

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt
06:47:17.0030 6572 TDSS rootkit removing tool 2.8.16.0 Feb 11 2013 18:50:42
06:47:18.0403 6572 =====
06:47:18.0403 6572 Current date / time: 2013/03/30 06:47:18.0403
06:47:18.0403 6572 SystemInfo:
06:47:18.0403 6572
06:47:18.0403 6572 OS Version: 6.1.7600 ServicePack: 0.0
06:47:18.0403 6572 Product type: Workstation
06:47:18.0403 6572 ComputerName: BREB-HP
06:47:18.0419 6572 UserName: Breb
06:47:18.0419 6572 Windows directory: C:\windows
06:47:18.0419 6572 System windows directory: C:\windows
06:47:18.0419 6572 Processor architecture: Intel x86
06:47:18.0419 6572 Number of processors: 4
06:47:18.0419 6572 Page size: 0x1000
06:47:18.0419 6572 Boot type: Normal boot
06:47:18.0419 6572 =====
06:47:19.0261 6572 Drive \Device\Harddisk0\DR0 - Size: 0x4A85D56000 (298.09
gb), SectorsSize: 0x200, Cylinders: 0x9801, SectorsPerTrack: 0x3F,
TracksPerCylinder: 0xFF, Type 'K0', Flags 0x00000050
06:47:19.0277 6572 =====
06:47:19.0277 6572 \Device\Harddisk0\DR0:
06:47:19.0277 6572 MBR partitions:
06:47:19.0277 6572 \Device\Harddisk0\DR0\Partition1: MBR, Type 0x7, StartLBA
0x800, BlocksNum 0x96000
06:47:19.0277 6572 \Device\Harddisk0\DR0\Partition2: MBR, Type 0x7, StartLBA
0x96800, BlocksNum 0x22F96800
06:47:19.0277 6572 \Device\Harddisk0\DR0\Partition3: MBR, Type 0x7, StartLBA
0x2302D000, BlocksNum 0x1A00000
06:47:19.0277 6572 \Device\Harddisk0\DR0\Partition4: MBR, Type 0xC, StartLBA
0x24A2D000, BlocksNum 0x9FD800
06:47:19.0277 6572 =====
06:47:19.0292 6572 C: <-> \Device\Harddisk0\DR0\Partition2
06:47:19.0401 6572 E: <-> \Device\Harddisk0\DR0\Partition3
06:47:19.0417 6572 F: <-> \Device\Harddisk0\DR0\Partition4
06:47:19.0417 6572 =====
06:47:19.0417 6572 Initialize success
06:47:19.0417 6572 =====
06:47:26.0375 6332 =====
06:47:26.0375 6332 Scan started
06:47:26.0375 6332 Mode: Manual;
06:47:26.0375 6332 =====
06:47:27.0857 6332 ===== Scan system memory =====
06:47:27.0857 6332 System memory - ok
06:47:27.0857 6332 ===== Scan services =====
06:47:28.0091 6332 [ BF02F806C873ABB04B197161E8E5A316 ] 1394ohci
C:\windows\system32\DRIVERS\1394ohci.sys
06:47:28.0106 6332 1394ohci - ok
06:47:28.0137 6332 [ 10DD847C196782B0A5F05F6CDD91872E ] Accelerometer
C:\windows\system32\DRIVERS\Accelerometer.sys
06:47:28.0137 6332 Accelerometer - ok
06:47:28.0184 6332 [ F0E07D144C8685B8774BC32FC8DA4DF0 ] ACPI
C:\windows\system32\DRIVERS\ACPI.sys
06:47:28.0200 6332 ACPI - ok
06:47:28.0215 6332 [ 98D81CA942D19F7D9153B095162AC013 ] AcpiPmi
C:\windows\system32\DRIVERS\acpipmi.sys
06:47:28.0231 6332 AcpiPmi - ok
06:47:28.0247 6332 [ 21E785EBD7DC90A06391141AAC7892FB ] adp94xx
C:\windows\system32\DRIVERS\adp94xx.sys
06:47:28.0262 6332 adp94xx - ok
06:47:28.0309 6332 [ 0C676BC278D5B59FF5ABD57BBE9123F2 ] adpahci
C:\windows\system32\DRIVERS\adpahci.sys
06:47:28.0325 6332 adpahci - ok
06:47:28.0340 6332 [ 7C7B5EE4B7B822EC85321FE23A27DB33 ] adpu320
C:\windows\system32\DRIVERS\adpu320.sys
06:47:28.0340 6332 adpu320 - ok
06:47:28.0371 6332 [ 8B5EEFEEC1E6D1A72A06C526628AD161 ] AeLookupSvc
C:\windows\system32\aelupsvc.dll
06:47:28.0387 6332 AeLookupSvc - ok

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt
 06:47:28.0465 6332 [827DBC22C96EECF6D36A13162FABAFD3] AESTFilters
 C:\Program Files\IDT\WDM\AESTSRV.exe
 06:47:28.0465 6332 AESTFilters - ok
 06:47:28.0512 6332 [0DB7A48388D54D154EBEC120461A0FCD] AFD
 C:\windows\system32\drivers\afd.sys
 06:47:28.0543 6332 AFD - ok
 06:47:28.0605 6332 [7E10E3BB9B258AD8A9300F91214D67B9] AgereSoftModem
 C:\windows\system32\DRIVERS\AGRSM.sys
 06:47:28.0637 6332 AgereSoftModem - ok
 06:47:28.0683 6332 [507812C3054C21CEF746B6EE3D04DD6E] agp440
 C:\windows\system32\DRIVERS\agp440.sys
 06:47:28.0683 6332 agp440 - ok
 06:47:28.0715 6332 [8B30250D573A8F6B4BD23195160D8707] aic78xx
 C:\windows\system32\DRIVERS\djsvs.sys
 06:47:28.0715 6332 aic78xx - ok
 06:47:28.0777 6332 [18A54E132947CD98FEA9ACCC57F98F13] ALG
 C:\windows\System32\alg.exe
 06:47:28.0777 6332 ALG - ok
 06:47:28.0793 6332 [0D40BCF52EA90FC7DF2AEAB6503DEA44] aliide
 C:\windows\system32\DRIVERS\aliide.sys
 06:47:28.0793 6332 aliide - ok
 06:47:28.0808 6332 [3C6600A0696E90A463771C7422E23AB5] amdagp
 C:\windows\system32\DRIVERS\amdagp.sys
 06:47:28.0808 6332 amdagp - ok
 06:47:28.0824 6332 [CD5914170297126B6266860198D1D4F0] amdide
 C:\windows\system32\DRIVERS\amdide.sys
 06:47:28.0824 6332 amdide - ok
 06:47:28.0839 6332 [00DDA200D71BAC534BF56A9DB5DFD666] AmdK8
 C:\windows\system32\DRIVERS\amdk8.sys
 06:47:28.0839 6332 AmdK8 - ok
 06:47:28.0855 6332 [3CBF30F5370FDA40DD3E87DF38EA53B6] AmdPPM
 C:\windows\system32\DRIVERS\amdppm.sys
 06:47:28.0855 6332 AmdPPM - ok
 06:47:28.0886 6332 [19CE906B4CDC11FC4FEF5745F33A63B6] amdsata
 C:\windows\system32\drivers\amdsata.sys
 06:47:28.0886 6332 amdsata - ok
 06:47:28.0902 6332 [EA43AF0C423FF267355F74E7A53BDABA] amdsbs
 C:\windows\system32\DRIVERS\amdsbs.sys
 06:47:28.0902 6332 amdsbs - ok
 06:47:28.0933 6332 [869E67D66BE326A5A9159FBA8746FA70] amdxta
 C:\windows\system32\drivers\amdxta.sys
 06:47:28.0933 6332 amdxta - ok
 06:47:28.0995 6332 [E4EDE40F326B3B815EC06FF03A8697D6] ameisvc
 C:\Program Files\T-Mobile\web'n'walk Manager\ameisvc.exe
 06:47:29.0042 6332 ameisvc - ok
 06:47:29.0089 6332 [FEB834C02CE1E84B6A38F953CA067706] AppID
 C:\windows\system32\drivers\appid.sys
 06:47:29.0089 6332 AppID - ok
 06:47:29.0120 6332 [62A9C86CB6085E20DB4823E4E97826F5] AppIDSvc
 C:\windows\System32\appidsvc.dll
 06:47:29.0136 6332 AppIDSvc - ok
 06:47:29.0151 6332 [7DEAD9E3F65DCB2794F2711003BBF650] Appinfo
 C:\windows\System32\appinfo.dll
 06:47:29.0167 6332 Appinfo - ok
 06:47:29.0183 6332 [A45D184DF6A8803DA13A0B329517A64A] AppMgmt
 C:\windows\System32\appmgmts.dll
 06:47:29.0183 6332 AppMgmt - ok
 06:47:29.0198 6332 [2932004F49677BD84DBC72EDB754FFB3] arc
 C:\windows\system32\DRIVERS\arc.sys
 06:47:29.0214 6332 arc - ok
 06:47:29.0214 6332 [5D6F36C46FD283AE1B57BD2E9FEB0BC7] arcsas
 C:\windows\system32\DRIVERS\arcsas.sys
 06:47:29.0229 6332 arcsas - ok
 06:47:29.0276 6332 [0309F8D544F565BE13EEFC21824CA827] ARCVCM
 C:\windows\system32\DRIVERS\ArcSoftVcapture.sys
 06:47:29.0276 6332 ARCVCM - ok
 06:47:29.0385 6332 [776ACEFA0CA9DF0FAA51A5FB2F435705] aspnet_state
 C:\windows\Microsoft.NET\Framework\v4.0.30319\aspnet_state.exe

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:29.0417 6332 aspnet_state - ok
06:47:29.0432 6332 [ ADD2ADE1C2B285AB8378D2DAAF991481 ] AsyncMac
C:\windows\system32\DRIVERS\asyncmac.sys
06:47:29.0432 6332 AsyncMac - ok
06:47:29.0463 6332 [ 338C86357871C167A96AB976519BF59E ] atapi
C:\windows\system32\DRIVERS\atapi.sys
06:47:29.0479 6332 atapi - ok
06:47:29.0510 6332 [ 510C873BF4135AA829F4180352772734 ] AudioEndpointBuilder
C:\windows\System32\Audiosrv.dll
06:47:29.0541 6332 AudioEndpointBuilder - ok
06:47:29.0573 6332 [ 510C873BF4135AA829F4180352772734 ] Audiosrv
C:\windows\System32\Audiosrv.dll
06:47:29.0573 6332 Audiosrv - ok
06:47:29.0619 6332 [ DD6A431B43E34B91A767D1CE33728175 ] AxInstSV
C:\windows\System32\AxInstSV.dll
06:47:29.0619 6332 AxInstSV - ok
06:47:29.0666 6332 [ 1A231ABEC60FD316EC54C66715543CEC ] b06bdrv
C:\windows\system32\DRIVERS\bxvbdx.sys
06:47:29.0697 6332 b06bdrv - ok
06:47:29.0744 6332 [ BD8869EB9CDE6BBE4508D869929869EE ] b57nd60x
C:\windows\system32\DRIVERS\b57nd60x.sys
06:47:29.0760 6332 b57nd60x - ok
06:47:29.0853 6332 [ A2494901E7226B356B8C1005C45F1C5F ] BBSvc
C:\Program Files\Microsoft\BingBar\7.1.361.0\BBSvc.exe
06:47:29.0853 6332 BBSvc - ok
06:47:29.0885 6332 [ 63B1CBBAE4790B5BAC98F01BF9449722 ] BBUpdate
C:\Program Files\Microsoft\BingBar\7.1.361.0\SeaPort.exe
06:47:29.0916 6332 BBUpdate - ok
06:47:29.0947 6332 [ EE1E9C3BB8228AE423DD38DB69128E71 ] BDESVC
C:\windows\system32\bdesvc.dll
06:47:29.0947 6332 BDESVC - ok
06:47:29.0978 6332 [ 505506526A9D467307B3C393DEDAF858 ] Beep
C:\windows\system32\drivers\Beep.sys
06:47:29.0978 6332 Beep - ok
06:47:30.0009 6332 [ 85AC71C045CEB054ED48A7841AAE0C11 ] BFE
C:\windows\system32\bfe.dll
06:47:30.0041 6332 BFE - ok
06:47:30.0134 6332 [ 75A51EA67D28E41543B8B354A47DF430 ] BHDrvx86
C:\ProgramData\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NIS_18.1.0.37\Defin
itions\BASHDefs\20130322.001\BHDrvx86.sys
06:47:30.0181 6332 BHDrvx86 - ok
06:47:30.0243 6332 [ 53F476476F55A27F580661BDE09C4EC4 ] BITS
C:\windows\System32\qmgr.dll
06:47:30.0306 6332 BITS - ok
06:47:30.0321 6332 [ 2287078ED48FCFC477B05B20CF38F36F ] blbdrive
C:\windows\system32\DRIVERS\blbdrive.sys
06:47:30.0337 6332 blbdrive - ok
06:47:30.0353 6332 [ 9A5C671B7FBAE4865149BB11F59B91B2 ] bowser
C:\windows\system32\DRIVERS\bowser.sys
06:47:30.0368 6332 bowser - ok
06:47:30.0399 6332 [ 9F9ACC7F7CCDE8A15C282D3F88B43309 ] BrFiltLo
C:\windows\system32\DRIVERS\BrFiltLo.sys
06:47:30.0399 6332 BrFiltLo - ok
06:47:30.0415 6332 [ 56801AD62213A41F6497F96DEE83755A ] BrFiltUp
C:\windows\system32\DRIVERS\BrFiltUp.sys
06:47:30.0415 6332 BrFiltUp - ok
06:47:30.0446 6332 [ A0E691DC6589D4D2CBE373171D1A49E5 ] Browser
C:\windows\System32\browser.dll
06:47:30.0446 6332 Browser - ok
06:47:30.0462 6332 [ 845B8CE732E67F3B4133164868C666EA ] Brserid
C:\windows\System32\Drivers\Brserid.sys
06:47:30.0477 6332 Brserid - ok
06:47:30.0493 6332 [ 203F0B1E73ADADBBB7B7B1FABD901F6B ] BrSerWdm
C:\windows\System32\Drivers\BrSerWdm.sys
06:47:30.0493 6332 BrSerWdm - ok
06:47:30.0509 6332 [ BD456606156BA17E60A04E18016AE54B ] BrUsbMdm
C:\windows\System32\Drivers\BrUsbMdm.sys
06:47:30.0509 6332 BrUsbMdm - ok

```

```

06:47:30.0524 6332 [ AF72ED54503F717A43268B3CC5FAEC2E ] BrUsbSer
C:\windows\System32\Drivers\BrUsbSer.sys
06:47:30.0524 6332 BrUsbSer - ok
06:47:30.0602 6332 [ 2865A5C8E98C70C605F417908CEBB3A4 ] BthEnum
C:\windows\system32\drivers\BthEnum.sys
06:47:30.0602 6332 BthEnum - ok
06:47:30.0618 6332 [ ED3DF7C56CE0084EB2034432FC56565A ] BTHMODEM
C:\windows\system32\DRIVERS\bthmodem.sys
06:47:30.0633 6332 BTHMODEM - ok
06:47:30.0665 6332 [ AD1872E5829E8A2C3B5B4B641C3EAB0E ] BthPan
C:\windows\system32\DRIVERS\bthpan.sys
06:47:30.0665 6332 BthPan - ok
06:47:30.0711 6332 [ 3D43C01E9B134C6BF38A37C9354B2504 ] BTHPORT
C:\windows\System32\Drivers\BTHport.sys
06:47:30.0727 6332 BTHPORT - ok
06:47:30.0774 6332 [ 1DF19C96EEF6C29D1C3E1A8678E07190 ] bthserv
C:\windows\system32\bthserv.dll
06:47:30.0774 6332 bthserv - ok
06:47:30.0805 6332 [ FCD2ADFC38D5A4E3BDA7F85E37160CAE ] BTHUSB
C:\windows\System32\Drivers\BTHUSB.sys
06:47:30.0805 6332 BTHUSB - ok
06:47:30.0836 6332 [ 525432CFD6D8C004860AF7ECD0A84234 ] btwampfl
C:\windows\system32\drivers\btwampfl.sys
06:47:30.0867 6332 btwampfl - ok
06:47:30.0883 6332 [ CF8799A563F734984D4E053CACEC1426 ] btwaudio
C:\windows\system32\drivers\btwaudio.sys
06:47:30.0899 6332 btwaudio - ok
06:47:30.0914 6332 [ 9ED9932043D599AEA04F6EA2D86964A1 ] btwavdt
C:\windows\system32\drivers\btwavdt.sys
06:47:30.0914 6332 btwavdt - ok
06:47:30.0945 6332 [ 110496CF8143FEA63B7A31DAD175829B ] btwdins
C:\Program Files\WIDCOMM\Bluetooth Software\btwdins.exe
06:47:30.0977 6332 btwdins - ok
06:47:30.0992 6332 [ DE53089F0678CB5F0AFEB867ACB0FB05 ] btwl2cap
C:\windows\system32\DRIVERS\btwl2cap.sys
06:47:31.0008 6332 btwl2cap - ok
06:47:31.0008 6332 [ 373D1BB0F7DC8F1931F9B7E0DE3E9A30 ] btwrchid
C:\windows\system32\DRIVERS\btwrchid.sys
06:47:31.0023 6332 btwrchid - ok
06:47:31.0039 6332 [ 77EA11B065E0A8AB902D78145CA51E10 ] cdfs
C:\windows\system32\DRIVERS\cdfs.sys
06:47:31.0039 6332 cdfs - ok
06:47:31.0086 6332 [ BA6E70AA0E6091BC39DE29477D866A77 ] cdrom
C:\windows\system32\DRIVERS\cdrom.sys
06:47:31.0086 6332 cdrom - ok
06:47:31.0133 6332 [ 628A9E30EC5E18DD5DE6BE4DBDC12198 ] CertPropSvc
C:\windows\System32\certprop.dll
06:47:31.0133 6332 CertPropSvc - ok
06:47:31.0148 6332 [ 3FE3FE94A34DF6FB06E6418D0F6A0060 ] circlass
C:\windows\system32\DRIVERS\circlass.sys
06:47:31.0148 6332 circlass - ok
06:47:31.0179 6332 [ 635181E0E9BBF16871BF5380D71DB02D ] CLFS
C:\windows\system32\CLFS.sys
06:47:31.0195 6332 CLFS - ok
06:47:31.0242 6332 [ D88040F816FDA31C3B466F0FA0918F29 ]
clr_optimization_v2.0.50727_32
C:\windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.exe
06:47:31.0257 6332 clr_optimization_v2.0.50727_32 - ok
06:47:31.0304 6332 [ C5A75EB48E2344ABDC162BDA79E16841 ]
clr_optimization_v4.0.30319_32
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.exe
06:47:31.0335 6332 clr_optimization_v4.0.30319_32 - ok
06:47:31.0367 6332 [ DEA805815E587DAD1DD2C502220B5616 ] CmBatt
C:\windows\system32\DRIVERS\CmBatt.sys
06:47:31.0367 6332 CmBatt - ok
06:47:31.0382 6332 [ C537B1DB64D495B9B4717B4D6D9EDBF2 ] cmdide
C:\windows\system32\DRIVERS\cmdide.sys
06:47:31.0382 6332 cmdide - ok

```

```

06:47:31.0429 6332 [ DB5E008B3744DD60C8498CBBF2A1CFA6 ] CNG
C:\windows\system32\Drivers\cng.sys
06:47:31.0460 6332 CNG - ok
06:47:31.0476 6332 [ A6023D3823C37043986713F118A89BEE ] Compbatt
C:\windows\system32\DRIVERS\compbatt.sys
06:47:31.0476 6332 Compbatt - ok
06:47:31.0507 6332 [ F1724BA27E97D627F808FB0BA77A28A6 ] CompositeBus
C:\windows\system32\DRIVERS\CompositeBus.sys
06:47:31.0507 6332 CompositeBus - ok
06:47:31.0538 6332 COMSysApp - ok
06:47:31.0554 6332 [ 2C4EBCFC84A9B44F209DFF6C6E6C61D1 ] crcdisk
C:\windows\system32\DRIVERS\crcdisk.sys
06:47:31.0569 6332 crcdisk - ok
06:47:31.0616 6332 [ F2FDE6C8DBAAD44CC58D1E07E4AF4EED ] CryptSvc
C:\windows\system32\cryptsvc.dll
06:47:31.0616 6332 CryptSvc - ok
06:47:31.0647 6332 [ 27C9490BDD0AE48911AB8CF1932591ED ] CSC
C:\windows\system32\drivers\csc.sys
06:47:31.0679 6332 CSC - ok
06:47:31.0725 6332 [ 56FB5F222EA30D3D3FC459879772CB73 ] CscService
C:\windows\System32\cscsvc.dll
06:47:31.0741 6332 CscService - ok
06:47:31.0835 6332 [ 72794D112CBAFF3BC0C29BF7350D4741 ] cvhsvc
C:\Program Files\Common Files\Microsoft Shared\Virtualization Handler\CVHVC.EXE
06:47:31.0866 6332 cvhsvc - ok
06:47:31.0897 6332 [ 87F8C293377D53E977523A0ECC18650D ] DAMDrv
C:\windows\system32\DRIVERS\DAMDrv.sys
06:47:31.0897 6332 DAMDrv - ok
06:47:31.0959 6332 [ B82CD39E336973359D7C9BF911E8E84F ] DcomLaunch
C:\windows\system32\rpcss.dll
06:47:32.0006 6332 DcomLaunch - ok
06:47:32.0022 6332 [ 8D6E10A2D9A5EED59562D9B82CF804E1 ] defragsvc
C:\windows\System32\defragsvc.dll
06:47:32.0037 6332 defragsvc - ok
06:47:32.0053 6332 [ 83D1ECEA8FAAE75604C0FA49AC7AD996 ] Dfsc
C:\windows\system32\Drivers\dfsc.sys
06:47:32.0069 6332 Dfsc - ok
06:47:32.0100 6332 [ C56495FBD770712367CAD35E5DE72DA6 ] Dhcp
C:\windows\system32\dhcpcore.dll
06:47:32.0115 6332 Dhcp - ok
06:47:32.0131 6332 [ 1A050B0274BFB3890703D490F330C0DA ] discache
C:\windows\system32\drivers\discache.sys
06:47:32.0131 6332 discache - ok
06:47:32.0162 6332 [ 565003F326F99802E68CA78F2A68E9FF ] Disk
C:\windows\system32\DRIVERS\disk.sys
06:47:32.0162 6332 Disk - ok
06:47:32.0193 6332 [ B15BE77A2BACF9C3177D27518AFE26A9 ] Dnscache
C:\windows\System32\dnsrslvr.dll
06:47:32.0209 6332 Dnscache - ok
06:47:32.0256 6332 [ 4408C85C21EEA48EB0CE486BAEEF0502 ] dot3svc
C:\windows\System32\dot3svc.dll
06:47:32.0271 6332 dot3svc - ok
06:47:32.0334 6332 [ BB7E879C2E0E74180253DAF4F8924E8E ] DpHost
C:\Program Files\Hewlett-Packard\HP ProtectTools Security
Manager\Bin\DpHostw.exe
06:47:32.0349 6332 DpHost - ok
06:47:32.0365 6332 [ 7FA81C6E11CAA594ADB52084DA73A1E5 ] DPS
C:\windows\system32\dps.dll
06:47:32.0381 6332 DPS - ok
06:47:32.0412 6332 [ B918E7C5F9BF77202F89E1A9539F2EB4 ] drmkau
C:\windows\system32\drivers\drmkau.sys
06:47:32.0412 6332 drmkau - ok
06:47:32.0443 6332 [ 687AF6BB383885FF6A64071B189A7F3E ] dtsoftbus01
C:\windows\system32\DRIVERS\dtsoftbus01.sys
06:47:32.0459 6332 dtsoftbus01 - ok
06:47:32.0505 6332 [ 1679A4669326CB1A67CC95658D273234 ] DXGKrn
C:\windows\System32\drivers\dxgkrl.sys
06:47:32.0537 6332 DXGKrn - ok

```

