute: (......0.) Right to read, write or execute the information in an object's SecurityDescriptor
                                    structure
       WriteDAC:         (.....0..) Right to change the DACL in the object's SecurityDescriptor structure
       WriteOwner:       (....0...) Right to change the owner member in the object's SecurityDescriptor structure
       Synchronize:      (...0....) Right to use the object for synchronization
       Reserved:         (000.....)
    + GenericRights: 0x00

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =264
- Smb2: R  IOCTL (0xb), Mid = 15
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 15 (0xF)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837781 (0x4000C000055)
     Sig: Binary Large Object (16 Bytes)
  - RIoCtl:
     Size: 49 (0x31)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x10000000A9, Volatile: 0xFFFFFFFF00000005
     InputOffset: 112 (0x70)
     InputCount: 100 (0x64)
     OutputOffset: 216 (0xD8)
     OutputCount: 48 (0x30)
     Flags: 0 (0x0)
     Reserved2: 0 (0x0)
     InputData: Binary Large Object (100 Bytes)
     OutputPadding: Binary Large Object (4 Bytes)
- msrpc: c/o Response: LSARpc {12345778-1234-ABCD-EF00-0123456789AB}  Call=0x2  Context=0x0  Hint=0x18  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   + PfcFlags: 3 (0x3)
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 48 (0x30)
     AuthLength: 0 (0x0)
     CallId: 2 (0x2)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
- Lsad: LsarOpenTrustedDomainByName Response, TrustedDomainHandle: {996BD153-ABA45347-84A6-36A0-319C-D88300000000},
Status = 0x00000000 - STATUS_SUCCESS
  + Pointer: Pointer To NULL
    TrustedDomainHandle: {996BD153-ABA45347-84A6-36A0-319C-D88300000000}
```

5.5 Netlogonr

5.5.1 Netlogonr: Session Control

5.5.1.1 Netlogonr: Session Control (SMB2)

5.5.1.1.1 SMB2: SMB2 CREATE NETLOGON

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =136
- Smb2: C  CREATE (0x5), Name=NETLOGON, Mid = 15
    SMBIdentifier: SMB
  + SMB2Header: C CREATE (0x5)
  - CCreate:
     Size: 57 (0x39)
   - SecurityFlags: 0x00000000
      DynamicTrakcing:  (.......0) Security tracking mode is not dynamic.
      EffectiveOnly:    (......0.) Not Only the enabled aspects of the client security context are available to the
                                   server.
      Reserved_bits2_7: (000000..) UnUsed
     RequestedOplockLevel: SMB2_OPLOCK_LEVEL_NONE - No oplock is granted.
     ImpersonationLevel: Impersonation - The server can impersonate the client's security context while acting on
                                   behalf of the client.
     SmbCreateFlags: 0 (0x0)
     Reserved: 0 (0x0)
   - DesiredAccess: 0x12019F
      ReadData:             (...............................1) Set FILE_READ_DATA (file & named pipe),
                                                               FILE_LIST_DIRECTORY (directory)
      WriteData:            (..............................1.) Set FILE_WRITE_DATA (file & named pipe), FILE_ADD_FILE
                                                               (directory
      AppendData:           (.............................1..) Set FILE_APPEND_DATA (file), FILE_ADD_SUBDIRECTORY
                                                               (directory), FILE_CREATE_PIPE_INSTANCE (named pipe)
      ReadEA:               (............................1...) Set FILE_READ_EA (file & directory)
      WriteEA:              (...........................1....) Set FILE_WRITE_EA (file & directory)
      Execute:              (..........................0.....) NOT Set FILE_EXECUTE (file), FILE_TRAVERSE (directory)
      Reserved_bit6:        (.........................0......) Reserved
      ReadAttributes:       (........................1.......) Set FILE_READ_ATTRIBUTES (all)
      WriteAttributes:      (.......................1........) Set FILE_WRITE_ATTRIBUTES (all)
      Reserved_bits9_15:    (................0000000.........) Reserved
      Delete:               (...............0................) NOT Set DELETE (the right to delete the object)
      ReadControl:          (..............1.................) Set READ_CONTROL (read the object's security descriptor
                                                               NOT including SACL)
      WriteDAC:             (.............0..................) NOT Set WRITE_DAC (modify the DACL in the object's
                                                               security descriptor)
      WriteOwner:           (............0...................) NOT Set WRITE_OWNER (change the owner in the object's
                                                               security descriptor)
      Synchronize:          (...........1....................) Set SYNCHRONIZE (use the object for synchronization)
      Reserved_bits21_23:   (........000.....................) Reserved
      AccessSystemSecurity: (.......0........................) NOT Set ACCESS_SYSTEM_SECURITY (get or set the SACL in
                                                               an object's security descriptor)
      MaximumAllowed:       (......0.........................) NOT Set MAXIMUM_ALLOWED (all access rights valid for the
                                                               caller)
      Reserved_bits26_27:   (....00..........................) Reserved
      GenericAll:           (...0............................) NOT Set GENERIC_ALL
      GenericExecute:       (..0.............................) NOT Set GENERIC_EXECUTE
      GenericWrite:         (.0..............................) NOT Set GENERIC_WRITE
      GenericRead:          (0...............................) NOT Set GENERIC_READ
   - FileAttributes:
    - FSCCFileAttribute: 0 (0x0)
       ReadOnly:           (...............................0) Read/Write
       Hidden:             (..............................0.) Not Hidden
       System:             (.............................0..) Not System
       Reserved_bits3:     (............................0...) Reserved
       Directory:          (...........................0....) File
       Archive:            (..........................0.....) Not Archive
       Device:             (.........................0......) Not Device
       Normal:             (........................0.......) Not Normal
       Temporary:          (.......................0........) Permanent
       Sparse:             (......................0.........) Not Sparse
       Reparse:            (.....................0..........) Not Reparse Point
       Compressed:         (....................0...........) Uncompressed
       Offline:            (...................0............) Online
       NotIndexed:         (..................0.............) Content indexed
       Encrypted:          (.................0..............) Unencrypted
       Reserved_bits15_31: (00000000000000000...............) Reserved
     ShareAccess: Shared for Read/Write (0x00000003)
     CreateDisposition: Opened (0x00000001)
   - CreateOptions: 0x400040
      FILE_DIRECTORY_FILE:            (...............................0) non-directory
      FILE_WRITE_THROUGH:             (..............................0.) non-write through
      FILE_SEQUENTIAL_ONLY:           (.............................0..) non-sequentially writing allowed
      FILE_NO_INTERMEDIATE_BUFFERING: (............................0...) intermediate buffering allowed
      Reserved_bits4_5:               (..........................00....) NOT ignored by the server
      FILE_NON_DIRECTORY_FILE:        (.........................1......) NOT be a directory file or this call MUST be
                                                                         failed
      Reserved_bits7_8:               (.......................00.......) Reserved
      FILE_NO_EA_KNOWLEDGE:           (......................0.........) no EA knowledge bit is not set
      Reserved_bits10:                (.....................0..........) Reserved
      FILE_RANDOM_ACCESS:             (....................0...........) accesses to the file can NOT be random
      FILE_DELETE_ON_CLOSE:           (...................0............) the DesiredAccess field MUST NOT include the
                                                                         DELETE flag
      Reserved_bits13:                (..................0.............) Reserved
      FILE_OPEN_FOR_BACKUP_INTENT:    (.................0..............) the file is not being opened for backup intent
      FILE_NO_COMPRESSION:            (................0...............) the file can be compressed
      Reserved_bits16_20:             (............0000................) Reserved
      FILE_RESERVE_OPFILTER:          (...........0....................) Reserved. The client SHOULD set this bit to 0
      FILE_OPEN_REPARSE_POINT:        (..........0.....................) open the reparse the target that the reparse
                                                                         point references
      FILE_OPEN_NO_RECALL:            (.........1......................) the file should not be recalled from tertiary
                                                                         storage such as tape
      FILE_OPEN_FOR_FREE_SPACE_QUERY: (........0.......................) No file open to query for free space
      Reserved_bits23_31:             (00000000........................) Reserved
     NameOffset: 120 (0x78)
     NameLength: 16 (0x10)
     CreateContextsOffset: 0 (0x0)
     CreateContextsLength: 0 (0x0)
     Name: NETLOGON

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =152
- Smb2: R  CREATE (0x5), FID=0xFFFFFFFF00000005, Mid = 15
```

```
  SMBIdentifier: SMB
- SMB2Header: R CREATE (0x5)
   Size: 64 (0x40)
   Epoch: 0 (0x0)
 + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
   Command: CREATE (0x5)
   Credits: 1 (0x1)
 - Flags: 0x9
    ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
    AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
    Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
    Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
    Reserved4_27:  (....000000000000000000000000....)
    DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
    Reserved29_31: (000.............................)
   NextCommand: 0 (0x0)
   MessageId: 15 (0xF)
   ProcessId: 65279 (0xFEFF)
   TreeId: 1 (0x1)
   SessionId: 4398247837773 (0x4000C00004D)
   Sig: Binary Large Object (16 Bytes)
- RCreate: 0x1
   Size: 89 (0x59)
   OplockLevel: SMB2_OPLOCK_LEVEL_NONE - No oplock is granted.
   Reserved: 0 (0x0)
   CreateAction: Opened (0x00000001)
   CreationTime: No Time Specified (0)
   LastAccessTime: No Time Specified (0)
   LastWriteTime: No Time Specified (0)
   LastChangeTime: No Time Specified (0)
   AllocationSize: 4096 (0x1000)
   EndOfFile: 0 (0x0)
 - FileAttributes:
  - FSCCFileAttribute: 128 (0x80)
     ReadOnly:           (...............................0) Read/Write
```

```
       Hidden:             (..............................0.) Not Hidden
       System:             (.............................0..) Not System
       Reserved_bits3:     (............................0...) Reserved
       Directory:          (...........................0....) File
       Archive:            (..........................0.....) Not Archive
       Device:             (.........................0......) Not Device
       Normal:             (........................1.......) Normal
       Temporary:          (.......................0........) Permanent
       Sparse:             (......................0.........) Not Sparse
       Reparse:            (.....................0..........) Not Reparse Point
       Compressed:         (....................0...........) Uncompressed
       Offline:            (...................0............) Online
       NotIndexed:         (..................0.............) Content indexed
       Encrypted:          (.................0..............) Unencrypted
       Reserved_bits15_31: (00000000000000000...............) Reserved
     Reserved2: 4980820 (0x4C0054)
   + Fid: Persistent: 0x1000000091, Volatile: 0xFFFFFFFF00000005
     CreateContextsOffset: 0 (0x0)
     CreateContextsLength: 0 (0x0)
```

5.5.1.1.2 RPC: Bind to Netlogonr ([C706])

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =228
- Smb2: C  WRITE (0x9), FID=0xFFFFFFFF00000005, 0x74 bytes at offset 0 (0x0), Mid = 16
    SMBIdentifier: SMB
  - SMB2Header: C WRITE (0x9)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: WRITE (0x9)
     Credits: 27 (0x1B)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 16 (0x10)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CWrite: 0x1
     Size: 49 (0x31)
     DataOffset: 112 (0x70)
     DataLength: 116 (0x74)
     Offset: 0 (0x0)
   + Fid: Persistent: 0x1000000091, Volatile: 0xFFFFFFFF00000005
     Channel: 0 (0x0)
     RemainingBytes: 0 (0x0)
     WriteChannelInfoOffset: 0 (0x0)
     WriteChannelInfoLength: 0 (0x0)
     Flags: 0 (0x0)
- msrpc: c/o Bind:  UUID{12345678-1234-ABCD-EF00-01234567CFFB} Logon  Call=0x1  Assoc Grp=0x0  Xmit=0x10B8  Recv=0x10B8
  - Bind: {12345678-1234-ABCD-EF00-01234567CFFB} Logon
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0B - Bind
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 116 (0x74)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 4280 (0x10B8)
     MaxRecvFrag: 4280 (0x10B8)
     AssocGroupId: 0 (0x0)
   - PContextElem:
      NContextElem: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PContElem: 0x1
       PContId: 0 (0x0)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {12345678-1234-ABCD-EF00-01234567CFFB} Logon
     + TransferSyntaxes: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PContElem: 0x1
       PContId: 1 (0x1)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {12345678-1234-ABCD-EF00-01234567CFFB} Logon
     + TransferSyntaxes: {6CB71C2C-9812-4540-0300000000000000} BTFN - Security Context Multiplexing Supported
```

```
     AuthVerifier: 0x1

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =80
- Smb2: R  WRITE (0x9), 0x74 bytes written, Mid = 16
    SMBIdentifier: SMB
  - SMB2Header: R WRITE (0x9)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: WRITE (0x9)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 16 (0x10)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - RWrite: 0x1
     Size: 17 (0x11)
     Reserved: 0 (0x0)
     DataLength: 116 (0x74)
     Remaining: 0 (0x0)
     WriteChannelInfoOffset: 0 (0x0)
     WriteChannelInfoLength: 0 (0x0)
```

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =113
- Smb2: C  READ (0x8), FID=0xFFFFFFFF00000005, 0x400 bytes from offset 0 (0x0), Mid = 17
    SMBIdentifier: SMB
  - SMB2Header: C READ (0x8)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: READ (0x8)
     Credits: 27 (0x1B)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 17 (0x11)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CRead: 0x1
     Size: 49 (0x31)
     Padding: 80 (0x50)
     Reserved: 0 (0x0)
     DataLength: 1024 (0x400)
     Offset: 0 (0x0)
   + Fid: Persistent: 0x1000000091, Volatile: 0xFFFFFFFF00000005
     MinimumCount: 0 (0x0)
     Channel: 0 (0x0)
     RemainingBytes: 0 (0x0)
     ReadChannelInfoOffset: 0 (0x0)
     ReadChannelInfoLength: 0 (0x0)
     Buffer: 0 (0x0)


+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =172
- Smb2: R  READ (0x8), 0x5c bytes read, Mid = 17
    SMBIdentifier: SMB
  - SMB2Header: R READ (0x8)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: READ (0x8)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 17 (0x11)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - RRead: 0x1
     Size: 17 (0x11)
     DataOffset: 80 (0x50)
     Reserved: 0 (0x0)
     DataLength: 92 (0x5C)
     DataRemaining: 0 (0x0)
     Reserved2: 0 (0x0)
- msrpc: c/o Bind Ack:  Call=0x1  Assoc Grp=0xC6DC  Xmit=0x10B8  Recv=0x10B8
  - BindAck:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0C - Bind Ack
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 92 (0x5C)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 4280 (0x10B8)
     MaxRecvFrag: 4280 (0x10B8)
     AssocGroupId: 50908 (0xC6DC)
   - SecAddr: \pipe\lsass
      Length: 12 (0xC)
      PortSpec: \pipe\lsass
   + Pad2: 0x1
   - PResultList:
      NResults: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
```

```
    - PResults: Acceptance, Reason=n/a
       Result: Acceptance
       Reason: n/a
     + TransferSyntax: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PResults: Negotiate Ack, Security Context Multiplexing Supported
       Result: Negotiate Ack
     + bitmask: Security Context Multiplexing Supported
     + TransferSyntax: {00000000-0000-0000-0000-000000000000} unknown
     AuthVerifier:
```

