TWI3 Tools Description

**Win32dd/Win64dd - Ram Dumper**

This utility is an open source RAM dumper with support for 32 and 64 bit systems.

**MD5Deep**

This tool was written by former OSI Special Agent, and MIT graduate Jesse Kornblum. It is used by TWI to generate an MD5 Checksum of all the output files.

**Pclip**

This tool was written by Windows Forensics Analysis author Harlan Carvey, and is used to gather the contents on the Windows clipboard.

**Ostest**

This tool was written by renown Windows IT Professional Bill Stewart. It is used by TWI to gather operating system information.

**Netstat**

This utility is native to the Windows operating system and is used to gather network data such as network connections, connection status and Process IDs.

**TCPVcon**

This utility is part of the Sysinternal's Suite supported by Microsoft. It gathers information regarding process to port mappings.

**FPORT**

This tool was created by Foundstone and is supported by McAfee. Like TCPVcon, it gathers information regarding process to port mappings. This tool only support Windows NT4, 2000, and XP.

**Wget**

TWI3 uses WGET to reach out to www.checkip.dns.org and identify the host's externally facing IP address.

**Openports**

This tool was written by Diamond Console Tools and is also use to gather process to port mappings.

**RASConns**

This tool was written by renown Windows IT Professional Bill Stewart. It is used by TWI to gather current Remote Access Server connections.

**Arp**

Apr.exe is a native Windows operating system utility that is used IP to Physical address translation tables.

**NBTStat**

This tool is part of the Sysinternal's Suite by Microsoft and is used to display protocol statistics and current TCP/IP connections using NBT (NetBios over TCP/IP).

**Psloggedon**

This tool is part of the Sysinternal's Suite by Microsoft and is used to display currently logged in users.

**IPConfig**

This tool is native to the Microsoft Windows operating system and is used by TWI to gather data regarding IP address and DNS routing.

**PSList**

This tool is part of the Sysinternal's Suite by Microsoft and is used to display process listings and memory threads.

**CProcess**

This tool has been developed and is currently maintained by NirSoft. It is used by TWI to display an extremely detailed process listing.

**Tasklist**

This tool is supported by Microsoft and is used by TWI to generate a process list that contains the user name under which that process was documented.

**Tlist**

This tool is supported by Microsoft and is used by TWI to generate a process list that contains the command line argument that was used to initiate the process.

**OpenedFilesView**

This tool has been developed and is currently maintained by NirSoft. It is used by TWI to display a list of all open files on the system.

**Cmdline**

This tool was written by Diamond Console Tools and is also use to gather a history of commands issued from the Windows command line.

**Handle**

This tool is part of the Sysinternal's Suite by Microsoft. It is used by TWI to display information about open handles for every process in the system. It is used to identify the programs that have a file open, or to see the object types and names of all the handles of a program.

**PsFile**

This tool is part of the Systinternal's Suite by Microsoft. It is used by TWI to identify any files that have been opened remotely.

**Dumpwin**

This tools was written by Arjun Pednekar of Network Intelligence India. It is used by TWI to display a listing of active processes and their associated modules (dlls), modem details, network shares, and installed programs.

**DI**

This tool was written by Windows Forensic Analysis author Harlan Carvey and is used to gather drive information to include assigned drive letter and size.

**Autorunsc**

This tool is part of the Sysinternal's Suite by Microsoft. It is used by TWI to display all of the programs that are set to automatically start on reboot.

**Psservice**

This tool is part of the Sysinternal's Suite by Microsoft. It is used by TWI to display service information and configuration.

**At**

This tools is native to the Windows operating system and is used by TWI to identify if any "at" jobs are present.

**PsInfo**

This tool is part of the Sysinternal's Suite by Microsoft. It is used by TWI to display system information such as Uptime, Kernel version, product version, system root and processor speed.

**Auditpol**

This tool was written by Christopher Robert, and is used to display the system's auditing policies.

**Net**

This utility is native to the Windows operating system and is used in conjunction with the "share" switch to display current network shares on the local system.

**NTLast**

This tool was created and is currently maintained by Foundstone and is used by TWI to display login history and information.

**PsLoglist**

This tool is part of the Sysinternal's Suite by Microsoft. It is used by TWI to dump Windows event logs.

**Dumpel**

This tool is part of the Microsoft's Windows 2000 Resource Tool Kit. It is used by TWI to dump Windows event logs.

**SC**

This tool is native to the Windows operating system and is used by TWI to gather network drivers as well as display service information.

**Drivers**

This tool has been coded and is currently supported by Microsoft. It is used by TWI to display system driver information.

**GPList**

This tool was written by Arne Vidstrom of NTSecurity and is used by TWI to display applied group policies.

**Promiscdetect**

This tool was written by Arne Vidstrom of NTSecurity and is used by TWI to display the status of the Network Interface Card(s), specifically if they are in promiscuous mode or not.

**HDD**

This tool was created by Indigo Star and is used to gather data about any attached storage devices to include serial number, make, model, and size.

**USBDview**

This tool was written and is currently maintained by NirSoft. It is used to view all installed and connected USB devices on the system.

**Volume\_Dump**

This tool was written by George M. Garner Jr. of Forensic Acquisition Utilities. It is used to gather volume data from any attached storage device(s).

**LADS**

This tool was written by Frank Heyne of Frank Heyne Software. It is used by TWI to identify and list any Alternate Data Streams.

**SR**

This tool was written by Windows Forensic Analysis author Harlan Carvey and is used to gather resort point data from Windows XP systems.

**Uassist\_LV**

This tool was written by Windows Forensic Analysis author Harlan Carvey and is used to gather the User Assist Registry Key for the current user from Windows XP systems.