```

06:47:32.0568 6332 [ 890A46FB3D58667BE559CEE1A0252049 ] elcexpress
C:\windows\system32\DRIVERS\elc6232.sys
06:47:32.0583 6332 elcexpress - ok
06:47:32.0615 6332 [ 8600142FA91C1B96367D3300AD0F3F3A ] EapHost
C:\windows\System32\eamsvc.dll
06:47:32.0615 6332 EapHost - ok
06:47:32.0724 6332 [ 024E1B5CAC09731E4D868E64DBFB4AB0 ] ebdrv
C:\windows\system32\DRIVERS\evbdx.sys
06:47:32.0817 6332 ebdrv - ok
06:47:32.0880 6332 [ 85B8B4032A895A746D46A288A9B30DED ] eeCtrl
C:\Program Files\Common Files\Symantec Shared\EENGINE\eeCtrl.sys
06:47:32.0895 6332 eeCtrl - ok
06:47:32.0911 6332 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] EFS
C:\windows\System32\lsass.exe
06:47:32.0927 6332 EFS - ok
06:47:32.0973 6332 [ 1697C39978CD69F6FBC15302EDCECE1F ] ehRecvr
C:\windows\ehome\ehRecvr.exe
06:47:33.0005 6332 ehRecvr - ok
06:47:33.0020 6332 [ D389BFF34F80CAEDE417BF9D1507996A ] ehSched
C:\windows\ehome\ehsched.exe
06:47:33.0020 6332 ehSched - ok
06:47:33.0036 6332 [ 0ED67910C8C326796FAA00B2BF6D9D3C ] elxstor
C:\windows\system32\DRIVERS\elxstor.sys
06:47:33.0051 6332 elxstor - ok
06:47:33.0098 6332 [ B5A8A04A6E5B4E86B95B1553AA918F5F ] EraserUtilRebootDrv
C:\Program Files\Common Files\Symantec Shared\EENGINE\EraserUtilRebootDrv.sys
06:47:33.0098 6332 EraserUtilRebootDrv - ok
06:47:33.0129 6332 [ 8FC3208352DD3912C94367A206AB3F11 ] ErrDev
C:\windows\system32\DRIVERS\errdev.sys
06:47:33.0129 6332 ErrDev - ok
06:47:33.0192 6332 [ F6916EFC29D9953D5D0DF06882AE8E16 ] EventSystem
C:\windows\system32\es.dll
06:47:33.0207 6332 EventSystem - ok
06:47:33.0239 6332 [ 57C171EA22F0A7F068FCB0CAEDD1E8E7 ] ew_hwsusbdev
C:\windows\system32\DRIVERS\ew_hwsusbdev.sys
06:47:33.0254 6332 ew_hwsusbdev - ok
06:47:33.0285 6332 [ 2DC9108D74081149CC8B651D3A26207F ] exfat
C:\windows\system32\drivers\exfat.sys
06:47:33.0301 6332 exfat - ok
06:47:33.0332 6332 [ 7E0AB74553476622FB6AE36F73D97D35 ] fastfat
C:\windows\system32\drivers\fastfat.sys
06:47:33.0332 6332 fastfat - ok
06:47:33.0363 6332 [ F7EA23CC5E6BF2181F3F399D54F6EFC1 ] Fax
C:\windows\system32\fxssvc.exe
06:47:33.0395 6332 Fax - ok
06:47:33.0395 6332 [ E817A017F82DF2A1F8CFDBDA29388B29 ] fdc
C:\windows\system32\DRIVERS\fdc.sys
06:47:33.0410 6332 fdc - ok
06:47:33.0426 6332 [ F3222C893BD2F5821A0179E5C71E88FB ] fdPHost
C:\windows\system32\fdPHost.dll
06:47:33.0426 6332 fdPHost - ok
06:47:33.0441 6332 [ 7DBE8CBFE79EFBDEB98C9FB08D3A9A5B ] FDResPub
C:\windows\system32\fdrespub.dll
06:47:33.0441 6332 FDResPub - ok
06:47:33.0457 6332 [ 6CF00369C97F3CF563BE99BE983D13D8 ] FileInfo
C:\windows\system32\drivers\fileinfo.sys
06:47:33.0457 6332 FileInfo - ok
06:47:33.0473 6332 [ 42C51DC94C91DA21CB9196EB64C45DB9 ] Filetrace
C:\windows\system32\drivers\filetrace.sys
06:47:33.0473 6332 Filetrace - ok
06:47:33.0488 6332 [ 00160891E41480997565F2BE35476AC0 ] FLCLOCK
C:\Windows\system32\flcdlock.exe
06:47:33.0504 6332 FLCLOCK - ok
06:47:33.0519 6332 [ 87907AA70CB3C56600F1C2FB8841579B ] flpydisk
C:\windows\system32\DRIVERS\flpydisk.sys
06:47:33.0519 6332 flpydisk - ok
06:47:33.0535 6332 [ 7520EC808E0C35E0EE6F841294316653 ] FltMgr
C:\windows\system32\drivers\fltMgr.sys

```

TDSKiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:33.0551 6332 FltMgr - ok
06:47:33.0582 6332 [ 7FE4995528A7529A761875151EE3D512 ] FontCache
C:\windows\system32\FntCache.dll
06:47:33.0613 6332 FontCache - ok
06:47:33.0660 6332 [ E56F39F6B7FDA0AC77A79B0FD3DE1A2F ] FontCache3.0.0.0
C:\windows\Microsoft.Net\Framework\v3.0\WPF\PresentationFontCache.exe
06:47:33.0660 6332 FontCache3.0.0.0 - ok
06:47:33.0675 6332 [ 1A16B57943853E598CFF37FE2B8CBF1D ] FsDepends
C:\windows\system32\drivers\FsDepends.sys
06:47:33.0691 6332 FsDepends - ok
06:47:33.0738 6332 [ 500A9814FD9446A8126858A5A7F7D273 ] Fs_Rec
C:\windows\system32\drivers\Fs_Rec.sys
06:47:33.0753 6332 Fs_Rec - ok
06:47:33.0785 6332 [ DAFBD9FE39197495AED6D51F3B85B5D2 ] fvevol
C:\windows\system32\DRIVERS\fvevol.sys
06:47:33.0800 6332 fvevol - ok
06:47:33.0831 6332 [ 65EE0C7A58B65E74AE05637418153938 ] gagp30kx
C:\windows\system32\DRIVERS\gagp30kx.sys
06:47:33.0847 6332 gagp30kx - ok
06:47:33.0878 6332 [ 8BA3C04702BF8F927AB36AE8313CA4EE ] gpsvc
C:\windows\System32\gpsvc.dll
06:47:33.0909 6332 gpsvc - ok
06:47:33.0925 6332 [ C172F0D0329E46513B09E1FC60A27B9D ] HBtnKey
C:\windows\system32\DRIVERS\cpqbtn.sys
06:47:33.0925 6332 HBtnKey - ok
06:47:33.0956 6332 [ C44E3C2BAB6837DB337DDEE7544736DB ] hcw85cir
C:\windows\system32\drivers\hcw85cir.sys
06:47:33.0956 6332 hcw85cir - ok
06:47:33.0987 6332 [ 3530CAD25DEBA7DC7DE8BB51632CBC5F ] HdAudAddService
C:\windows\system32\drivers\HdAudio.sys
06:47:33.0987 6332 HdAudAddService - ok
06:47:34.0034 6332 [ 717A2207FD6F13AD3E664C7D5A43C7BF ] HDAudBus
C:\windows\system32\DRIVERS\HDAudBus.sys
06:47:34.0034 6332 HDAudBus - ok
06:47:34.0050 6332 [ 1D58A7F3E11A9731D0EAAA8405ACC36 ] HidBatt
C:\windows\system32\DRIVERS\HidBatt.sys
06:47:34.0050 6332 HidBatt - ok
06:47:34.0081 6332 [ 89448F40E6DF260C206A193A4683BA78 ] HidBth
C:\windows\system32\DRIVERS\hidbth.sys
06:47:34.0081 6332 HidBth - ok
06:47:34.0097 6332 [ CF50B4CF4A4F229B9F3C08351F99CA5E ] HidIr
C:\windows\system32\DRIVERS\hidir.sys
06:47:34.0097 6332 HidIr - ok
06:47:34.0112 6332 [ 2BC6F6A1992B3A77F5F41432CA6B3B6B ] hidserv
C:\windows\system32\hidserv.dll
06:47:34.0128 6332 hidserv - ok
06:47:34.0143 6332 [ 25072FB35AC90B25F9E4E3BACF774102 ] HidUsb
C:\windows\system32\DRIVERS\hidusb.sys
06:47:34.0143 6332 HidUsb - ok
06:47:34.0175 6332 [ 741C2A45CA8407E374AABA3E330B7872 ] hkmsvc
C:\windows\system32\kmsvc.dll
06:47:34.0190 6332 hkmsvc - ok
06:47:34.0206 6332 [ A768CA158BB06782A2835B907F4873C3 ] HomeGroupListener
C:\windows\system32>ListSvc.dll
06:47:34.0221 6332 HomeGroupListener - ok
06:47:34.0253 6332 [ FB08DEC5EF43D0C66D83B8E9694E7549 ] HomeGroupProvider
C:\windows\system32\provsrv.dll
06:47:34.0253 6332 HomeGroupProvider - ok
06:47:34.0299 6332 [ 45A12CACB97B4F15858FCFD59355A1E9 ] HP Health Check Service
C:\Program Files\Hewlett-Packard\HP Health Check\hphc_service.exe
06:47:34.0315 6332 HP Health Check Service - ok
06:47:34.0346 6332 [ 6DD70FB3092FD3EA7FA4CA26A1FE049D ] HP Power Assistant
Service C:\Program Files\Hewlett-Packard\HP Power Assistant\HPPA_Service.exe
06:47:34.0346 6332 HP Power Assistant Service - ok
06:47:34.0409 6332 [ 771E3B558C66416860EFB3683CAF4B0F ] HP ProtectTools Service
C:\Program Files\Hewlett-Packard\2009 Password Filter for HP
ProtectTools\PTChangeFilterService.exe
06:47:34.0409 6332 HP ProtectTools Service - ok

```

TDSSKiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:34.0471 6332 [ D4B198E9B3CE6D05771E116D2D560F2F ] hpCMSrv
c:\Program Files\Hewlett-Packard\HP Connection Manager\hpCMSrv.exe
06:47:34.0518 6332 hpCMSrv - ok
06:47:34.0565 6332 [ A9FC4D7EA174BBF5A675B299FFAD80A2 ] HPDayStarterService
c:\Program Files\Hewlett-Packard\HP DayStarter\HPDayStarterService.exe
06:47:34.0565 6332 HPDayStarterService - ok
06:47:34.0611 6332 [ BCC4A8B2E2E902F52E7F2E7D8E125765 ] HPDrvMntSvc.exe
c:\Program Files\Hewlett-Packard\Shared\HPDrvMntSvc.exe
06:47:34.0611 6332 HPDrvMntSvc.exe - ok
06:47:34.0643 6332 [ BA57CFD48E79DA9CBCD708EF98683DA6 ] hpdskflt
c:\windows\system32\DRIVERS\hpdskflt.sys
06:47:34.0643 6332 hpdskflt - ok
06:47:34.0705 6332 [ 79EB59856CC7AEBE5DAE0211A9A1E5A9 ] HPFSService
c:\Program Files\Hewlett-Packard\File Sanitizer\HPFSService.exe
06:47:34.0845 6332 HPFSService - ok
06:47:34.0892 6332 [ FA6107E9434810F8644412BA7AFB891F ] hpHotkeyMonitor
c:\Program Files\Hewlett-Packard\HP Hotkey Support\HpHotkeyMonitor.exe
06:47:34.0970 6332 hpHotkeyMonitor - ok
06:47:35.0048 6332 [ EE9F88368739554DCCA142AE0214BCB1 ] HpqKbFiltr
c:\windows\system32\DRIVERS\HpqKbFiltr.sys
06:47:35.0048 6332 HpqKbFiltr - ok
06:47:35.0095 6332 [ EC9739A46F1F83C6E52A7A4697F44A65 ] hpqwmiex
c:\Program Files\Hewlett-Packard\Shared\hpqwmiEx.exe
06:47:35.0111 6332 hpqwmiex - ok
06:47:35.0142 6332 [ 295FDC419039090EB8B49FFDBB374549 ] HpSAMD
c:\windows\system32\DRIVERS\HpSAMD.sys
06:47:35.0142 6332 HpSAMD - ok
06:47:35.0157 6332 [ 6744EB927DA2DB58D5E1A77488EF143B ] hpsrv
c:\windows\system32\Hpservice.exe
06:47:35.0157 6332 hpsrv - ok
06:47:35.0220 6332 [ C531C7FD9E8B62021112787C4E2C5A5A ] HTTP
c:\windows\system32\drivers\HTTP.sys
06:47:35.0235 6332 HTTP - ok
06:47:35.0282 6332 [ 3170044AA8090F80839D3D4330BF733A ] huawei_cdcacm
c:\windows\system32\DRIVERS\ew_jucdcacm.sys
06:47:35.0298 6332 huawei_cdcacm - ok
06:47:35.0313 6332 [ F44461E66F1B7DD267957FE9BAA63ED0 ] huawei_enumerator
c:\windows\system32\DRIVERS\ew_jubusenum.sys
06:47:35.0313 6332 huawei_enumerator - ok
06:47:35.0360 6332 [ 8305F33CDE89AD6C7A0763ED0B5A8D42 ] hwpolicy
c:\windows\system32\drivers\hwpolicy.sys
06:47:35.0376 6332 hwpolicy - ok
06:47:35.0407 6332 [ F151F0BDC47F4A28B1B20A0818EA36D6 ] i8042prt
c:\windows\system32\DRIVERS\i8042prt.sys
06:47:35.0407 6332 i8042prt - ok
06:47:35.0454 6332 [ F989555F1662581032CCE1578A8FF28E ] iaStor
c:\windows\system32\DRIVERS\iaStor.sys
06:47:35.0469 6332 iaStor - ok
06:47:35.0516 6332 [ 117FF657E0D9BBD61B5C3E71E63D3919 ] IAStorDataMgrSvc
c:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe
06:47:35.0516 6332 IAStorDataMgrSvc - ok
06:47:35.0563 6332 [ 71F1A494FEDF4B33C02C4A6A28D6D9E9 ] iaStorV
c:\windows\system32\drivers\iaStorV.sys
06:47:35.0579 6332 iaStorV - ok
06:47:35.0641 6332 [ 5AF815EB5BC9802E5A064E2BA62BFC0C ] idsvc
c:\windows\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\infocard.exe
06:47:35.0672 6332 idsvc - ok
06:47:35.0797 6332 [ 404FB2AAF532BC7BBACC8880BE401C74 ] IDSVix86
c:\ProgramData\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NIS_18.1.0.37\Defin
itions\IPSDefs\20130329.001\IDSVix86.sys
06:47:35.0813 6332 IDSVix86 - ok
06:47:35.0875 6332 [ D59429259F82924E4D3B90C0F0FF7144 ] IFXSpMgtSrv
c:\Program Files\Hewlett-Packard\Embedded Security Software\ifxspmgmt.exe
06:47:35.0906 6332 IFXSpMgtSrv - ok
06:47:35.0953 6332 [ 0D1BFD3318674D0D6E9465936D7CC17F ] IFXTCS
c:\Program Files\Hewlett-Packard\Embedded Security Software\ifxtcs.exe
06:47:36.0062 6332 IFXTCS - ok

```

```

06:47:36.0281 6332 [ 60CC34AD19AF2716FF18EC756D55B9AB ] igfx
C:\windows\system32\DRIVERS\igdkmd32.sys
06:47:36.0515 6332 igfx - ok
06:47:36.0546 6332 [ 4173FF5708F3236CF25195FEC742915 ] iirsp
C:\windows\system32\DRIVERS\iirsp.sys
06:47:36.0546 6332 iirsp - ok
06:47:36.0593 6332 [ FAC0EE6562B121B1399D6E855583F7A5 ] IKEEXT
C:\windows\System32\ikeext.dll
06:47:36.0624 6332 IKEEXT - ok
06:47:36.0671 6332 [ 5576AD2F0039D2BCCCA3567FC0BF981C ] IntcDAud
C:\windows\system32\DRIVERS\IntcDAud.sys
06:47:36.0686 6332 IntcDAud - ok
06:47:36.0686 6332 [ A0F12F2C9BA6C72F3987CE780E77C130 ] intelide
C:\windows\system32\DRIVERS\intelide.sys
06:47:36.0702 6332 intelide - ok
06:47:36.0733 6332 [ 3B514D27BFC4ACCB4037BC6685F766E0 ] intelppm
C:\windows\system32\DRIVERS\intelppm.sys
06:47:36.0733 6332 intelppm - ok
06:47:36.0764 6332 [ ACB364B9075A45C0736E5C47BE5CAE19 ] IPBusEnum
C:\windows\system32\ipbusenum.dll
06:47:36.0764 6332 IPBusEnum - ok
06:47:36.0780 6332 [ 709D1761D3B19A932FF0238EA6D50200 ] IpFilterDriver
C:\windows\system32\DRIVERS\ipfltdrv.sys
06:47:36.0795 6332 IpFilterDriver - ok
06:47:36.0827 6332 [ 477397B432A256A50EE7E4339EB9EA14 ] iphlpsvc
C:\windows\System32\iphlpvc.dll
06:47:36.0842 6332 iphlpsvc - ok
06:47:36.0858 6332 [ E4454B6C37D7FFD5649611F6496308A7 ] IPMIDRV
C:\windows\system32\DRIVERS\IPMIDrv.sys
06:47:36.0858 6332 IPMIDRV - ok
06:47:36.0873 6332 [ A5FA468D67ABCDAA36264E463A7BB0CD ] IPNAT
C:\windows\system32\drivers\ipnat.sys
06:47:36.0873 6332 IPNAT - ok
06:47:36.0889 6332 [ 42996CFF20A3084A56017B7902307E9F ] IRENUM
C:\windows\system32\drivers\irenum.sys
06:47:36.0889 6332 IRENUM - ok
06:47:36.0905 6332 [ 1F32BB6B38F62F7DF1A7AB7292638A35 ] isapnp
C:\windows\system32\DRIVERS\isapnp.sys
06:47:36.0905 6332 isapnp - ok
06:47:36.0936 6332 [ ED46C223AE46C6866AB77CDC41C404B7 ] iScsiPrt
C:\windows\system32\DRIVERS\msiscsi.sys
06:47:36.0951 6332 iScsiPrt - ok
06:47:36.0998 6332 [ 6C85719A21B3F62C2C76280F4BD36C7B ] jhi_service
C:\Program Files\Intel\Services\IPT\jhi_service.exe
06:47:37.0014 6332 jhi_service - ok
06:47:37.0061 6332 [ 831F342877333859291D4171B5EDD3CA ] JMCR
C:\windows\system32\DRIVERS\jmcr.sys
06:47:37.0061 6332 JMCR - ok
06:47:37.0092 6332 [ 07712CEF42A89B76ADB2FC8124FCCD14 ] johci
C:\windows\system32\DRIVERS\johci.sys
06:47:37.0092 6332 johci - ok
06:47:37.0107 6332 [ ADEF52CA1AEAE82B50DF86B56413107E ] kbdclass
C:\windows\system32\DRIVERS\kbdclass.sys
06:47:37.0123 6332 kbdclass - ok
06:47:37.0139 6332 [ 3D9F0EBF350EDCFD6498057301455964 ] kbdhid
C:\windows\system32\DRIVERS\kbdhid.sys
06:47:37.0139 6332 kbdhid - ok
06:47:37.0154 6332 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] KeyIso
C:\windows\system32\lsass.exe
06:47:37.0170 6332 KeyIso - ok
06:47:37.0201 6332 [ 52FC17C8589F11747D01D3CF592673D0 ] KSecDD
C:\windows\system32\Drivers\ksecdd.sys
06:47:37.0201 6332 KSecDD - ok
06:47:37.0217 6332 [ 3E5474B03568CFAB834DA3C38E8C9EFA ] KSecPkg
C:\windows\system32\Drivers\ksecpkg.sys
06:47:37.0232 6332 KSecPkg - ok
06:47:37.0263 6332 [ 89A7B9CC98D0D80C6F31B91C0A310FCD ] KtmRm
C:\windows\system32\msdtckrm.dll

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:37.0279 6332 KtmRm - ok
06:47:37.0310 6332 [ 8F6BF790D3168224C16F2AF68A84438C ] LanmanServer
C:\windows\system32\srsvsvc.dll
06:47:37.0326 6332 LanmanServer - ok
06:47:37.0357 6332 [ B9891F885DCF1F0513A51CB58493CB1F ] LanmanWorkstation
C:\windows\system32\wkssvc.dll
06:47:37.0388 6332 LanmanWorkstation - ok
06:47:37.0419 6332 [ F7611EC07349979DA9B0AE1F18CCC7A6 ] lltdio
C:\windows\system32\DRIVERS\lltdio.sys
06:47:37.0419 6332 lltdio - ok
06:47:37.0451 6332 [ 5700673E13A2117FA3B9020C852C01E2 ] lltdsvc
C:\windows\system32\lltdsvc.dll
06:47:37.0466 6332 lltdsvc - ok
06:47:37.0497 6332 [ 55CA01BA19D0006C8F2639B6C045E08B ] lmhosts
C:\windows\system32\lmhsvc.dll
06:47:37.0497 6332 lmhosts - ok
06:47:37.0560 6332 [ 97F9EAAAC985A663394CD8F54DCD3E73A ] LMS
C:\Program Files\Intel\Intel(R) Management Engine Components\LMS\LMS.exe
06:47:37.0575 6332 LMS - ok
06:47:37.0607 6332 [ EB119A53CCF2ACC000AC71B065B78FEF ] LSI_FC
C:\windows\system32\DRIVERS\lsi_fc.sys
06:47:37.0622 6332 LSI_FC - ok
06:47:37.0638 6332 [ 8ADE1C877256A22E49B75D1CC9161F9C ] LSI_SAS
C:\windows\system32\DRIVERS\lsi_sas.sys
06:47:37.0638 6332 LSI_SAS - ok
06:47:37.0653 6332 [ DC9DC3D3DAA0E276FD2EC262E38B11E9 ] LSI_SAS2
C:\windows\system32\DRIVERS\lsi_sas2.sys
06:47:37.0653 6332 LSI_SAS2 - ok
06:47:37.0669 6332 [ 0A036C7D7CAB643A7F07135AC47E0524 ] LSI_SCSI
C:\windows\system32\DRIVERS\lsi_scsi.sys
06:47:37.0669 6332 LSI_SCSI - ok
06:47:37.0685 6332 [ 6703E366CC18D3B6E534F5CF7DF39CEE ] luafv
C:\windows\system32\drivers\luafv.sys
06:47:37.0700 6332 luafv - ok
06:47:37.0731 6332 [ 629CABB0421668C9D3D402A3C3D77E14 ] MBAMProtector
C:\windows\system32\drivers\mbam.sys
06:47:37.0731 6332 MBAMProtector - ok
06:47:37.0778 6332 [ 1ACAA67676E9E7BDA5E0C41B6E0DECAF ] MBAMScheduler
C:\Program Files\Malwarebytes' Anti-Malware\mbamscheduler.exe
06:47:37.0794 6332 MBAMScheduler - ok
06:47:37.0841 6332 [ 916B8954AC3E06DC9E898AFFB41F3FB6 ] MBAMService
C:\Program Files\Malwarebytes' Anti-Malware\mbamservice.exe
06:47:37.0872 6332 MBAMService - ok
06:47:37.0950 6332 [ 71D6D4B6D91BC39C07FAC2F3D7D20E6B ] McAfee Endpoint
Encryption Agent C:\Program Files\Hewlett-Packard\Drive
Encryption\EEAgent\MfeEpeHost.exe
06:47:38.0028 6332 McAfee Endpoint Encryption Agent - ok
06:47:38.0059 6332 [ E2B0887816ED336685954E3D8FDAA51D ] Mcx2Svc
C:\windows\system32\Mcx2Svc.dll
06:47:38.0059 6332 Mcx2Svc - ok
06:47:38.0075 6332 [ 0FFF5B045293002AB38EB1FD1FC2FB74 ] megasas
C:\windows\system32\DRIVERS\megasas.sys
06:47:38.0075 6332 megasas - ok
06:47:38.0090 6332 [ DCBAB2920C75F390CAF1D29F675D03D6 ] MegaSR
C:\windows\system32\DRIVERS\MegaSR.sys
06:47:38.0090 6332 MegaSR - ok
06:47:38.0137 6332 [ D86AC00883B9C98B570E7643AAF8E554 ] MEI
C:\windows\system32\DRIVERS\HECI.sys
06:47:38.0137 6332 MEI - ok
06:47:38.0184 6332 [ 3440E714EF738FBAE242F26179DDE56F ] MfeEpePc
C:\windows\system32\drivers\MfeEpePc.sys
06:47:38.0184 6332 MfeEpePc - ok
06:47:38.0231 6332 [ 146B6F43A673379A3C670E86D89BE5EA ] MMCSS
C:\windows\system32\mmcscs.dll
06:47:38.0231 6332 MMCSS - ok
06:47:38.0246 6332 [ F001861E5700EE84E2D4E52C712F4964 ] Modem
C:\windows\system32\drivers\modem.sys
06:47:38.0246 6332 Modem - ok

```

```

06:47:38.0277 6332 [ 79D10964DE86B292320E9DFE02282A23 ] monitor
C:\windows\system32\DRIVERS\monitor.sys
06:47:38.0277 6332 monitor - ok
06:47:38.0293 6332 [ FB18CC1D4C2E716B6B903B0AC0CC0609 ] mouclass
C:\windows\system32\DRIVERS\mouclass.sys
06:47:38.0293 6332 mouclass - ok
06:47:38.0309 6332 [ 2C388D2CD01C9042596CF3C8F3C7B24D ] mouhid
C:\windows\system32\DRIVERS\mouhid.sys
06:47:38.0309 6332 mouhid - ok
06:47:38.0340 6332 [ 921C18727C5920D6C0300736646931C2 ] mountmgr
C:\windows\system32\drivers\mountmgr.sys
06:47:38.0340 6332 mountmgr - ok
06:47:38.0355 6332 [ 2AF5997438C55FB79D33D015C30E1974 ] mpio
C:\windows\system32\DRIVERS\mpio.sys
06:47:38.0371 6332 mpio - ok
06:47:38.0387 6332 [ AD2723A7B53DD1AACAE6AD8C0BFBF4D0 ] mpsdrv
C:\windows\system32\drivers\mpsdrv.sys
06:47:38.0387 6332 mpsdrv - ok
06:47:38.0418 6332 [ 5CD996CECF45CBC3E8D109C86B82D69E ] MpsSvc
C:\windows\system32\mpssvc.dll
06:47:38.0449 6332 MpsSvc - ok
06:47:38.0449 6332 [ B1BE47008D20E43DA3ADC37C24CDB89D ] MRxDAV
C:\windows\system32\drivers\mrxdav.sys
06:47:38.0465 6332 MRxDAV - ok
06:47:38.0496 6332 [ CA7570E42522E24324A12161DB14EC02 ] mrxsm
C:\windows\system32\DRIVERS\mrxsm.sys
06:47:38.0496 6332 mrxsm - ok
06:47:38.0527 6332 [ F965C3AB2B2AE5C378F4562486E35051 ] mrxsm10
C:\windows\system32\DRIVERS\mrxsm10.sys
06:47:38.0543 6332 mrxsm10 - ok
06:47:38.0558 6332 [ 25C38264A3C72594DD21D355D70D7A5D ] mrxsm20
C:\windows\system32\DRIVERS\mrxsm20.sys
06:47:38.0574 6332 mrxsm20 - ok
06:47:38.0574 6332 [ 4E00965BB3C471D52B07C9C3C59A82CF ] msahci
C:\windows\system32\DRIVERS\msahci.sys
06:47:38.0589 6332 msahci - ok
06:47:38.0621 6332 [ 455029C7174A2DBB03DBA8A0D8BDDD9A ] msdsm
C:\windows\system32\DRIVERS\msdsm.sys
06:47:38.0636 6332 msdsm - ok
06:47:38.0652 6332 [ E1BCE74A3BD9902B72599C0192A07E27 ] MSDTC
C:\windows\System32\msdtc.exe
06:47:38.0667 6332 MSDTC - ok
06:47:38.0683 6332 [ DAEFB28E3AF5A76ABCC2C3078C07327F ] Msfs
C:\windows\system32\drivers\Msfs.sys
06:47:38.0699 6332 Msfs - ok
06:47:38.0699 6332 [ 3E1E5767043C5AF9367F0056295E9F84 ] mshidkmdf
C:\windows\System32\drivers\mshidkmdf.sys
06:47:38.0714 6332 mshidkmdf - ok
06:47:38.0730 6332 [ 0A4E5757AE09FA9622E3158CC1AEF114 ] msisadv
C:\windows\system32\DRIVERS\msisadv.sys
06:47:38.0730 6332 msisadv - ok
06:47:38.0761 6332 [ 90F7D9E6B6F27E1A707D4A297F077828 ] MSiSCSI
C:\windows\system32\iscsiexe.dll
06:47:38.0777 6332 MSiSCSI - ok
06:47:38.0777 6332 msiserver - ok
06:47:38.0808 6332 [ 8C0860D6366AAFFB6C5BB9DF9448E631 ] MSKSSRV
C:\windows\system32\drivers\MSKSSRV.sys
06:47:38.0808 6332 MSKSSRV - ok
06:47:38.0823 6332 [ 3EA8B949F963562CEDBB549EAC0C11CE ] MSPCLOCK
C:\windows\system32\drivers\MSPCLOCK.sys
06:47:38.0855 6332 MSPCLOCK - ok
06:47:38.0870 6332 [ F456E973590D663B1073E9C463B40932 ] MSPQM
C:\windows\system32\drivers\MSPQM.sys
06:47:38.0870 6332 MSPQM - ok
06:47:38.0886 6332 [ 0E008FC4819D238C51D7C93E7B41E560 ] MsRPC
C:\windows\system32\drivers\MsRPC.sys
06:47:38.0901 6332 MsRPC - ok
06:47:38.0917 6332 [ FC6B9FF600CC585EA38B12589BD4E246 ] mssmbios

```