5.5.1.1.3 SMB2: SMB2 CLOSE

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =88
- Smb2: C  CLOSE (0x6), FID=0xFFFFFFFF00000009, Mid = 24
    SMBIdentifier: SMB
  - SMB2Header: C CLOSE (0x6)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: CLOSE (0x6)
     Credits: 27 (0x1B)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 24 (0x18)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CClose: 0x1
     Size: 24 (0x18)
   - Flags: Not Contain additional fields in response packet
      POSTQUERY:         (...............0) NOT use the values returned in the response
      Reserved_bits1_15: (000000000000000.) Reserved
     Reserved: 0 (0x0)
   + Fid: Persistent: 0x1000000095, Volatile: 0xFFFFFFFF00000009

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =124
- Smb2: R  CLOSE (0x6), Mid = 25
    SMBIdentifier: SMB
  - SMB2Header: R CLOSE (0x6)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: CLOSE (0x6)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 25 (0x19)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - RClose:
     Size: 60 (0x3C)
     Flags: 0 (0x0)
     Reserved: 0 (0x0)
     CreationTime: No Time Specified (0)
     LastAccessTime: No Time Specified (0)
     LastWriteTime: No Time Specified (0)
     LastChangeTime: No Time Specified (0)
     AllocationSize: 0 (0x0)
     EndOfFile: 0 (0x0)
   - FileAttributes:
    - FSCCFileAttribute: 0 (0x0)
       ReadOnly:           (...............................0) Read/Write
       Hidden:             (..............................0.) Not Hidden
       System:             (.............................0..) Not System
       Reserved_bits3:     (............................0...) Reserved
       Directory:          (...........................0....) File
       Archive:            (..........................0.....) Not Archive
       Device:             (.........................0......) Not Device
       Normal:             (........................0.......) Not Normal
       Temporary:          (.......................0........) Permanent
       Sparse:             (......................0.........) Not Sparse
       Reparse:            (.....................0..........) Not Reparse Point
       Compressed:         (....................0...........) Uncompressed
       Offline:            (...................0............) Online
       NotIndexed:         (..................0.............) Content indexed
       Encrypted:          (.................0..............) Unencrypted
       Reserved_bits15_31: (00000000000000000...............) Reserved
```

5.5.1.1.4 SMB2: SMB2 TREE_DISCONNECT

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: C  TREE DISCONNECT (0x4), TID=0x1, Mid = 26
    SMBIdentifier: SMB
  - SMB2Header: C TREE DISCONNECT (0x4)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: TREE DISCONNECT (0x4)
     Credits: 2 (0x2)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 26 (0x1A)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CTreeDisconnect: 0x1
     Size: 4 (0x4)
     Reserved: 0 (0x0)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: R  TREE DISCONNECT (0x4), Mid = 26
    SMBIdentifier: SMB
  - SMB2Header: R TREE DISCONNECT (0x4)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: TREE DISCONNECT (0x4)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 26 (0x1A)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - RTreeDisconnect:
     Size: 4 (0x4)
     Reserved: 0 (0x0)
```

5.5.1.1.5 SMB2: SMB2 LOGOFF

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: C  LOGOFF (0x2), Mid = 27
    SMBIdentifier: SMB
  - SMB2Header: C LOGOFF (0x2)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: LOGOFF (0x2)
     Credits: 1 (0x1)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 27 (0x1B)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CLogoff:
     Size: 4 (0x4)
     Reserved: 0 (0x0)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =68
- Smb2: R  LOGOFF (0x2), Mid = 27
    SMBIdentifier: SMB
  - SMB2Header: R LOGOFF (0x2)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: LOGOFF (0x2)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 27 (0x1B)
     ProcessId: 65279 (0xFEFF)
     TreeId: 0 (0x0)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - RLogoff:
     Size: 4 (0x4)
     Reserved: 0 (0x0)
```

5.5.1.2 Netlogonr: Session Control (EPT)

5.5.1.2.1 RPC: c/o Bind (EPT) ([C706])

```
+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=54491, DstPort=DCE endpoint resolution(135)
- RPC: c/o Bind:  UUID{E1AF8308-5D1F-11C9-91A4-08002B14A0FA} EPT  Call=0x1  Assoc Grp=0x0  Xmit=0x16D0  Recv=0x16D0
  - Bind: {E1AF8308-5D1F-11C9-91A4-08002B14A0FA} EPT
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0B - Bind
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 116 (0x74)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 0 (0x0)
   - PContextElem:
      NContextElem: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PContElem: 0x1
       PContId: 0 (0x0)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {E1AF8308-5D1F-11C9-91A4-08002B14A0FA} EPT
     + TransferSyntaxes: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PContElem: 0x1
       PContId: 1 (0x1)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {E1AF8308-5D1F-11C9-91A4-08002B14A0FA} EPT
     + TransferSyntaxes: {6CB71C2C-9812-4540-0300000000000000} BTFN - Security Context Multiplexing Supported
     AuthVerifier: 0x1

+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=DCE endpoint resolution(135), DstPort=54491
- RPC: c/o Bind Ack:  Call=0x1  Assoc Grp=0xD7E2  Xmit=0x16D0  Recv=0x16D0
  - BindAck:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0C - Bind Ack
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 84 (0x54)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 55266 (0xD7E2)
   - SecAddr: 135
      Length: 4 (0x4)
      PortSpec: 135
   + Pad2: 0x1
   - PResultList:
      NResults: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PResults: Acceptance, Reason=n/a
       Result: Acceptance
       Reason: n/a
     + TransferSyntax: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PResults: Negotiate Ack, Security Context Multiplexing Supported
       Result: Negotiate Ack
     - bitmask: Security Context Multiplexing Supported
        BitMask: 3 (0x3)
        Unused: 0 (0x0)
     + TransferSyntax: {00000000-0000-0000-0000-000000000000} unknown
     AuthVerifier:
```

5.5.1.2.2 Epm: Request: ept_map (Netlogonr) ([C706])

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=54491, DstPort=DCE endpoint resolution(135)
- RPC: c/o Request: EPT {E1AF8308-5D1F-11C9-91A4-08002B14A0FA}  Call=0x1  Opnum=0x3  Context=0x0  Hint=0x84
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 156 (0x9C)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 132 (0x84)
     PContId: 0 (0x0)
     Opnum: 3 (0x3)
   + StubData: 132 bytes
- Epm: Request: ept_map: NDR, Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0, RPC v5, 0.0.0.0:135 (0x87)
                        [DCE endpoint resolution(135)]
  + Object: {00000000-0000-0000-0000-000000000000}
  - MapTower: Pointer To 0x00000002
   + align: 0 Bytes
   + TwrTPointer: Pointer To 0x00000002
   - Tower: NDR, Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0, RPC v5, 0.0.0.0:135 (0x87)
```

```
       [DCE endpoint resolution(135)]
+ Length: 75 Elements
  TowerLength: 75 (0x4B)
- Floors: NDR, Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0, RPC v5, 0.0.0.0:135 (0x87)
          [DCE endpoint resolution(135)]
   FloorCount: 5 (0x5)
 - InterfaceIdentifier: Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0
    LHSBytecount: 19 (0x13)
    InterfaceIdent: UUID: 13 (0xD)
  + InterfaceUuid: {12345678-1234-ABCD-EF00-01234567CFFB}
    MajorVersion: 1 (0x1)
    RHSBytecount: 2 (0x2)
    MinorVersion: 0 (0x0)
 - DataRepresentation: UUID NDR {8A885D04-1CEB-11C9-9FE8-08002B104860} v2.0
    LHSBytecount: 19 (0x13)
    DrepIdentifier: UUID: 13 (0xD)
  + DataRepUuid: {8A885D04-1CEB-11C9-9FE8-08002B104860}
    MajorVersion: 2 (0x2)
    RHSBytecount: 2 (0x2)
    MinorVersion: 0 (0x0)
 - ProtocolIdentifier: RPC Connection-oriented v5.0
    LHSBytecount: 1 (0x1)
    ProtIdentifier: RPC Connection-oriented v5: 11 (0xB)
    RHSBytecount: 2 (0x2)
    VersionMinor: 0 (0x0)
 - PortAddr: port: 135 (0x87) [DCE endpoint resolution(135)], type: DOD TCP port
    LHSBytecount: 1 (0x1)
    PortIdentifier: DOD TCP port: 7 (0x7)
    RHSBytecount: 2 (0x2)
    IpPort: 135 (0x87) [DCE endpoint resolution(135)]
 - HostAddr: address: 0.0.0.0, type: DOD IP v4 big-endian
    LHSBytecount: 1 (0x1)
    HostAddressId: DOD IP v4 big-endian: 9 (0x9)
    RHSBytecount: 4 (0x4)
    Ip4addr: 0.0.0.0
    + Align: 1 Bytes
  - EntryHandle: 0x1
     ContextType: 0 (0x0)
     ContextUuid: {00000000-0000-0000-0000-000000000000}
    MaxTowers: 4 (0x4)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=DCE endpoint resolution(135), DstPort=54491
- RPC: c/o Response: EPT {E1AF8308-5D1F-11C9-91A4-08002B14A0FA}  Call=0x1  Context=0x0  Hint=0xD8  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 240 (0xF0)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 216 (0xD8)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 216 bytes
```

```
- Epm: Response: ept_map: NDR, Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0, RPC v510.237.0.22, 10.237.0.22:49155
(0xC003) [49155]
  - EntryHandle: 
     ContextType: 0 (0x0)
     ContextUuid: {00000000-0000-0000-0000-000000000000}
    NumTowers: 2 (0x2)
  - Towers: 2 Elements
   + ArrayInfo: 2 Elements
   + TwrPtr: Pointer To 0x00000003
   + TwrPtr: Pointer To 0x00000004
   - Tower: NDR, Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0, RPC v5, 10.237.0.22:49156 (0xC004) [49156]
    + Length: 75 Elements
      TowerLength: 75 (0x4B)
    - Floors: NDR, Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0, RPC v5, 10.237.0.22:49156 (0xC004) [49156]
       FloorCount: 5 (0x5)
     - InterfaceIdentifier: Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0
        LHSBytecount: 19 (0x13)
        InterfaceIdent: UUID: 13 (0xD)
      + InterfaceUuid: {12345678-1234-ABCD-EF00-01234567CFFB}
        MajorVersion: 1 (0x1)
        RHSBytecount: 2 (0x2)
        MinorVersion: 0 (0x0)
     - DataRepresentation: UUID NDR {8A885D04-1CEB-11C9-9FE8-08002B104860} v2.0
        LHSBytecount: 19 (0x13)
        DrepIdentifier: UUID: 13 (0xD)
      + DataRepUuid: {8A885D04-1CEB-11C9-9FE8-08002B104860}
        MajorVersion: 2 (0x2)
        RHSBytecount: 2 (0x2)
        MinorVersion: 0 (0x0)
     - ProtocolIdentifier: RPC Connection-oriented v5.0
        LHSBytecount: 1 (0x1)
        ProtIdentifier: RPC Connection-oriented v5: 11 (0xB)
        RHSBytecount: 2 (0x2)
        VersionMinor: 0 (0x0)
     - PortAddr: port: 49156 (0xC004) [49156], type: DOD TCP port
        LHSBytecount: 1 (0x1)
        PortIdentifier: DOD TCP port: 7 (0x7)
        RHSBytecount: 2 (0x2)
        IpPort: 49156 (0xC004) [49156]
     - HostAddr: address: 10.237.0.22, type: DOD IP v4 big-endian
        LHSBytecount: 1 (0x1)
        HostAddressId: DOD IP v4 big-endian: 9 (0x9)
        RHSBytecount: 4 (0x4)
        Ip4addr: 10.237.0.22
    + Align: 1 Bytes
   - Tower: NDR, Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0, RPC v510.237.0.22, 10.237.0.22:49155
                       (0xC003) [49155]
    + Length: 75 Elements
      TowerLength: 75 (0x4B)
    - Floors: NDR, Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0, RPC v510.237.0.22, 10.237.0.22:49155
                         (0xC003) [49155]
       FloorCount: 5 (0x5)
     - InterfaceIdentifier: Logon {12345678-1234-ABCD-EF00-01234567CFFB} v1.0
        LHSBytecount: 19 (0x13)
        InterfaceIdent: UUID: 13 (0xD)
      + InterfaceUuid: {12345678-1234-ABCD-EF00-01234567CFFB}
        MajorVersion: 1 (0x1)
        RHSBytecount: 2 (0x2)
        MinorVersion: 0 (0x0)
     - DataRepresentation: UUID NDR {8A885D04-1CEB-11C9-9FE8-08002B104860} v2.0
        LHSBytecount: 19 (0x13)
        DrepIdentifier: UUID: 13 (0xD)
      + DataRepUuid: {8A885D04-1CEB-11C9-9FE8-08002B104860}
        MajorVersion: 2 (0x2)
        RHSBytecount: 2 (0x2)
        MinorVersion: 0 (0x0)
     - ProtocolIdentifier: RPC Connection-oriented v5.0
        LHSBytecount: 1 (0x1)
        ProtIdentifier: RPC Connection-oriented v5: 11 (0xB)
        RHSBytecount: 2 (0x2)
```

```
        VersionMinor: 0 (0x0)
     - PortAddr: port: 49155 (0xC003) [49155], type: DOD TCP port
        LHSBytecount: 1 (0x1)
        PortIdentifier: DOD TCP port: 7 (0x7)
        RHSBytecount: 2 (0x2)
        IpPort: 49155 (0xC003) [49155]
     - HostAddr: address: 10.237.0.22, type: DOD IP v4 big-endian
        LHSBytecount: 1 (0x1)
        HostAddressId: DOD IP v4 big-endian: 9 (0x9)
        RHSBytecount: 4 (0x4)
        Ip4addr: 10.237.0.22
    + Align: 1 Bytes
  + Status: 0x00000000 - EP_S_SUCCESS
```

5.5.1.2.3 RPC: Bind to Netlogonr ([C706])

```
+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=54492, DstPort=49156
- RPC: c/o Bind:  UUID{12345678-1234-ABCD-EF00-01234567CFFB} Logon  Call=0x1  Assoc Grp=0x0  Xmit=0x16D0  Recv=0x16D0
  - Bind: {12345678-1234-ABCD-EF00-01234567CFFB} Logon
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0B - Bind
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 116 (0x74)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 0 (0x0)
   - PContextElem:
      NContextElem: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PContElem: 0x1
       PContId: 0 (0x0)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {12345678-1234-ABCD-EF00-01234567CFFB} Logon
     + TransferSyntaxes: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PContElem: 0x1
       PContId: 1 (0x1)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {12345678-1234-ABCD-EF00-01234567CFFB} Logon
     + TransferSyntaxes: {6CB71C2C-9812-4540-0300000000000000} BTFN - Security Context Multiplexing Supported
     AuthVerifier: 0x1

+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=54492
- RPC: c/o Bind Ack:  Call=0x1  Assoc Grp=0x9CD3  Xmit=0x16D0  Recv=0x16D0
```

```
  - BindAck:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0C - Bind Ack
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 84 (0x54)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 40147 (0x9CD3)
   - SecAddr: 49156
      Length: 6 (0x6)
      PortSpec: 49156
     Pad2: 0x1
   - PResultList:
      NResults: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PResults: Acceptance, Reason=n/a
       Result: Acceptance
       Reason: n/a
     + TransferSyntax: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PResults: Negotiate Ack, Security Context Multiplexing Supported
       Result: Negotiate Ack
     - bitmask: Security Context Multiplexing Supported
        BitMask: 3 (0x3)
        Unused: 0 (0x0)
     + TransferSyntax: {00000000-0000-0000-0000-000000000000} unknown
     AuthVerifier:
```

