- **TTTracer.exe –** Use this tool to capture a trace of your target process.

```
Usage: tttracer [options] [mode] [PID | program [<arguments>]]

Options:
 -?                Display this help.
 -help             Display this help.
 -quiet            Do not display any standard output.
 -noRing           Take a full trace of the guest process (default).
 -ring             Trace to a ring buffer.
 -maxFile <size>   Maximum size of the trace file in MB.  When in full trace
                   mode the default is 1024GB and the minimum value is 1MB.
                   When in ring buffer mode the default is 16MB, the minimum
                   value is 1MB, and the maximum value is 2048MB.
 -timer <seconds>  Stops recording after the specified amount of time.
 -tExit <ecode>    (Only with -timer) Forces the application to terminate with
                   the specified exit code after the timer runs out.
 -noUI             Disables the UI for manual control of recording.
 -out <file>       Specify a trace file name or a directory.  If a file, the
                   tracer will replace the first instance of '%' with a
                   version number.  By default the executable's base name with
                   a version number is used to prefix the trace file name.
 -console <file>   Re-direct console output to the specified file or directory.
                   <file> format is similar to format of -out.
 -saveCrash <file> If the guest process hits an unhandled exception,
                   exit the process and save the trace file to
                   <file>.%.crash.  Do not combine with -out.
 -children         Trace through family of child processes.
 -passThroughExit  Pass the guest process exit value through as the
                   tracer's exit value.
 -ni               Attach to a process in non-interactive mode.  The tracer
                   cannot attach to a waiting/sleeping process, so -ni prevents
                   timing out while waiting for the guest.
 -bg               Attach to a process in non-interactive mode and return
                   control to the console after it starts tracing.
 -tracingOff       Starts application with trace recording off.  You can
                   use the UI to turn tracing on.
 -e2e <depth>      Make the RD process a start point for E2E tracing.
 -context <name>   Launches the guest process with the security context
                   of the passed in process name.  The process must
                   be in the same session as this client.  This
                   feature is only supported on Vista+ releases.
 -dumpModules      Dumps a copy of every loaded module image into the trace
                   file.  This option may significantly increase the size of
                   the trace file.
 -dumpFull         In addition to dumping every loaded module image into the
                   trace file, takes a snapshot of the guest process on attach.
 -parent <name>    Use with -onLaunch to specify a currently running parent
                   process when the traced process will run with low privileges.
 -fastAtomicOps    Loosen the restriction that atomic operations on the same
                   address will replay in the same order they executed live.

Modes:
 -launch           Launch and trace the program (default).  This is the only
                   mode that uses the program arguments.
 -attach <PID>     Attach to a running process specified by process ID.
 -loadOnly <PID>   Loads TTT into the process, but does not start a trace
                   session.  This is useful if the client starting the trace
                   session is not running with high enough privileges to load
                   TTT into the process.
 -onLaunch         Trace programs or services each time they are started
                   (until reboot).  When combining this with -out, use the
                   full pathname.
 -persistent       Trace programs or services each time they are started
                   (forever).  When combining this with -out, use the
                   full pathname.
 -delete           Stop future tracing of a program previously specified
                   with -onLaunch or -persistent.  Does not stop current
                   tracing.
 -autoStart        If tracing stops in a guest process, automatically restart
```

```
                  it if the guest is still active.  Use -stop all to cancel
                  auto mode.

Control:
 -stop            Stop tracing the process specified (name, PID or "all").
 -terminate <code> <PID>
                  Terminate with the specified exit code a process
                  specified by process ID.
 -status          Show programs scheduled for future tracing.
 -wait <timeout>  Wait for up to the amount of seconds specified for all
                  trace sessions on the system to end.  Specify -1 to wait
                  infinitely.
 -mark "<string>" <PID>
                  Signal a guest process to insert the string into its
                  trace file.  The string must be less than 32 characters.
 -initialize      Manually initialize your system for tracing.  On a x86
                  system, you can trace without administrator privileges
                  after the system is initialized.
```

- **TTTIndexer.exe –** Use this tool to add a snapshot index to your trace file.

```
Usage: TTTIndexer.exe [-delete] <trace file>
```

- **TTTester.exe –** Use this tool to validate your trace file. This tool returns exit code zero if TTT can successfully replay through the entire trace file.

```
Usage: TTTester.exe <trace file>
```

- **TTTRecover.exe –** If your trace file is not readable because the system crashed or rebooted while you were taking a trace, this utility may be able to recover the file.

```
Usage: TTTRecover.exe <trace file> <recovered trace file>
```

0. Example Scenarios

- I want to trace Notepad.

  Run "TTTracer Notepad".

- I want to trace an already running Internet Explorer.

  Find the process ID of Internet Explorer.

  Run "TTTracer -attach *processID*".

- I want to trace the first 15 seconds of the calculator when it starts.

  Run "TTTracer -timer 15 -onLaunch calc".

  This will trace calc.exe each time it starts until the machine is booted.

- I want to trace lsass.exe from its start.

  Run "TTTracer -persistent lsass.exe".

This will trace lsass.exe each time it starts until you run "TTTracer -delete lsass.exe".

- I want to trace the WinDefend service and the LocalService service group and their children from their start, and put the results in C:\test. (Vista only)

  Run "TTTracer -children -out C:\test -persistent WinDefend LocalService".

If you run TTTracer in persistent or onLaunch mode with services later, these settings will be replaced.

- I want to know what is being traced and what will trace at launch.

  Run "TTTracer -status".

- I want to stop all tracing on my system.

  Run "TTTracer –stop all".

  You may still need to use delete mode to stop future tracing from starting.