```

C:\windows\system32\DRIVERS\mssmbios.sys
06:47:38.0917 6332 mssmbios - ok
06:47:38.0948 6332 [ B42C6B921F61A6E55159B8BE6CD54A36 ] MSTEE
C:\windows\system32\drivers\MSTEE.sys
06:47:38.0948 6332 MSTEE - ok
06:47:38.0964 6332 [ 33599130F44E1F34631CEA241DE8AC84 ] MTConfig
C:\windows\system32\DRIVERS\MTConfig.sys
06:47:38.0964 6332 MTConfig - ok
06:47:38.0979 6332 [ 159FAD02F64E6381758C990F753BCC80 ] Mup
C:\windows\system32\Drivers\mup.sys
06:47:38.0979 6332 Mup - ok
06:47:39.0026 6332 [ 80284F1985C70C86F0B5F86DA2DFE1DF ] napagent
C:\windows\system32\qagentRT.dll
06:47:39.0026 6332 napagent - ok
06:47:39.0073 6332 [ 26384429FCD85D83746F63E798AB1480 ] NativewifiP
C:\windows\system32\DRIVERS\nwifi.sys
06:47:39.0089 6332 NativewifiP - ok
06:47:39.0167 6332 [ 7D7A3BC6640C1A0D1442816B30856928 ] NAVENG
C:\ProgramData\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NIS_18.1.0.37\Definitions\VirusDefs\20130329.025\NAVENG.SYS
06:47:39.0167 6332 NAVENG - ok
06:47:39.0229 6332 [ 28494C43D62AA7584BDCA2FADFBC4D11 ] NAVEX15
C:\ProgramData\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NIS_18.1.0.37\Definitions\VirusDefs\20130329.025\NAVEX15.SYS
06:47:39.0291 6332 NAVEX15 - ok
06:47:39.0323 6332 [ 23759D175A0A9BAAF04D05047BC135A8 ] NDIS
C:\windows\system32\drivers\ndis.sys
06:47:39.0354 6332 NDIS - ok
06:47:39.0385 6332 [ 0E1787AA6C9191D3D319E8BAFE86F80C ] NdisCap
C:\windows\system32\DRIVERS\ndiscap.sys
06:47:39.0385 6332 NdisCap - ok
06:47:39.0416 6332 [ E4A8AEC125A2E43A9E32AFEEA7C9C888 ] NdisTapi
C:\windows\system32\DRIVERS\ndistapi.sys
06:47:39.0416 6332 NdisTapi - ok
06:47:39.0432 6332 [ B30AE7F2B6D7E343B0DF32E6C08FCE75 ] Ndisuio
C:\windows\system32\DRIVERS\ndisuio.sys
06:47:39.0447 6332 Ndisuio - ok
06:47:39.0447 6332 [ 267C415EADCB53C9CA873DEE39CF3A4 ] Ndiswan
C:\windows\system32\DRIVERS\ndiswan.sys
06:47:39.0463 6332 Ndiswan - ok
06:47:39.0479 6332 [ AF7E7C63DCEF3F8772726F86039D6EB4 ] NDPProxy
C:\windows\system32\drivers\NDPProxy.sys
06:47:39.0479 6332 NDPProxy - ok
06:47:39.0494 6332 [ 80B275B1CE3B0E79909DB7B39AF74D51 ] NetBIOS
C:\windows\system32\DRIVERS\netbios.sys
06:47:39.0494 6332 NetBIOS - ok
06:47:39.0510 6332 [ DD52A733BF4CA5AF84562A5E2F963B91 ] NetBT
C:\windows\system32\DRIVERS\netbt.sys
06:47:39.0525 6332 NetBT - ok
06:47:39.0557 6332 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] Netlogon
C:\windows\system32\lsass.exe
06:47:39.0557 6332 Netlogon - ok
06:47:39.0603 6332 [ 7CCCFCFA7510684768DA22092D1FA4DB2 ] Netman
C:\windows\system32\netman.dll
06:47:39.0619 6332 Netman - ok
06:47:39.0697 6332 [ D22CD77D4F0D63D1169BB35911BFF12D ] NetMsmqActivator
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMsvchost.exe
06:47:39.0713 6332 NetMsmqActivator - ok
06:47:39.0713 6332 [ D22CD77D4F0D63D1169BB35911BFF12D ] NetPipeActivator
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMsvchost.exe
06:47:39.0713 6332 NetPipeActivator - ok
06:47:39.0744 6332 [ 8C338238C16777A802D6A9211EB2BA50 ] netprofm
C:\windows\system32\netprofm.dll
06:47:39.0759 6332 netprofm - ok
06:47:39.0775 6332 [ D22CD77D4F0D63D1169BB35911BFF12D ] NetTcpActivator
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMsvchost.exe
06:47:39.0775 6332 NetTcpActivator - ok
06:47:39.0791 6332 [ D22CD77D4F0D63D1169BB35911BFF12D ] NetTcpPortSharing

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt
 C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMsvchost.exe
 06:47:39.0791 6332 NetTcpPortSharing - ok
 06:47:39.0962 6332 [5C531E96643A74CE8BD9AB16B6C7EAD7] NETWNS32
 C:\windows\system32\DRIVERS\NETWNS32.sys
 06:47:40.0149 6332 NETWNS32 - ok
 06:47:40.0181 6332 [1D85C4B390B0EE09C7A46B91EFB2C097] nfrd960
 C:\windows\system32\DRIVERS\nfrd960.sys
 06:47:40.0181 6332 nfrd960 - ok
 06:47:40.0227 6332 [E78A365CC3E0FBFC018A33DCE01909F8] NIS
 C:\Program Files\Norton Internet Security\Engine\18.7.2.3\ccSvcHst.exe
 06:47:40.0227 6332 NIS - ok
 06:47:40.0259 6332 [2226496E34BD40734946A054B1CD657F] NlaSvc
 C:\windows\system32\nlasvc.dll
 06:47:40.0274 6332 NlaSvc - ok
 06:47:40.0306 6332 [1DB262A9F8C087E8153D89BEF3D2235F] Npfs
 C:\windows\system32\drivers\Npfs.sys
 06:47:40.0306 6332 Npfs - ok
 06:47:40.0321 6332 [BA387E955E890C8A88306D9B8D06BF17] nsi
 C:\windows\system32\nsisvc.dll
 06:47:40.0321 6332 nsi - ok
 06:47:40.0352 6332 [E9A0A4D07E53D8FEA2BB8387A3293C58] nsiproxy
 C:\windows\system32\drivers\nsiproxy.sys
 06:47:40.0352 6332 nsiproxy - ok
 06:47:40.0415 6332 [5126C5402C730C2A953275D8497A4715] Ntfs
 C:\windows\system32\drivers\Ntfs.sys
 06:47:40.0477 6332 Ntfs - ok
 06:47:40.0493 6332 [F9756A98D69098DCA8945D62858A812C] Null
 C:\windows\system32\drivers\Null.sys
 06:47:40.0508 6332 Null - ok
 06:47:40.0540 6332 [F1B0BED906F97E16F6D0C3629D2F21C6] nvraid
 C:\windows\system32\drivers\nvraid.sys
 06:47:40.0555 6332 nvraid - ok
 06:47:40.0586 6332 [4520B63899E867F354EE012D34E11536] nvstor
 C:\windows\system32\drivers\nvstor.sys
 06:47:40.0618 6332 nvstor - ok
 06:47:40.0633 6332 [5A0983915F02BAE73267CC2A041F717D] nv_agp
 C:\windows\system32\DRIVERS\nv_agp.sys
 06:47:40.0633 6332 nv_agp - ok
 06:47:40.0664 6332 [08A70A1F2CDDE9BB49B885CB817A66EB] ohci1394
 C:\windows\system32\DRIVERS\ohci1394.sys
 06:47:40.0680 6332 ohci1394 - ok
 06:47:40.0758 6332 [9D10F99A6712E28F8ACD5641E3A7EA6B] ose
 C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
 06:47:40.0758 6332 ose - ok
 06:47:40.0898 6332 [358A9CCA612C68EB2F07DDAD4CE1D8D7] osppsvc
 C:\Program Files\Common Files\Microsoft
 Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
 06:47:41.0023 6332 osppsvc - ok
 06:47:41.0054 6332 [82A8521DDC60710C3D3D3E7325209BEC] p2pimsvc
 C:\windows\system32\pnrpvc.dll
 06:47:41.0070 6332 p2pimsvc - ok
 06:47:41.0101 6332 [59C3DDD501E39E006DAC31BF55150D91] p2psvc
 C:\windows\system32\p2psvc.dll
 06:47:41.0117 6332 p2psvc - ok
 06:47:41.0148 6332 [2EA877ED5DD9713C5AC74E8EA7348D14] Parport
 C:\windows\system32\DRIVERS\parport.sys
 06:47:41.0148 6332 Parport - ok
 06:47:41.0179 6332 [66D3415C159741ADE7038A277EFFF99F] partmgr
 C:\windows\system32\drivers\partmgr.sys
 06:47:41.0179 6332 partmgr - ok
 06:47:41.0210 6332 [EB0A59F29C19B86479D36B35983DAADC] Parvdm
 C:\windows\system32\DRIVERS\parvdm.sys
 06:47:41.0210 6332 Parvdm - ok
 06:47:41.0242 6332 [358AB7956D3160000726574083DFC8A6] PcaSvc
 C:\windows\system32\pcasvc.dll
 06:47:41.0242 6332 PcaSvc - ok
 06:47:41.0257 6332 [C858CB77C577780ECC456A892E7E7D0F] pci
 C:\windows\system32\DRIVERS\pci.sys

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:41.0257 6332 pci - ok
06:47:41.0273 6332 [ AFE86F419014DB4E5593F69FFE26CE0A ] pciide
C:\windows\system32\DRIVERS\pciide.sys
06:47:41.0273 6332 pciide - ok
06:47:41.0288 6332 [ F396431B31693E71E8A80687EF523506 ] pcmcia
C:\windows\system32\DRIVERS\pcmcia.sys
06:47:41.0288 6332 pcmcia - ok
06:47:41.0288 6332 [ 250F6B43D2B613172035C6747AEED19F ] pcw
C:\windows\system32\drivers\pcw.sys
06:47:41.0304 6332 pcw - ok
06:47:41.0335 6332 pdfcdDispatcher - ok
06:47:41.0351 6332 [ 4A8CC4D25525F456069887D5E8C53225 ] PdiService
C:\Program Files\Common Files\Portrait Displays\Drivers\pdisrv.exe
06:47:41.0366 6332 PdiService - ok
06:47:41.0398 6332 [ 9E0104BA49F4E6973749A02BF41344ED ] PEAUTH
C:\windows\system32\drivers\peauth.sys
06:47:41.0413 6332 PEAUTH - ok
06:47:41.0444 6332 [ AF4D64D2A57B9772CF3801950B8058A6 ] PeerDistSvc
C:\windows\system32\peerdistsvc.dll
06:47:41.0460 6332 PeerDistSvc - ok
06:47:41.0522 6332 [ B27F1DF5ABC5240480D4D2D9666867A5 ] PersonalSecureDrive
C:\windows\system32\drivers\psd.sys
06:47:41.0522 6332 PersonalSecureDrive - ok
06:47:41.0538 6332 [ F473D5D43FA7D5C657A3137C5171CB77 ]
PersonalSecureDriveService c:\Program Files\Hewlett-Packard\Embedded Security
Software\IfxPsdSv.exe
06:47:41.0585 6332 PersonalSecureDriveService - ok
06:47:41.0632 6332 [ 9C1BFF7910C89A1D12E57343475840CB ] pla
C:\windows\system32\pla.dll
06:47:41.0678 6332 pla - ok
06:47:41.0710 6332 [ 71DEF5EC79774C798342D0EA16E41780 ] PlugPlay
C:\windows\system32\umpnpgm.dll
06:47:41.0741 6332 PlugPlay - ok
06:47:41.0756 6332 [ 63FF8572611249931EB16BB8EED6AFC8 ] PNRPAutoReg
C:\windows\system32\pnrpauto.dll
06:47:41.0772 6332 PNRPAutoReg - ok
06:47:41.0788 6332 [ 82A8521DDC60710C3D3D3E7325209BEC ] PNRPsvc
C:\windows\system32\pnrpsvc.dll
06:47:41.0803 6332 PNRPsvc - ok
06:47:41.0834 6332 [ 48E1B75C6DC0232FD92BAAE4BD344721 ] PolicyAgent
C:\windows\system32\ipsecsvc.dll
06:47:41.0850 6332 PolicyAgent - ok
06:47:41.0897 6332 [ DBFF83F709A91049621C1D35DD45C92C ] Power
C:\windows\system32\umpo.dll
06:47:41.0912 6332 Power - ok
06:47:41.0944 6332 [ 631E3E205AD6D86F2AED6A4A8E69F2DB ] PptpMiniport
C:\windows\system32\DRIVERS\rasppptp.sys
06:47:41.0944 6332 PptpMiniport - ok
06:47:41.0975 6332 [ 85B1E3A0C7585BC4AAE6899EC6FCF011 ] Processor
C:\windows\system32\DRIVERS\processr.sys
06:47:41.0975 6332 Processor - ok
06:47:42.0006 6332 [ AEA3BDBDBA667AA6F678CB38907E4F5E ] ProfSvc
C:\windows\system32\profsvc.dll
06:47:42.0022 6332 ProfSvc - ok
06:47:42.0053 6332 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] ProtectedStorage
C:\windows\system32\lsass.exe
06:47:42.0053 6332 ProtectedStorage - ok
06:47:42.0068 6332 [ 6270CCAE2A86DE6D146529FE55B3246A ] Psched
C:\windows\system32\DRIVERS\pacer.sys
06:47:42.0068 6332 Psched - ok
06:47:42.0100 6332 [ E42E3433DBB4CFFE8FDD91EAB29AEA8E ] PxHelp20
C:\windows\system32\Drivers\PxHelp20.sys
06:47:42.0100 6332 PxHelp20 - ok
06:47:42.0162 6332 [ AB95ECF1F6659A60DDC166D8315B0751 ] ql2300
C:\windows\system32\DRIVERS\ql2300.sys
06:47:42.0224 6332 ql2300 - ok
06:47:42.0240 6332 [ B4DD51DD25182244B86737DC51AF2270 ] ql40xx
C:\windows\system32\DRIVERS\ql40xx.sys

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:42.0240 6332 ql40xx - ok
06:47:42.0271 6332 [ 31AC809E7707EB580B2BDB760390765A ] QWAVE
C:\windows\system32\qwavedrv.dll
06:47:42.0302 6332 QWAVE - ok
06:47:42.0302 6332 [ 584078CA1B95CA72DF2A27C336F9719D ] QWAVEdrv
C:\windows\system32\drivers\qwavedrv.sys
06:47:42.0318 6332 QWAVEdrv - ok
06:47:42.0318 6332 [ 30A81B53C766D0133BB86D234E5556AB ] RasAcad
C:\windows\system32\DRIVERS\rasacd.sys
06:47:42.0334 6332 RasAcad - ok
06:47:42.0365 6332 [ 57EC4AEF73660166074D8F7F31C0D4FD ] RasAgileVpn
C:\windows\system32\DRIVERS\AgileVpn.sys
06:47:42.0365 6332 RasAgileVpn - ok
06:47:42.0396 6332 [ A60F1839849C0C00739787FD5EC03F13 ] RasAuto
C:\windows\system32\rasauto.dll
06:47:42.0412 6332 RasAuto - ok
06:47:42.0427 6332 [ D9F91EAFEC2815365CBE6D167E4E332A ] Rasl2tp
C:\windows\system32\DRIVERS\rasl2tp.sys
06:47:42.0427 6332 Rasl2tp - ok
06:47:42.0458 6332 [ 0CE66EC736B7FC526D78F7624C7D2A94 ] RasMan
C:\windows\system32\rasmans.dll
06:47:42.0474 6332 RasMan - ok
06:47:42.0474 6332 [ 0FE8B15916307A6AC12BFB6A63E45507 ] RasPppoe
C:\windows\system32\DRIVERS\raspppoe.sys
06:47:42.0490 6332 RasPppoe - ok
06:47:42.0505 6332 [ 44101F495A83EA6401D886E7FD70096B ] RasSstp
C:\windows\system32\DRIVERS\rassstp.sys
06:47:42.0505 6332 RasSstp - ok
06:47:42.0521 6332 [ 835D7E81BF517A3B72384BDCC85E1CE6 ] rdbss
C:\windows\system32\DRIVERS\rdbss.sys
06:47:42.0536 6332 rdbss - ok
06:47:42.0552 6332 [ 0D8F05481CB76E70E1DA06EE9F0DA9DF ] rdpbus
C:\windows\system32\DRIVERS\rdpbus.sys
06:47:42.0568 6332 rdpbus - ok
06:47:42.0583 6332 [ 1E016846895B15A99F9A176A05029075 ] RDPCDD
C:\windows\system32\DRIVERS\RDPCDD.sys
06:47:42.0583 6332 RDPCDD - ok
06:47:42.0630 6332 [ C5FF95883FFEF704D50C40D21CFB3AB5 ] RDPDR
C:\windows\system32\drivers\rdpdr.sys
06:47:42.0646 6332 RDPDR - ok
06:47:42.0661 6332 [ 5A53CA1598DD4156D44196D200C94B8A ] RDPENCDD
C:\windows\system32\drivers\rdpencdd.sys
06:47:42.0661 6332 RDPENCDD - ok
06:47:42.0692 6332 [ 44B0A53CD4F27D50ED461DAE0C0B4E1F ] RDPREFMP
C:\windows\system32\drivers\rdprefmp.sys
06:47:42.0692 6332 RDPREFMP - ok
06:47:42.0724 6332 [ C5B8D47A4688DE9D335204EA757C2240 ] RDPWD
C:\windows\system32\drivers\rdpwws.sys
06:47:42.0739 6332 RDPWD - ok
06:47:42.0755 6332 [ 4EA225BF1CF05E158853F30A99CA29A7 ] rdyboost
C:\windows\system32\drivers\rdyboost.sys
06:47:42.0786 6332 rdyboost - ok
06:47:42.0833 6332 [ 7B5E1419717FAC363A31CC302895217A ] RemoteAccess
C:\windows\system32\mprdim.dll
06:47:42.0833 6332 RemoteAccess - ok
06:47:42.0864 6332 [ CB9A8683F4EF2BF99E123D79950D7935 ] RemoteRegistry
C:\windows\system32\regsvc.dll
06:47:42.0880 6332 RemoteRegistry - ok
06:47:42.0926 6332 [ CB928D9E6DAF51879DD6BA8D02F01321 ] RFCOMM
C:\windows\system32\DRIVERS\rfcomm.sys
06:47:42.0926 6332 RFCOMM - ok
06:47:42.0958 6332 [ 78D072F35BC45D9E4E1B61895C152234 ] RpcEptMapper
C:\windows\system32\RpcEpMap.dll
06:47:42.0958 6332 RpcEptMapper - ok
06:47:42.0989 6332 [ 94D36C0E44677DD26981D2BFEEF2A29D ] RpcLocator
C:\windows\system32\locator.exe
06:47:43.0004 6332 RpcLocator - ok
06:47:43.0036 6332 [ B82CD39E336973359D7C9BF911E8E84F ] RpcSs

```

```

C:\windows\system32\rpcss.dll
06:47:43.0036 6332 Rpcss - ok
06:47:43.0082 6332 [ 032B0D36AD92B582D869879F5AF5B928 ] rspndr
C:\windows\system32\DRIVERS\rspndr.sys
06:47:43.0082 6332 rspndr - ok
06:47:43.0114 6332 [ 5423D8437051E89DD34749F242C98648 ] s3cap
C:\windows\system32\DRIVERS\vms3cap.sys
06:47:43.0114 6332 s3cap - ok
06:47:43.0145 6332 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] SamSs
C:\windows\system32\lsass.exe
06:47:43.0145 6332 SamSs - ok
06:47:43.0176 6332 [ 662B7F49CB295F15B5A1A36AD3AE9C2C ] sbp2port
C:\windows\system32\DRIVERS\sbp2port.sys
06:47:43.0176 6332 sbp2port - ok
06:47:43.0192 6332 [ 8FC518FFE9519C2631D37515A68009C4 ] SCardSvr
C:\windows\system32\SCardSvr.dll
06:47:43.0207 6332 SCardSvr - ok
06:47:43.0223 6332 [ A95C54B2AC3CC9C73FCDF9E51A1D6B51 ] scfilter
C:\windows\system32\DRIVERS\scfilter.sys
06:47:43.0223 6332 scfilter - ok
06:47:43.0270 6332 [ DF1E5C82E4D09CF8105CC644980C4803 ] schedule
C:\windows\system32\schedsvc.dll
06:47:43.0301 6332 Schedule - ok
06:47:43.0332 6332 [ 628A9E30EC5E18DD5DE6BE4DBDC12198 ] SCPolicySvc
C:\windows\system32\certprop.dll
06:47:43.0332 6332 SCPolicySvc - ok
06:47:43.0348 6332 [ AA826E35F6D28A8E5D1EFEB337F24BA2 ] sdbus
C:\windows\system32\DRIVERS\sdbus.sys
06:47:43.0348 6332 sdbus - ok
06:47:43.0363 6332 [ 5FD90ABDBFAEE85986802622CBB03446 ] SDRSVC
C:\windows\system32\SDRSVC.dll
06:47:43.0379 6332 SDRSVC - ok
06:47:43.0410 6332 [ 90A3935D05B49A5A39D37E71F09A677 ] secdrv
C:\windows\system32\drivers\secdrv.sys
06:47:43.0426 6332 secdrv - ok
06:47:43.0441 6332 [ A59B3A4442C52060CC7A85293AA3546F ] seclogon
C:\windows\system32\seclogon.dll
06:47:43.0457 6332 seclogon - ok
06:47:43.0457 6332 [ DCB7FCDCC97F87360F75D77425B81737 ] SENS
C:\windows\system32\sens.dll
06:47:43.0472 6332 SENS - ok
06:47:43.0488 6332 [ 50087FE1EE447009C9CC2997B90DE53F ] SensrSvc
C:\windows\system32\sensrsvc.dll
06:47:43.0488 6332 SensrSvc - ok
06:47:43.0519 6332 [ 9AD8B8B515E3DF6ACD4212EF465DE2D1 ] Serenum
C:\windows\system32\DRIVERS\serenum.sys
06:47:43.0519 6332 Serenum - ok
06:47:43.0535 6332 [ 5FB7FCEA0490D821F26F39CC5EA3D1E2 ] Serial
C:\windows\system32\DRIVERS\serial.sys
06:47:43.0550 6332 Serial - ok
06:47:43.0566 6332 [ 79BFFB520327FF916A582DFEA17AA813 ] sermouse
C:\windows\system32\DRIVERS\sermouse.sys
06:47:43.0566 6332 sermouse - ok
06:47:43.0597 6332 [ 8F55CE568C543D5ADF45C409D16718FC ] SessionEnv
C:\windows\system32\sessenv.dll
06:47:43.0597 6332 SessionEnv - ok
06:47:43.0597 6332 [ 9F976E1EB233DF46FCE808D9DEA3EB9C ] sffdisk
C:\windows\system32\DRIVERS\sffdisk.sys
06:47:43.0597 6332 sffdisk - ok
06:47:43.0613 6332 [ 932A68EE27833CFD57C1639D375F2731 ] sffp_mmc
C:\windows\system32\DRIVERS\sffp_mmc.sys
06:47:43.0613 6332 sffp_mmc - ok
06:47:43.0613 6332 [ A0708BBD07D245C06FF9DE549CA47185 ] sffp_sd
C:\windows\system32\DRIVERS\sffp_sd.sys
06:47:43.0613 6332 sffp_sd - ok
06:47:43.0628 6332 [ DB96666CC8312EBC45032F30B007A547 ] sfloppy
C:\windows\system32\DRIVERS\sfloppy.sys
06:47:43.0644 6332 sfloppy - ok

```