5.5.1.2.4 RPC: Alter Context (security context) ([C706])

```
+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=54492, DstPort=49156
- RPC: c/o Alter Cont:  UUID{12345678-1234-ABCD-EF00-01234567CFFB} Logon  Call=0x3
  - AlterContext:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0E - Alter Context
   - PfcFlags: 7 (0x7)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....1.. PFC_SUPPORT_HEADER_SIGN - SET, Header Sign was supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 148 (0x94)
     AuthLength: 68 (0x44)
     CallId: 3 (0x3)
     MaxXmitFrag: ignored
     MaxRecvFrag: ignored
     AssocGroupId: ignored
   - PContextElem:
      NContextElem: 1 (0x1)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PContElem: 0x1
       PContId: 0 (0x0)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {12345678-1234-ABCD-EF00-01234567CFFB} Logon
     + TransferSyntaxes: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
   - AuthVerifier: 0x1
      AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                 privacy (encryption) of stub call arguments only. All run-time and lower-layer headers are still
                 transmitted in clear text.
      AuthPadLength: 0 (0x0)
      AuthReserved: 0 (0x0)
      AuthContextId: 1 (0x1)
    - AuthValue:
     - NetlogonMessage:
        MessageType: 0x0, Negotiate Message
      - Flags: 23 (0x17)
         NLAuthNetbiosDomainName:        (...............................1) Buffer contains NetBIOS domain name as an
                                                                            OEM string
         NLAuthNetbiosComputerName:      (..............................1.) Buffer contains NetBIOS computer name as an
                                                                            OEM string
```

```
         NLAuthDNSDomainName:            (.............................1..) Buffer contains DNS domain name as UTF-8
                                                                            string
         NLAuthDNSHostName:              (............................0...) Buffer does not contain DNS host name
         NLAuthUTF8NetbiosComputerName:  (...........................1....) Buffer contains computer name as UTF-8
                                                                            string
        NetBiosDomainName: 2008DOMAIN1
        NetBiosComputerName: 2008DOMAIN2DC1
        DNSDomainName: 2008DOMAIN1.COM
        UTF8NetBiosComputerName: 2008DOMAIN2DC1

+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=54492- RPC: c/o Alter Cont Resp:  Call=0x3  Assoc Grp=0x9CD3  Xmit=0x16D0
Recv=0x16D0
  - AlterContextResponse:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0F - Alter Context Resp
   - PfcFlags: 7 (0x7)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....1.. PFC_SUPPORT_HEADER_SIGN - SET, Header Sign was supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 76 (0x4C)
     AuthLength: 12 (0xC)
     CallId: 3 (0x3)
     MaxXmitFrag: ignored
     MaxRecvFrag: ignored
     AssocGroupId: ignored
   - SecAddr:
      Length: 0 (0x0)
   + Pad2: 0x1
   - PResultList:
      NResults: 1 (0x1)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PResults: Acceptance, Reason=n/a
       Result: Acceptance
       Reason: n/a
     + TransferSyntax: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
   - AuthVerifier:
      AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
privacy (encryption) of stub call arguments only. All run-time and lower-layer headers are still transmitted in clear
text.
      AuthPadLength: 0 (0x0)
      AuthReserved: 0 (0x0)
      AuthContextId: 1 (0x1)
    - AuthValue:
     - NetlogonMessage:
        MessageType: 0x1, Negotiate Response Message
      - Flags: 0 (0x0)
         NLAuthNetbiosDomainName:        (..............................0) Buffer does not contain NetBIOS domain name
         NLAuthNetbiosComputerName:      (.............................0.) Buffer does not contain NetBIOS computer
                                                                           name
         NLAuthDNSDomainName:            (............................0..) Buffer does not contain DNS domain name
         NLAuthDNSHostName:              (...........................0...) Buffer does not contain DNS host name
         NLAuthUTF8NetbiosComputerName:  (..........................0....) Buffer does not contain computer name
        Buffer: Binary Large Object (4 Bytes)
```

5.5.2 Netlogonr: Procedure calls

5.5.2.1 Netlogonr: DsrEnumerateDomainTrusts

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =228
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000005, Mid = 18
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 27 (0x1B)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 18 (0x12)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl: 
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x1000000091, Volatile: 0xFFFFFFFF00000005
     InputOffset: 120 (0x78)
     InputCount: 108 (0x6C)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x1  Opnum=0x28  Context=0x0  Hint=0x54
  - Request: 
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 108 (0x6C)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 84 (0x54)
     PContId: 0 (0x0)
     Opnum: 40 (0x28)
   + StubData: 84 bytes
- Netlogonr: DsrEnumerateDomainTrusts Request, ServerName: 2008DOMAIN2DC1.2008DOMAIN2.COM, Flags: 0x00000023
  - ServerName: 2008DOMAIN2DC1.2008DOMAIN2.COM
   + Pointer: Pointer To 0x00020000
   + stringValue: 2008DOMAIN2DC1.2008DOMAIN2.COM
  + pad: 2 Bytes
  - Flags: 0x00000023
     DSDomainInForest:        (...............................1) Domain is a member of a forest
     DSDomainDirectOutbound:  (..............................1.) Domain is directly trusted by the current domain
     DSDomainTreeRoot:        (.............................0..) Domain is NOT the root of a forest
     DSDomainPrimary:         (............................0...) Domain is NOT the primary domain of the queried server
     DSDomainNativeMode:      (...........................0....) Primary domain is NOT running in native mode
     DSDomainDirectInbound:   (..........................1.....) Domain directly trusts the current domain
     unused:                  (.........................0......)
     bit24:                   (........................0.......) Domain is NOT MIT Kerberos realm, trusted with RC4
                                                                 encryption
     bit23:                   (.......................0........) Kerberos does NOT use AES keys to encrypt Kerberos
                                                                 TGTs
     Reserved:                (00000000000000000000000.........)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =568
- Smb2: R  IOCTL (0xb), Mid = 18
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0x9
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 18 (0x12)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl:
- msrpc: c/o Response: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x1  Context=0x0  Hint=0x140  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 344 (0x158)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 320 (0x140)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 320 bytes
- Netlogonr: DsrEnumerateDomainTrusts Response,ERROR_SUCCESS
  - Domains: DomainCount: 2
   + pad: 0 Bytes
     DomainCount: 2 (0x2)
   + Pointer: Pointer To 0x00020000
   - MaxCount: 0x2
      MaxCount: 2
   + Domain: 0x1
   + Domain: 0x2
   - DomainData: 0x1 2008DOMAIN1
    + NetbiosDomainName: 2008DOMAIN1
    + DnsDomainName: 2008DOMAIN1.COM
    + DomainSID: S-1-5-21-2074671935-2981103931-2886920652 Unknown SID
   - DomainData: 0x2 2008DOMAIN2
    + NetbiosDomainName: 2008DOMAIN2
    + DnsDomainName: 2008DOMAIN2.COM
    + DomainSID: S-1-5-21-3252065517-4011377361-1377730089 Unknown SID
    pad: 0 Bytes
    ReturnValue: 0x00000000 - ERROR_SUCCESS - The operation completed successfully.
```

5.5.2.2 Netlogonr: NetrLogonControl2Ex

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59952, DstPort=Microsoft-DS(445)
+ Nbtss: SESSION MESSAGE, Length =284
- Smb2: C  IOCTL (0xb), FID=0xFFFFFFFF00000009, Mid = 23
    SMBIdentifier: SMB
  - SMB2Header: C IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 27 (0x1B)
   - Flags: 0x8
      ServerToRedir: (...............................0) Client to Server (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................0.) Command is not asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 23 (0x17)
     ProcessId: 65279 (0xFEFF)
     TreeId: 1 (0x1)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - CIoCtl:
     Size: 57 (0x39)
     Reserved: 0 (0x0)
     CtlCode: FSCTL_PIPE_TRANSCEIVE(0x11c017)
   + Fid: Persistent: 0x1000000095, Volatile: 0xFFFFFFFF00000009
     InputOffset: 120 (0x78)
     InputCount: 164 (0xA4)
     MaxInputResponse: 0 (0x0)
     OutputOffset: 120 (0x78)
     OutputCount: 0 (0x0)
     MaxOutputResponse: 1024 (0x400)
     Flags: (00000000000000000000000000000001) FSCTL request
     Reserved2: 0 (0x0)
- msrpc: c/o Request: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x1  Opnum=0x12  Context=0x0  Hint=0x8C
Unparsed RPC payload
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 164 (0xA4)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 140 (0x8C)
     PContId: 0 (0x0)
     Opnum: 18 (0x12)
   + StubData: 140 bytes
- Netlogonr: NetrLogonControl2Ex Request, ServerName: 2008DOMAIN2DC1.2008DOMAIN2.COM,
             FunctionCode: NETLOGON_CONTROL_TC_VERIFY (0x0000000A) , TrustedDomainName: 2008DOMAIN1.COM,
             QueryLevel: NETLOGON_INFO_2 (0x00000002)
  + ServerName: 2008DOMAIN2DC1.2008DOMAIN2.COM
  + Pad: 2 Bytes
```

```
    FunctionCode: NETLOGON_CONTROL_TC_VERIFY (0x0000000A) Windows Server 2003 and later: Verifies the current status of
                                                          the specified trusted domain secure channel
    QueryLevel: NETLOGON_INFO_2 (0x00000002)
  - ControlDataInformation: FunctionCode: NETLOGON_CONTROL_TC_VERIFY (0x0000000A) , TrustedDomainName: 2008DOMAIN1.COM
     FunctionCode: NETLOGON_CONTROL_TC_VERIFY (0x0000000A) Windows Server 2003 and later: Verifies the current status
                   of the specified trusted domain secure channel
   + TrustedDomainName: 2008DOMAIN1.COM

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =73
- Smb2: R  Interim Response, Mid = 23
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x103, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (259) STATUS_PENDING
     Command: IOCTL (0xb)
     Credits: 1 (0x1)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 23 (0x17)
     AsyncId: 262157 (0x4000D)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  - ErrorMessage: 0x1
     Size: 9 (0x9)
     Reserved: 0 (0x0)
     ByteCount: 0 (0x0)
     ErrorMessage: 149 (0x95)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=59952
+ Nbtss: SESSION MESSAGE, Length =412
- Smb2: R  IOCTL (0xb), Mid = 23
    SMBIdentifier: SMB
  - SMB2Header: R IOCTL (0xb)
     Size: 64 (0x40)
     Epoch: 0 (0x0)
   + Status: 0x0, Facility = FACILITY_SYSTEM, Severity = STATUS_SEVERITY_SUCCESS, Code = (0) STATUS_SUCCESS
     Command: IOCTL (0xb)
     Credits: 0 (0x0)
   - Flags: 0xB
      ServerToRedir: (...............................1) Server to Client (SMB2_FLAGS_SERVER_TO_REDIR)
      AsyncCommand:  (..............................1.) Command is asynchronous (SMB2_FLAGS_ASYNC_COMMAND)
      Related:       (.............................0..) Packet is single message (SMB2_FLAGS_RELATED_OPERATIONS)
      Signed:        (............................1...) Packet is signed (SMB2_FLAGS_SIGNED)
      Reserved4_27:  (....000000000000000000000000....)
      DFS:           (...0............................) Command is not a DFS Operation (SMB2_FLAGS_DFS_OPERATIONS)
      Reserved29_31: (000.............................)
     NextCommand: 0 (0x0)
     MessageId: 23 (0x17)
     AsyncId: 262157 (0x4000D)
     SessionId: 4398247837773 (0x4000C00004D)
     Sig: Binary Large Object (16 Bytes)
  + RIoCtl:
- msrpc: c/o Response: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x1  Context=0x0  Hint=0x6C  Cancels=0x0
Unparsed RPC payload
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
```

```
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 132 (0x84)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 108 (0x6C)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 108 bytes
- Netlogonr: NetrLogonControl2Ex Response, QueryLevel: NETLOGON_INFO_2 (0x00000002),
             TrustedDCName: \\2008DOMAIN1DC1.2008DOMAIN1.COM, Flags: 0x000000B0,
             PDCConnectionStatus: NERR_SUCCESS [Completion without errors],
  - ControlQueryInformation: QueryLevel: NETLOGON_INFO_2 (0x00000002), TrustedDCName: \\2008DOMAIN1DC1.2008DOMAIN1.COM,
Flags: 0x000000B0, PDCConnectionStatus: NERR_SUCCESS [Completion without errors]
     QueryLevel: NETLOGON_INFO_2 (0x00000002)
   - NetLogonInfo2: TrustedDCName: \\2008DOMAIN1DC1.2008DOMAIN1.COM, Flags: 0x000000B0, PDCConnectionStatus:
NERR_SUCCESS [Completion without errors]
    + Pointer: Pointer To 0x00020000
    - Flags: 0x000000B0
     - Flags: 0x000000B0
        ReplicationNeeded:      (...............................0) SAM database replication is NOT needed
        ReplicationInProgress:  (..............................0.) SAM database is NOT currently replicated
        FullSyncReplication:    (.............................0..) SAM database does NOT require a full synchronization
```

```
                                                                   update
        RedoNeeded:             (............................0...) Last SAM database replication was successful
        HasIP:                  (...........................1....) Windows 2000 and later: Trusted domain DC has an IP
                                                                   address
        HasTimeserv:            (..........................1.....) Windows 2000 and later: Trusted domain DC runs the
                                                                   Windows Time Service
        DNSUpdateFailure:       (.........................0......) Last update to the DNS records on the DC succeeded
        Unused:                  (0000000000000000000000001.......)
      PDCConnectionStatus: NERR_SUCCESS [Completion without errors]
    + PointerToTrustedDCName: Pointer To 0x00020004
      TcConnectionStatus: NERR_SUCCESS [Completion without errors]
    + TrustedDCName: \\2008DOMAIN1DC1.2008DOMAIN1.COM
  + pad: 2 Bytes
    ReturnValue: NERR_SUCCESS [Completion without errors]
```