**Systeminfo**

This tool was written and is currently maintained by Microsoft. It displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.

**Reg**

This is utility is native to the Windows operating system and is used by TWI to extract the Windows Registry hives and NTUSER.DAT files.

**RegRipper**

This tool was written by Windows Forensic Analysis author Harlan Carvey and is used interpret the extracted Windows Registry Hives, as well as NTUSER.DAT files into a human readable format.

**FLS**

This tool was written by Brian Carrier and is currently part of The Sleuth Kit. It is used by TWI to generate a body file of the active file system. This body file is later interpreted by a second TSK utility written by Rob Lee called, Mactime. This tool converts the bodyfile into a human readable timeline.

Tool MD5 Hashes:

2f0050f870b2d49e0880334e4938d528 auditpol.exe

bcb876d992a8a454823207ab4c366f3b autorunsc.exe

2d75635f4fab479e3385dc0a1ee51f36 cmdline.exe

57e67b34dcffb7966a8e08cf5f56b416 CProcess.cfg

5af6b376e660805759683865437acbc0 CProcess.exe

e9757f1678ece31c59997c073a6527a2 cut.exe

2820f639a5e7b1c2bca5199eb8c41ce8 delay.exe

9af87e8248d0e8a518705bc40750042b di.exe

43e2b940767d4f671a7d27a7b29d8a22 drivers.exe

3c2447e278318c4e6b50d5095e7028e5 dumpel.exe

66969b541e960ecc262855effddd6e7b DumpWin.exe

dbb75488aa2fa22ba6950aead1ef30d5 fport.exe

3436eab6988e8a911895122ed1862836 gawk.exe

5185f31a90703bc7379725690fa82db7 gplist.exe

83a3d89f40a05038760110b1e6e54762 grep.exe

b2347b57ae73d52ee509d2037bf10f83 handle.exe

c07c17cc01996afe4de32a32ce1fa157 hdd.exe

d6fbc4ef77b65c3fbd137d4e6d178a66 isadmin.exe

6b8af3a2a3d9059008b55c444461ca00 lads.exe

6b854ffc12e5e2c32683a03714cf6c5d libeay32.dll

e0dc8c6bbc787b972a9a468648dbfd85 libiconv2.dll

d202baa425176287017ffe1fb5d1b77c libintl3.dll

37580b9354e984bf7c1a2b4ed7fa824b libssl32.dll

6db9565378d0268dcd88288c5e961611 listdlls.exe

81b68d181440d59c0565986abc141139 ls.exe

434037609272560d708c4b0b339e19d5 md5deep.exe

d04f7aaca2319a3bcdb2c5d5dd6f6026 MSVCP70.DLL

9972a6ed4f2388dbfa8e0a96f6f3fdf1 msvcr70.dll

b01a4d9fbb85b387dd890fca73c212d3 NetUsers.exe

1128a558328023f6006327570c4d201f ntlast.exe

d2dc88afaa26bacb0f0bb848c048d3b7 OpenedFilesView.cfg

0e98b9637d5b5c5aced291137e8b9047 OpenedFilesView.exe

77d7dbc1b29a04b63395f1fbf662ba75 openports.exe

54abe899378be7041ddc062757afaaa4 OSTest.exe

ab773b261948b8d1ded5454db66cbb41 p2x561.dll

acc5e4c705c43d0a75a4f0ea05599ba3 p2x580.dll

a236999c6d5cf814cd562cfab4bab8fa p2x588.dll

1c35d256ac672a8738d5a172c06cc125 pclip.exe

57cac848fa14ae38f14f9441f8933282 pcre3.dll

117ec27602980ae13307a7c2021a5d90 promiscdetect.exe

7f7005d2f1d9c579179807818c3ac4c7 psapi.dll

cb623488009f084ec53cb62e45cbcf72 psfile.exe

af4ecbb4470223db83e47a81bcc118ff psinfo.exe

61fd7759f215f9f88ae88525fd30af21 pslist.exe

6500c15f856bbfd0b28bd4ebf6e1662a psloggedon.exe

328ba584bd06c3083e3a66cb47779eac psloglist.exe

1c33debdb26390539bac68596ac88327 psservice.exe

1708ae5a0b54a7f0fce9d3849dd9e76a RASConns.exe

bbc3afa4512e90491787b3da837c057f regdmp.exe

0247922cf06cd595240cb21786e15b29 RegDump.exe

547c43567ab8c08eb30f6c6bacb479a3 regex2.dll

7519bf4ad24a56d1fd628ce2fec56d46 rip.exe

76bec5ddafad0b6b0eb9296aa71f3e27 sr.exe

7e16d8e09ea4a1458105ce2fa3ebf08d ssleay32.dll

305e40dee29d261d0a3dc466f2184e35 strings.exe

e8d220db959e99cefb78ceb8d12537a1 tcpvcon.exe

0a5b140fa36ff056b14724d74ed14684 tlist.exe

8d03e713ab4e4e37d73fdf51f4313d74 twi3.bat

5298ec0aaf1935e80163628dea1ab9e9 uassist\_lv.exe

9f9a9ddbb6131181a471d0930516377b USBDeview.cfg

3168affd9f6d3539a46fcf0dc2dba2ed USBDeview.exe

a12f26883d3094423fa9437538e5f716 volume\_dump.exe

aa173375c21ea31b8cc615dccb54e43b wget.exe

731bef47403066f24fd009045c343f01 win32dd.exe

fce773d6c5493a411379b55987bc8b42 win32dd.sys

f6b0e0c4492034fa6ccafddd59d2dc67 win64dd.exe

d02502510331cabe96993508c6f6edbb win64dd.sys