```

06:47:43.0691 6332 [ D9B734638DD8DBA9D59AAD3189CD0FAD ] sftfs
C:\windows\system32\DRIVERS\Sftfslh.sys
06:47:43.0722 6332 sftfs - ok
06:47:43.0753 6332 [ CB73BC422C07FB611F194DA18D1E7F36 ] sftlist
C:\Program Files\Microsoft Application Virtualization Client\sftlist.exe
06:47:43.0784 6332 sftlist - ok
06:47:43.0800 6332 [ 2F61BD46C0BFF4EB36E1E359CA17BFC5 ] sftplay
C:\windows\system32\DRIVERS\Sftplaylh.sys
06:47:43.0816 6332 sftplay - ok
06:47:43.0831 6332 [ 518BAC0179F94304F422696B47C0EC12 ] sftredir
C:\windows\system32\DRIVERS\Sftredirlh.sys
06:47:43.0831 6332 sftredir - ok
06:47:43.0847 6332 [ 747325236D88B3F05FFD27FF9EC711C5 ] sftvol
C:\windows\system32\DRIVERS\Sftvol1h.sys
06:47:43.0847 6332 sftvol - ok
06:47:43.0862 6332 [ A5812F0281CA5081BF696626F9BF324D ] sftvsa
C:\Program Files\Microsoft Application Virtualization Client\sftvsa.exe
06:47:43.0878 6332 sftvsa - ok
06:47:43.0909 6332 [ D1A079A0DE2EA524513B6930C24527A2 ] SharedAccess
C:\windows\System32\ipnathlp.dll
06:47:43.0925 6332 SharedAccess - ok
06:47:43.0956 6332 [ CD2E48FA5B29EE2B3B5858056D246EF2 ] ShellHWDetection
C:\windows\System32\shsvcs.dll
06:47:43.0987 6332 ShellHWDetection - ok
06:47:44.0003 6332 [ 2565CAC0DC9FE0371BDCE60832582B2E ] sisagp
C:\windows\system32\DRIVERS\sisagp.sys
06:47:44.0003 6332 sisagp - ok
06:47:44.0018 6332 [ A9F0486851BECB6DDA1D89D381E71055 ] SiSRaid2
C:\windows\system32\DRIVERS\SiSRaid2.sys
06:47:44.0018 6332 SiSRaid2 - ok
06:47:44.0034 6332 [ 3727097B55738E2F554972C3BE5BC1AA ] SiSRaid4
C:\windows\system32\DRIVERS\sisraid4.sys
06:47:44.0034 6332 SiSRaid4 - ok
06:47:44.0081 6332 [ 2F5AF9D91D51E832773D4A9EAF65CB33 ] SkypeUpdate
C:\Program Files\Skype\Updater\Updater.exe
06:47:44.0081 6332 SkypeUpdate - ok
06:47:44.0128 6332 [ 3E21C083B8A01CB70BA1F09303010FCE ] Smb
C:\windows\system32\DRIVERS\smb.sys
06:47:44.0128 6332 Smb - ok
06:47:44.0174 6332 [ 6A984831644ECA1A33FFAE4126F4F37 ] SNMPTRAP
C:\windows\System32\snmptrap.exe
06:47:44.0190 6332 SNMPTRAP - ok
06:47:44.0268 6332 [ 1A67C5880233A8BDEA5D9E8B48CD178F ] SNP2UVC
C:\windows\system32\DRIVERS\snp2uvc.sys
06:47:44.0315 6332 SNP2UVC - ok
06:47:44.0330 6332 [ 95CF1AE7527FB70F7816563CBC09D942 ] spldr
C:\windows\system32\drivers\spldr.sys
06:47:44.0330 6332 spldr - ok
06:47:44.0377 6332 [ E17323B0AA9FB3FF9945731D736EDA2F ] Spooler
C:\windows\System32\spoolsv.exe
06:47:44.0393 6332 Spooler - ok
06:47:44.0471 6332 [ 4C287F9069FEDBD791178876EE9DE536 ] sppsvc
C:\windows\system32\sppsvc.exe
06:47:44.0518 6332 sppsvc - ok
06:47:44.0533 6332 [ D8E3E19EEBDAB49DD4A8D3062EAD4EC7 ] sppuinotify
C:\windows\system32\sppuinotify.dll
06:47:44.0533 6332 sppuinotify - ok
06:47:44.0611 6332 [ 83726CF02ECED69138948083E06B6EAC ] SRTSP
C:\windows\System32\Drivers\NIS\1207020.003\SRTSP.SYS
06:47:44.0627 6332 SRTSP - ok
06:47:44.0658 6332 [ 4E7EAB2E5615D39CF1F1DF9C71E5E225 ] SRTSPX
C:\windows\system32\drivers\NIS\1207020.003\SRTSPX.SYS
06:47:44.0658 6332 SRTSPX - ok
06:47:44.0689 6332 [ C4A027B8C0BD3FC0699F41FA5E9E0C87 ] srv
C:\windows\system32\DRIVERS\srv.sys
06:47:44.0705 6332 srv - ok
06:47:44.0736 6332 [ 414BB592CAD8A79649D01F9D94318FB3 ] srv2
C:\windows\system32\DRIVERS\srv2.sys

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:44.0752 6332 srv2 - ok
06:47:44.0767 6332 [ FF207D67700AA18242AAF985D3E7D8F4 ] srvnet
C:\windows\system32\DRIVERS\srvnet.sys
06:47:44.0767 6332 srvnet - ok
06:47:44.0798 6332 [ D887C9FD02AC9FA880F6E5027A43E118 ] SSDPSRV
C:\windows\System32\ssdpsrv.dll
06:47:44.0814 6332 SSDPSRV - ok
06:47:44.0830 6332 [ D318F23BE45D5E3A107469EB64815B50 ] SstpSvc
C:\windows\system32\sstpsvc.dll
06:47:44.0845 6332 SstpSvc - ok
06:47:44.0892 6332 [ 79A7B1C2C15F675BAA919D4D44EC3C7D ] STacSV
C:\Program Files\IDT\WDM\STacSV.exe
06:47:44.0908 6332 STacSV - ok
06:47:44.0954 6332 [ DB32D325C192B801DF274BFD12A7E72B ] stexstor
C:\windows\system32\DRIVERS\stexstor.sys
06:47:44.0954 6332 stexstor - ok
06:47:44.0986 6332 [ C8D2AF5C07D8FE3E088D2E3A3001922C ] STHDA
C:\windows\system32\DRIVERS\stwrt.sys
06:47:45.0017 6332 STHDA - ok
06:47:45.0064 6332 [ A22825E7BB7018E8AF3E229A5AF17221 ] stisvc
C:\windows\System32\wiaservc.dll
06:47:45.0079 6332 stisvc - ok
06:47:45.0110 6332 [ 7731F46EC0D687A931CBA063E8F90EF0 ] stllssvr
C:\Program Files\Common Files\SureThing Shared\stllssvr.exe
06:47:45.0126 6332 stllssvr - ok
06:47:45.0157 6332 [ 957E346CA948668F2496A6CCF6FF82CC ] storflt
C:\windows\system32\DRIVERS\vmstorfl.sys
06:47:45.0157 6332 storflt - ok
06:47:45.0188 6332 [ 0BF669F0A910BEDA4A32258D363AF2A5 ] storSvc
C:\windows\system32\storsvc.dll
06:47:45.0188 6332 storSvc - ok
06:47:45.0204 6332 [ D5751969DC3E4B88BF482AC8EC9FE019 ] storvsc
C:\windows\system32\DRIVERS\storvsc.sys
06:47:45.0204 6332 storvsc - ok
06:47:45.0220 6332 [ E58C78A848ADD9610A4DB6D214AF5224 ] swenum
C:\windows\system32\DRIVERS\swenum.sys
06:47:45.0235 6332 swenum - ok
06:47:45.0266 6332 [ A28BD92DF340E57B024BA433165D34D7 ] swprv
C:\windows\system32\swprv.dll
06:47:45.0298 6332 swprv - ok
06:47:45.0329 6332 [ 9BBEB8C6258E72D62E7560E6667AAD39 ] SymDS
C:\windows\system32\drivers\NIS\1207020.003\SYMDS.SYS
06:47:45.0360 6332 SymDS - ok
06:47:45.0391 6332 [ D5C02629C02A820A7E71BCA3D44294A3 ] SymEFA
C:\windows\system32\drivers\NIS\1207020.003\SYMEFA.SYS
06:47:45.0422 6332 SymEFA - ok
06:47:45.0454 6332 [ AB33C3B196197CA467CBDDA717860DBA ] SymEvent
C:\windows\system32\Drivers\SYMEVENT.SYS
06:47:45.0454 6332 SymEvent - ok
06:47:45.0500 6332 [ A73399804D5D4A8B20BA60FCF70C9F1F ] SymIRON
C:\windows\system32\drivers\NIS\1207020.003\Ironx86.SYS
06:47:45.0500 6332 SymIRON - ok
06:47:45.0547 6332 [ 2C688094650D23B62B0A809DECD0B12F ] SymNets
C:\windows\System32\Drivers\NIS\1207020.003\SYMNETS.SYS
06:47:45.0563 6332 SymNets - ok
06:47:45.0610 6332 [ 480B47D6702ADCE130204F71F116D205 ] SynTP
C:\windows\system32\DRIVERS\SynTP.sys
06:47:45.0625 6332 SynTP - ok
06:47:45.0688 6332 [ 04105C8DA62353589C29BDAEB8D88BD8 ] SysMain
C:\windows\system32\sysmain.dll
06:47:45.0734 6332 SysMain - ok
06:47:45.0750 6332 [ FCFB6C552FBC0DA299799CBD50AD9FD4 ] TabletInputService
C:\windows\System32\TabSvc.dll
06:47:45.0766 6332 TabletInputService - ok
06:47:45.0797 6332 [ 2F46B0C70A4ADC8C90CF825DA3B4FEAF ] Tapisrv
C:\windows\System32\tapisrv.dll
06:47:45.0812 6332 Tapisrv - ok
06:47:45.0812 6332 [ B799D9FDB26111737F58288D8DC172D9 ] TBS

```

```

C:\windows\system32\tbssvc.dll
06:47:45.0828 6332 TBS - ok
06:47:45.0890 6332 [ BBCEAEFF1FD72A026F827CBB2F4AA8AD ] Tcpip
C:\windows\system32\drivers\tcpip.sys
06:47:45.0953 6332 Tcpip - ok
06:47:45.0984 6332 [ BBCEAEFF1FD72A026F827CBB2F4AA8AD ] TCPIP6
C:\windows\system32\DRIVERS\tcpip.sys
06:47:46.0000 6332 TCPIP6 - ok
06:47:46.0015 6332 [ E64444523ADD154F86567C469BC0B17F ] tcpipreg
C:\windows\system32\drivers\tcpipreg.sys
06:47:46.0031 6332 tcpipreg - ok
06:47:46.0046 6332 [ 1875C1490D99E70E449E3AFAE9FCBADF ] TDPIPE
C:\windows\system32\drivers\tdpipe.sys
06:47:46.0046 6332 TDPIPE - ok
06:47:46.0078 6332 [ 7156308896D34EA75A582F9A09E50C17 ] TDTCP
C:\windows\system32\drivers\tdtcp.sys
06:47:46.0078 6332 TDTCP - ok
06:47:46.0093 6332 [ CB39E896A2A83702D1737BFD402B3542 ] tdx
C:\windows\system32\DRIVERS\tdx.sys
06:47:46.0093 6332 tdx - ok
06:47:46.0109 6332 [ C36F41EE20E6999DBF4B0425963268A5 ] TermDD
C:\windows\system32\DRIVERS\termdd.sys
06:47:46.0109 6332 TermDD - ok
06:47:46.0140 6332 [ A01E50A04D7B1960B33E92B9080E6A94 ] TermService
C:\windows\system32\termsrv.dll
06:47:46.0156 6332 TermService - ok
06:47:46.0171 6332 [ 42FB6AFD6B79D9FE07381609172E7CA4 ] Themes
C:\windows\system32\themeservice.dll
06:47:46.0187 6332 Themes - ok
06:47:46.0202 6332 [ 146B6F43A673379A3C670E86D89BE5EA ] THREADORDER
C:\windows\system32\mmcss.dll
06:47:46.0202 6332 THREADORDER - ok
06:47:46.0218 6332 [ 5AD05191DC8B444A7BA4D79B76C42A30 ] TPM
C:\windows\system32\drivers\tpm.sys
06:47:46.0234 6332 TPM - ok
06:47:46.0234 6332 [ 4792C0378DB99A9BC2AE2DE6CFFF0C3A ] TrkWks
C:\windows\system32\trkwks.dll
06:47:46.0234 6332 TrkWks - ok
06:47:46.0296 6332 [ 41A4C781D2286208D397D72099304133 ] TrustedInstaller
C:\windows\servicing\TrustedInstaller.exe
06:47:46.0296 6332 TrustedInstaller - ok
06:47:46.0327 6332 [ 98AE6FA07D12CB4EC5CF4A9BFA5F4242 ] tssecsrv
C:\windows\system32\DRIVERS\tssecsrv.sys
06:47:46.0343 6332 tssecsrv - ok
06:47:46.0358 6332 [ 3E461D890A97F9D4C168F5FDA36E1D00 ] tunnel
C:\windows\system32\DRIVERS\tunnel.sys
06:47:46.0374 6332 tunnel - ok
06:47:46.0390 6332 [ 750FBCB269F4D7DD2E420C56B795DB6D ] uagp35
C:\windows\system32\DRIVERS\uagp35.sys
06:47:46.0390 6332 uagp35 - ok
06:47:46.0452 6332 [ E92F73AD3E9FEF408422B4555B95B02E ] uArcCapture
C:\windows\system32\ArcVCapRender\uArcCapture.exe
06:47:46.0514 6332 uArcCapture - ok
06:47:46.0546 6332 [ 6557D75E8B7D6A06CDC21CD39DBF255C ] udfs
C:\windows\system32\DRIVERS\udfs.sys
06:47:46.0546 6332 udfs - ok
06:47:46.0577 6332 [ 8344FD4FCE927880AA1AA7681D4927E5 ] UI0Detect
C:\windows\system32\UI0Detect.exe
06:47:46.0577 6332 UI0Detect - ok
06:47:46.0592 6332 [ 44E8048ACE47BEFBFDC2E9BE4CBC8880 ] uliagpkx
C:\windows\system32\DRIVERS\uliagpkx.sys
06:47:46.0592 6332 uliagpkx - ok
06:47:46.0608 6332 [ 049B3A50B3D646BAEEEE9EEC9B0668DC ] umbus
C:\windows\system32\DRIVERS\umbus.sys
06:47:46.0608 6332 umbus - ok
06:47:46.0624 6332 [ 7550AD0C6998BA1CB4843E920EE0FEAC ] UmPass
C:\windows\system32\DRIVERS\umpass.sys
06:47:46.0624 6332 UmPass - ok

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:46.0639 6332 [ 8ECA5454844F66386F7BE4AE0D7CD1 ] UmRdpService
C:\windows\system32\umrdp.dll
06:47:46.0639 6332 UmRdpService - ok
06:47:46.0780 6332 [ A69CD6BDB82872999D2E46F9324ADA83 ] UNS
C:\Program Files\Intel\Intel(R) Management Engine Components\UNS\UNS.exe
06:47:46.0873 6332 UNS - ok
06:47:46.0889 6332 [ 833FBB672460EFCE8011D262175FAD33 ] upnphost
C:\windows\system32\upnphost.dll
06:47:46.0920 6332 upnphost - ok
06:47:46.0936 6332 [ 5C233AEFB566EE78C1EFBC0493FB066A ] usbccgp
C:\windows\system32\DRIVERS\usbccgp.sys
06:47:46.0936 6332 usbccgp - ok
06:47:46.0951 6332 [ 04EC7CEC62EC3B6D9354EEE93327FC82 ] usbcir
C:\windows\system32\DRIVERS\usbcir.sys
06:47:46.0951 6332 usbcir - ok
06:47:46.0982 6332 [ 5B71019A6ACA0116FD21B368F19C0B91 ] usbehci
C:\windows\system32\drivers\usbehci.sys
06:47:46.0982 6332 usbehci - ok
06:47:47.0014 6332 [ 5823D3965C2A4F6F785ED1A3B403F3B8 ] usbhub
C:\windows\system32\DRIVERS\usbhub.sys
06:47:47.0029 6332 usbhub - ok
06:47:47.0045 6332 [ E753ED6C49DA13967EBABF9EA616454A ] usbohci
C:\windows\system32\drivers\usbohci.sys
06:47:47.0045 6332 usbohci - ok
06:47:47.0076 6332 [ 797D862FE0875E75C7CC4C1AD7B30252 ] usbprint
C:\windows\system32\DRIVERS\usbprint.sys
06:47:47.0076 6332 usbprint - ok
06:47:47.0092 6332 [ 1C4287739A93594E57E2A9E6A3ED7353 ] USBSTOR
C:\windows\system32\drivers\USBSTOR.SYS
06:47:47.0092 6332 USBSTOR - ok
06:47:47.0107 6332 [ 6A30928A469CE802600E1EA8C0F2F53F ] usbhci
C:\windows\system32\drivers\usbhici.sys
06:47:47.0107 6332 usbhici - ok
06:47:47.0138 6332 [ B5F6A992D996282B7FAE7048E50AF83A ] usbvideo
C:\windows\system32\Drivers\usbvideo.sys
06:47:47.0138 6332 usbvideo - ok
06:47:47.0154 6332 [ 081E6E1C91AEC36758902A9F727CD23C ] UxSms
C:\windows\system32\uxsms.dll
06:47:47.0154 6332 UxSms - ok
06:47:47.0170 6332 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] VaultSvc
C:\windows\system32\lsass.exe
06:47:47.0170 6332 VaultSvc - ok
06:47:47.0263 6332 [ 60CF5CBC7F5349E1400B6554E0F040A7 ] vcsFPService
C:\windows\system32\vcsFPService.exe
06:47:47.0450 6332 vcsFPService - ok
06:47:47.0466 6332 [ A059C4C3EDB09E07D21A8E5C0AABD3CB ] vdrvroot
C:\windows\system32\DRIVERS\vdrvroot.sys
06:47:47.0482 6332 vdrvroot - ok
06:47:47.0497 6332 [ 8C4E7C49D3641BC9E299E466A7F8867D ] vds
C:\windows\system32\vds.exe
06:47:47.0513 6332 vds - ok
06:47:47.0528 6332 [ 17C408214EA61696CEC9C66E388B14F3 ] vga
C:\windows\system32\DRIVERS\vgapnp.sys
06:47:47.0544 6332 vga - ok
06:47:47.0544 6332 [ 8E38096AD5C8570A6F1570A61E251561 ] VgaSave
C:\windows\system32\drivers\vga.sys
06:47:47.0544 6332 VgaSave - ok
06:47:47.0560 6332 [ 3BE6E1F3A4F1AFEC8CEE0D7883F93583 ] vhdmp
C:\windows\system32\DRIVERS\vhdmp.sys
06:47:47.0560 6332 vhdmp - ok
06:47:47.0591 6332 [ C829317A37B4BEA8F39735D4B076E923 ] viaagp
C:\windows\system32\DRIVERS\viaagp.sys
06:47:47.0591 6332 viaagp - ok
06:47:47.0591 6332 [ E02F079A6AA107F06B16549C6E5C7B74 ] viac7
C:\windows\system32\DRIVERS\viac7.sys
06:47:47.0591 6332 viac7 - ok
06:47:47.0606 6332 [ E43574F6A56A0EE11809B48C09E4FD3C ] viaide
C:\windows\system32\DRIVERS\viaide.sys

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:47.0606 6332 viaide - ok
06:47:47.0622 6332 [ 379B349F65F453D2A6E75EA6B7448E49 ] vmbus
C:\windows\system32\DRIVERS\vmbus.sys
06:47:47.0638 6332 vmbus - ok
06:47:47.0638 6332 [ EC2BBAB4B84D0738C6C83D2234DC36FE ] VMBusHID
C:\windows\system32\DRIVERS\VMBusHID.sys
06:47:47.0638 6332 VMBusHID - ok
06:47:47.0653 6332 [ 384E5A2AA49934295171E499F86BA6F3 ] volmgr
C:\windows\system32\DRIVERS\volmgr.sys
06:47:47.0653 6332 volmgr - ok
06:47:47.0669 6332 [ B5BB72067DDDBBFB04B2F89FF8C3C87 ] volmgrx
C:\windows\system32\drivers\volmgrx.sys
06:47:47.0684 6332 volmgrx - ok
06:47:47.0716 6332 [ 59F06B4968E58BC83DFC56CA4517960E ] volsnap
C:\windows\system32\drivers\volmgrx.sys
06:47:47.0716 6332 volsnap - ok
06:47:47.0731 6332 [ 33E74DF34753FCAAB06F6F2BDC8CABF5 ] vpcbus
C:\windows\system32\DRIVERS\vpchbus.sys
06:47:47.0731 6332 vpcbus - ok
06:47:47.0731 6332 [ 5F04362CEB5FB5901037E9D9EADD3760 ] vpcnfltr
C:\windows\system32\DRIVERS\vpchbus.sys
06:47:47.0747 6332 vpcnfltr - ok
06:47:47.0762 6332 [ 625088D6EE9EDE977FD03CF18D1CD5C5 ] vpcusb
C:\windows\system32\DRIVERS\vpchbus.sys
06:47:47.0762 6332 vpcusb - ok
06:47:47.0778 6332 [ 1023C696D42268E9071BB376DBEC8396 ] vpcvmm
C:\windows\system32\drivers\vpchbus.sys
06:47:47.0794 6332 vpcvmm - ok
06:47:47.0809 6332 [ 9DFA0CC2F8855A04816729651175B631 ] vsmraid
C:\windows\system32\DRIVERS\vpchbus.sys
06:47:47.0809 6332 vsmraid - ok
06:47:47.0840 6332 [ 7EA2BCD94D9CFAF4C556F5CC94532A6C ] VSS
C:\windows\system32\ssvc.exe
06:47:47.0887 6332 VSS - ok
06:47:47.0887 6332 [ 90567B1E658001E79D7C8BBD3DDE5AA6 ] vwifibus
C:\windows\system32\DRIVERS\vwifibus.sys
06:47:47.0887 6332 vwifibus - ok
06:47:47.0903 6332 [ 7090D3436EEB4E7DA3373090A23448F7 ] vwififlt
C:\windows\system32\DRIVERS\vwifibus.sys
06:47:47.0903 6332 vwififlt - ok
06:47:47.0934 6332 [ 55187FD710E27D5095D10A472C8BAF1C ] w32Time
C:\windows\system32\w32time.dll
06:47:47.0934 6332 w32Time - ok
06:47:47.0965 6332 [ 427A8BC96F16C40DF81C2D2F4EDD32DD ] wacomousefilter
C:\windows\system32\DRIVERS\wacomousefilter.sys
06:47:47.0965 6332 wacomousefilter - ok
06:47:47.0981 6332 [ DE3721E89C653AA281428C8A69745D90 ] wacomPen
C:\windows\system32\DRIVERS\wacompen.sys
06:47:47.0981 6332 wacomPen - ok
06:47:48.0012 6332 [ 846B58EA44BF8C92E4B59F4E2252C4C0 ] wacomvhid
C:\windows\system32\DRIVERS\wacomvhid.sys
06:47:48.0012 6332 wacomvhid - ok
06:47:48.0028 6332 [ C497C0A80BAD225244B1CA6C86FA3463 ] wacomVTHid
C:\windows\system32\DRIVERS\wacomVTHid.sys
06:47:48.0043 6332 wacomVTHid - ok
06:47:48.0043 6332 [ 692A712062146E96D28BA0B7D75DE31B ] WANARP
C:\windows\system32\DRIVERS\wanarp.sys
06:47:48.0043 6332 WANARP - ok
06:47:48.0059 6332 [ 692A712062146E96D28BA0B7D75DE31B ] wanarpv6
C:\windows\system32\DRIVERS\wanarp.sys
06:47:48.0059 6332 wanarpv6 - ok
06:47:48.0121 6332 [ 353A04C273EC58475D8633E75CCD5604 ] watAdminSvc
C:\windows\system32\wat\watAdminSvc.exe
06:47:48.0152 6332 watAdminSvc - ok
06:47:48.0215 6332 [ 7790B77FE1E5EE47DCC66247095BB4C9 ] wbengine
C:\windows\system32\wbengine.exe
06:47:48.0277 6332 wbengine - ok
06:47:48.0308 6332 [ 9614B5D29DC76AC3C29F6D2D3AA70E67 ] wbioSrv