5.5.2.3 Netlogonr: NetrServerReqChallenge

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59960, DstPort=49156
- RPC: c/o Request: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x1  Opnum=0x4  Context=0x0  Hint=0x86
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 158 (0x9E)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 134 (0x86)
     PContId: 0 (0x0)
     Opnum: 4 (0x4)
   + StubData: 134 bytes
- Netlogonr: NetrServerReqChallenge Request, Domain Controller:\\2008DOMAIN2DC1.2008DOMAIN2.COM
                                             Client ComputerName:2008DOMAIN1DC1
  - PrimaryName: \\2008DOMAIN2DC1.2008DOMAIN2.COM
   + Pointer: Pointer To 0x00020000
   + stringValue: \\2008DOMAIN2DC1.2008DOMAIN2.COM
  + ComputerName: 2008DOMAIN1DC1
  - ClientChallenge:
     Data: Binary Large Object (8 Bytes)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=59960
- RPC: c/o Response: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x1  Context=0x0  Hint=0xC  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 36 (0x24)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 12 (0xC)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 12 bytes
- Netlogonr: NetrServerReqChallenge Response,
  - ServerChallenge:
     Data: Binary Large Object (8 Bytes)
    pad: 0 Bytes
  - ReturnValue: Success
     Sev:       (..............................00) Success
     C:         (.............................0..) Microsoft-defined
     N:         (............................0...) Not NTSTATUS
     Facility:  (................000000000000....) 0x0
     Code:      (0000000000000000................) 0x0
```

5.5.2.4 Netlogonr: NetrServerAuthenticate3

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59960, DstPort=49156
- RPC: c/o Request: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x2  Opnum=0x1A  Context=0x0  Hint=0xBC Unparsed
RPC payload
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 212 (0xD4)
     AuthLength: 0 (0x0)
     CallId: 2 (0x2)
     AllocHint: 188 (0xBC)
     PContId: 0 (0x0)
     Opnum: 26 (0x1A)
   + StubData: 188 bytes
```

```
- Netlogonr: NetrServerAuthenticate3 Request, Domain Controller: \\2008DOMAIN2DC1.2008DOMAIN2.COM, AccountName: 
2008DOMAIN1.COM., ClientName: 2008DOMAIN1DC1
  - PrimaryName: \\2008DOMAIN2DC1.2008DOMAIN2.COM
   + Pointer: Pointer To 0x00020000
   + stringValue: \\2008DOMAIN2DC1.2008DOMAIN2.COM
  - AccountName: 2008DOMAIN1.COM.
   + Length: 17 Elements
   + Array: 2008DOMAIN1.COM.
  - SecureChannelType: 
   + AccountType: 3 TrustedDnsDomainSecureChannel [Secure channel between two Windows 2000 or Windows Server 2003 DCs]
     Pad: 0 Bytes
  - ComputerName: 2008DOMAIN1DC1
   + Length: 15 Elements
   + Array: 2008DOMAIN1DC1
  - ClientCredential: 
     Data: Binary Large Object (8 Bytes)
  - NegotiateFlags: 0xFFFF0000
   - NegotiateFlags: 0xFFFF0000
      NetlogonSupportsAccountLockout:          (...............................0) The logon service does not support
                                                                                 account lockout
      NetlogonSupportsPersistentBDC:           (..............................0.) The logon server does not have a
                                                                                 persistent backup domain
                                                                                 controller(BDC)
      NetlogonSupportsRC4Encryption:           (.............................0..) The logon service does not support RC4
                                                                                 message encryption
      NetlogonSupportsPromotionCount:          (............................0...) The logon service does not support the
                                                                                 domain controller promotion count
      NetlogonSupportsBDCChallengeLog:         (...........................0....) The logon service does not support
                                                                                 changelog activity on the BDC
      NetlogonSupportsFullSyncRestart:         (..........................0.....) The logon service does not support a
                                                                                 full synchronization restart of the
                                                                                 service
      NetlogonSupportsMultipleSIDs:            (.........................0......) The logon service does not allow for
                                                                                 multiple security identifiers
      NetlogonSupportsRedo:                    (........................0.......) The logon service does not support
```

```
                                                                           multiple logon attempts
NetlogonSupportsRefuseChangePwd:        (.......................0........) The logon service cannot refuse a
                                                                           password change request
NetlogonSupportsPDCPassword:            (......................0.........) The logon service does not allow for
                                                                           remote PDC logon
NetlogonSupportsGenericPassThru:        (.....................0..........) The logon service does not support
                                                                           generic domain passthru
NetlogonSupportsConcurrentRPC:          (....................0...........) The logon service does not support
                                                                           concurrent RPC
NetlogonSupportsAvoidSamrEPL:           (...................0............) The logon service does not allow the
                                                                           avoidance of SAM database replication
NetlogonSupportsAvoidLsarEPL:           (..................0.............) The logon service does not allow the
                                                                           avoidance of LSA database replication
NetlogonSupportsStrongKey:              (.................0..............) The logon service does not support
                                                                           strong key password authentication
NetlogonSupportsTransitive:             (................0...............) The logon service does not support
                                                                           transitive domain trusts
NetlogonSupportsDNSDomainTrust:         (...............1................) The logon service supports DNS domain
                                                                           trusts
NetlogonSupportsPasswordSet2:           (..............1.................) The logon service supports calls to
                                                                           the NetrServerPasswordSet2 method
NetlogonSupportsGetDomainInfo:          (.............1..................) The logon service supports calls to
                                                                           the NetrLogonGetDomainInfo method
NetlogonSupportsCrossForest:            (............1...................) The logon service supports cross-
                                                                           forest trusts
NetlogonSupportsNT4EmulatorNeutralizer: (...........1....................) The logon service supports
                                                                           neutralizing Windows NT4.0 emulation
NetlogonSupportsCDCPassthru:            (..........1.....................) The logon service supports read-only
                                                                           DC pass-through to different domains
Unused:                                 (...1111111......................)
NetlogonSupportsLSAAuthRPC:             (..1.............................) The logon service supports LSA-
                                                                           authenticated RPC
NetlogonSupportsAuthRPC:                (.1..............................) The logon service supports
                                                                           authenticated RPC
Reserved:                               (1...............................)
```

```
+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21,
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=59960
- RPC: c/o Response: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x2  Context=0x0  Hint=0x14  Cancels=0x0
  - Response:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 44 (0x2C)
     AuthLength: 0 (0x0)
     CallId: 2 (0x2)
     AllocHint: 20 (0x14)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 20 bytes
- Netlogonr: NetrServerAuthenticate3 Response, NegotiateFlags: 0x603FFFFF, AccountRid: 1105,
  - ServerCredential:
     Data: Binary Large Object (8 Bytes)
  - NegotiateFlags: 0x603FFFFF
   - NegotiateFlags: 0x603FFFFF
```

```
NetlogonSupportsAccountLockout:         (...............................1) The logon service supports account
                                                                           lockout
NetlogonSupportsPersistentBDC:          (..............................1.) The logon server has a persistent
                                                                           backup domain controller(BDC)
NetlogonSupportsRC4Encryption:          (.............................1..) The logon service supports RC4 message
                                                                           encryption
NetlogonSupportsPromotionCount:         (............................1...) The logon service supports the domain
                                                                           controller promotion count
NetlogonSupportsBDCChallengeLog:        (...........................1....) The logon service supports changelog
                                                                           activity on the BDC
NetlogonSupportsFullSyncRestart:        (..........................1.....) The logon service supports a full
                                                                           synchronization restart of the service
NetlogonSupportsMultipleSIDs:           (.........................1......) The logon service allows for multiple
                                                                           security identifiers
NetlogonSupportsRedo:                   (........................1.......) The logon service supports multiple
                                                                           logon attempts
NetlogonSupportsRefuseChangePwd:        (.......................1........) The logon service can refuse a
                                                                           password change request
NetlogonSupportsPDCPassword:            (......................1.........) The logon service allows for remote
                                                                           PDC logon
NetlogonSupportsGenericPassThru:        (.....................1..........) The logon service supports generic
                                                                           domain passthru
NetlogonSupportsConcurrentRPC:          (....................1...........) The logon service supports concurrent
                                                                           RPC
NetlogonSupportsAvoidSamrEPL:           (...................1............) The logon service allows the avoidance
                                                                           of SAM database replication
NetlogonSupportsAvoidLsarEPL:           (..................1.............) The logon service allows the avoidance
                                                                           of LSA database replication
NetlogonSupportsStrongKey:              (.................1..............) The logon service supports strong key
                                                                           password authentication
NetlogonSupportsTransitive:             (................1...............) The logon service supports transitive
                                                                           domain trusts
NetlogonSupportsDNSDomainTrust:         (...............1................) The logon service supports DNS domain
                                                                           trusts
NetlogonSupportsPasswordSet2:           (..............1.................) The logon service supports calls to
```

```
                                                                                 the NetrServerPasswordSet2 method
      NetlogonSupportsGetDomainInfo:          (.............1..................) The logon service supports calls to
                                                                                 the NetrLogonGetDomainInfo method
      NetlogonSupportsCrossForest:            (............1...................) The logon service supports cross-
                                                                                 forest trusts
      NetlogonSupportsNT4EmulatorNeutralizer: (...........1....................) The logon service supports
                                                                                 neutralizing Windows NT4.0 emulation
      NetlogonSupportsCDCPassthru:            (..........1.....................) The logon service supports read-only
                                                                                 DC pass-through to different domains
      Unused:                                 (...0000000......................)
      NetlogonSupportsLSAAuthRPC:             (..1.............................) The logon service supports LSA-
                                                                                 authenticated RPC
      NetlogonSupportsAuthRPC:                (.1..............................) The logon service supports
                                                                                 authenticated RPC
      Reserved:                               (0...............................)
    AccountRid: 1105 (0x451)
  - ReturnValue: Success
     Sev:       (..............................00) Success
     C:         (.............................0..) Microsoft-defined
     N:         (............................0...) Not NTSTATUS
     Facility:  (................000000000000....) 0x0
     Code:      (0000000000000000................) 0x0
```

5.5.2.5 Netlogonr: NetrServerGetTrustInfo

Get the Trust Password

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59960, DstPort=49156
- RPC: c/o Request: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x3  Opnum=0x2E  Context=0x0  Hint=0xBC
  - Request:
```

```
  RpcVers: 5 (0x5)
  RpcVersMinor: 0 (0x0)
  PType: 0x00 - Request
- PfcFlags: 3 (0x3)
   Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
   Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
   Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
   Bit3: ....0... PFC_RESERVED_1 - reserved
   Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
   Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
   Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
   Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
- PackedDrep: 0x10
   Octet0: 0x10 - Little-endian Integer, ASCII Character representation
   Octet1: 0x00 - IEEE Floating Point representation
   Octet2: 0x00 - Reserved
   Octet3: 0x00 - Reserved
  FragLength: 256 (0x100)
  AuthLength: 32 (0x20)
  CallId: 3 (0x3)
  AllocHint: 188 (0xBC)
  PContId: 0 (0x0)
  Opnum: 46 (0x2E)
+ StubData: 188 bytes
- AuthVerifier:
   AuthPad: Binary Large Object (4 Bytes)
   AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
   AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                              privacy (encryption) of stub call arguments only. All run-time and
                                              lower-layer headers are still transmitted in clear text.
   AuthPadLength: 4 (0x4)
   AuthReserved: 0 (0x0)
   AuthContextId: 1 (0x1)
 - AuthValue:
  - NetlogonSignature:
        SignatureAlgorithm: 0x77 KERB_CHECKSUM_MD5_HMAC - The packet is signed using MD5-HMAC-64
        SealAlgorithm: 0x7A KERB_ETYPE_RC4_PLAIN_OLD - The packet is enrypted using RC4
        Pad: 65535 (0xFFFF)
        Flags: 0x0 No flags defined, must be 0
        SequenceNumber: Binary Large Object (8 Bytes)
        Checksum: Binary Large Object (8 Bytes)
        Confounder: Binary Large Object (8 Bytes)
- Netlogonr: NetrServerGetTrustInfo Request, TrustedDcName:NULL  AccountName:  ComputerName: 
    EncryptedData: Binary Large Object (188 Bytes)
  - TrustedDcName: NULL
     Pointer: Pointer To NULL

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=59960
- RPC: c/o Response: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x3  Context=0x0  Hint=0x4C  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 144 (0x90)
     AuthLength: 32 (0x20)
     CallId: 3 (0x3)
     AllocHint: 76 (0x4C)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 76 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (4 Bytes)
      AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 4 (0x4)
      AuthReserved: 0 (0x0)
      AuthContextId: 1 (0x1)
    - AuthValue:
     - NetlogonSignature:
        SignatureAlgorithm: 0x77 KERB_CHECKSUM_MD5_HMAC - The packet is signed using MD5-HMAC-64
        SealAlgorithm: 0x7A KERB_ETYPE_RC4_PLAIN_OLD - The packet is enrypted using RC4
        Pad: 65535 (0xFFFF)
        Flags: 0x0 No flags defined, must be 0
        SequenceNumber: Binary Large Object (8 Bytes)
        Checksum: Binary Large Object (8 Bytes)
        Confounder: Binary Large Object (8 Bytes)
- Netlogonr: NetrServerGetTrustInfo Response,
    EncryptedData: Binary Large Object (76 Bytes)
  - ReturnAuthenticator:
     Credential:
```

5.5.2.6 Netlogonr: NetrLogonSamLogonWithFlags

```
+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=58246, DstPort=49157
- RPC: c/o Request: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x3  Opnum=0x2D  Context=0x0  Hint=0x2D4
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 800 (0x320)
     AuthLength: 32 (0x20)
     CallId: 3 (0x3)
     AllocHint: 724 (0x2D4)
     PContId: 0 (0x0)
     Opnum: 45 (0x2D)
   + StubData: 724 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (12 Bytes)
      AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 12 (0xC)
      AuthReserved: 0 (0x0)
      AuthContextId: 1 (0x1)
    - AuthValue:
     - NetlogonSignature:
        SignatureAlgorithm: 0x77 KERB_CHECKSUM_MD5_HMAC - The packet is signed using MD5-HMAC-64
        SealAlgorithm: 0x7A KERB_ETYPE_RC4_PLAIN_OLD - The packet is enrypted using RC4
        Pad: 65535 (0xFFFF)
        Flags: 0x0 No flags defined, must be 0
        SequenceNumber: Binary Large Object (8 Bytes)
        Checksum: Binary Large Object (8 Bytes)
        Confounder: Binary Large Object (8 Bytes)
- Netlogonr: NetrLogonSamLogonWithFlags Request, LogonServer:NULL  ComputerName:
    EncryptedData: Binary Large Object (724 Bytes)
  - LogonServer: NULL
     Pointer: Pointer To NULL

+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=49157, DstPort=58246
- RPC: c/o Response: Logon {12345678-1234-ABCD-EF00-01234567CFFB}  Call=0x3  Context=0x0  Hint=0x27C  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 704 (0x2C0)
     AuthLength: 32 (0x20)
     CallId: 3 (0x3)
     AllocHint: 636 (0x27C)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 636 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (4 Bytes)
      AuthType: RPC_C_AUTHN_NETLOGON - Netlogon authentication will be used.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 4 (0x4)
      AuthReserved: 0 (0x0)
      AuthContextId: 1 (0x1)
    - AuthValue:
     - NetlogonSignature:
        SignatureAlgorithm: 0x77 KERB_CHECKSUM_MD5_HMAC - The packet is signed using MD5-HMAC-64
        SealAlgorithm: 0x7A KERB_ETYPE_RC4_PLAIN_OLD - The packet is enrypted using RC4
        Pad: 65535 (0xFFFF)
        Flags: 0x0 No flags defined, must be 0
        SequenceNumber: Binary Large Object (8 Bytes)
        Checksum: Binary Large Object (8 Bytes)
        Confounder: Binary Large Object (8 Bytes)
- Netlogonr: NetrLogonSamLogonWithFlags Response,
    EncryptedData: Binary Large Object (636 Bytes)
```

```
  - ReturnAuthenticator:
     Ptr: Pointer To NULL
```

5.6 DRSUAPI

5.6.1 DRSUAPI: Session Control

5.6.1.1 RPC Bind to ept ([C706])

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60329, DstPort=DCE endpoint resolution(135)
- RPC: c/o Bind:  UUID{E1AF8308-5D1F-11C9-91A4-08002B14A0FA} EPT  Call=0x1  Assoc Grp=0x0  Xmit=0x16D0  Recv=0x16D0
  - Bind: {E1AF8308-5D1F-11C9-91A4-08002B14A0FA} EPT
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0B - Bind
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 116 (0x74)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 0 (0x0)
   - PContextElem:
      NContextElem: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PContElem: 0x1
       PContId: 0 (0x0)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {E1AF8308-5D1F-11C9-91A4-08002B14A0FA} EPT
     + TransferSyntaxes: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PContElem: 0x1
       PContId: 1 (0x1)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {E1AF8308-5D1F-11C9-91A4-08002B14A0FA} EPT
     + TransferSyntaxes: {6CB71C2C-9812-4540-0300000000000000} BTFN - Security Context Multiplexing Supported
     AuthVerifier: 0x1

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=DCE endpoint resolution(135)
- RPC: c/o Bind Ack:  Call=0x1  Assoc Grp=0x101A0  Xmit=0x16D0  Recv=0x16D0
  - BindAck:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0C - Bind Ack
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 84 (0x54)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 65952 (0x101A0)
   - SecAddr: 135
      Length: 4 (0x4)
      PortSpec: 135
   + Pad2: 0x1
   - PResultList:
      NResults: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PResults: Acceptance, Reason=n/a
       Result: Acceptance
       Reason: n/a
     + TransferSyntax: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PResults: Negotiate Ack, Security Context Multiplexing Supported
       Result: Negotiate Ack
     + bitmask: Security Context Multiplexing Supported
     + TransferSyntax: {00000000-0000-0000-0000-000000000000} unknown
     AuthVerifier:
```

5.6.1.2 ept_map to DRSUAPI ([C706])

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60329, DstPort=DCE endpoint resolution(135)
- RPC: c/o Request: EPT {E1AF8308-5D1F-11C9-91A4-08002B14A0FA}  Call=0x1  Opnum=0x3  Context=0x0  Hint=0x84
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 156 (0x9C)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 132 (0x84)
     PContId: 0 (0x0)
     Opnum: 3 (0x3)
   + StubData: 132 bytes
- Epm: Request: ept_map:
  + Object: {00000000-0000-0000-0000-000000000000}
  - MapTower: Pointer To 0x00000002
   + align: 0 Bytes
   + TwrTPointer: Pointer To 0x00000002
   - Tower:
    + Length: 75 Elements
      TowerLength: 75 (0x4B)
      TowerOctetString: Binary Large Object (75 Bytes)
    + Align: 1 Bytes
  - EntryHandle: 0x1
     ContextType: 0 (0x0)
     ContextUuid: {00000000-0000-0000-0000-000000000000}
    MaxTowers: 4 (0x4)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=DCE endpoint resolution(135), DstPort=60329
- RPC: c/o Response: EPT {E1AF8308-5D1F-11C9-91A4-08002B14A0FA}  Call=0x1  Context=0x0  Hint=0xD8  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 240 (0xF0)
     AuthLength: 0 (0x0)
     CallId: 1 (0x1)
     AllocHint: 216 (0xD8)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 216 bytes
- Epm: Response: ept_map:
  - EntryHandle:
     ContextType: 0 (0x0)
     ContextUuid: {00000000-0000-0000-0000-000000000000}
    NumTowers: 2 (0x2)
  - Towers: 2 Elements
   + ArrayInfo: 2 Elements
   + TwrPtr: Pointer To 0x00000003
   + TwrPtr: Pointer To 0x00000004
   - Tower:
    + Length: 75 Elements
      TowerLength: 75 (0x4B)
      TowerOctetString: Binary Large Object (75 Bytes)
    + Align: 1 Bytes
   - Tower:
    + Length: 75 Elements
      TowerLength: 75 (0x4B)
      TowerOctetString: Binary Large Object (75 Bytes)
    + Align: 1 Bytes
  + Status: 0x00000000 - EP_S_SUCCESS
```

5.6.1.3 RPC: c/o Bind to DRSUAPI ([C706])

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...A...., SrcPort=60330, DstPort=49156
- RPC: c/o Bind:  UUID{E3514235-4B06-11D1-AB04-00C04FC2DCD2} DRSR  Call=0x1  Assoc Grp=0x0  Xmit=0x16D0  Recv=0x16D0
  - Bind: {E3514235-4B06-11D1-AB04-00C04FC2DCD2} DRSR
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0B - Bind
   - PfcFlags: 7 (0x7)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....1.. PFC_SUPPORT_HEADER_SIGN - SET, Header Sign was supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 1717 (0x6B5)
     AuthLength: 1593 (0x639)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 0 (0x0)
   - PContextElem:
      NContextElem: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PContElem: 0x1
       PContId: 0 (0x0)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {E3514235-4B06-11D1-AB04-00C04FC2DCD2} DRSR
     + TransferSyntaxes: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
    - PContElem: 0x1
       PContId: 1 (0x1)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {E3514235-4B06-11D1-AB04-00C04FC2DCD2} DRSR
     + TransferSyntaxes: {6CB71C2C-9812-4540-0300000000000000} BTFN - Security Context Multiplexing Supported
   - AuthVerifier: 0x1
      AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                            either NT LAN Manager (NTLM) or Kerberos authentication.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 0 (0x0)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - GssApiNego:
      + ApplicationHeader:
      + ThisMech: SpnegoToken (1.3.6.1.5.5.2)
      - InnerContextToken: Blob Value
       + AsnOctetStringHeader:
```

```
+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=60330
- RPC: c/o Bind Ack:  Call=0x1  Assoc Grp=0xC7B1  Xmit=0x16D0  Recv=0x16D0
  - BindAck:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0C - Bind Ack
   - PfcFlags: 7 (0x7)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....1.. PFC_SUPPORT_HEADER_SIGN - SET, Header Sign was supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 261 (0x105)
     AuthLength: 169 (0xA9)
     CallId: 1 (0x1)
     MaxXmitFrag: 5840 (0x16D0)
     MaxRecvFrag: 5840 (0x16D0)
     AssocGroupId: 51121 (0xC7B1)
   - SecAddr: 49156
      Length: 6 (0x6)
      PortSpec: 49156
     Pad2: 0x1
   - PResultList:
      NResults: 2 (0x2)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
```

```
 - PResults: Acceptance, Reason=n/a
    Result: Acceptance
    Reason: n/a
  + TransferSyntax: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
 - PResults: Negotiate Ack, Security Context Multiplexing Supported
    Result: Negotiate Ack
  + bitmask: Security Context Multiplexing Supported
  + TransferSyntax: {00000000-0000-0000-0000-000000000000} unknown
- AuthVerifier:
   AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                         either NT LAN Manager (NTLM) or Kerberos authentication.
   AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                              privacy (encryption) of stub call arguments only. All run-time and
                                              lower-layer headers are still transmitted in clear text.
   AuthPadLength: 0 (0x0)
   AuthReserved: 0 (0x0)
   AuthContextId: 0 (0x0)
 - AuthValue:
  - GssApiNego:
   - SpnegoNegotiationToken:
    + Tag1:
    - NegTokenResp: 0x1
     + SequenceHeader:
     + Tag0:
     + NegState: accept-incomplete (1)
     + Tag1:
     + SupportedMech: MsKerberosToken (1.2.840.48018.1.2.2)
     + Tag2:
     - ResponseToken:
      + OctetStringHeader:
      - SecurityBlob: 0x1
       - MsKerberosToken: 0x1
        - Kerberos: AP Response
         - ApRep: KRB_AP_REP (15)
          + ApplicationTag:
          + SequenceHeader:
          + Tag0:
          + PvNo: 5
          + Tag1:
          + MsgType: KRB_AP_REP (15)
          + Tag2: 0x1
          - AuthorizationData:
           + SequenceHeader:
           + Tag0:
           + EType: aes256-cts-hmac-sha1-96 (18)
           + Tag2:
           + Cipher: ...
```

5.6.1.4 RPC: c/o Alter Cont (update security context) ([C706])

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60330, DstPort=49156
- RPC: c/o Alter Cont:  UUID{E3514235-4B06-11D1-AB04-00C04FC2DCD2} DRSR  Call=0x1
  - AlterContext:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0E - Alter Context
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 220 (0xDC)
     AuthLength: 140 (0x8C)
     CallId: 1 (0x1)
     MaxXmitFrag: ignored
     MaxRecvFrag: ignored
     AssocGroupId: ignored
   - PContextElem:
      NContextElem: 1 (0x1)
      Reserved: 0 (0x0)
      Reserved2: 0 (0x0)
    - PContElem: 0x1
       PContId: 0 (0x0)
       NTransferSyn: 1 (0x1)
       Reserved: 0 (0x0)
     + AbstractSyntax: {E3514235-4B06-11D1-AB04-00C04FC2DCD2} DRSR
     + TransferSyntaxes: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
   - AuthVerifier: 0x1
      AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                            either NT LAN Manager (NTLM) or Kerberos authentication.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 0 (0x0)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - GssApiNego:
      - SpnegoNegotiationToken:
       + Tag1:
       - NegTokenResp: 0x1
        + SequenceHeader:
        + Tag0:
        + NegState: accept-incomplete (1)
        + Tag2:
        - ResponseToken:
         + OctetStringHeader:
           OctetStream: Binary Large Object (93 Bytes)
        + Tag3:
        - MechListMic:
         + OctetStringHeader:
           OctetStream: Binary Large Object (28 Bytes)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=60330
- RPC: c/o Alter Cont Resp:  Call=0x1  Assoc Grp=0xC7B1  Xmit=0x16D0  Recv=0x16D0
  - AlterContextResponse:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x0F - Alter Context Resp
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_SUPPORT_HEADER_SIGN - NOT set, Header Sign was NOT supported at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
```

```
    FragLength: 105 (0x69)
    AuthLength: 41 (0x29)
    CallId: 1 (0x1)
    MaxXmitFrag: ignored
    MaxRecvFrag: ignored
    AssocGroupId: ignored
  - SecAddr:
     Length: 0 (0x0)
  + Pad2: 0x1
  - PResultList:
     NResults: 1 (0x1)
     Reserved: 0 (0x0)
     Reserved2: 0 (0x0)
   - PResults: Acceptance, Reason=n/a
      Result: Acceptance
      Reason: n/a
    + TransferSyntax: {8A885D04-1CEB-11C9-9FE8-08002B104860} NDR
  - AuthVerifier:
     AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                           either NT LAN Manager (NTLM) or Kerberos authentication.
     AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                privacy (encryption) of stub call arguments only. All run-time and
                                                lower-layer headers are still transmitted in clear text.
     AuthPadLength: 0 (0x0)
     AuthReserved: 0 (0x0)
     AuthContextId: 0 (0x0)
   - AuthValue:
    - GssApiNego:
     - SpnegoNegotiationToken:
      + Tag1:
      - NegTokenResp: 0x1
       + SequenceHeader:
       + Tag0:
       + NegState: accept-completed (0)
       + Tag3:
```

```
- MechListMic:
 + OctetStringHeader:
   OctetStream: Binary Large Object (28 Bytes)
```

5.6.2 DRSUAPI: Procedure calls

5.6.2.1 DRSUAPI: IDLDRSBind (IDL_DRSBind)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60330, DstPort=49156
- RPC: c/o Request: DRSR {E3514235-4B06-11D1-AB04-00C04FC2DCD2}  Call=0x1  Opnum=0x0  Context=0x0  Hint=0x84
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 252 (0xFC)
     AuthLength: 76 (0x4C)
     CallId: 1 (0x1)
     AllocHint: 132 (0x84)
     PContId: 0 (0x0)
     Opnum: 0 (0x0)
   + StubData: 132 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (12 Bytes)
      AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                            either NT LAN Manager (NTLM) or Kerberos authentication.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 12 (0xC)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - GssApiNego:
      - KerberosToken:
         Krb5tokId: GSS_Wrap (0x504)
       - Krb5GssV2Wrap:
        - Flags: 6 (0x6)
           Unused: (00000...) Unused
           Bit2:   (.....1..) AcceptorSubkey - A subkey asserted by the context acceptor is used to protect the
                                               message.
           Bit1:   (......1.) Sealed - Indicates confidentiality is provided
           Bit0:   (.......0) SentByAcceptor - The sender is the context initiator.
          Filler: 255 (0xFF)
          EC: 16 (0x10)
          RRC: 28 (0x1C)
          SndSeq: 808898829 (0x3036D10D)
```

```
          EncryptedData: Binary Large Object (60 Bytes)
- Drsr: DRSR:IDL_DRSBind Request, *Encrypted*
    EncryptedData: Binary Large Object (132 Bytes)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=60330
- RPC: c/o Response: DRSR {E3514235-4B06-11D1-AB04-00C04FC2DCD2}  Call=0x1  Context=0x0  Hint=0x54  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 204 (0xCC)
     AuthLength: 76 (0x4C)
     CallId: 1 (0x1)
     AllocHint: 84 (0x54)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 84 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (12 Bytes)
      AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                            either NT LAN Manager (NTLM) or Kerberos authentication.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 12 (0xC)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - GssApiNego:
      - KerberosToken:
         Krb5tokId: GSS_Wrap (0x504)
       - Krb5GssV2Wrap:
        - Flags: 7 (0x7)
           Unused: (00000...) Unused
           Bit2:   (.....1..) AcceptorSubkey - A subkey asserted by the context acceptor is used to protect the
                                               message.
           Bit1:   (......1.) Sealed - Indicates confidentiality is provided
           Bit0:   (.......1) SentByAcceptor - The sender is the context acceptor.
          Filler: 255 (0xFF)
          EC: 16 (0x10)
          RRC: 28 (0x1C)
          SndSeq: 809023950 (0x3038B9CE)
          EncryptedData: Binary Large Object (60 Bytes)
- Drsr: DRSR:IDL_DRSBind Response, *Encrypted*
    EncryptedData: Binary Large Object (84 Bytes)
```