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

C:\windows\system32\wbiosrv.dll
06:47:48.0308 6332 wbioSrv - ok
06:47:48.0340 6332 [ 6D9B75275C3E3A5F51AEF81AFFADB2B6 ] wcnscsv
C:\windows\system32\wcnscsv.dll
06:47:48.0355 6332 wcnscsv - ok
06:47:48.0371 6332 [ 5D930B6357A6D2AF4D7653BDABBF352F ] WcsPlugInService
C:\windows\system32\WcsPlugInService.dll
06:47:48.0371 6332 WcsPlugInService - ok
06:47:48.0402 6332 [ 1112A9BADACB47B7C0BB0392E3158DFF ] wd
C:\windows\system32\DRIVERS\wd.sys
06:47:48.0402 6332 wd - ok
06:47:48.0449 6332 [ A840213F1ACDCC175B4D1D5AAEAC0D7A ] wdf01000
C:\windows\system32\drivers\wdf01000.sys
06:47:48.0464 6332 wdf01000 - ok
06:47:48.0496 6332 [ 46EF9DC96265FD0B423DB72E7C38C2A5 ] wdiServiceHost
C:\windows\system32\wdi.dll
06:47:48.0511 6332 wdiServiceHost - ok
06:47:48.0527 6332 [ 46EF9DC96265FD0B423DB72E7C38C2A5 ] wdiSystemHost
C:\windows\system32\wdi.dll
06:47:48.0527 6332 wdiSystemHost - ok
06:47:48.0558 6332 [ BB5EC38F8D4600119B4720BC5D4211F1 ] WebClient
C:\windows\system32\webclnt.dll
06:47:48.0589 6332 WebClient - ok
06:47:48.0620 6332 [ 760F0AFE937A77CFF27153206534F275 ] wecsvc
C:\windows\system32\wecsvc.dll
06:47:48.0636 6332 wecsvc - ok
06:47:48.0667 6332 [ AC804569BB2364FB6017370258A4091B ] wercplsupport
C:\windows\system32\wercplsupport.dll
06:47:48.0667 6332 wercplsupport - ok
06:47:48.0698 6332 [ 08E420D873E4FD85241EE2421B02C4A4 ] wercplsupport
C:\windows\system32\wercplsupport.dll
06:47:48.0714 6332 wercplsupport - ok
06:47:48.0730 6332 [ 8B9A943F3B53861F2BFAF6C186168F79 ] wfpLwf
C:\windows\system32\DRIVERS\wfpLwf.sys
06:47:48.0730 6332 wfpLwf - ok
06:47:48.0745 6332 [ 5CF95B35E59E2A38023836FFF31BE64C ] WIMMount
C:\windows\system32\drivers\wimmount.sys
06:47:48.0761 6332 WIMMount - ok
06:47:48.0823 6332 [ 3FAE8F94296001C32EAB62CD7D82E0FD ] winDefend
C:\Program Files\windows Defender\mpsvc.dll
06:47:48.0839 6332 winDefend - ok
06:47:48.0870 6332 winHttpAutoProxySvc - ok
06:47:48.0917 6332 [ F62E510B6AD4C21EB9FE8668ED251826 ] winmgmt
C:\windows\system32\wbem\WMISvc.dll
06:47:48.0932 6332 winmgmt - ok
06:47:48.0979 6332 [ C4F5D3901D1B41D602DDC196E0B95B51 ] winRM
C:\windows\system32\wsmSvc.dll
06:47:49.0010 6332 winRM - ok
06:47:49.0057 6332 [ B5BA3CC19D00F2EBA92F1CFBEBB5D650 ] winUSB
C:\windows\system32\DRIVERS\winUSB.sys
06:47:49.0057 6332 winUSB - ok
06:47:49.0088 6332 [ FF17B6A01A9FEB2A8D322BF369D36C96 ] wisdpen
C:\windows\system32\DRIVERS\wisdpen.sys
06:47:49.0088 6332 wisdpen - ok
06:47:49.0120 6332 [ 16935C98FF639D185086A3529B1F2067 ] wlansvc
C:\windows\system32\wlansvc.dll
06:47:49.0151 6332 wlansvc - ok
06:47:49.0213 6332 [ 5144AE67D60EC653F97DDF3FEED29E77 ] wldidsvc
C:\Program Files\Common Files\Microsoft Shared\windows Live\WLIDSVC.EXE
06:47:49.0244 6332 wldidsvc - ok
06:47:49.0260 6332 [ 0217679B8FCA58714C3BF2726D2CA84E ] wmiAcpi
C:\windows\system32\DRIVERS\wmiacpi.sys
06:47:49.0260 6332 wmiAcpi - ok
06:47:49.0291 6332 [ 6EB6B66517B048D87DC1856DDF1F4C3F ] wmiApSrv
C:\windows\system32\wbem\wmiApSrv.exe
06:47:49.0307 6332 wmiApSrv - ok
06:47:49.0354 6332 [ 77FBD400984CF72BA0FC4B3489D65F74 ] WMPNetworkSvc
C:\Program Files\windows Media Player\wmpnetwk.exe

```

TDSKiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:47:49.0400 6332 WMPNetworkSvc - ok
06:47:49.0416 6332 [ A2F0EC770A92F2B3F9DE6D518E11409C ] WPCsvcs
C:\windows\system32\wpcsvc.dll
06:47:49.0432 6332 WPCsvcs - ok
06:47:49.0447 6332 [ B7F658A2EBC07129538AD9AB35212637 ] WPDBusEnum
C:\windows\system32\wpdbusenum.dll
06:47:49.0447 6332 WPDBusEnum - ok
06:47:49.0478 6332 [ 6DB3276587B853BF886B69528FDB048C ] ws2ifsl
C:\windows\system32\drivers\ws2ifsl.sys
06:47:49.0478 6332 ws2ifsl - ok
06:47:49.0494 6332 [ A661A76333057B383A06E65F0073222F ] wscsvcs
C:\windows\system32\wscsvcs.dll
06:47:49.0494 6332 wscsvcs - ok
06:47:49.0494 6332 WSearch - ok
06:47:49.0588 6332 [ 8A9ECBFB1B822EC2D9E140DF0DA21BA3 ] WTouchService
C:\Program Files\WTouch\WTouchService.exe
06:47:49.0634 6332 WTouchService - ok
06:47:49.0681 6332 [ FC3EC24FCE372C89423E015A2AC1A31E ] wuauerv
C:\windows\system32\wuaueng.dll
06:47:49.0744 6332 wuauerv - ok
06:47:49.0775 6332 [ 06E6F32C8D0A3F66D956F57B43A2E070 ] wudfPf
C:\windows\system32\drivers\wudfPf.sys
06:47:49.0775 6332 wudfPf - ok
06:47:49.0822 6332 [ 867C301E8B790040AE9CF6486E8041DF ] WUDFRd
C:\windows\system32\DRIVERS\WUDFRd.sys
06:47:49.0822 6332 WUDFRd - ok
06:47:49.0853 6332 [ FE47B7BC8EA320C2D9B5E5BF6E303765 ] wudfsvc
C:\windows\system32\WUDFSvc.dll
06:47:49.0868 6332 wudfsvc - ok
06:47:49.0900 6332 [ FF2D745B560F7C71B31F30F4D49F73D2 ] wwanSvc
C:\windows\system32\wwansvc.dll
06:47:49.0915 6332 wwanSvc - ok
06:47:49.0962 6332 ===== Scan global =====
06:47:49.0993 6332 [ 9A595DF601070DA78C40481120DD2C06 ]
C:\windows\system32\basesrv.dll
06:47:50.0024 6332 [ 8531AAF69394EFB93BC653916C46D245 ]
C:\windows\system32\winsrv.dll
06:47:50.0056 6332 [ 8531AAF69394EFB93BC653916C46D245 ]
C:\windows\system32\winsrv.dll
06:47:50.0087 6332 [ 364455805E64882844EE9ACB72522830 ]
C:\windows\system32\sxssrv.dll
06:47:50.0118 6332 [ 5F1B6A9C35D3D5CA72D6D6FDEF9747D6 ]
C:\windows\system32\services.exe
06:47:50.0134 6332 [Global] - ok
06:47:50.0134 6332 ===== Scan MBR =====
06:47:50.0149 6332 [ A36C5E4F47E84449FF07ED3517B43A31 ] \Device\Harddisk0\DR0
06:47:50.0539 6332 \Device\Harddisk0\DR0 - ok
06:47:50.0539 6332 ===== Scan VBR =====
06:47:50.0570 6332 [ 8CBB78C18728ED4B40486C51DA75EAA9 ]
\Device\Harddisk0\DR0\Partition1
06:47:50.0570 6332 \Device\Harddisk0\DR0\Partition1 - ok
06:47:50.0586 6332 [ 8C3EE3CBE82BA2D5CC0DD2DC8A9731CA ]
\Device\Harddisk0\DR0\Partition2
06:47:50.0602 6332 \Device\Harddisk0\DR0\Partition2 - ok
06:47:50.0633 6332 [ D09097A1C75BB9B87169F378D7C8541F ]
\Device\Harddisk0\DR0\Partition3
06:47:50.0648 6332 \Device\Harddisk0\DR0\Partition3 - ok
06:47:50.0664 6332 [ C22C4B1B501C2CF8EA1F7E7712D8DB9D ]
\Device\Harddisk0\DR0\Partition4
06:47:50.0664 6332 \Device\Harddisk0\DR0\Partition4 - ok
06:47:50.0664 6332 =====
06:47:50.0664 6332 Scan finished
06:47:50.0664 6332 =====
06:47:50.0695 5524 Detected object count: 0
06:47:50.0695 5524 Actual detected object count: 0
06:48:38.0880 4280 =====
06:48:38.0880 4280 Scan started
06:48:38.0880 4280 Mode: Manual;

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:48:38.0880 4280 =====
06:48:39.0629 4280 ===== Scan system memory =====
06:48:39.0629 4280 System memory - ok
06:48:39.0629 4280 ===== Scan services =====
06:48:39.0848 4280 [ BF02F806C873ABB04B197161E8E5A316 ] 1394ohci
C:\windows\system32\DRIVERS\1394ohci.sys
06:48:39.0848 4280 1394ohci - ok
06:48:39.0879 4280 [ 10DD847C196782B0A5F05F6CDD91872E ] Accelerometer
C:\windows\system32\DRIVERS\Accelerometer.sys
06:48:39.0879 4280 Accelerometer - ok
06:48:39.0910 4280 [ F0E07D144C8685B8774BC32FC8DA4DF0 ] ACPI
C:\windows\system32\DRIVERS\ACPI.sys
06:48:39.0910 4280 ACPI - ok
06:48:39.0941 4280 [ 98D81CA942D19F7D9153B095162AC013 ] AcpiPmi
C:\windows\system32\DRIVERS\acpipmi.sys
06:48:39.0941 4280 AcpiPmi - ok
06:48:39.0957 4280 [ 21E785EBD7DC90A06391141AAC7892FB ] adp94xx
C:\windows\system32\DRIVERS\adp94xx.sys
06:48:39.0972 4280 adp94xx - ok
06:48:39.0988 4280 [ 0C676BC278D5B59FF5ABD57BBE9123F2 ] adpahci
C:\windows\system32\DRIVERS\adpahci.sys
06:48:39.0988 4280 adpahci - ok
06:48:40.0004 4280 [ 7C7B5EE4B7B822EC85321FE23A27DB33 ] adpu320
C:\windows\system32\DRIVERS\adpu320.sys
06:48:40.0019 4280 adpu320 - ok
06:48:40.0050 4280 [ 8B5EEFEEC1E6D1A72A06C526628AD161 ] AeLookupSvc
C:\windows\system32\aelupsvc.dll
06:48:40.0050 4280 AeLookupSvc - ok
06:48:40.0175 4280 [ 827DBC22C96EECF6D36A13162FABAFD3 ] AESTFilters
C:\Program Files\IDT\WDM\ aestsrv.exe
06:48:40.0175 4280 AESTFilters - ok
06:48:40.0206 4280 [ 0DB7A48388D54D154EBEC120461A0FCD ] AFD
C:\windows\system32\drivers\afd.sys
06:48:40.0206 4280 AFD - ok
06:48:40.0253 4280 [ 7E10E3BB9B258AD8A9300F91214D67B9 ] AgereSoftModem
C:\windows\system32\DRIVERS\AGRSM.sys
06:48:40.0269 4280 AgereSoftModem - ok
06:48:40.0300 4280 [ 507812C3054C21CEF746B6EE3D04DD6E ] agp440
C:\windows\system32\DRIVERS\agp440.sys
06:48:40.0300 4280 agp440 - ok
06:48:40.0316 4280 [ 8B30250D573A8F6B4BD23195160D8707 ] aic78xx
C:\windows\system32\DRIVERS\djsvs.sys
06:48:40.0316 4280 aic78xx - ok
06:48:40.0347 4280 [ 18A54E132947CD98FEA9ACCC57F98F13 ] ALG
C:\windows\system32\alg.exe
06:48:40.0347 4280 ALG - ok
06:48:40.0362 4280 [ 0D40BCF52EA90FC7DF2AEAB6503DEA44 ] aliide
C:\windows\system32\DRIVERS\aliide.sys
06:48:40.0378 4280 aliide - ok
06:48:40.0378 4280 [ 3C6600A0696E90A463771C7422E23AB5 ] amdagp
C:\windows\system32\DRIVERS\amdagp.sys
06:48:40.0378 4280 amdagp - ok
06:48:40.0394 4280 [ CD5914170297126B6266860198D1D4F0 ] amdide
C:\windows\system32\DRIVERS\amdide.sys
06:48:40.0394 4280 amdide - ok
06:48:40.0409 4280 [ 00DDA200D71BAC534BF56A9DB5DFD666 ] AmdK8
C:\windows\system32\DRIVERS\amdk8.sys
06:48:40.0409 4280 AmdK8 - ok
06:48:40.0425 4280 [ 3CBF30F5370FDA40DD3E87DF38EA53B6 ] AmdPPM
C:\windows\system32\DRIVERS\amdppm.sys
06:48:40.0425 4280 AmdPPM - ok
06:48:40.0472 4280 [ 19CE906B4CDC11FC4FEF5745F33A63B6 ] amdsata
C:\windows\system32\drivers\amdsata.sys
06:48:40.0472 4280 amdsata - ok
06:48:40.0487 4280 [ EA43AF0C423FF267355F74E7A53BDABA ] amdsbs
C:\windows\system32\DRIVERS\amdsbs.sys
06:48:40.0487 4280 amdsbs - ok
06:48:40.0534 4280 [ 869E67D66BE326A5A9159FBA8746FA70 ] amdxtata

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt
 C:\windows\system32\drivers\amdxdx.sys
 06:48:40.0534 4280 amdxdx - ok
 06:48:40.0581 4280 [E4EDE40F326B3B815EC06FF03A8697D6] ameisvc
 C:\Program Files\T-Mobile\web'n'walk Manager\ameisvc.exe
 06:48:40.0581 4280 ameisvc - ok
 06:48:40.0596 4280 [FEB834C02CE1E84B6A38F953CA067706] AppID
 C:\windows\system32\drivers\appid.sys
 06:48:40.0596 4280 AppID - ok
 06:48:40.0643 4280 [62A9C86CB6085E20DB4823E4E97826F5] AppIDSvc
 C:\windows\system32\appidsvc.dll
 06:48:40.0643 4280 AppIDSvc - ok
 06:48:40.0659 4280 [7DEAD9E3F65DCB2794F2711003BBF650] Appinfo
 C:\windows\system32\appinfo.dll
 06:48:40.0659 4280 Appinfo - ok
 06:48:40.0674 4280 [A45D184DF6A8803DA13A0B329517A64A] AppMgmt
 C:\windows\system32\appmgmts.dll
 06:48:40.0690 4280 AppMgmt - ok
 06:48:40.0706 4280 [2932004F49677BD84DBC72EDB754FFB3] arc
 C:\windows\system32\DRIVERS\arc.sys
 06:48:40.0706 4280 arc - ok
 06:48:40.0721 4280 [5D6F36C46FD283AE1B57BD2E9FEB0BC7] arcsas
 C:\windows\system32\DRIVERS\arcsas.sys
 06:48:40.0721 4280 arcsas - ok
 06:48:40.0768 4280 [0309F8D544F565BE13EEFC21824CA827] ARCVCM
 C:\windows\system32\DRIVERS\ArcSoftVCMcapture.sys
 06:48:40.0768 4280 ARCVCM - ok
 06:48:40.0862 4280 [776ACEFA0CA9DF0FAA51A5FB2F435705] aspnet_state
 C:\windows\Microsoft.NET\Framework\v4.0.30319\aspnet_state.exe
 06:48:40.0862 4280 aspnet_state - ok
 06:48:40.0877 4280 [ADD2ADE1C2B285AB8378D2DAAF991481] AsyncMac
 C:\windows\system32\DRIVERS\asynmac.sys
 06:48:40.0877 4280 AsyncMac - ok
 06:48:40.0908 4280 [338C86357871C167A96AB976519BF59E] atapi
 C:\windows\system32\DRIVERS\atapi.sys
 06:48:40.0908 4280 atapi - ok
 06:48:40.0940 4280 [510C873BFA135AA829F4180352772734] AudioEndpointBuilder
 C:\windows\system32\Audiosrv.dll
 06:48:40.0955 4280 AudioEndpointBuilder - ok
 06:48:41.0002 4280 [510C873BFA135AA829F4180352772734] Audiosrv
 C:\windows\system32\Audiosrv.dll
 06:48:41.0002 4280 Audiosrv - ok
 06:48:41.0049 4280 [DD6A431B43E34B91A767D1CE33728175] AxInstSV
 C:\windows\system32\AxInstSV.dll
 06:48:41.0049 4280 AxInstSV - ok
 06:48:41.0096 4280 [1A231ABEC60FD316EC54C66715543CEC] b06bdrv
 C:\windows\system32\DRIVERS\bxvbdx.sys
 06:48:41.0111 4280 b06bdrv - ok
 06:48:41.0127 4280 [BD8869EB9CDE6BBE4508D869929869EE] b57nd60x
 C:\windows\system32\DRIVERS\b57nd60x.sys
 06:48:41.0127 4280 b57nd60x - ok
 06:48:41.0220 4280 [A2494901E7226B356B8C1005C45F1C5F] BBSvc
 C:\Program Files\Microsoft\BingBar\7.1.361.0\BBSvc.exe
 06:48:41.0220 4280 BBSvc - ok
 06:48:41.0252 4280 [63B1CBBAE4790B5BAC98F01BF9449722] BBUpdate
 C:\Program Files\Microsoft\BingBar\7.1.361.0\SeaPort.exe
 06:48:41.0252 4280 BBUpdate - ok
 06:48:41.0267 4280 [EE1E9C3BB8228AE423DD38DB69128E71] BDESVC
 C:\windows\system32\bdesvc.dll
 06:48:41.0267 4280 BDESVC - ok
 06:48:41.0298 4280 [505506526A9D467307B3C393DEDAF858] Beep
 C:\windows\system32\drivers\Beep.sys
 06:48:41.0298 4280 Beep - ok
 06:48:41.0330 4280 [85AC71C045CEB054ED48A7841AAE0C11] BFE
 C:\windows\system32\bfe.dll
 06:48:41.0330 4280 BFE - ok
 06:48:41.0454 4280 [75A51EA67D28E41543B8B354A47DF430] BHDrvx86
 C:\ProgramData\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NIS_18.1.0.37\Defin
 itions\BASHDefs\20130322.001\BHDrvx86.sys

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:48:41.0470 4280 BHDrvx86 - ok
06:48:41.0501 4280 [ 53F476476F55A27F580661BDE09C4EC4 ] BITS
C:\windows\system32\qmgr.dll
06:48:41.0517 4280 BITS - ok
06:48:41.0548 4280 [ 2287078ED48FCFC477B05B20CF38F36F ] blbdrive
C:\windows\system32\DRIVERS\blbdrive.sys
06:48:41.0564 4280 blbdrive - ok
06:48:41.0579 4280 [ 9A5C671B7FBAE4865149BB11F59B91B2 ] bowser
C:\windows\system32\DRIVERS\bowser.sys
06:48:41.0579 4280 bowser - ok
06:48:41.0610 4280 [ 9F9ACC7F7CCDE8A15C282D3F88B43309 ] BrFiltLo
C:\windows\system32\DRIVERS\BrFiltLo.sys
06:48:41.0610 4280 BrFiltLo - ok
06:48:41.0626 4280 [ 56801AD62213A41F6497F96DEE83755A ] BrFiltUp
C:\windows\system32\DRIVERS\BrFiltUp.sys
06:48:41.0626 4280 BrFiltUp - ok
06:48:41.0657 4280 [ A0E691DC6589D4D2CBE373171D1A49E5 ] Browser
C:\windows\system32\browser.dll
06:48:41.0657 4280 Browser - ok
06:48:41.0673 4280 [ 845B8CE732E67F3B4133164868C666EA ] Brserid
C:\windows\system32\Drivers\Brserid.sys
06:48:41.0688 4280 Brserid - ok
06:48:41.0688 4280 [ 203F0B1E73ADADBBB7B7B1FABD901F6B ] BrSerWdm
C:\windows\system32\Drivers\BrSerWdm.sys
06:48:41.0704 4280 BrSerWdm - ok
06:48:41.0704 4280 [ BD456606156BA17E60A04E18016AE54B ] BrUsbMdm
C:\windows\system32\Drivers\BrUsbMdm.sys
06:48:41.0704 4280 BrUsbMdm - ok
06:48:41.0720 4280 [ AF72ED54503F717A43268B3CC5FAEC2E ] BrUsbSer
C:\windows\system32\Drivers\BrUsbSer.sys
06:48:41.0720 4280 BrUsbSer - ok
06:48:41.0735 4280 [ 2865A5C8E98C70C605F417908CEBB3A4 ] BthEnum
C:\windows\system32\drivers\BthEnum.sys
06:48:41.0751 4280 BthEnum - ok
06:48:41.0751 4280 [ ED3DF7C56CE0084EB2034432FC56565A ] BTHMODEM
C:\windows\system32\DRIVERS\bthmodem.sys
06:48:41.0751 4280 BTHMODEM - ok
06:48:41.0798 4280 [ AD1872E5829E8A2C3B5B4B641C3EAB0E ] BthPan
C:\windows\system32\DRIVERS\bthpan.sys
06:48:41.0798 4280 BthPan - ok
06:48:41.0829 4280 [ 3D43C01E9B134C6BF38A37C9354B2504 ] BTHPORT
C:\windows\system32\Drivers\BTHport.sys
06:48:41.0829 4280 BTHPORT - ok
06:48:41.0860 4280 [ 1DF19C96EEF6C29D1C3E1A8678E07190 ] bthserv
C:\windows\system32\bthserv.dll
06:48:41.0860 4280 bthserv - ok
06:48:41.0876 4280 [ FCD2ADFC38D5A4E3BDA7F85E37160CAE ] BTHUSB
C:\windows\system32\Drivers\BTHUSB.sys
06:48:41.0876 4280 BTHUSB - ok
06:48:41.0922 4280 [ 525432CFD6D8C004860AF7ECD0A84234 ] btwampfl
C:\windows\system32\drivers\btwampfl.sys
06:48:41.0922 4280 btwampfl - ok
06:48:41.0938 4280 [ CF8799A563F734984D4E053CACEC1426 ] btwaudio
C:\windows\system32\drivers\btwaudio.sys
06:48:41.0938 4280 btwaudio - ok
06:48:41.0954 4280 [ 9ED9932043D599AEA04F6EA2D86964A1 ] btwavdt
C:\windows\system32\drivers\btwavdt.sys
06:48:41.0969 4280 btwavdt - ok
06:48:42.0016 4280 [ 110496CF8143FEA63B7A31DAD175829B ] btwdins
C:\Program Files\WIDCOMM\Bluetooth Software\btwdins.exe
06:48:42.0032 4280 btwdins - ok
06:48:42.0047 4280 [ DE53089F0678CB5F0AFEB867ACB0FB05 ] btwl2cap
C:\windows\system32\DRIVERS\btwl2cap.sys
06:48:42.0047 4280 btwl2cap - ok
06:48:42.0063 4280 [ 373D1BB0F7DC8F1931F9B7E0DE3E9A30 ] btwrchid
C:\windows\system32\DRIVERS\btwrchid.sys
06:48:42.0063 4280 btwrchid - ok
06:48:42.0094 4280 [ 77EA11B065E0A8AB902D78145CA51E10 ] cdifs

```

```

C:\windows\system32\DRIVERS\cdfs.sys
06:48:42.0094 4280 cdfs - ok
06:48:42.0125 4280 [ BA6E70AA0E6091BC39DE29477D866A77 ] cdrom
C:\windows\system32\DRIVERS\cdrom.sys
06:48:42.0125 4280 cdrom - ok
06:48:42.0156 4280 [ 628A9E30EC5E18DD5DE6BE4DBDC12198 ] CertPropSvc
C:\windows\system32\certprop.dll
06:48:42.0156 4280 CertPropSvc - ok
06:48:42.0172 4280 [ 3FE3FE94A34DF6FB06E6418D0F6A0060 ] circlass
C:\windows\system32\DRIVERS\circlass.sys
06:48:42.0172 4280 circlass - ok
06:48:42.0203 4280 [ 635181E0E9BBF16871BF5380D71DB02D ] CLFS
C:\windows\system32\CLFS.sys
06:48:42.0219 4280 CLFS - ok
06:48:42.0266 4280 [ D88040F816FDA31C3B466F0FA0918F29 ]
clr_optimization_v2.0.50727_32
C:\windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
06:48:42.0266 4280 clr_optimization_v2.0.50727_32 - ok
06:48:42.0281 4280 [ C5A75EB48E2344ABDC162BDA79E16841 ]
clr_optimization_v4.0.30319_32
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
06:48:42.0281 4280 clr_optimization_v4.0.30319_32 - ok
06:48:42.0297 4280 [ DEA805815E587DAD1DD2C502220B5616 ] CmBatt
C:\windows\system32\DRIVERS\CmBatt.sys
06:48:42.0297 4280 CmBatt - ok
06:48:42.0297 4280 [ C537B1DB64D495B9B4717B4D6D9EDBF2 ] cmdide
C:\windows\system32\DRIVERS\cmdide.sys
06:48:42.0297 4280 cmdide - ok
06:48:42.0328 4280 [ DB5E008B3744DD60C8498CBBF2A1CFA6 ] CNG
C:\windows\system32\Drivers\cng.sys
06:48:42.0328 4280 CNG - ok
06:48:42.0344 4280 [ A6023D3823C37043986713F118A89BEE ] Compbatt
C:\windows\system32\DRIVERS\compbatt.sys
06:48:42.0344 4280 Compbatt - ok
06:48:42.0359 4280 [ F1724BA27E97D627F808FB0BA77A28A6 ] CompositeBus
C:\windows\system32\DRIVERS\CompositeBus.sys
06:48:42.0359 4280 CompositeBus - ok
06:48:42.0359 4280 COMSysApp - ok
06:48:42.0359 4280 [ 2C4EBCFC84A9B44F209DFF6C6E6C61D1 ] crcdisk
C:\windows\system32\DRIVERS\crcdisk.sys
06:48:42.0359 4280 crcdisk - ok
06:48:42.0390 4280 [ F2FDE6C8DBAAD44CC58D1E07E4AF4EED ] CryptSvc
C:\windows\system32\cryptsvc.dll
06:48:42.0390 4280 CryptSvc - ok
06:48:42.0406 4280 [ 27C9490BDD0AE48911AB8CF1932591ED ] CSC
C:\windows\system32\drivers\csc.sys
06:48:42.0422 4280 CSC - ok
06:48:42.0453 4280 [ 56FB5F222EA30D3D3FC459879772CB73 ] CscService
C:\windows\System32\cscsvc.dll
06:48:42.0453 4280 CscService - ok
06:48:42.0546 4280 [ 72794D112CB AFF3BC0C29BF7350D4741 ] cvhsvc
C:\Program Files\Common Files\Microsoft Shared\Virtualization Handler\CVH SVC.EXE
06:48:42.0562 4280 cvhsvc - ok
06:48:42.0609 4280 [ 87F8C293377D53E977523A0ECC18650D ] DAMDrv
C:\windows\system32\DRIVERS\DAMDrv.sys
06:48:42.0609 4280 DAMDrv - ok
06:48:42.0640 4280 [ B82CD39E336973359D7C9BF911E8E84F ] DcomLaunch
C:\windows\system32\rpcss.dll
06:48:42.0671 4280 DcomLaunch - ok
06:48:42.0687 4280 [ 8D6E10A2D9A5EED59562D9B82CF804E1 ] defragsvc
C:\windows\System32\defragsvc.dll
06:48:42.0687 4280 defragsvc - ok
06:48:42.0702 4280 [ 83D1ECEA8FAAE75604C0FA49AC7AD996 ] Dfsc
C:\windows\system32\Drivers\dfsc.sys
06:48:42.0702 4280 Dfsc - ok
06:48:42.0718 4280 [ C56495FBD770712367CAD35E5DE72DA6 ] Dhcp
C:\windows\system32\dhcpcore.dll
06:48:42.0734 4280 Dhcp - ok

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt
 06:48:42.0749 4280 [1A050B0274BFB3890703D490F330C0DA] discache
 C:\windows\system32\drivers\discache.sys
 06:48:42.0749 4280 discache - ok
 06:48:42.0749 4280 [565003F326F99802E68CA78F2A68E9FF] Disk
 C:\windows\system32\DRIVERS\disk.sys
 06:48:42.0749 4280 Disk - ok
 06:48:42.0780 4280 [B15BE77A2BACF9C3177D27518AFE26A9] Dnscache
 C:\windows\system32\dnssrslvr.dll
 06:48:42.0796 4280 Dnscache - ok
 06:48:42.0812 4280 [4408C85C21EEA48EB0CE486BAEEF0502] dot3svc
 C:\windows\system32\dot3svc.dll
 06:48:42.0827 4280 dot3svc - ok
 06:48:42.0890 4280 [BB7E879C2E0E74180253DAF4F8924E8E] DpHost
 C:\Program Files\Hewlett-Packard\HP ProtectTools Security
 Manager\Bin\DpHostw.exe
 06:48:42.0905 4280 DpHost - ok
 06:48:42.0936 4280 [7FA81C6E11CAA594ADB52084DA73A1E5] DPS
 C:\windows\system32\dps.dll
 06:48:42.0936 4280 DPS - ok
 06:48:42.0952 4280 [B918E7C5F9BF77202F89E1A9539F2EB4] drmkau
 C:\windows\system32\drivers\drmkau.sys
 06:48:42.0952 4280 drmkau - ok
 06:48:42.0983 4280 [687AF6BB383885FF6A64071B189A7F3E] dtsoftbus01
 C:\windows\system32\DRIVERS\dtsoftbus01.sys
 06:48:42.0999 4280 dtsoftbus01 - ok
 06:48:43.0030 4280 [1679A4669326CB1A67CC95658D273234] DXGKrn
 C:\windows\system32\drivers\dxgkrnl.sys
 06:48:43.0061 4280 DXGKrn - ok
 06:48:43.0077 4280 [890A46FB3D58667BE559CEE1A0252049] e1cexpress
 C:\windows\system32\DRIVERS\e1c6232.sys
 06:48:43.0092 4280 e1cexpress - ok
 06:48:43.0124 4280 [8600142FA91C1B96367D3300AD0F3F3A] EapHost
 C:\windows\system32\eamsvc.dll
 06:48:43.0124 4280 EapHost - ok
 06:48:43.0202 4280 [024E1B5CAC09731E4D868E64DBFB4AB0] ebdrv
 C:\windows\system32\DRIVERS\evbdrv.sys
 06:48:43.0233 4280 ebdrv - ok
 06:48:43.0264 4280 [85B8B4032A895A746D46A288A9B30DED] eeCtrl
 C:\Program Files\Common Files\Symantec Shared\EENGINE\eeCtrl.sys
 06:48:43.0280 4280 eeCtrl - ok
 06:48:43.0295 4280 [C2243FF9E9AAD0C30E8B1A0914DA15B6] EFS
 C:\windows\system32\lsass.exe
 06:48:43.0295 4280 EFS - ok
 06:48:43.0358 4280 [1697C39978CD69F6FBC15302EDCECE1F] ehRecvr
 C:\windows\ehome\ehRecvr.exe
 06:48:43.0373 4280 ehRecvr - ok
 06:48:43.0404 4280 [D389BFF34F80CAEDE417BF9D1507996A] ehSched
 C:\windows\ehome\ehsched.exe
 06:48:43.0404 4280 ehSched - ok
 06:48:43.0436 4280 [0ED67910C8C326796FAA00B2BF6D9D3C] elxstor
 C:\windows\system32\DRIVERS\elxstor.sys
 06:48:43.0451 4280 elxstor - ok
 06:48:43.0482 4280 [B5A8A04A6E5B4E86B95B1553AA918F5F] EraserUtilRebootDrv
 C:\Program Files\Common Files\Symantec Shared\EENGINE\EraserUtilRebootDrv.sys
 06:48:43.0482 4280 EraserUtilRebootDrv - ok
 06:48:43.0514 4280 [8FC3208352DD3912C94367A206AB3F11] ErrDev
 C:\windows\system32\DRIVERS\errdev.sys
 06:48:43.0514 4280 ErrDev - ok
 06:48:43.0576 4280 [F6916EFC29D9953D5D0DF06882AE8E16] EventSystem
 C:\windows\system32\es.dll
 06:48:43.0576 4280 EventSystem - ok
 06:48:43.0607 4280 [57C171EA22F0A7F068FCB0CAEDD1E8E7] ew_hwsusbdev
 C:\windows\system32\DRIVERS\ew_hwsusbdev.sys
 06:48:43.0623 4280 ew_hwsusbdev - ok
 06:48:43.0638 4280 [2DC9108D74081149CC8B651D3A26207F] exfat
 C:\windows\system32\drivers\exfat.sys
 06:48:43.0654 4280 exfat - ok
 06:48:43.0670 4280 [7E0AB74553476622FB6AE36F73D97D35] fastfat

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

C:\windows\system32\drivers\fastfat.sys
06:48:43.0670 4280 fastfat - ok
06:48:43.0701 4280 [ F7EA23CC5E6BF2181F3F399D54F6EFC1 ] Fax
C:\windows\system32\fxssvc.exe
06:48:43.0732 4280 Fax - ok
06:48:43.0748 4280 [ E817A017F82DF2A1F8CFDBDA29388B29 ] fdc
C:\windows\system32\DRIVERS\fdc.sys
06:48:43.0748 4280 fdc - ok
06:48:43.0763 4280 [ F3222C893BD2F5821A0179E5C71E88FB ] fdPHost
C:\windows\system32\fdPHost.dll
06:48:43.0763 4280 fdPHost - ok
06:48:43.0779 4280 [ 7DBE8CBFE79EFBDEB98C9FB08D3A9A5B ] FDResPub
C:\windows\system32\fdrespub.dll
06:48:43.0779 4280 FDResPub - ok
06:48:43.0810 4280 [ 6CF00369C97F3CF563BE99BE983D13D8 ] FileInfo
C:\windows\system32\drivers\fileinfo.sys
06:48:43.0810 4280 FileInfo - ok
06:48:43.0826 4280 [ 42C51DC94C91DA21CB9196EB64C45DB9 ] Filetrace
C:\windows\system32\drivers\filetrace.sys
06:48:43.0826 4280 Filetrace - ok
06:48:43.0857 4280 [ 00160891E41480997565F2BE35476AC0 ] FLCLOCK
C:\windows\system32\flcdlock.exe
06:48:43.0888 4280 FLCLOCK - ok
06:48:43.0888 4280 [ 87907AA70CB3C56600F1C2FB8841579B ] flpydisk
C:\windows\system32\DRIVERS\flpydisk.sys
06:48:43.0904 4280 flpydisk - ok
06:48:43.0919 4280 [ 7520EC808E0C35E0EE6F841294316653 ] FltMgr
C:\windows\system32\drivers\fltMgr.sys
06:48:43.0935 4280 FltMgr - ok
06:48:43.0982 4280 [ 7FE4995528A7529A761875151EE3D512 ] FontCache
C:\windows\system32\FntCache.dll
06:48:43.0997 4280 FontCache - ok
06:48:44.0060 4280 [ E56F39F6B7FDA0AC77A79B0FD3DE1A2F ] FontCache3.0.0.0
C:\windows\Microsoft.Net\Framework\v3.0\WPF\PresentationFontCache.exe
06:48:44.0060 4280 FontCache3.0.0.0 - ok
06:48:44.0075 4280 [ 1A16B57943853E598CFF37FE2B8CBF1D ] FsDepends
C:\windows\system32\drivers\FsDepends.sys
06:48:44.0075 4280 FsDepends - ok
06:48:44.0106 4280 [ 500A9814FD9446A8126858A5A7F7D273 ] Fs_Rec
C:\windows\system32\drivers\Fs_Rec.sys
06:48:44.0106 4280 Fs_Rec - ok
06:48:44.0138 4280 [ DAFBD9FE39197495AED6D51F3B85B5D2 ] fvevol
C:\windows\system32\DRIVERS\fvevol.sys
06:48:44.0153 4280 fvevol - ok
06:48:44.0169 4280 [ 65EE0C7A58B65E74AE05637418153938 ] gagp30kx
C:\windows\system32\DRIVERS\gagp30kx.sys
06:48:44.0184 4280 gagp30kx - ok
06:48:44.0216 4280 [ 8BA3C04702BF8F927AB36AE8313CA4EE ] gpsvc
C:\windows\System32\gpsvc.dll
06:48:44.0247 4280 gpsvc - ok
06:48:44.0262 4280 [ C172F0D0329E46513B09E1FC60A27B9D ] HBtnKey
C:\windows\system32\DRIVERS\cpqbttn.sys
06:48:44.0262 4280 HBtnKey - ok
06:48:44.0294 4280 [ C44E3C2BAB6837DB337DDEE7544736DB ] hcw85cir
C:\windows\system32\drivers\hcw85cir.sys
06:48:44.0294 4280 hcw85cir - ok
06:48:44.0325 4280 [ 3530CAD25DEBA7DC7DE8BB51632CBC5F ] HdAudAddService
C:\windows\system32\drivers\HdAudio.sys
06:48:44.0340 4280 HdAudAddService - ok
06:48:44.0356 4280 [ 717A2207FD6F13AD3E664C7D5A43C7BF ] HDAudBus
C:\windows\system32\DRIVERS\HDAudBus.sys
06:48:44.0372 4280 HDAudBus - ok
06:48:44.0387 4280 [ 1D58A7F3E11A9731D0EAAAAA8405ACC36 ] HidBatt
C:\windows\system32\DRIVERS\HidBatt.sys
06:48:44.0387 4280 HidBatt - ok
06:48:44.0403 4280 [ 89448F40E6DF260C206A193A4683BA78 ] HidBth
C:\windows\system32\DRIVERS\hidbth.sys
06:48:44.0403 4280 HidBth - ok

```

```

06:48:44.0418 4280 [ CF50B4CF4A4F229B9F3C08351F99CA5E ] HidIr
C:\windows\system32\DRIVERS\hidir.sys
06:48:44.0418 4280 HidIr - ok
06:48:44.0450 4280 [ 2BC6F6A1992B3A77F5F41432CA6B3B6B ] hidserv
C:\windows\system32\hidserv.dll
06:48:44.0450 4280 hidserv - ok
06:48:44.0465 4280 [ 25072FB35AC90B25F9E4E3BACF774102 ] HidUsb
C:\windows\system32\DRIVERS\hidusb.sys
06:48:44.0465 4280 HidUsb - ok
06:48:44.0496 4280 [ 741C2A45CA8407E374AABA3E330B7872 ] hkmsvc
C:\windows\system32\kmsvc.dll
06:48:44.0512 4280 hkmsvc - ok
06:48:44.0528 4280 [ A768CA158BB06782A2835B907F4873C3 ] HomeGroupListener
C:\windows\system32\ListSvc.dll
06:48:44.0528 4280 HomeGroupListener - ok
06:48:44.0574 4280 [ FB08DEC5EF43D0C66D83B8E9694E7549 ] HomeGroupProvider
C:\windows\system32\provsrv.dll
06:48:44.0574 4280 HomeGroupProvider - ok
06:48:44.0621 4280 [ 45A12CACB97B4F15858FCFD59355A1E9 ] HP Health Check Service
C:\Program Files\Hewlett-Packard\HP Health Check\hphc_service.exe
06:48:44.0621 4280 HP Health Check Service - ok
06:48:44.0652 4280 [ 6DD70FB3092FD3EA7FA4CA26A1FE049D ] HP Power Assistant
Service C:\Program Files\Hewlett-Packard\HP Power Assistant\HPPA_Service.exe
06:48:44.0668 4280 HP Power Assistant Service - ok
06:48:44.0715 4280 [ 771E3B558C66416860EFB3683CAF4B0F ] HP ProtectTools Service
C:\Program Files\Hewlett-Packard\2009 Password Filter for HP
ProtectTools\PTChangeFilterService.exe
06:48:44.0730 4280 HP ProtectTools Service - ok
06:48:44.0793 4280 [ D4B198E9B3CE6D05771E116D2D560F2F ] hpCMSrv
C:\Program Files\Hewlett-Packard\HP Connection Manager\hpCMSrv.exe
06:48:44.0824 4280 hpCMSrv - ok
06:48:44.0871 4280 [ A9FC4D7EA174BBF5A675B299FFAD80A2 ] HPDayStarterService
C:\Program Files\Hewlett-Packard\HP DayStarter\HPDayStarterService.exe
06:48:44.0871 4280 HPDayStarterService - ok
06:48:44.0918 4280 [ BCC4A8B2E2E902F52E7F2E7D8E125765 ] HPDrvMntSvc.exe
C:\Program Files\Hewlett-Packard\Shared\HPDrvMntSvc.exe
06:48:44.0918 4280 HPDrvMntSvc.exe - ok
06:48:44.0949 4280 [ BA57CFD48E79DA9CBCD708EF98683DA6 ] hpdskflt
C:\windows\system32\DRIVERS\hpdskflt.sys
06:48:44.0949 4280 hpdskflt - ok
06:48:44.0996 4280 [ 79EB59856CC7AEBE5DAE0211A9A1E5A9 ] HPFSService
C:\Program Files\Hewlett-Packard\File Sanitizer\HPFSService.exe
06:48:45.0011 4280 HPFSService - ok
06:48:45.0058 4280 [ FA6107E9434810F8644412BA7AFB891F ] hpHotkeyMonitor
C:\Program Files\Hewlett-Packard\HP Hotkey Support\HpHotkeyMonitor.exe
06:48:45.0058 4280 hpHotkeyMonitor - ok
06:48:45.0089 4280 [ EE9F88368739554DCCA142AE0214BCB1 ] HpqKbFiltr
C:\windows\system32\DRIVERS\HpqKbFiltr.sys
06:48:45.0089 4280 HpqKbFiltr - ok
06:48:45.0167 4280 [ EC9739A46F1F83C6E52A7A4697F44A65 ] hpqwmix
C:\Program Files\Hewlett-Packard\Shared\hpqwmix.exe
06:48:45.0198 4280 hpqwmix - ok
06:48:45.0230 4280 [ 295FDC419039090EB8B49FFDBB374549 ] HpsAMD
C:\windows\system32\DRIVERS\HpsAMD.sys
06:48:45.0230 4280 HpsAMD - ok
06:48:45.0245 4280 [ 6744EB927DA2DB58D5E1A77488EF143B ] hpsrv
C:\windows\system32\Hpservice.exe
06:48:45.0261 4280 hpsrv - ok
06:48:45.0292 4280 [ C531C7FD9E8B62021112787C4E2C5A5A ] HTTP
C:\windows\system32\drivers\HTTP.sys
06:48:45.0308 4280 HTTP - ok
06:48:45.0323 4280 [ 3170044AA8090F80839D3D4330BF733A ] huawei_cdcacm
C:\windows\system32\DRIVERS\ew_jucdcacm.sys
06:48:45.0339 4280 huawei_cdcacm - ok
06:48:45.0354 4280 [ F44461E66F1B7DD267957FE9BAA63ED0 ] huawei_enumerator
C:\windows\system32\DRIVERS\ew_jubusenum.sys
06:48:45.0354 4280 huawei_enumerator - ok
06:48:45.0370 4280 [ 8305F33CDE89AD6C7A0763ED0B5A8D42 ] hwpolicy

```

```

C:\windows\system32\drivers\hwpolicy.sys
06:48:45.0370 4280 hwpolicy - ok
06:48:45.0386 4280 [ F151F0BDC47F4A28B1B20A0818EA36D6 ] i8042prt
C:\windows\system32\DRIVERS\i8042prt.sys
06:48:45.0401 4280 i8042prt - ok
06:48:45.0432 4280 [ F989555F1662581032CCE1578A8FF28E ] iaStor
C:\windows\system32\DRIVERS\iaStor.sys
06:48:45.0448 4280 iaStor - ok
06:48:45.0495 4280 [ 117FF657E0D9BBD61B5C3E71E63D3919 ] IAStorDataMgrSvc
C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe
06:48:45.0510 4280 IAStorDataMgrSvc - ok
06:48:45.0557 4280 [ 71F1A494FEDF4B33C02C4A6A28D6D9E9 ] iaStorV
C:\windows\system32\drivers\iaStorV.sys
06:48:45.0573 4280 iaStorV - ok
06:48:45.0635 4280 [ 5AF815EB5BC9802E5A064E2BA62BFC0C ] idsvc
C:\windows\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\infocard.exe
06:48:45.0666 4280 idsvc - ok
06:48:45.0776 4280 [ 404FB2AAF532BC7BBACC8880BE401C74 ] IDSVix86
C:\ProgramData\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NIS_18.1.0.37\Defin
itions\IPSDefs\20130329.001\IDSVix86.sys
06:48:45.0807 4280 IDSVix86 - ok
06:48:45.0869 4280 [ D59429259F82924E4D3B90C0F0FF7144 ] IFXSpMgtSrv
c:\Program Files\Hewlett-Packard\Embedded Security Software\ifxspmgt.exe
06:48:45.0885 4280 IFXSpMgtSrv - ok
06:48:45.0900 4280 [ 0D1BFD3318674D0D6E9465936D7CC17F ] IFXTCS
c:\Program Files\Hewlett-Packard\Embedded Security Software\ifxtcs.exe
06:48:45.0916 4280 IFXTCS - ok
06:48:46.0119 4280 [ 60CC34AD19AF2716FF18EC756D55B9AB ] igfx
C:\windows\system32\DRIVERS\igdkmd32.sys
06:48:46.0353 4280 igfx - ok
06:48:46.0368 4280 [ 4173FF5708F3236CF25195FEC742915 ] iirsp
C:\windows\system32\DRIVERS\iirsp.sys
06:48:46.0368 4280 iirsp - ok
06:48:46.0400 4280 [ FAC0EE6562B121B1399D6E855583F7A5 ] IKEEXT
C:\windows\system32\ikeext.dll
06:48:46.0431 4280 IKEEXT - ok
06:48:46.0478 4280 [ 5576AD2F0039D2BCCCA3567FC0BF981C ] IntcDAud
C:\windows\system32\DRIVERS\IntcDAud.sys
06:48:46.0493 4280 IntcDAud - ok
06:48:46.0509 4280 [ A0F12F2C9BA6C72F3987CE780E77C130 ] intelide
C:\windows\system32\DRIVERS\intelide.sys
06:48:46.0509 4280 intelide - ok
06:48:46.0540 4280 [ 3B514D27BFC4ACCB4037BC6685F766E0 ] intelppm
C:\windows\system32\DRIVERS\intelppm.sys
06:48:46.0540 4280 intelppm - ok
06:48:46.0571 4280 [ ACB364B9075A45C0736E5C47BE5CAE19 ] IPBusEnum
C:\windows\system32\ipbusenum.dll
06:48:46.0571 4280 IPBusEnum - ok
06:48:46.0587 4280 [ 709D1761D3B19A932FF0238EA6D50200 ] IpFilterDriver
C:\windows\system32\DRIVERS\ipfltdrv.sys
06:48:46.0602 4280 IpFilterDriver - ok
06:48:46.0634 4280 [ 477397B432A256A50EE7E4339EB9EA14 ] iphlpsvc
C:\windows\system32\iphlpvc.dll
06:48:46.0665 4280 iphlpsvc - ok
06:48:46.0665 4280 [ E4454B6C37D7FFD5649611F6496308A7 ] IPMIDRV
C:\windows\system32\DRIVERS\IPMIDrv.sys
06:48:46.0680 4280 IPMIDRV - ok
06:48:46.0696 4280 [ A5FA468D67ABCDAA36264E463A7BB0CD ] IPNAT
C:\windows\system32\drivers\ipnat.sys
06:48:46.0696 4280 IPNAT - ok
06:48:46.0774 4280 [ 42996CFF20A3084A56017B7902307E9F ] IRENUM
C:\windows\system32\drivers\irenum.sys
06:48:46.0774 4280 IRENUM - ok
06:48:46.0790 4280 [ 1F32BB6B38F62F7DF1A7AB7292638A35 ] isapnp
C:\windows\system32\DRIVERS\isapnp.sys
06:48:46.0790 4280 isapnp - ok
06:48:46.0821 4280 [ ED46C223AE46C686AB77CDC41C404B7 ] iscsiPrt