5.6.2.2 DRSUAPI: IDLDRSCrackNames (IDL_DRSCrackNames)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60330, DstPort=49156
- RPC: c/o Request: DRSR {E3514235-4B06-11D1-AB04-00C04FC2DCD2}  Call=0x2  Opnum=0xC  Context=0x0  Hint=0x6E
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 220 (0xDC)
     AuthLength: 76 (0x4C)
     CallId: 2 (0x2)
     AllocHint: 110 (0x6E)
     PContId: 0 (0x0)
     Opnum: 12 (0xC)
   + StubData: 110 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (2 Bytes)
      AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                            either NT LAN Manager (NTLM) or Kerberos authentication.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 2 (0x2)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - GssApiNego:
      - KerberosToken:
         Krb5tokId: GSS_Wrap (0x504)
       - Krb5GssV2Wrap:
        - Flags: 6 (0x6)
           Unused: (00000...) Unused
           Bit2:   (.....1..) AcceptorSubkey - A subkey asserted by the context acceptor is used to protect the
                                               message.
           Bit1:   (......1.) Sealed - Indicates confidentiality is provided
           Bit0:   (.......0) SentByAcceptor - The sender is the context initiator.
          Filler: 255 (0xFF)
          EC: 16 (0x10)
          RRC: 28 (0x1C)
          SndSeq: 808898830 (0x3036D10E)
          EncryptedData: Binary Large Object (60 Bytes)
- Drsr: DRSR:IDL_DRSCrackNames Request, *Encrypted*
    EncryptedData: Binary Large Object (110 Bytes)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=60330
- RPC: c/o Response: DRSR {E3514235-4B06-11D1-AB04-00C04FC2DCD2}  Call=0x2  Context=0x0  Hint=0x8C  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 252 (0xFC)
     AuthLength: 76 (0x4C)
     CallId: 2 (0x2)
     AllocHint: 140 (0x8C)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 140 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (4 Bytes)
      AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                            either NT LAN Manager (NTLM) or Kerberos authentication.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 4 (0x4)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - GssApiNego:
      - KerberosToken:
         Krb5tokId: GSS_Wrap (0x504)
       - Krb5GssV2Wrap:
        - Flags: 7 (0x7)
           Unused: (00000...) Unused
           Bit2:   (.....1..) AcceptorSubkey - A subkey asserted by the context acceptor is used to protect the
                                               message.
```

```
           Bit1:   (......1.) Sealed - Indicates confidentiality is provided
           Bit0:   (.......1) SentByAcceptor - The sender is the context acceptor.
          Filler: 255 (0xFF)
          EC: 16 (0x10)
          RRC: 28 (0x1C)
          SndSeq: 809023951 (0x3038B9CF)
          EncryptedData: Binary Large Object (60 Bytes)
- Drsr: DRSR:IDL_DRSCrackNames Response, *Encrypted*
    EncryptedData: Binary Large Object (140 Bytes)
```

5.6.2.3 DRSUAPI: IDLDRSUnbind (IDL_DRSUnbind)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60330, DstPort=49156
- RPC: c/o Request: DRSR {E3514235-4B06-11D1-AB04-00C04FC2DCD2}  Call=0x3  Opnum=0x1  Context=0x0  Hint=0x14
  - Request:
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x00 - Request
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 140 (0x8C)
     AuthLength: 76 (0x4C)
     CallId: 3 (0x3)
     AllocHint: 20 (0x14)
     PContId: 0 (0x0)
     Opnum: 1 (0x1)
   + StubData: 20 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (12 Bytes)
      AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                            either NT LAN Manager (NTLM) or Kerberos authentication.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 12 (0xC)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - GssApiNego:
      - KerberosToken:
         Krb5tokId: GSS_Wrap (0x504)
       - Krb5GssV2Wrap:
        - Flags: 6 (0x6)
           Unused: (00000...) Unused
           Bit2:   (.....1..) AcceptorSubkey - A subkey asserted by the context acceptor is used to protect the
                                               message.
           Bit1:   (......1.) Sealed - Indicates confidentiality is provided
           Bit0:   (.......0) SentByAcceptor - The sender is the context initiator.
          Filler: 255 (0xFF)
          EC: 16 (0x10)
          RRC: 28 (0x1C)
```

```
          SndSeq: 808898831 (0x3036D10F)
          EncryptedData: Binary Large Object (60 Bytes)
- Drsr: DRSR:IDL_DRSUnbind Request, *Encrypted*
    EncryptedData: Binary Large Object (20 Bytes)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=49156, DstPort=60330
- RPC: c/o Response: DRSR {E3514235-4B06-11D1-AB04-00C04FC2DCD2}  Call=0x3  Context=0x0  Hint=0x18  Cancels=0x0
  - Response: 0x1
     RpcVers: 5 (0x5)
     RpcVersMinor: 0 (0x0)
     PType: 0x02 - Response
   - PfcFlags: 3 (0x3)
      Bit0: .......1 PFC_FIRST_FRAG - SET, Is first fragment
      Bit1: ......1. PFC_LAST_FRAG - SET, Is last fragment
      Bit2: .....0.. PFC_PENDING_CANCEL - NOT set, Cancel was NOT pending at sender
      Bit3: ....0... PFC_RESERVED_1 - reserved
      Bit4: ...0.... PFC_CONC_MPX - NOT set, Does NOT support concurrent multiplexing of a single connection.
      Bit5: ..0..... PFC_DID_NOT_EXECUTE - N/A; Only meaningful on `fault' packet.
      Bit6: .0...... PFC_MAYBE - NOT set, `maybe' call semantics NOT requested
      Bit7: 0....... PFC_OBJECT_UUID - NOT set, The object field is omitted.
   - PackedDrep: 0x10
      Octet0: 0x10 - Little-endian Integer, ASCII Character representation
      Octet1: 0x00 - IEEE Floating Point representation
      Octet2: 0x00 - Reserved
      Octet3: 0x00 - Reserved
     FragLength: 140 (0x8C)
     AuthLength: 76 (0x4C)
     CallId: 3 (0x3)
     AllocHint: 24 (0x18)
     PContId: 0 (0x0)
     CancelCount: 0 (0x0)
     Rsvd1: 0 (0x0)
   + StubData: 24 bytes
   - AuthVerifier:
      AuthPad: Binary Large Object (8 Bytes)
      AuthType: RPC_C_AUTHN_GSS_NEGOTIATE - The Simple and Protected GSS-API Negotiation (SPNEGO) mechanism selects
                                            either NT LAN Manager (NTLM) or Kerberos authentication.
      AuthLevel: dce_c_authn_level_pkt_privacy - This level offers the dce_c_authn_level_pkt_integrity services plus
                                                 privacy (encryption) of stub call arguments only. All run-time and
                                                 lower-layer headers are still transmitted in clear text.
      AuthPadLength: 8 (0x8)
      AuthReserved: 0 (0x0)
      AuthContextId: 0 (0x0)
    - AuthValue:
     - GssApiNego:
      - KerberosToken:
         Krb5tokId: GSS_Wrap (0x504)
       - Krb5GssV2Wrap:
        - Flags: 7 (0x7)
           Unused: (00000...) Unused
           Bit2:   (.....1..) AcceptorSubkey - A subkey asserted by the context acceptor is used to protect the
                                               message.
           Bit1:   (......1.) Sealed - Indicates confidentiality is provided
           Bit0:   (.......1) SentByAcceptor - The sender is the context acceptor.
          Filler: 255 (0xFF)
          EC: 16 (0x10)
          RRC: 28 (0x1C)
          SndSeq: 809023952 (0x3038B9D0)
          EncryptedData: Binary Large Object (60 Bytes)
- Drsr: DRSR:IDL_DRSUnbind Response, *Encrypted*
    EncryptedData: Binary Large Object (24 Bytes)
```

5.7 Kerberos

5.7.1 Kerberos: AS Request Sname: krbtgt/ (KDC_ERR_PREAUTH_REQUIRED)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59953, DstPort=Kerberos(88)
- Kerberos: AS Request Cname: Administrator Realm: 2008DOMAIN2.COM Sname: krbtgt/2008DOMAIN2.COM
  + Length: Length = 242
  - AsReq: Kerberos AS Request
   + ApplicationTag:
   - KdcReq: KRB_AS_REQ (10)
    + SequenceHeader:
    + Tag1:
    + Pvno: 5
    + Tag2:
    + MsgType: KRB_AS_REQ (10)
    + Tag3:
    + PaData:
    + Tag4:
    - ReqBody:
     + SequenceHeader:
     + Tag0:
     - KdcOptions: 0x40810010
      + KerberosFlagsHeader:
      + Padding:
      - KrbFlags: 0x40810010
         Reserved:              (0...............................)
         Forwardable:           (.1..............................) Ticket to be issued is to have its FORWARDABLE flag
                                                                   set
         Forwarded:             (..0.............................) This is not a request for forwarding
         Proxiable:             (...0............................) Ticket to be issued is not to have its PROXIABLE
                                                                   flag set
         Proxy:                 (....0...........................) This is not a request for a proxy
         AllowPostDate:         (.....0..........................) Ticket to be issued is not to have its MAY_POSTDATE
```

```
                                                                  flag set
        PostDated:             (......0.........................) This is not a request for a postdated ticket
        Unused7:               (.......0........................)
        Renewable:             (........1.......................) Ticket to be issued is to have its RENEWABLE flag
                                                                  set
        Unused9:               (.........0......................)
        Unused10:              (..........0.....................)
        OptHardwareAuth:       (...........0....................)
        Unused12:              (............0...................)
        Unused13:              (.............0..................)
        CnameInAddlTkt:        (..............0.................) This is not a request for S4U2proxy functionality
        Canonicalize:          (...............1................)
        Unused16:              (................0000000000......)
        DisableTransitedCheck: (..........................0.....) Checking of the transited field is enabled
        RenewableOk:           (...........................1....) Indicates that the renewable ticket is acceptable if
                                                                  a ticket with the requested life cannot be provided
        EncTktInSkey:          (............................0...) Ticket for the end server is to be encrypted in the
                                                                  session key
        Unused29:              (.............................0..)
        Renew:                 (..............................0.) Present request is not for a renewal
        Validate:              (...............................0) Request is not to validate a postdated ticket
    + Tag1:
    - Cname: Administrator
     + SequenceHeader:
     + Tag0:
     + NameType: NT-PRINCIPAL (1)
     + Tag1:
     + SequenceOfHeader:
     + NameString: Administrator
    + Tag2: 0x1
    - Realm: 2008DOMAIN2.COM
     + Realm: 2008DOMAIN2.COM
    + Tag3:
    - Sname: krbtgt/2008DOMAIN2.COM
     + SequenceHeader:
      + Tag0:
      + NameType: NT-SRV-INST (2)
      + Tag1:
      + SequenceOfHeader:
      + NameString: krbtgt
      + NameString: 2008DOMAIN2.COM
     + Tag5: 0x1
     + Till: 09/13/2037 02:48:05 UTC
     + Tag6:
     + Rtime: 09/13/2037 02:48:05 UTC
     + Tag7:
     + Nonce: 1075326609 (0x40182E91)
     + Tag8:
     - Etype:
      + SequenceOfHeader:
      + EType: aes256-cts-hmac-sha1-96 (18)
      + EType: aes128-cts-hmac-sha1-96 (17)
      + EType: rc4-hmac (23)
      + EType: des-cbc-md5 (3)
      + EType: des-cbc-crc (1)
      + EType: rc4-hmac-exp (24)
      + EType: rc4 hmac old exp (0xff79)
     + Tag9:
     - Addresses:
      + SequenceOfHeader:
      + Address: 2008DOMAIN1DC1

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=Kerberos(88), DstPort=59953
- Kerberos: KRB_ERROR  - KDC_ERR_PREAUTH_REQUIRED (25)
  + Length: Length = 163
  - KrbError: KRB_ERROR (30)
   + ApplicationTag:
   + SequenceHeader:
   + Tag0:
```

```
+ PvNo: 5
+ Tag1:
+ MsgType: KRB_ERROR (30)
+ Tag4:
+ Stime: 09/15/2008 15:43:10 UTC
+ Tag5:
+ SuSec: 225249
+ Tag6:
+ ErrorCode: KDC_ERR_PREAUTH_REQUIRED (25)
+ Tag9:
- Realm: 2008DOMAIN2.COM
 + Realm: 2008DOMAIN2.COM
+ TagA:
- Sname: krbtgt/2008DOMAIN2.COM
 + SequenceHeader:
 + Tag0:
 + NameType: NT-SRV-INST (2)
 + Tag1:
 + SequenceOfHeader:
 + NameString: krbtgt
 + NameString: 2008DOMAIN2.COM
+ TagC:
- EData:
 + OctetStringHeader:
 - MethodData:
  + SequenceOfHeader:
  + Padata: PA-ETYPE-INFO2 (19)
  + Padata: PA-ENC-TIMESTAMP (2)
  + Padata: PA-PK-AS-REQ (16)
  + Padata: PA-PK-AS-REP_OLD (15)
```

5.7.2 Kerberos: AS Request Sname: krbtgt/ (Success)

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=59954, DstPort=Kerberos(88)
- Kerberos: AS Request Cname: Administrator Realm: 2008DOMAIN2.COM Sname: krbtgt/2008DOMAIN2.COM
  + Length: Length = 318
  - AsReq: Kerberos AS Request
   + ApplicationTag:
   - KdcReq: KRB_AS_REQ (10)
    + SequenceHeader:
    + Tag1:
    + Pvno: 5
    + Tag2:
    + MsgType: KRB_AS_REQ (10)
    + Tag3:
    + PaData:
    + Tag4:
    - ReqBody:
     + SequenceHeader:
     + Tag0:
     - KdcOptions: 0x40810010
      + KerberosFlagsHeader:
      + Padding:
      - KrbFlags: 0x40810010
         Reserved:              (0...............................)
         Forwardable:           (.1..............................) Ticket to be issued is to have its FORWARDABLE flag
                                                                   set
         Forwarded:             (..0.............................) This is not a request for forwarding
         Proxiable:             (...0............................) Ticket to be issued is not to have its PROXIABLE
                                                                   flag set
         Proxy:                 (....0...........................) This is not a request for a proxy
         AllowPostDate:         (.....0..........................) Ticket to be issued is not to have its MAY_POSTDATE
```

```
                                                              flag set
    PostDated:             (......0.........................) This is not a request for a postdated ticket
    Unused7:               (.......0........................)
    Renewable:             (........1.......................) Ticket to be issued is to have its RENEWABLE flag
                                                              set
    Unused9:               (.........0......................)
    Unused10:              (..........0.....................)
    OptHardwareAuth:       (...........0....................)
    Unused12:              (............0...................)
    Unused13:              (.............0..................)
    CnameInAddlTkt:        (..............0.................) This is not a request for S4U2proxy functionality
    Canonicalize:          (...............1................)
    Unused16:              (................0000000000......)
    DisableTransitedCheck: (..........................0.....) Checking of the transited field is enabled
    RenewableOk:           (...........................1....) Indicates that the renewable ticket is acceptable if
                                                              a ticket with the requested life cannot be provided
    EncTktInSkey:          (............................0...) Ticket for the end server is to be encrypted in the
                                                              session key
    Unused29:              (.............................0..)
    Renew:                 (..............................0.) Present request is not for a renewal
    Validate:              (...............................0) Request is not to validate a postdated ticket
+ Tag1:
- Cname: Administrator
 + SequenceHeader:
 + Tag0:
 + NameType: NT-PRINCIPAL (1)
 + Tag1:
 + SequenceOfHeader:
 + NameString: Administrator
+ Tag2: 0x1
- Realm: 2008DOMAIN2.COM
 + Realm: 2008DOMAIN2.COM
+ Tag3:
- Sname: krbtgt/2008DOMAIN2.COM
 + SequenceHeader:
      + Tag0:
      + NameType: NT-SRV-INST (2)
      + Tag1:
      + SequenceOfHeader:
      + NameString: krbtgt
      + NameString: 2008DOMAIN2.COM
     + Tag5: 0x1
     + Till: 09/13/2037 02:48:05 UTC
     + Tag6:
     + Rtime: 09/13/2037 02:48:05 UTC
     + Tag7:
     + Nonce: 1075326609 (0x40182E91)
     + Tag8:
     - Etype:
      + SequenceOfHeader:
      + EType: aes256-cts-hmac-sha1-96 (18)
      + EType: aes128-cts-hmac-sha1-96 (17)
      + EType: rc4-hmac (23)
      + EType: des-cbc-md5 (3)
      + EType: des-cbc-crc (1)
      + EType: rc4-hmac-exp (24)
      + EType: rc4 hmac old exp (0xff79)
     + Tag9:
     - Addresses:
      + SequenceOfHeader:
      + Address: 2008DOMAIN1DC1

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...A...., SrcPort=Kerberos(88), DstPort=59954
- Kerberos: AS Response Ticket[Realm: 2008DOMAIN2.COM, Sname: krbtgt/2008DOMAIN2.COM]
  + Length: Length = 1531
  - AsRep: Kerberos AS Response
   + ApplicationTag:
   - KdcRep: KRB_AS_REP (11)
    + SequenceHeader:
```

```
+ Tag0:
+ PvNo: 5
+ Tag1:
+ MsgType: KRB_AS_REP (11)
+ Tag3:
- Crealm: 2008DOMAIN2.COM
 + Realm: 2008DOMAIN2.COM
+ Tag4:
- Cname: Administrator
 + SequenceHeader:
 + Tag0:
 + NameType: NT-PRINCIPAL (1)
 + Tag1:
 + SequenceOfHeader:
 + NameString: Administrator
+ Tag5:
- Ticket: Realm: 2008DOMAIN2.COM, Sname: krbtgt/2008DOMAIN2.COM
 + ApplicationTag:
 + SequenceHeader:
 + Tag0:
 + TktVno: 5
 + Tag1:
 - Realm: 2008DOMAIN2.COM
  + Realm: 2008DOMAIN2.COM
 + Tag2: 0x1
 - Sname: krbtgt/2008DOMAIN2.COM
  + SequenceHeader:
  + Tag0:
  + NameType: NT-SRV-INST (2)
  + Tag1:
  + SequenceOfHeader:
  + NameString: krbtgt
  + NameString: 2008DOMAIN2.COM
 + Tag3: 0x1
 + EncPart:
+ Tag6:
- EncPart:
 + SequenceHeader:
 + Tag0:
 + EType: rc4-hmac (23)
 + Tag1:
 + KvNo: 1
 + Tag2:
 + Cipher: ...
```