```

```

C:\windows\system32\DRIVERS\msiscsi.sys
06:48:46.0836 4280 iScsiPrt - ok
06:48:46.0868 4280 [ 6C85719A21B3F62C2C76280F4BD36C7B ] jhi_service
C:\Program Files\Intel\Services\IPT\jhi_service.exe
06:48:46.0883 4280 jhi_service - ok
06:48:46.0914 4280 [ 831F342877333859291D4171B5EDD3CA ] JMCR
C:\windows\system32\DRIVERS\jmcr.sys
06:48:46.0914 4280 JMCR - ok
06:48:46.0930 4280 [ 07712CEF42A89B76ADB2FC8124FCCD14 ] johci
C:\windows\system32\DRIVERS\johci.sys
06:48:46.0930 4280 johci - ok
06:48:46.0946 4280 [ ADEF52CA1AEAE82B50DF86B56413107E ] kbdclass
C:\windows\system32\DRIVERS\kbdclass.sys
06:48:46.0961 4280 kbdclass - ok
06:48:46.0961 4280 [ 3D9F0EBF350EDCFD6498057301455964 ] kbdhid
C:\windows\system32\DRIVERS\kbdhid.sys
06:48:46.0977 4280 kbdhid - ok
06:48:46.0992 4280 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] KeyIso
C:\windows\system32\lsass.exe
06:48:46.0992 4280 KeyIso - ok
06:48:47.0024 4280 [ 52FC17C8589F11747D01D3CF592673D0 ] KSecDD
C:\windows\system32\Drivers\ksecdd.sys
06:48:47.0024 4280 KSecDD - ok
06:48:47.0039 4280 [ 3E5474B03568CFAB834DA3C38E8C9EFA ] KSecPkg
C:\windows\system32\Drivers\ksecpkg.sys
06:48:47.0039 4280 KSecPkg - ok
06:48:47.0070 4280 [ 89A7B9CC98D0D80C6F31B91C0A310FCD ] KtmRm
C:\windows\system32\msdtckrm.dll
06:48:47.0070 4280 KtmRm - ok
06:48:47.0102 4280 [ 8F6BF790D3168224C16F2AF68A84438C ] LanmanServer
C:\windows\system32\svrsvcs.dll
06:48:47.0117 4280 LanmanServer - ok
06:48:47.0133 4280 [ B9891F885DCF1F0513A51CB58493CB1F ] LanmanWorkstation
C:\windows\System32\wkssvc.dll
06:48:47.0164 4280 LanmanWorkstation - ok
06:48:47.0180 4280 [ F7611EC07349979DA9B0AE1F18CCC7A6 ] lltdio
C:\windows\system32\DRIVERS\lltdio.sys
06:48:47.0180 4280 lltdio - ok
06:48:47.0211 4280 [ 5700673E13A2117FA3B9020C852C01E2 ] lltdsvc
C:\windows\System32\lltdsvc.dll
06:48:47.0226 4280 lltdsvc - ok
06:48:47.0258 4280 [ 55CA01BA19D0006C8F2639B6C045E08B ] lmhosts
C:\windows\System32\lmhsvc.dll
06:48:47.0258 4280 lmhosts - ok
06:48:47.0320 4280 [ 97F9EAAAC985A663394CD8F54DCD3E73A ] LMS
C:\Program Files\Intel\Intel(R) Management Engine Components\LMS\LMS.exe
06:48:47.0336 4280 LMS - ok
06:48:47.0367 4280 [ EB119A53CCF2ACC000AC71B065B78FEF ] LSI_FC
C:\windows\system32\DRIVERS\lsi_fc.sys
06:48:47.0367 4280 LSI_FC - ok
06:48:47.0382 4280 [ 8ADE1C877256A22E49B75D1CC9161F9C ] LSI_SAS
C:\windows\system32\DRIVERS\lsi_sas.sys
06:48:47.0382 4280 LSI_SAS - ok
06:48:47.0398 4280 [ DC9DC3D3DAA0E276FD2EC262E38B11E9 ] LSI_SAS2
C:\windows\system32\DRIVERS\lsi_sas2.sys
06:48:47.0398 4280 LSI_SAS2 - ok
06:48:47.0414 4280 [ 0A036C7D7CAB643A7F07135AC47E0524 ] LSI_SCSI
C:\windows\system32\DRIVERS\lsi_scsi.sys
06:48:47.0414 4280 LSI_SCSI - ok
06:48:47.0429 4280 [ 6703E366CC18D3B6E534F5CF7DF39CEE ] luafv
C:\windows\system32\drivers\luafv.sys
06:48:47.0429 4280 luafv - ok
06:48:47.0460 4280 [ 629CABB0421668C9D3D402A3C3D77E14 ] MBAMProtector
C:\windows\system32\drivers\mbam.sys
06:48:47.0460 4280 MBAMProtector - ok
06:48:47.0492 4280 [ 1ACAA67676E9E7BDA5E0C41B6E0DECAF ] MBAMScheduler
C:\Program Files\Malwarebytes' Anti-Malware\mbamscheduler.exe
06:48:47.0507 4280 MBAMScheduler - ok

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:48:47.0538 4280 [ 916B8954AC3E06DC9E898AFFB41F3FB6 ] MBAMService
C:\Program Files\Malwarebytes' Anti-Malware\mbamservice.exe
06:48:47.0570 4280 MBAMService - ok
06:48:47.0632 4280 [ 71D6D4B6D91BC39C07FAC2F3D7D20E6B ] McAfee Endpoint
Encryption Agent C:\Program Files\Hewlett-Packard\Drive
Encryption\EEAgent\MfeEpeHost.exe
06:48:47.0648 4280 McAfee Endpoint Encryption Agent - ok
06:48:47.0663 4280 [ E2B0887816ED336685954E3D8FDAA51D ] Mcx2Svc
C:\windows\system32\Mcx2Svc.dll
06:48:47.0663 4280 Mcx2Svc - ok
06:48:47.0679 4280 [ 0FFF5B045293002AB38EB1FD1FC2FB74 ] megasas
C:\windows\system32\DRIVERS\megasas.sys
06:48:47.0679 4280 megasas - ok
06:48:47.0694 4280 [ DCBAB2920C75F390CAF1D29F675D03D6 ] MegaSR
C:\windows\system32\DRIVERS\MegaSR.sys
06:48:47.0694 4280 MegaSR - ok
06:48:47.0726 4280 [ D86AC00883B9C98B570E7643AAF8E554 ] MEI
C:\windows\system32\DRIVERS\HECI.sys
06:48:47.0726 4280 MEI - ok
06:48:47.0741 4280 [ 3440E714EF738FBAE242F26179DDE56F ] MfeEpePc
C:\windows\system32\drivers\MfeEpePc.sys
06:48:47.0757 4280 MfeEpePc - ok
06:48:47.0788 4280 [ 146B6F43A673379A3C670E86D89BE5EA ] MMCSS
C:\windows\system32\mmcsc.dll
06:48:47.0788 4280 MMCSS - ok
06:48:47.0804 4280 [ F001861E5700EE84E2D4E52C712F4964 ] Modem
C:\windows\system32\drivers\modem.sys
06:48:47.0804 4280 Modem - ok
06:48:47.0819 4280 [ 79D10964DE86B292320E9DFE02282A23 ] monitor
C:\windows\system32\DRIVERS\monitor.sys
06:48:47.0819 4280 monitor - ok
06:48:47.0835 4280 [ FB18CC1D4C2E716B6B903B0AC0CC0609 ] mouclass
C:\windows\system32\DRIVERS\mouclass.sys
06:48:47.0850 4280 mouclass - ok
06:48:47.0866 4280 [ 2C388D2CD01C9042596CF3C8F3C7B24D ] mouhid
C:\windows\system32\DRIVERS\mouhid.sys
06:48:47.0866 4280 mouhid - ok
06:48:47.0882 4280 [ 921C18727C5920D6C0300736646931C2 ] mountmgr
C:\windows\system32\drivers\mountmgr.sys
06:48:47.0882 4280 mountmgr - ok
06:48:47.0913 4280 [ 2AF5997438C55FB79D33D015C30E1974 ] mpio
C:\windows\system32\DRIVERS\mpio.sys
06:48:47.0928 4280 mpio - ok
06:48:47.0928 4280 [ AD2723A7B53DD1AACAE6AD8C0BFBF4D0 ] mpsdrv
C:\windows\system32\drivers\mpsdrv.sys
06:48:47.0944 4280 mpsdrv - ok
06:48:47.0975 4280 [ 5CD996CECF45CBC3E8D109C86B82D69E ] MpsSvc
C:\windows\system32\mpssvc.dll
06:48:48.0006 4280 MpsSvc - ok
06:48:48.0006 4280 [ B1BE47008D20E43DA3ADC37C24CDB89D ] MRxDAV
C:\windows\system32\drivers\mrxdav.sys
06:48:48.0022 4280 MRxDAV - ok
06:48:48.0053 4280 [ CA7570E42522E24324A12161DB14EC02 ] mrxsmb
C:\windows\system32\DRIVERS\mrxsmb.sys
06:48:48.0053 4280 mrxsmb - ok
06:48:48.0069 4280 [ F965C3AB2B2AE5C378F4562486E35051 ] mrxsmb10
C:\windows\system32\DRIVERS\mrxsmb10.sys
06:48:48.0084 4280 mrxsmb10 - ok
06:48:48.0116 4280 [ 25C38264A3C72594DD21D355D70D7A5D ] mrxsmb20
C:\windows\system32\DRIVERS\mrxsmb20.sys
06:48:48.0116 4280 mrxsmb20 - ok
06:48:48.0116 4280 [ 4E00965BB3C471D52B07C9C3C59A82CF ] msahci
C:\windows\system32\DRIVERS\msahci.sys
06:48:48.0131 4280 msahci - ok
06:48:48.0147 4280 [ 455029C7174A2DBB03DBA8A0D8BDDD9A ] msdsm
C:\windows\system32\DRIVERS\msdsm.sys
06:48:48.0162 4280 msdsm - ok
06:48:48.0178 4280 [ E1BCE74A3BD9902B72599C0192A07E27 ] MSDTC

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

C:\windows\system32\msdtc.exe
06:48:48.0194 4280 MSDTC - ok
06:48:48.0209 4280 [ DAEFB28E3AF5A76ABCC2C3078C07327F ] Msfs
C:\windows\system32\drivers\Msfs.sys
06:48:48.0209 4280 Msfs - ok
06:48:48.0209 4280 [ 3E1E5767043C5AF9367F0056295E9F84 ] mshidkmdf
C:\windows\system32\drivers\mshidkmdf.sys
06:48:48.0225 4280 mshidkmdf - ok
06:48:48.0240 4280 [ 0A4E5757AE09FA9622E3158CC1AEF114 ] msisadv
C:\windows\system32\DRIVERS\msisadv.sys
06:48:48.0256 4280 msisadv - ok
06:48:48.0272 4280 [ 90F7D9E6B6F27E1A707D4A297F077828 ] MSiSCSI
C:\windows\system32\iscsiexe.dll
06:48:48.0287 4280 MSiSCSI - ok
06:48:48.0287 4280 msiserver - ok
06:48:48.0303 4280 [ 8C0860D6366AAFFB6C5BB9DF9448E631 ] MSKSSRV
C:\windows\system32\drivers\MSKSSRV.sys
06:48:48.0303 4280 MSKSSRV - ok
06:48:48.0303 4280 [ 3EA8B949F963562CEDBB549EAC0C11CE ] MSPCLOCK
C:\windows\system32\drivers\MSPCLOCK.sys
06:48:48.0318 4280 MSPCLOCK - ok
06:48:48.0318 4280 [ F456E973590D663B1073E9C463B40932 ] MSPQM
C:\windows\system32\drivers\MSPQM.sys
06:48:48.0318 4280 MSPQM - ok
06:48:48.0334 4280 [ 0E008FC4819D238C51D7C93E7B41E560 ] MsRPC
C:\windows\system32\drivers\MsRPC.sys
06:48:48.0334 4280 MsRPC - ok
06:48:48.0350 4280 [ FC6B9FF600CC585EA38B12589BD4E246 ] mssmbios
C:\windows\system32\DRIVERS\mssmbios.sys
06:48:48.0350 4280 mssmbios - ok
06:48:48.0365 4280 [ B42C6B921F61A6E55159B8BE6CD54A36 ] MSTEE
C:\windows\system32\drivers\MSTEE.sys
06:48:48.0365 4280 MSTEE - ok
06:48:48.0381 4280 [ 33599130F44E1F34631CEA241DE8AC84 ] MTConfig
C:\windows\system32\DRIVERS\MTConfig.sys
06:48:48.0381 4280 MTConfig - ok
06:48:48.0381 4280 [ 159FAD02F64E6381758C990F753BCC80 ] Mup
C:\windows\system32\Drivers\mup.sys
06:48:48.0381 4280 Mup - ok
06:48:48.0412 4280 [ 80284F1985C70C86F0B5F86DA2DFE1DF ] napagent
C:\windows\system32\qagentRT.dll
06:48:48.0412 4280 napagent - ok
06:48:48.0428 4280 [ 26384429FCD85D83746F63E798AB1480 ] NativewifiP
C:\windows\system32\DRIVERS\nwifi.sys
06:48:48.0459 4280 NativewifiP - ok
06:48:48.0506 4280 [ 7D7A3BC6640C1A0D1442816B30856928 ] NAVENG
C:\ProgramData\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NIS_18.1.0.37\Definitions\VirusDefs\20130329.025\NAVENG.SYS
06:48:48.0506 4280 NAVENG - ok
06:48:48.0568 4280 [ 28494C43D62AA7584BDCA2FADFBC4D11 ] NAVEX15
C:\ProgramData\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NIS_18.1.0.37\Definitions\VirusDefs\20130329.025\NAVEX15.SYS
06:48:48.0646 4280 NAVEX15 - ok
06:48:48.0677 4280 [ 23759D175A0A9BAAF04D05047BC135A8 ] NDIS
C:\windows\system32\drivers\ndis.sys
06:48:48.0693 4280 NDIS - ok
06:48:48.0724 4280 [ 0E1787AA6C9191D3D319E8BAFE86F80C ] NdisCap
C:\windows\system32\DRIVERS\ndiscap.sys
06:48:48.0724 4280 NdisCap - ok
06:48:48.0724 4280 [ E4A8AEC125A2E43A9E32AFEEA7C9C888 ] NdisTapi
C:\windows\system32\DRIVERS\ndistapi.sys
06:48:48.0740 4280 NdisTapi - ok
06:48:48.0755 4280 [ B30AE7F2B6D7E343B0DF32E6C08FCE75 ] Ndisuio
C:\windows\system32\DRIVERS\ndisuio.sys
06:48:48.0755 4280 Ndisuio - ok
06:48:48.0755 4280 [ 267C415EADCB53C9CA873DEE39CF3A4 ] Ndiswan
C:\windows\system32\DRIVERS\ndiswan.sys
06:48:48.0755 4280 Ndiswan - ok

```

```

06:48:48.0771 4280 [ AF7E7C63DCEF3F8772726F86039D6EB4 ] NDPProxy
C:\windows\system32\drivers\NDProxy.sys
06:48:48.0771 4280 NDPProxy - ok
06:48:48.0771 4280 [ 80B275B1CE3B0E79909DB7B39AF74D51 ] NetBIOS
C:\windows\system32\DRIVERS\netbios.sys
06:48:48.0771 4280 NetBIOS - ok
06:48:48.0786 4280 [ DD52A733BF4CA5AF84562A5E2F963B91 ] NetBT
C:\windows\system32\DRIVERS\netbt.sys
06:48:48.0786 4280 NetBT - ok
06:48:48.0802 4280 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] Netlogon
C:\windows\system32\lsass.exe
06:48:48.0802 4280 Netlogon - ok
06:48:48.0833 4280 [ 7CCCFA7510684768DA22092D1FA4DB2 ] Netman
C:\windows\System32\netman.dll
06:48:48.0833 4280 Netman - ok
06:48:48.0896 4280 [ D22CD77D4F0D63D1169BB35911BFF12D ] NetMsmqActivator
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe
06:48:48.0896 4280 NetMsmqActivator - ok
06:48:48.0911 4280 [ D22CD77D4F0D63D1169BB35911BFF12D ] NetPipeActivator
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe
06:48:48.0911 4280 NetPipeActivator - ok
06:48:48.0942 4280 [ 8C338238C16777A802D6A9211EB2BA50 ] netprofm
C:\windows\System32\netprofm.dll
06:48:48.0958 4280 netprofm - ok
06:48:48.0974 4280 [ D22CD77D4F0D63D1169BB35911BFF12D ] NetTcpActivator
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe
06:48:48.0974 4280 NetTcpActivator - ok
06:48:48.0974 4280 [ D22CD77D4F0D63D1169BB35911BFF12D ] NetTcpPortSharing
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe
06:48:48.0989 4280 NetTcpPortSharing - ok
06:48:49.0145 4280 [ 5C531E96643A74CE8BD9AB16B6C7EAD7 ] NETWNS32
C:\windows\system32\DRIVERS\NETWNS32.sys
06:48:49.0301 4280 NETWNS32 - ok
06:48:49.0317 4280 [ 1D85C4B390B0EE09C7A46B91EFB2C097 ] nfrd960
C:\windows\system32\DRIVERS\nfrd960.sys
06:48:49.0317 4280 nfrd960 - ok
06:48:49.0348 4280 [ E78A365CC3E0FBFC018A33DCE01909F8 ] NIS
C:\Program Files\Norton Internet Security\Engine\18.7.2.3\ccSvcHst.exe
06:48:49.0364 4280 NIS - ok
06:48:49.0379 4280 [ 2226496E34BD40734946A054B1CD657F ] Nlasvc
C:\windows\System32\nlasvc.dll
06:48:49.0395 4280 Nlasvc - ok
06:48:49.0426 4280 [ 1DB262A9F8C087E8153D89BEF3D2235F ] Npfs
C:\windows\system32\drivers\Npfs.sys
06:48:49.0426 4280 Npfs - ok
06:48:49.0442 4280 [ BA387E955E890C8A88306D9B8D06BF17 ] nsi
C:\windows\system32\nsisvc.dll
06:48:49.0457 4280 nsi - ok
06:48:49.0473 4280 [ E9A0A4D07E53D8FEA2BB8387A3293C58 ] nsiproxy
C:\windows\system32\drivers\nsiproxy.sys
06:48:49.0473 4280 nsiproxy - ok
06:48:49.0535 4280 [ 5126C5402C730C2A953275D8497A4715 ] Ntfs
C:\windows\system32\drivers\Ntfs.sys
06:48:49.0566 4280 Ntfs - ok
06:48:49.0613 4280 [ F9756A98D69098DCA8945D62858A812C ] Null
C:\windows\system32\drivers\Null.sys
06:48:49.0613 4280 Null - ok
06:48:49.0644 4280 [ F1B0BED906F97E16F6D0C3629D2F21C6 ] nvraid
C:\windows\system32\drivers\nvraid.sys
06:48:49.0644 4280 nvraid - ok
06:48:49.0660 4280 [ 4520B63899E867F354EE012D34E11536 ] nvstor
C:\windows\system32\drivers\nvstor.sys
06:48:49.0676 4280 nvstor - ok
06:48:49.0691 4280 [ 5A0983915F02BAE73267CC2A041F717D ] nv_agp
C:\windows\system32\DRIVERS\nv_agp.sys
06:48:49.0691 4280 nv_agp - ok
06:48:49.0707 4280 [ 08A70A1F2CDDE9BB49B885CB817A66EB ] ohci1394
C:\windows\system32\DRIVERS\ohci1394.sys

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:48:49.0707 4280 ohci1394 - ok
06:48:49.0769 4280 [ 9D10F99A6712E28F8ACD5641E3A7EA6B ] ose
C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
06:48:49.0769 4280 ose - ok
06:48:49.0910 4280 [ 358A9CCA612C68EB2F07DDAD4CE1D8D7 ] osppsvc
C:\Program Files\Common Files\Microsoft
Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
06:48:50.0019 4280 osppsvc - ok
06:48:50.0050 4280 [ 82A8521DDC60710C3D3D3E7325209BEC ] p2pimsvc
C:\windows\system32\pnrpsvc.dll
06:48:50.0050 4280 p2pimsvc - ok
06:48:50.0081 4280 [ 59C3DDD501E39E006DAC31BF55150D91 ] p2psvc
C:\windows\system32\p2psvc.dll
06:48:50.0081 4280 p2psvc - ok
06:48:50.0112 4280 [ 2EA877ED5DD9713C5AC74E8EA7348D14 ] Parport
C:\windows\system32\DRIVERS\parport.sys
06:48:50.0112 4280 Parport - ok
06:48:50.0128 4280 [ 66D3415C159741ADE7038A277EFFF99F ] partmgr
C:\windows\system32\drivers\partmgr.sys
06:48:50.0128 4280 partmgr - ok
06:48:50.0159 4280 [ EB0A59F29C19B86479D36B35983DAADC ] Parvdm
C:\windows\system32\DRIVERS\parvdm.sys
06:48:50.0159 4280 Parvdm - ok
06:48:50.0175 4280 [ 358AB7956D3160000726574083DFC8A6 ] PcaSvc
C:\windows\system32\pcasvc.dll
06:48:50.0190 4280 PcaSvc - ok
06:48:50.0190 4280 [ C858CB77C577780ECC456A892E7E7D0F ] pci
C:\windows\system32\DRIVERS\pci.sys
06:48:50.0190 4280 pci - ok
06:48:50.0206 4280 [ AFE86F419014DB4E5593F69FFE26CE0A ] pciide
C:\windows\system32\DRIVERS\pciide.sys
06:48:50.0206 4280 pciide - ok
06:48:50.0222 4280 [ F396431B31693E71E8A80687EF523506 ] pcmcia
C:\windows\system32\DRIVERS\pcmcia.sys
06:48:50.0222 4280 pcmcia - ok
06:48:50.0237 4280 [ 250F6B43D2B613172035C6747AEEB19F ] pcw
C:\windows\system32\drivers\pcw.sys
06:48:50.0237 4280 pcw - ok
06:48:50.0253 4280 pdfcdDispatcher - ok
06:48:50.0284 4280 [ 4A8CC4D25525F456069887D5E8C53225 ] Pdiservice
C:\Program Files\Common Files\Portrait Displays\Drivers\pdisrv.exe
06:48:50.0284 4280 Pdiservice - ok
06:48:50.0315 4280 [ 9E0104BA49F4E6973749A02BF41344ED ] PEAUTH
C:\windows\system32\drivers\peauth.sys
06:48:50.0346 4280 PEAUTH - ok
06:48:50.0393 4280 [ AF4D64D2A57B9772CF3801950B8058A6 ] PeerDistSvc
C:\windows\system32\peerdistsvc.dll
06:48:50.0409 4280 PeerDistSvc - ok
06:48:50.0456 4280 [ B27F1DF5ABC5240480D4D2D9666867A5 ] PersonalSecureDrive
C:\windows\system32\drivers\psd.sys
06:48:50.0471 4280 PersonalSecureDrive - ok
06:48:50.0487 4280 [ F473D5D43FA7D5C657A3137C5171CB77 ]
PersonalSecureDriveService c:\Program Files\Hewlett-Packard\Embedded Security
Software\IfxPsdSv.exe
06:48:50.0487 4280 PersonalSecureDriveService - ok
06:48:50.0549 4280 [ 9C1BFF7910C89A1D12E57343475840CB ] pla
C:\windows\system32\pla.dll
06:48:50.0565 4280 pla - ok
06:48:50.0596 4280 [ 71DEF5EC79774C798342D0EA16E41780 ] PlugPlay
C:\windows\system32\umpnvmgr.dll
06:48:50.0612 4280 PlugPlay - ok
06:48:50.0627 4280 [ 63FF8572611249931EB16BB8EED6AFC8 ] PNRPAutoReg
C:\windows\system32\pnrpauto.dll
06:48:50.0627 4280 PNRPAutoReg - ok
06:48:50.0643 4280 [ 82A8521DDC60710C3D3D3E7325209BEC ] PNRPSvc
C:\windows\system32\pnrpsvc.dll
06:48:50.0643 4280 PNRPSvc - ok
06:48:50.0674 4280 [ 48E1B75C6DC0232FD92BAAE4BD344721 ] PolicyAgent

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

C:\windows\system32\ipsecsvc.dll
06:48:50.0705 4280 PolicyAgent - ok
06:48:50.0752 4280 [ DBFF83F709A91049621C1D35DD45C92C ] Power
C:\windows\system32\umpo.dll
06:48:50.0768 4280 Power - ok
06:48:50.0783 4280 [ 631E3E205AD6D86F2AED6A4A8E69F2DB ] PptpMiniport
C:\windows\system32\DRIVERS\raspttp.sys
06:48:50.0783 4280 PptpMiniport - ok
06:48:50.0814 4280 [ 85B1E3A0C7585BC4AAE6899EC6FCF011 ] Processor
C:\windows\system32\DRIVERS\processr.sys
06:48:50.0814 4280 Processor - ok
06:48:50.0861 4280 [ AEA3BDBDBA667AA6F678CB38907E4F5E ] ProfSvc
C:\windows\system32\profsvc.dll
06:48:50.0877 4280 ProfSvc - ok
06:48:50.0892 4280 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] ProtectedStorage
C:\windows\system32\lsass.exe
06:48:50.0892 4280 ProtectedStorage - ok
06:48:50.0908 4280 [ 6270CCAE2A86DE6D146529FE55B3246A ] Psched
C:\windows\system32\DRIVERS\pacer.sys
06:48:50.0908 4280 Psched - ok
06:48:50.0924 4280 [ E42E3433DBB4CFFE8FDD91EAB29AEA8E ] PxHelp20
C:\windows\system32\Drivers\PxHelp20.sys
06:48:50.0924 4280 PxHelp20 - ok
06:48:50.0970 4280 [ AB95ECF1F6659A60DDC166D8315B0751 ] ql2300
C:\windows\system32\DRIVERS\ql2300.sys
06:48:51.0017 4280 ql2300 - ok
06:48:51.0017 4280 [ B4DD51DD25182244B86737DC51AF2270 ] ql40xx
C:\windows\system32\DRIVERS\ql40xx.sys
06:48:51.0033 4280 ql40xx - ok
06:48:51.0064 4280 [ 31AC809E7707EB580B2BDB760390765A ] QWAVE
C:\windows\system32\qwave.dll
06:48:51.0064 4280 QWAVE - ok
06:48:51.0080 4280 [ 584078CA1B95CA72DF2A27C336F9719D ] QWAVEdrv
C:\windows\system32\drivers\qwavedrv.sys
06:48:51.0080 4280 QWAVEdrv - ok
06:48:51.0095 4280 [ 30A81B53C766D0133BB86D234E5556AB ] RasAcad
C:\windows\system32\DRIVERS\rasacd.sys
06:48:51.0095 4280 RasAcad - ok
06:48:51.0126 4280 [ 57EC4AEF73660166074D8F7F31C0D4FD ] RasAgileVpn
C:\windows\system32\DRIVERS\AgileVpn.sys
06:48:51.0126 4280 RasAgileVpn - ok
06:48:51.0142 4280 [ A60F1839849C0C00739787FD5EC03F13 ] RasAuto
C:\windows\system32\rasauto.dll
06:48:51.0142 4280 RasAuto - ok
06:48:51.0158 4280 [ D9F91EAFEC2815365CBE6D167E4E332A ] Rasl2tp
C:\windows\system32\DRIVERS\rasl2tp.sys
06:48:51.0158 4280 Rasl2tp - ok
06:48:51.0189 4280 [ 0CE66EC736B7FC526D78F7624C7D2A94 ] RasMan
C:\windows\system32\rasmans.dll
06:48:51.0204 4280 RasMan - ok
06:48:51.0204 4280 [ 0FE8B15916307A6AC12BFB6A63E45507 ] RasPppoe
C:\windows\system32\DRIVERS\rasppoe.sys
06:48:51.0220 4280 RasPppoe - ok
06:48:51.0220 4280 [ 44101F495A83EA6401D886E7FD70096B ] RasSstp
C:\windows\system32\DRIVERS\rassstp.sys
06:48:51.0236 4280 RasSstp - ok
06:48:51.0251 4280 [ 835D7E81BF517A3B72384BDCC85E1CE6 ] rdbss
C:\windows\system32\DRIVERS\rdbss.sys
06:48:51.0267 4280 rdbss - ok
06:48:51.0282 4280 [ 0D8F05481CB76E70E1DA06EE9F0DA9DF ] rdpbus
C:\windows\system32\DRIVERS\rdpbus.sys
06:48:51.0282 4280 rdpbus - ok
06:48:51.0298 4280 [ 1E016846895B15A99F9A176A05029075 ] RDPCDD
C:\windows\system32\DRIVERS\RDPCDD.sys
06:48:51.0314 4280 RDPCDD - ok
06:48:51.0329 4280 [ C5FF95883FFEF704D50C40D21CFB3AB5 ] RDPDR
C:\windows\system32\drivers\rdpdr.sys
06:48:51.0345 4280 RDPDR - ok

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:48:51.0345 4280 [ 5A53CA1598DD4156D44196D200C94B8A ] RDPENCDD
C:\windows\system32\drivers\rdpencdd.sys
06:48:51.0345 4280 RDPENCDD - ok
06:48:51.0360 4280 [ 44B0A53CD4F27D50ED461DAE0C0B4E1F ] RDPREFMP
C:\windows\system32\drivers\rdprefmp.sys
06:48:51.0360 4280 RDPREFMP - ok
06:48:51.0392 4280 [ C5B8D47A4688DE9D335204EA757C2240 ] RDPWD
C:\windows\system32\drivers\RDPWD.sys
06:48:51.0407 4280 RDPWD - ok
06:48:51.0438 4280 [ 4EA225BF1CF05E158853F30A99CA29A7 ] rdyboost
C:\windows\system32\drivers\rdyboost.sys
06:48:51.0438 4280 rdyboost - ok
06:48:51.0470 4280 [ 7B5E1419717FAC363A31CC302895217A ] RemoteAccess
C:\windows\System32\mprdim.dll
06:48:51.0470 4280 RemoteAccess - ok
06:48:51.0485 4280 [ CB9A8683F4EF2BF99E123D79950D7935 ] RemoteRegistry
C:\windows\system32\regsvc.dll
06:48:51.0501 4280 RemoteRegistry - ok
06:48:51.0532 4280 [ CB928D9E6DAF51879DD6BA8D02F01321 ] RFCOMM
C:\windows\system32\DRIVERS\rfcomm.sys
06:48:51.0532 4280 RFCOMM - ok
06:48:51.0579 4280 [ 78D072F35BC45D9E4E1B61895C152234 ] RpcEptMapper
C:\windows\System32\RpcEpMap.dll
06:48:51.0579 4280 RpcEptMapper - ok
06:48:51.0610 4280 [ 94D36C0E44677DD26981D2BFEEF2A29D ] RpcLocator
C:\windows\system32\locator.exe
06:48:51.0626 4280 RpcLocator - ok
06:48:51.0641 4280 [ B82CD39E336973359D7C9BF911E8E84F ] RpcSs
C:\windows\system32\rpcss.dll
06:48:51.0657 4280 RpcSs - ok
06:48:51.0688 4280 [ 032B0D36AD92B582D869879F5AF5B928 ] rspndr
C:\windows\system32\DRIVERS\rspndr.sys
06:48:51.0688 4280 rspndr - ok
06:48:51.0719 4280 [ 5423D8437051E89DD34749F242C98648 ] s3cap
C:\windows\system32\DRIVERS\vms3cap.sys
06:48:51.0719 4280 s3cap - ok
06:48:51.0735 4280 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] SamSs
C:\windows\system32\lsass.exe
06:48:51.0750 4280 SamSs - ok
06:48:51.0766 4280 [ 662B7F49CB295F15B5A1A36AD3AE9C2C ] sbp2port
C:\windows\system32\DRIVERS\sbp2port.sys
06:48:51.0782 4280 sbp2port - ok
06:48:51.0797 4280 [ 8FC518FFE9519C2631D37515A68009C4 ] SCardsvr
C:\windows\System32\SCardSvr.dll
06:48:51.0813 4280 SCardSvr - ok
06:48:51.0828 4280 [ A95C54B2AC3CC9C73FCDF9E51A1D6B51 ] scfilter
C:\windows\system32\DRIVERS\scfilter.sys
06:48:51.0828 4280 scfilter - ok
06:48:51.0860 4280 [ DF1E5C82E4D09CF8105CC644980C4803 ] schedule
C:\windows\system32\schedsvc.dll
06:48:51.0891 4280 schedule - ok
06:48:51.0906 4280 [ 628A9E30EC5E18DD5DE6BE4DBDC12198 ] SCPolicySvc
C:\windows\System32\certprop.dll
06:48:51.0906 4280 SCPolicySvc - ok
06:48:51.0906 4280 [ AA826E35F6D28A8E5D1EFEB337F24BA2 ] sdbus
C:\windows\system32\DRIVERS\sdbus.sys
06:48:51.0922 4280 sdbus - ok
06:48:51.0938 4280 [ 5FD90ABDBFAEE85986802622CBB03446 ] SDRSVC
C:\windows\System32\SDRSVC.dll
06:48:51.0938 4280 SDRSVC - ok
06:48:51.0953 4280 [ 90A3935D05B49A5A39D37E71F09A677 ] secdrv
C:\windows\system32\drivers\secdrv.sys
06:48:51.0953 4280 secdrv - ok
06:48:51.0969 4280 [ A59B3A4442C52060CC7A85293AA3546F ] seclogon
C:\windows\system32\seclogon.dll
06:48:51.0969 4280 seclogon - ok
06:48:51.0984 4280 [ DCB7FCDCC97F87360F75D77425B81737 ] SENS
C:\windows\System32\sens.dll

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:48:51.0984 4280 SENS - ok
06:48:52.0000 4280 [ 50087FE1EE447009C9CC2997B90DE53F ] SensrSvc
C:\windows\system32\sensrsvc.dll
06:48:52.0000 4280 SensrSvc - ok
06:48:52.0016 4280 [ 9AD8B8B515E3DF6ACD4212EF465DE2D1 ] Serenum
C:\windows\system32\DRIVERS\serenum.sys
06:48:52.0016 4280 Serenum - ok
06:48:52.0031 4280 [ 5FB7FCEA0490D821F26F39CC5EA3D1E2 ] Serial
C:\windows\system32\DRIVERS\serial.sys
06:48:52.0031 4280 Serial - ok
06:48:52.0047 4280 [ 79BFFB520327FF916A582DFEA17AA813 ] sermouse
C:\windows\system32\DRIVERS\sermouse.sys
06:48:52.0047 4280 sermouse - ok
06:48:52.0062 4280 [ 8F55CE568C543D5ADF45C409D16718FC ] SessionEnv
C:\windows\system32\sessenv.dll
06:48:52.0062 4280 SessionEnv - ok
06:48:52.0062 4280 [ 9F976E1EB233DF46FCE808D9DEA3EB9C ] sffdisk
C:\windows\system32\DRIVERS\sffdisk.sys
06:48:52.0078 4280 sffdisk - ok
06:48:52.0078 4280 [ 932A68EE27833CFD57C1639D375F2731 ] sffp_mmc
C:\windows\system32\DRIVERS\sffp_mmc.sys
06:48:52.0078 4280 sffp_mmc - ok
06:48:52.0094 4280 [ A0708BBD07D245C06FF9DE549CA47185 ] sffp_sd
C:\windows\system32\DRIVERS\sffp_sd.sys
06:48:52.0094 4280 sffp_sd - ok
06:48:52.0109 4280 [ DB96666CC8312EBC45032F30B007A547 ] sfloppy
C:\windows\system32\DRIVERS\sfloppy.sys
06:48:52.0109 4280 sfloppy - ok
06:48:52.0140 4280 [ D9B734638DD8DBA9D59AAD3189CD0FAD ] sftfs
C:\windows\system32\DRIVERS\Sftfslh.sys
06:48:52.0172 4280 sftfs - ok
06:48:52.0203 4280 [ CB73BC422C07FB611F194DA18D1E7F36 ] sftlist
C:\Program Files\Microsoft Application Virtualization Client\sftlist.exe
06:48:52.0218 4280 sftlist - ok
06:48:52.0250 4280 [ 2F61BD46C0BFF4EB36E1E359CA17BFC5 ] sftplay
C:\windows\system32\DRIVERS\Sftplaylh.sys
06:48:52.0265 4280 sftplay - ok
06:48:52.0281 4280 [ 518BAC0179F94304F422696B47C0EC12 ] sftredir
C:\windows\system32\DRIVERS\Sftredirh.sys
06:48:52.0296 4280 sftredir - ok
06:48:52.0296 4280 [ 747325236D88B3F05FFD27FF9EC711C5 ] sftvol
C:\windows\system32\DRIVERS\Sftvollh.sys
06:48:52.0312 4280 sftvol - ok
06:48:52.0343 4280 [ A5812F0281CA5081BF696626F9BF324D ] sftvsa
C:\Program Files\Microsoft Application Virtualization Client\sftvsa.exe
06:48:52.0343 4280 sftvsa - ok
06:48:52.0374 4280 [ D1A079A0DE2EA524513B6930C24527A2 ] SharedAccess
C:\windows\system32\ipnathlp.dll
06:48:52.0374 4280 SharedAccess - ok
06:48:52.0421 4280 [ CD2E48FA5B29EE2B3B5858056D246EF2 ] ShellHWDetection
C:\windows\system32\shsvcs.dll
06:48:52.0437 4280 ShellHWDetection - ok
06:48:52.0452 4280 [ 2565CAC0DC9FE0371BDCE60832582B2E ] sisagp
C:\windows\system32\DRIVERS\sisagp.sys
06:48:52.0452 4280 sisagp - ok
06:48:52.0468 4280 [ A9F0486851BECB6DDA1D89D381E71055 ] sisraid2
C:\windows\system32\DRIVERS\SisRaid2.sys
06:48:52.0484 4280 SisRaid2 - ok
06:48:52.0484 4280 [ 3727097B55738E2F554972C3BE5BC1AA ] sisraid4
C:\windows\system32\DRIVERS\sisraid4.sys
06:48:52.0499 4280 sisraid4 - ok
06:48:52.0530 4280 [ 2F5AF9D91D51E832773D4A9EAF65CB33 ] skypeupdate
C:\Program Files\Skype\Updater\Updater.exe
06:48:52.0546 4280 skypeupdate - ok
06:48:52.0562 4280 [ 3E21C083B8A01CB70BA1F09303010FCE ] smb
C:\windows\system32\DRIVERS\smb.sys
06:48:52.0562 4280 smb - ok
06:48:52.0608 4280 [ 6A984831644ECA1A33FFEAE4126F4F37 ] SNMPTRAP

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

C:\windows\system32\snmptrap.exe
06:48:52.0624 4280 SNMPTRAP - ok
06:48:52.0686 4280 [ 1A67C5880233A8BDEA5D9E8B48CD178F ] SNP2UVC
C:\windows\system32\DRIVERS\snp2uvc.sys
06:48:52.0733 4280 SNP2UVC - ok
06:48:52.0749 4280 [ 95CF1AE7527FB70F7816563CBC09D942 ] spldr
C:\windows\system32\drivers\spldr.sys
06:48:52.0764 4280 spldr - ok
06:48:52.0796 4280 [ E17323B0AA9FB3FF9945731D736EDA2F ] Spooler
C:\windows\system32\spoolsv.exe
06:48:52.0811 4280 Spooler - ok
06:48:52.0920 4280 [ 4C287F9069FEDBD791178876EE9DE536 ] sppsVC
C:\windows\system32\sppsVC.exe
06:48:52.0998 4280 sppsVC - ok
06:48:53.0030 4280 [ D8E3E19EEBDAB49DD4A8D3062EAD4EC7 ] sppuinotify
C:\windows\system32\sppuinotify.dll
06:48:53.0030 4280 sppuinotify - ok
06:48:53.0092 4280 [ 83726CF02ECED69138948083E06B6EAC ] SRTSP
C:\windows\system32\Drivers\NIS\1207020.003\SRTSP.SYS
06:48:53.0108 4280 SRTSP - ok
06:48:53.0139 4280 [ 4E7EAB2E5615D39CF1F1DF9C71E5E225 ] SRTSPX
C:\windows\system32\drivers\NIS\1207020.003\SRTSPX.SYS
06:48:53.0139 4280 SRTSPX - ok
06:48:53.0170 4280 [ C4A027B8C0BD3FC0699F41FA5E9E0C87 ] srv
C:\windows\system32\DRIVERS\srv.sys
06:48:53.0186 4280 srv - ok
06:48:53.0201 4280 [ 414BB592CAD8A79649D01F9D94318FB3 ] srv2
C:\windows\system32\DRIVERS\srv2.sys
06:48:53.0217 4280 srv2 - ok
06:48:53.0232 4280 [ FF207D67700AA18242AAF985D3E7D8F4 ] srvnet
C:\windows\system32\DRIVERS\srvnet.sys
06:48:53.0232 4280 srvnet - ok
06:48:53.0264 4280 [ D887C9FD02AC9FA880F6E5027A43E118 ] SSDPSRV
C:\windows\system32\ssdpsrv.dll
06:48:53.0279 4280 SSDPSRV - ok
06:48:53.0295 4280 [ D318F23BE45D5E3A107469EB64815B50 ] SstpSvc
C:\windows\system32\sstpSvc.dll
06:48:53.0310 4280 SstpSvc - ok
06:48:53.0357 4280 [ 79A7B1C2C15F675BAA919D4D44EC3C7D ] STacSV
C:\Program Files\IDT\WDM\STacSV.exe
06:48:53.0357 4280 STacSV - ok
06:48:53.0388 4280 [ DB32D325C192B801DF274BFD12A7E72B ] stexstor
C:\windows\system32\DRIVERS\stexstor.sys
06:48:53.0404 4280 stexstor - ok
06:48:53.0435 4280 [ C8D2AF5C07D8FE3E088D2E3A3001922C ] STHDA
C:\windows\system32\DRIVERS\stwrt.sys
06:48:53.0451 4280 STHDA - ok
06:48:53.0498 4280 [ A22825E7BB7018E8AF3E229A5AF17221 ] StISvc
C:\windows\system32\wiaservc.dll
06:48:53.0513 4280 StISvc - ok
06:48:53.0544 4280 [ 7731F46EC0D687A931CBA063E8F90EF0 ] stllssvr
C:\Program Files\Common Files\SureThing Shared\stllssvr.exe
06:48:53.0544 4280 stllssvr - ok
06:48:53.0560 4280 [ 957E346CA948668F2496A6CCF6FF82CC ] storflt
C:\windows\system32\DRIVERS\vmstorfl.sys
06:48:53.0576 4280 storflt - ok
06:48:53.0591 4280 [ 0BF669F0A910BEDA4A32258D363AF2A5 ] StorSvc
C:\windows\system32\storsvc.dll
06:48:53.0607 4280 StorSvc - ok
06:48:53.0607 4280 [ D5751969DC3E4B88BF482AC8EC9FE019 ] storvsc
C:\windows\system32\DRIVERS\storvsc.sys
06:48:53.0607 4280 storvsc - ok
06:48:53.0638 4280 [ E58C78A848ADD9610A4DB6D214AF5224 ] swenum
C:\windows\system32\DRIVERS\swenum.sys
06:48:53.0638 4280 swenum - ok
06:48:53.0669 4280 [ A28BD92DF340E57B024BA433165D34D7 ] swprv
C:\windows\system32\swprv.dll
06:48:53.0685 4280 swprv - ok