5.7.3 Kerberos: TGS Request Realm: Sname: cifs/

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...A...., SrcPort=59955, DstPort=Kerberos(88)
- Kerberos: TGS Request Realm: 2008DOMAIN2.COM Sname: cifs/2008DOMAIN2DC1.2008DOMAIN2.COM
  + Length: Length = 1613
  - TgsReq: Kerberos TGS Request
   + ApplicationTag:
   - KdcReq: KRB_TGS_REQ (12)
    + SequenceHeader:
    + Tag1:
    + Pvno: 5
    + Tag2:
    + MsgType: KRB_TGS_REQ (12)
    + Tag3:
    + PaData:
    + Tag4:
    - ReqBody:
     + SequenceHeader:
```

```
+ Tag0:
- KdcOptions: 0x40810000
 + KerberosFlagsHeader:
 + Padding:
 - KrbFlags: 0x40810000
    Reserved:              (0...............................)
    Forwardable:           (.1..............................) Ticket to be issued is to have its FORWARDABLE flag
                                                              set
    Forwarded:             (..0.............................) This is not a request for forwarding
    Proxiable:             (...0............................) Ticket to be issued is not to have its PROXIABLE
                                                              flag set
    Proxy:                 (....0...........................) This is not a request for a proxy
    AllowPostDate:         (.....0..........................) Ticket to be issued is not to have its MAY_POSTDATE
                                                              flag set
    PostDated:             (......0.........................) This is not a request for a postdated ticket
    Unused7:               (.......0........................)
    Renewable:             (........1.......................) Ticket to be issued is to have its RENEWABLE flag
                                                              set
    Unused9:               (.........0......................)
    Unused10:              (..........0.....................)
    OptHardwareAuth:       (...........0....................)
    Unused12:              (............0...................)
    Unused13:              (.............0..................)
    CnameInAddlTkt:        (..............0.................) This is not a request for S4U2proxy functionality
    Canonicalize:          (...............1................)
    Unused16:              (................0000000000......)
    DisableTransitedCheck: (..........................0.....) Checking of the transited field is enabled
    RenewableOk:           (...........................0....) Renewable ticket is not acceptable
    EncTktInSkey:          (............................0...) Ticket for the end server is to be encrypted in the
                                                              session key
    Unused29:              (.............................0..)
    Renew:                 (..............................0.) Present request is not for a renewal
    Validate:              (...............................0) Request is not to validate a postdated ticket
+ Tag2: 0x1
- Realm: 2008DOMAIN2.COM
```

```
      + Realm: 2008DOMAIN2.COM
     + Tag3:
     - Sname: cifs/2008DOMAIN2DC1.2008DOMAIN2.COM
      + SequenceHeader:
      + Tag0:
      + NameType: NT-SRV-INST (2)
      + Tag1:
      + SequenceOfHeader:
      + NameString: cifs
      + NameString: 2008DOMAIN2DC1.2008DOMAIN2.COM
     + Tag5: 0x1
     + Till: 09/13/2037 0::
     + Tag7:

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...A...., SrcPort=Kerberos(88), DstPort=59955
- Kerberos: TGS Response Cname: Administrator
  + Length: Length = 1656
  - TgsRep: Kerberos TGS Response
   + ApplicationTag:
   - KdcRep: KRB_TGS_REP (13)
    + SequenceHeader:
    + Tag0:
    + PvNo: 5
    + Tag1:
    + MsgType: KRB_TGS_REP (13)
    + Tag3:
    - Crealm: 2008DOMAIN2.COM
    + Tag4:
    - Cname: Administrator
     + SequenceHeader:
     + Tag0:
     + NameType: NT-PRINCIPAL (1)
     + Tag1:
     + SequenceOfHeader:
```

```
     + NameString: Administrator
    + Tag5:
    - Ticket: Realm: 2008DOMAIN2.COM, Sname: cifs/2008DOMAIN2DC1.2008DOMAIN2.COM
     + ApplicationTag:
     + SequenceHeader:
     + Tag0:
     + TktVno: 5
     + Tag1:
     - Realm: 2008DOMAIN2.COM
      + Realm: 2008DOMAIN2.COM
     + Tag2: 0x1
     - Sname: cifs/2008DOMAIN2DC1.2008DOMAIN2.COM
      + SequenceHeader:
      + Tag0:
      + NameType: NT-SRV-INST (2)
      + Tag1:
      + SequenceOfHeader:
      + NameString: cifs
      + NameString: 2008DOMAIN2DC1.2008DOMAIN2.COM
     + Tag3: 0x1
     - EncPart:
      + SequenceHeader:
      + Tag0:
      + EType: aes256-cts-hmac-sha1-96 (18)
      + Tag1:
      + KvNo: 3
      + Tag2:
      + Cipher: ...
    + Tag6:
    - EncPart:
     + SequenceHeader:
     + Tag0:
     + EType: rc4-hmac (23)
     + Tag2:
     + Cipher: ...
```

5.7.4 Kerberos: TGS Request Sname: krbtgt/2008DOMAIN2.COM

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...A...., SrcPort=59355, DstPort=Kerberos(88)
- Kerberos: TGS Request Realm: 2008DOMAIN2.COM Sname: krbtgt/2008DOMAIN2.COM
  + Length: Length = 1477
  - TgsReq: Kerberos TGS Request
   + ApplicationTag:
   - KdcReq: KRB_TGS_REQ (12)
    + SequenceHeader:
    + Tag1:
    + Pvno: 5
    + Tag2:
    + MsgType: KRB_TGS_REQ (12)
    + Tag3:
    - PaData:
     + SequenceOfHeader:
     + PaData: PA-TGS-REQ (1)
     - PaData: Unknown PADATA Type (165)
      + SequenceHeader:
      + Tag1:
      + PaDataType: Unknown PADATA Type (165)
      + Tag2:
      + PadataValue:
    + Tag4:
    - ReqBody:
     + SequenceHeader:
     + Tag0:
     - KdcOptions: 0x60810010
```

```
 + KerberosFlagsHeader:
 - Padding:
    Padding: 0 (0x0)
 - KrbFlags: 0x60810010
    Reserved:              (0...............................)
    Forwardable:           (.1..............................) Ticket to be issued is to have its FORWARDABLE flag
                                                              set
    Forwarded:             (..1.............................) Indicates that this is a request for forwarding
    Proxiable:             (...0............................) Ticket to be issued is not to have its PROXIABLE
                                                              flag set
    Proxy:                 (....0...........................) This is not a request for a proxy
    AllowPostDate:         (.....0..........................) Ticket to be issued is not to have its MAY_POSTDATE
                                                              flag set
    PostDated:             (......0.........................) This is not a request for a postdated ticket
    Unused7:               (.......0........................)
    Renewable:             (........1.......................) Ticket to be issued is to have its RENEWABLE flag
                                                              set
    Unused9:               (.........0......................)
    Unused10:              (..........0.....................)
    OptHardwareAuth:       (...........0....................)
    Unused12:              (............0...................)
    Unused13:              (.............0..................)
    CnameInAddlTkt:        (..............0.................) This is not a request for S4U2proxy functionality
    Canonicalize:          (...............1................)
    Unused16:              (................0000000000......)
    DisableTransitedCheck: (..........................0.....) Checking of the transited field is enabled
    RenewableOk:           (...........................1....) Indicates that the renewable ticket is acceptable if
                                                              a ticket with the requested life cannot be provided
    EncTktInSkey:          (............................0...) Ticket for the end server is to be encrypted in the
                                                              session key
    Unused29:              (.............................0..)
    Renew:                 (..............................0.) Present request is not for a renewal
    Validate:              (...............................0) Request is not to validate a postdated ticket
+ Tag2: 0x1
+ Realm: 2008DOMAIN2.COM
```

```
     + Tag3:
     + Sname: krbtgt/2008DOMAIN2.COM
     + Tag5: 0x1
     + Till: 09/13/2037 0::
     + Tag7:

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...A...., SrcPort=Kerberos(88), DstPort=59355
- Kerberos: TGS Response Cname: Administrator
  + Length: Length = 1474
  - TgsRep: Kerberos TGS Response
   + ApplicationTag:
   - KdcRep: KRB_TGS_REP (13)
    + SequenceHeader:
    + Tag0:
    + PvNo: 5
    + Tag1:
    + MsgType: KRB_TGS_REP (13)
    + Tag3:
    + Crealm: 2008DOMAIN2.COM
    + Tag4:
    + Cname: Administrator
    + Tag5:
    - Ticket: Realm: 2008DOMAIN2.COM, Sname: krbtgt/2008DOMAIN2.COM
     + ApplicationTag:
     + SequenceHeader:
     + Tag0:
     + TktVno: 5
     + Tag1:
     + Realm: 2008DOMAIN2.COM
     + Tag2: 0x1
     + Sname: krbtgt/2008DOMAIN2.COM
     + Tag3: 0x1
     - EncPart:
      + SequenceHeader:
```

```
      + Tag0:
      + EType: rc4-hmac (23)
      + Tag1:
      + KvNo: 2
      + Tag2:
      + Cipher: ...
    + Tag6:
    - EncPart:
     + SequenceHeader:
     + Tag0:
     + EType: rc4-hmac (23)
     + Tag2:
     + Cipher: ...
```

5.7.5 Kerberos: TGS Request Realm: Sname: LDAP/

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...A...., SrcPort=60331, DstPort=Kerberos(88)
- Kerberos: TGS Request Realm: 2008DOMAIN2.COM Sname: LDAP/2008DOMAIN2DC1.2008DOMAIN2.COM
  + Length: Length = 1613
  - TgsReq: Kerberos TGS Request
   + ApplicationTag:
   - KdcReq: KRB_TGS_REQ (12)
    + SequenceHeader:
    + Tag1:
    + Pvno: 5
    + Tag2:
    + MsgType: KRB_TGS_REQ (12)
    + Tag3:
```

```
- PaData:
 + SequenceOfHeader:
 - PaData: PA-TGS-REQ (1)
  + SequenceHeader:
  + Tag1:
  + PaDataType: PA-TGS-REQ (1)
  + Tag2:
  + OctetStringHeader:
  - KrbApReq: KRB_AP_REQ (14)
   + ApplicationTag:
   + SequenceHeader:
   + Tag0:
   + PvNo: 5
   + Tag1:
   + MsgType: KRB_AP_REQ (14)
   + Tag2: 0x1
   + ApOptions:
   + Tag3:
   - Ticket: Realm: 2008DOMAIN2.COM, Sname: krbtgt/2008DOMAIN2.COM
    + ApplicationTag:
    + SequenceHeader:
    + Tag0:
    + TktVno: 5
    + Tag1:
    + Realm: 2008DOMAIN2.COM
    + Tag2: 0x1
    + Sname: krbtgt/2008DOMAIN2.COM
    + Tag3: 0x1
    - EncPart:
     + SequenceHeader:
     + Tag0:
     + EType: rc4-hmac (23)
     + Tag1:
     + KvNo: 2
     + Tag2:
```

```
     + Cipher: ...
   + Tag4:
   + Authenticator:
+ Tag4:
- ReqBody:
 + SequenceHeader:
 + Tag0:
 - KdcOptions: 0x40810000
  + KerberosFlagsHeader:
  + Padding:
  - KrbFlags: 0x40810000
     Reserved:              (0...............................)
     Forwardable:           (.1..............................) Ticket to be issued is to have its FORWARDABLE flag
                                                               set
     Forwarded:             (..0.............................) This is not a request for forwarding
     Proxiable:             (...0............................) Ticket to be issued is not to have its PROXIABLE
                                                               flag set
     Proxy:                 (....0...........................) This is not a request for a proxy
     AllowPostDate:         (.....0..........................) Ticket to be issued is not to have its MAY_POSTDATE
                                                               flag set
     PostDated:             (......0.........................) This is not a request for a postdated ticket
     Unused7:               (.......0........................)
     Renewable:             (........1.......................) Ticket to be issued is to have its RENEWABLE flag
                                                               set
     Unused9:               (.........0......................)
     Unused10:              (..........0.....................)
     OptHardwareAuth:       (...........0....................)
     Unused12:              (............0...................)
     Unused13:              (.............0..................)
     CnameInAddlTkt:        (..............0.................) This is not a request for S4U2proxy functionality
     Canonicalize:          (...............1................)
     Unused16:              (................0000000000......)
     DisableTransitedCheck: (..........................0.....) Checking of the transited field is enabled
     RenewableOk:           (...........................0....) Renewable ticket is not acceptable
     EncTktInSkey:          (............................0...) Ticket for the end server is to be encrypted in the
```

```
                                                                   session key
         Unused29:              (..............................0..)
         Renew:                 (...............................0.) Present request is not for a renewal
         Validate:              (................................0) Request is not to validate a postdated ticket
     + Tag2: 0x1
     + Realm: 2008DOMAIN2.COM
     + Tag3:
     + Sname: LDAP/2008DOMAIN2DC1.2008DOMAIN2.COM
     + Tag5: 0x1
     + Till: 09/13/2037 0::
     + Tag7:

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...A...., SrcPort=Kerberos(88), DstPort=60331
- Kerberos: TGS Response Cname: Administrator
  + Length: Length = 1656
  - TgsRep: Kerberos TGS Response
   + ApplicationTag:
   - KdcRep: KRB_TGS_REP (13)
    + SequenceHeader:
    + Tag0:
    + PvNo: 5
    + Tag1:
    + MsgType: KRB_TGS_REP (13)
    + Tag3:
    + Crealm: 2008DOMAIN2.COM
    + Tag4:
    + Cname: Administrator
    + Tag5:
    - Ticket: Realm: 2008DOMAIN2.COM, Sname: LDAP/2008DOMAIN2DC1.2008DOMAIN2.COM
     + ApplicationTag:
     + SequenceHeader:
     + Tag0:
     + TktVno: 5
     + Tag1:
```

```
     + Realm: 2008DOMAIN2.COM
     + Tag2: 0x1
     + Sname: LDAP/2008DOMAIN2DC1.2008DOMAIN2.COM
     + Tag3: 0x1
     - EncPart:
      + SequenceHeader:
      + Tag0:
      + EType: aes256-cts-hmac-sha1-96 (18)
      + Tag1:
      + KvNo: 3
      + Tag2:
      + Cipher: ...
    + Tag6:
    - EncPart:
     + SequenceHeader:
     + Tag0:
     + EType: rc4-hmac (23)
     + Tag2:
     + Cipher: ...
```

5.8 LDAP

5.8.1 LDAP: Search Request

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60332, DstPort=LDAP(389)
- Ldap: Search Request, MessageID: 88, BaseObject: NULL, SearchScope: base Object, SearchAlias: neverDerefAliases
  - Parser: Search Request, MessageID: 88
```

```
   + ParserHeader:
   + MessageID: 88
   + OperationHeader: Search Request, 3(0x3)
   - SearchRequest: BaseDN: NULL, SearchScope: base Object, SearchAlias: neverDerefAliases
    + BaseObject: NULL
    + Scope: base Object
    + Alias: neverDerefAliases
    + SizeLimit: No Limit
    + TimeLimit: 120 seconds
    + TypesOnly: False
    + Filter: (objectclass Present)
    - Attributes: ( subschemaSubentry )( dsServiceName )( namingContexts )( defaultNamingContext )
                  ( schemaNamingContext )( configurationNamingContext )( rootDomainNamingContext )( supportedControl )
                  ( supportedLDAPVersion )( supportedLDAPPolicies )( supportedSASLMec
     + AttributeSelectionHeader:
     + Attribute: subschemaSubentry
     + Attribute: dsServiceName
     + Attribute: namingContexts
     + Attribute: defaultNamingContext
     + Attribute: schemaNamingContext
     + Attribute: configurationNamingContext
     + Attribute: rootDomainNamingContext
     + Attribute: supportedControl
     + Attribute: supportedLDAPVersion
     + Attribute: supportedLDAPPolicies
     + Attribute: supportedSASLMechanisms
     + Attribute: dnsHostName
     + Attribute: ldapServiceName
     + Attribute: serverName
     + Attribute: supportedCapabilities

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...A...., SrcPort=LDAP(389), DstPort=60332
- Ldap: Search Result Entry, MessageID: 88
  - Parser: Search Result Entry, MessageID: 88
```

```
+ ParserHeader:
+ MessageID: 88
+ OperationHeader: Search Result Entry, 4(0x4)
- SearchResultEntry: NULL
 + ObjectName: NULL
 - Attributes: 9 Partial Attributes
  + SequenceHeader:
  - PartialAttribute: subschemaSubentry=( CN=Aggregate,CN=Schema,CN=Configuration,DC=2008DOMAIN2,DC=COM )
   + PartialAttributeHeader: 0x1
   + Type: subschemaSubentry
   + AttributeValuesHeader:
   + Attribute: CN=Aggregate,CN=Schema,CN=Configuration,DC=2008DOMAIN2,DC=COM
  - PartialAttribute: dsServiceName=( CN=NTDS Settings,CN=2008DOMAIN2DC1,
                                      CN=Servers,CN=Default-First-Site-Name,
                                      CN=Sites,CN=Configuration,DC=2008DOMAIN2,DC=COM )
   + PartialAttributeHeader: 0x1
   + Type: dsServiceName
   + AttributeValuesHeader:
   + Attribute: CN=NTDS Settings,CN=2008DOMAIN2DC1,CN=Servers,
                CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=2008DOMAIN2,DC=COM
  - PartialAttribute: namingContexts=( DC=2008DOMAIN2,DC=COM )( CN=Configuration,DC=2008DOMAIN2,DC=COM )
                                     ( CN=Schema,CN=Configuration,DC=2008DOMAIN2,DC=COM )
                                     ( DC=DomainDnsZones,DC=2008DOMAIN2,DC=COM )
                                     ( DC=ForestDnsZones,DC=2008DOMAIN2,DC=COM )
   + PartialAttributeHeader: 0x1
   + Type: namingContexts
   + AttributeValuesHeader:
   + Attribute: DC=2008DOMAIN2,DC=COM
   + Attribute: CN=Configuration,DC=2008DOMAIN2,DC=COM
   + Attribute: CN=Schema,CN=Configuration,DC=2008DOMAIN2,DC=COM
   + Attribute: DC=DomainDnsZones,DC=2008DOMAIN2,DC=COM
   + Attribute: DC=ForestDnsZones,DC=2008DOMAIN2,DC=COM
  - PartialAttribute: defaultNamingContext=( DC=2008DOMAIN2,DC=COM )
   + PartialAttributeHeader: 0x1
   + Type: defaultNamingContext
```

```
      + AttributeValuesHeader:
      + Attribute: DC=2008DOMAIN2,DC=COM
     - PartialAttribute: schemaNamingContext=( CN=Schema,CN=Configuration,DC=2008DOMAIN2,DC=COM )
      + PartialAttributeHeader: 0x1
      + Type: schemaNamingContext
      + AttributeValuesHeader:
      + Attribute: CN=Schema,CN=Configuration,DC=2008DOMAIN2,DC=COM
     - PartialAttribute: configurationNamingContext=( CN=Configuration,DC=2008DOMAIN2,DC=COM )
      + PartialAttributeHeader: 0x1
      + Type: configurationNamingContext
      + AttributeValuesHeader:
      + Attribute: CN=Configuration,DC=2008DOMAIN2,DC=COM
     - PartialAttribute: rootDomainNamingContext=( DC=2008DOMAIN2,DC=COM )
      + PartialAttributeHeader: 0x1
      + Type: rootDomainNamingContext
      + AttributeValuesHeader:
      + Attribute: DC=2008DOMAIN2,DC=COM
     - PartialAttribute: supportedControl=( ... )
      + PartialAttributeHeader: 0x1
      + Type: supportedControl
      + AttributeValuesHeader:
      + Attribute: 1.2.840.113556.1.4.319
      + Attribute: 1.2.840.113556.1.4.801
      + Attribute: 1.2.840.113556.1.4.473
      + Attribute: 1.2.840.113556.1.4.528
      + Attribute: 1.2.840.113556.1.4.417
      + Attribute: 1.2.840.113556.1.4.619
      + Attribute: 1.2.840.113556.1.4.841
      + Attribute: 1.2.840.113556.1.4.529
      + Attribute: 1.2.840.113556.1.4.805
      + Attribute: 1.2.840.113556.1.4.521
      + Attribute: 1.2.840.113556.1.4.970
      + Attribute: 1.2.840.113556.1.4.1338
      + Attribute: 1.2.840.113556.1.4.474
      + Attribute: 1.2.840.113556.1.4.1339
      + Attribute: 1.2.840.113556.1.4.1340
      + Attribute: 1.2.840.113556.1.4.1413
      + Attribute: 2.16.840.1.113730.3.4.9
      + Attribute: 2.16.840.1.113730.3.4.10
      + Attribute: 1.2.840.113556.1.4.1504
      + Attribute: 1.2.840.113556.1.4.1852
      + Attribute: 1.2.840.113556.1.4.802
      + Attribute: 1.2.840.113556.1.4.1907
      + Attribute: 1.2.840.113556.1.4.1948
      + Attribute: 1.2.840.113556.1.4.1974
      + Attribute: 1.2.840.113556.1.4.1341
      + Attribute: 1.2.840.113556.1.4.2026
```

5.8.2 LDAP: Bind Request

```
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...A...., SrcPort=60332, DstPort=LDAP(389)
- Ldap: Bind Request, MessageID: 90, Version: 3
  - Parser: Bind Request, MessageID: 90
   + ParserHeader:
   + MessageID: 90
   + OperationHeader: Bind Request, 0(0)
   - BindRequest: Version:3, Name:NULL, Authentication type = sasl
    + Version: 3
    + Name: NULL
    - authentication: Authentication type = sasl
     + AuthenticationTypeHeader: Authentication type = sasl
     - Credentials:
      + Mechanism: GSS-SPNEGO
```

```
- Credentials:
 - GSSSpnegoCredentials:
  + Header:
  - GSS_Spnego:
   + ApplicationHeader:
   + ThisMech: SpnegoToken (1.3.6.1.5.5.2)
   - InnerContextToken: 0x1
    - SpnegoToken: 0x1
     + Tag0:
     - NegTokenInit: 0x1
      + SequenceHeader:
      + Tag0:
      + MechTypes:
      + Tag2:
      + OctetStringHeader:
      - MechToken: 0x1
       - MsKerberosToken: 0x1
        - GssApi:
         + ApplicationHeader:
         + ThisMech: KerberosToken (1.2.840.113554.1.2.2)
         - InnerContextToken: 0x1
          - KerberosToken: 0x1
             Krb5tokId: Krb5ApReq (0x100)
           - ApReq: KRB_AP_REQ (14)
            + ApplicationTag:
            + SequenceHeader:
            + Tag0:
            + PvNo: 5
            + Tag1:
            + MsgType: KRB_AP_REQ (14)
            + Tag2: 0x1
            + ApOptions:
            + Tag3:
            - Ticket: Realm: 2008DOMAIN2.COM, Sname: LDAP/2008DOMAIN2DC1.2008DOMAIN2.COM
             + ApplicationTag:
                   + SequenceHeader:
                   + Tag0:
                   + TktVno: 5
                   + Tag1:
                   + Realm: 2008DOMAIN2.COM
                   + Tag2: 0x1
                   + Sname: LDAP/2008DOMAIN2DC1.2008DOMAIN2.COM
                   + Tag3: 0x1
                   - EncPart:
                    + SequenceHeader:
                    + Tag0:
                    + EType: aes256-cts-hmac-sha1-96 (18)
                    + Tag1:
                    + KvNo: 3
                    + Tag2:
                    + Cipher: ...
                  + Tag4:
                  - Authenticator:
                   + SequenceHeader:
                   + Tag0:
                   + EType: aes256-cts-hmac-sha1-96 (18)
                   + Tag2:
                   + Cipher: ...

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=LDAP(389), DstPort=60332
- Ldap: Bind Response, MessageID: 90, Status: Success
  - Parser: Bind Response, MessageID: 90
   + ParserHeader:
   + MessageID: 90
   + OperationHeader: Bind Response, 1(0x1)
   - BindResponse: Status: Success, MatchedDN: NULL, ErrorMessage: NULL
    + Result: Status: Success, MatchedDN: NULL, ErrorMessage: NULL
    - ServerSaslCreds:
     + Sequence_Header:
     - GSS_Spnego:
      + Tag1:
      - NegTokenResp: 0x1
       + SequenceHeader:
       + Tag0:
       + NegState: accept-completed (0)
       + Tag1:
       + SupportedMech: MsKerberosToken (1.2.840.48018.1.2.2)
       + Tag2:
       - ResponseToken:
        + OctetStringHeader:
        - SecurityBlob: 0x1
         - MsKerberosToken: 0x1
          - GssApi:
           + ApplicationHeader:
           + ThisMech: KerberosToken (1.2.840.113554.1.2.2)
           - InnerContextToken: 0x1
            - KerberosToken: 0x1
               Krb5tokId: Krb5ApRep (0x200)
             - ApRep: KRB_AP_REP (15)
              + ApplicationTag:
              + SequenceHeader:
              + Tag0:
              + PvNo: 5
              + Tag1:
              + MsgType: KRB_AP_REP (15)
              + Tag2: 0x1
              - AuthorizationData:
               + SequenceHeader:
               + Tag0:
               + EType: aes256-cts-hmac-sha1-96 (18)
               + Tag2:
               + Cipher: ...

+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60332, DstPort=LDAP(389)
- Ldap:
  - SASLBuffer:
     BufferLength: 145 (0x91)
   - GssapiKrb5:
      Krb5tokId: GSS_Wrap (0x504)
    - Krb5GssV2Wrap:
     + Flags: 6 (0x6)
       Filler: 255 (0xFF)
       EC: 0 (0x0)
       RRC: 28 (0x1C)
       SndSeq: 869632202 (0x33D588CA)
       EncryptedData: Binary Large Object (129 Bytes)

+ Ipv4: Src = 10.237.0.22, Dest = 10.237.0.21
+ Tcp: Flags=...AP..., SrcPort=LDAP(389), DstPort=60332
- Ldap:
  - SASLBuffer:
     BufferLength: 175 (0xAF)
   - GssapiKrb5:
      Krb5tokId: GSS_Wrap (0x504)
    - Krb5GssV2Wrap:
     + Flags: 7 (0x7)
       Filler: 255 (0xFF)
       EC: 0 (0x0)
       RRC: 28 (0x1C)
       SndSeq: 869720019 (0x33D6DFD3)
       EncryptedData: Binary Large Object (159 Bytes)
.
.
.
+ Ipv4: Src = 10.237.0.21, Dest = 10.237.0.22
+ Tcp: Flags=...AP..., SrcPort=60332, DstPort=LDAP(389)
- Ldap:
  - SASLBuffer:
     BufferLength: 71 (0x47)
   - GssapiKrb5:
      Krb5tokId: GSS_Wrap (0x504)
    - Krb5GssV2Wrap:
     + Flags: 6 (0x6)
       Filler: 255 (0xFF)
       EC: 0 (0x0)
       RRC: 28 (0x1C)
       SndSeq: 869632206 (0x33D588CE)
       EncryptedData: Binary Large Object (55 Bytes)
```

6 Summary of details