```

```

06:48:53.0716 4280 [ 9BBEB8C6258E72D62E7560E6667AAD39 ] SymDS
C:\windows\system32\drivers\NIS\1207020.003\SYMDS.SYS
06:48:53.0732 4280 SymDS - ok
06:48:53.0763 4280 [ D5C02629C02A820A7E71BCA3D44294A3 ] SymEFA
C:\windows\system32\drivers\NIS\1207020.003\SYMEFA.SYS
06:48:53.0794 4280 SymEFA - ok
06:48:53.0825 4280 [ AB33C3B196197CA467CBDDA717860DBA ] SymEvent
C:\windows\system32\Drivers\SYMEVENT.SYS
06:48:53.0825 4280 SymEvent - ok
06:48:53.0856 4280 [ A73399804D5D4A8B20BA60FCF70C9F1F ] SymIRON
C:\windows\system32\drivers\NIS\1207020.003\Ironx86.SYS
06:48:53.0872 4280 SymIRON - ok
06:48:53.0888 4280 [ 2C688094650D23B62B0A809DECD0B12F ] SymNets
C:\windows\system32\Drivers\NIS\1207020.003\SYMNETS.SYS
06:48:53.0903 4280 SymNets - ok
06:48:53.0934 4280 [ 480B47D6702ADCE130204F71F116D205 ] SynTP
C:\windows\system32\DRIVERS\SynTP.sys
06:48:53.0966 4280 SynTP - ok
06:48:53.0997 4280 [ 04105C8DA62353589C29BDAEB8D88BD8 ] SysMain
C:\windows\system32\sysmain.dll
06:48:54.0028 4280 SysMain - ok
06:48:54.0044 4280 [ FCFB6C552FBC0DA299799CBD50AD9FD4 ] TabletInputService
C:\windows\System32\TabSvc.dll
06:48:54.0059 4280 TabletInputService - ok
06:48:54.0090 4280 [ 2F46B0C70A4ADC8C90CF825DA3B4FEAF ] Tapisrv
C:\windows\System32\tapisrv.dll
06:48:54.0090 4280 Tapisrv - ok
06:48:54.0106 4280 [ B799D9FDB26111737F58288D8DC172D9 ] TBS
C:\windows\System32\tbssvc.dll
06:48:54.0106 4280 TBS - ok
06:48:54.0168 4280 [ BBCEAEFF1FD72A026F827CBB2F4AA8AD ] Tcpip
C:\windows\system32\drivers\tcpip.sys
06:48:54.0215 4280 Tcpip - ok
06:48:54.0262 4280 [ BBCEAEFF1FD72A026F827CBB2F4AA8AD ] TCPIP6
C:\windows\system32\DRIVERS\tcpip.sys
06:48:54.0293 4280 TCPIP6 - ok
06:48:54.0324 4280 [ E64444523ADD154F86567C469BC0B17F ] tcpipreg
C:\windows\system32\drivers\tcpipreg.sys
06:48:54.0324 4280 tcpipreg - ok
06:48:54.0356 4280 [ 1875C1490D99E70E449E3AF9FCBADF ] TDPIPE
C:\windows\system32\drivers\tdpipe.sys
06:48:54.0356 4280 TDPIPE - ok
06:48:54.0387 4280 [ 7156308896D34EA75A582F9A09E50C17 ] TDTCP
C:\windows\system32\drivers\tdtcp.sys
06:48:54.0387 4280 TDTCP - ok
06:48:54.0402 4280 [ CB39E896A2A83702D1737BFD402B3542 ] tdx
C:\windows\system32\DRIVERS\tdx.sys
06:48:54.0418 4280 tdx - ok
06:48:54.0418 4280 [ C36F41EE20E6999DBF4B0425963268A5 ] TermDD
C:\windows\system32\DRIVERS\termdd.sys
06:48:54.0418 4280 TermDD - ok
06:48:54.0480 4280 [ A01E50A04D7B1960B33E92B9080E6A94 ] TermService
C:\windows\System32\termsrv.dll
06:48:54.0496 4280 TermService - ok
06:48:54.0527 4280 [ 42FB6AFD6B79D9FE07381609172E7CA4 ] Themes
C:\windows\system32\themeservice.dll
06:48:54.0543 4280 Themes - ok
06:48:54.0574 4280 [ 146B6F43A673379A3C670E86D89BE5EA ] THREADORDER
C:\windows\system32\mmcss.dll
06:48:54.0574 4280 THREADORDER - ok
06:48:54.0574 4280 [ 5AD05191DC8B444A7BA4D79B76C42A30 ] TPM
C:\windows\system32\drivers\tpm.sys
06:48:54.0590 4280 TPM - ok
06:48:54.0590 4280 [ 4792C0378DB99A9BC2AE2DE6CFFF0C3A ] Trkwks
C:\windows\System32\trkwks.dll
06:48:54.0605 4280 Trkwks - ok
06:48:54.0652 4280 [ 41A4C781D2286208D397D72099304133 ] TrustedInstaller
C:\windows\servicing\TrustedInstaller.exe

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:48:54.0652 4280 TrustedInstaller - ok
06:48:54.0683 4280 [ 98AE6FA07D12CB4EC5CF4A9BFA5F4242 ] tssecsrv
C:\windows\system32\DRIVERS\tssecsrv.sys
06:48:54.0683 4280 tssecsrv - ok
06:48:54.0699 4280 [ 3E461D890A97F9D4C168F5FDA36E1D00 ] tunnel
C:\windows\system32\DRIVERS\tunnel.sys
06:48:54.0699 4280 tunnel - ok
06:48:54.0730 4280 [ 750FBCB269F4D7DD2E420C56B795DB6D ] uagp35
C:\windows\system32\DRIVERS\uagp35.sys
06:48:54.0730 4280 uagp35 - ok
06:48:54.0777 4280 [ E92F73AD3E9FEF408422B4555B95B02E ] uArcCapture
C:\windows\system32\ArcVCapRender\uArcCapture.exe
06:48:54.0792 4280 uArcCapture - ok
06:48:54.0808 4280 [ 6557D75E8B7D6A06CDC21CD39DBF255C ] udfs
C:\windows\system32\DRIVERS\udfs.sys
06:48:54.0839 4280 udfs - ok
06:48:54.0870 4280 [ 8344FD4FCE927880AA1AA7681D4927E5 ] UI0Detect
C:\windows\system32\UI0Detect.exe
06:48:54.0886 4280 UI0Detect - ok
06:48:54.0886 4280 [ 44E8048ACE47BEFBFC2E9BE4CBC8880 ] uliagpkx
C:\windows\system32\DRIVERS\uliagpkx.sys
06:48:54.0902 4280 uliagpkx - ok
06:48:54.0902 4280 [ 049B3A50B3D646BAEEEE9EEC9B0668DC ] umbus
C:\windows\system32\DRIVERS\umbus.sys
06:48:54.0917 4280 umbus - ok
06:48:54.0917 4280 [ 7550AD0C6998BA1CB4843E920EE0FEAC ] UmPass
C:\windows\system32\DRIVERS\umpass.sys
06:48:54.0933 4280 UmPass - ok
06:48:54.0948 4280 [ 8ECACA5454844F66386F7BE4AE0D7CD1 ] UmrDpService
C:\windows\system32\umrdp.dll
06:48:54.0964 4280 UmrDpService - ok
06:48:55.0073 4280 [ A69CD6BDB82872999D2E46F9324ADA83 ] UNS
C:\Program Files\Intel\Intel(R) Management Engine Components\UNS\UNS.exe
06:48:55.0136 4280 UNS - ok
06:48:55.0167 4280 [ 833FBB672460EFCE8011D262175FAD33 ] upnphost
C:\windows\system32\upnphost.dll
06:48:55.0167 4280 upnphost - ok
06:48:55.0198 4280 [ 5C233AEFB566EE78C1EFBC0493FB066A ] usbccgp
C:\windows\system32\DRIVERS\usbccgp.sys
06:48:55.0198 4280 usbccgp - ok
06:48:55.0214 4280 [ 04EC7CEC62EC3B6D9354EEE93327FC82 ] usbcir
C:\windows\system32\DRIVERS\usbcir.sys
06:48:55.0214 4280 usbcir - ok
06:48:55.0229 4280 [ 5B71019A6ACA0116FD21B368F19C0B91 ] usbehci
C:\windows\system32\drivers\usbehci.sys
06:48:55.0229 4280 usbehci - ok
06:48:55.0245 4280 [ 5823D3965C2A4F6F785ED1A3B403F3B8 ] usbhub
C:\windows\system32\DRIVERS\usbhub.sys
06:48:55.0260 4280 usbhub - ok
06:48:55.0276 4280 [ E753ED6C49DA13967EBABF9EA616454A ] usbohci
C:\windows\system32\drivers\usbohci.sys
06:48:55.0276 4280 usbohci - ok
06:48:55.0292 4280 [ 797D862FE0875E75C7CC4C1AD7B30252 ] usbprint
C:\windows\system32\DRIVERS\usbprint.sys
06:48:55.0292 4280 usbprint - ok
06:48:55.0323 4280 [ 1C4287739A93594E57E2A9E6A3ED7353 ] USBSTOR
C:\windows\system32\drivers\USBSTOR.SYS
06:48:55.0323 4280 USBSTOR - ok
06:48:55.0338 4280 [ 6A30928A469CE802600E1EA8C0F2F53F ] usbuhci
C:\windows\system32\drivers\usbuhci.sys
06:48:55.0338 4280 usbuhci - ok
06:48:55.0354 4280 [ B5F6A992D996282B7FAE7048E50AF83A ] usbvideo
C:\windows\system32\Drivers\usbvideo.sys
06:48:55.0370 4280 usbvideo - ok
06:48:55.0370 4280 [ 081E6E1C91AEC36758902A9F727CD23C ] UxSms
C:\windows\system32\uxsms.dll
06:48:55.0385 4280 UxSms - ok
06:48:55.0401 4280 [ C2243FF9E9AAD0C30E8B1A0914DA15B6 ] vaultsvc

```

```

C:\windows\system32\lsass.exe
06:48:55.0401 4280 VaultSvc - ok
06:48:55.0479 4280 [ 60CF5CBC7F5349E1400B6554E0F040A7 ] vcsFPService
C:\windows\system32\vcsFPService.exe
06:48:55.0510 4280 vcsFPService - ok
06:48:55.0510 4280 [ A059C4C3EDB09E07D21A8E5C0AABD3CB ] vdrvroot
C:\windows\system32\DRIVERS\vdrvroot.sys
06:48:55.0510 4280 vdrvroot - ok
06:48:55.0557 4280 [ 8C4E7C49D3641BC9E299E466A7F8867D ] vds
C:\windows\system32\vds.exe
06:48:55.0572 4280 vds - ok
06:48:55.0604 4280 [ 17C408214EA61696CEC9C66E388B14F3 ] vga
C:\windows\system32\DRIVERS\vgapnp.sys
06:48:55.0604 4280 vga - ok
06:48:55.0619 4280 [ 8E38096AD5C8570A6F1570A61E251561 ] VgaSave
C:\windows\system32\drivers\vga.sys
06:48:55.0619 4280 VgaSave - ok
06:48:55.0635 4280 [ 3BE6E1F3A4F1AFEC8CEE0D7883F93583 ] vhdmp
C:\windows\system32\DRIVERS\vhdmp.sys
06:48:55.0650 4280 vhdmp - ok
06:48:55.0650 4280 [ C829317A37B4BEA8F39735D4B076E923 ] viaagp
C:\windows\system32\DRIVERS\viaagp.sys
06:48:55.0650 4280 viaagp - ok
06:48:55.0666 4280 [ E02F079A6AA107F06B16549C6E5C7B74 ] via7
C:\windows\system32\DRIVERS\viac7.sys
06:48:55.0666 4280 viac7 - ok
06:48:55.0682 4280 [ E43574F6A56A0EE11809B48C09E4FD3C ] viaide
C:\windows\system32\DRIVERS\viaide.sys
06:48:55.0682 4280 viaide - ok
06:48:55.0697 4280 [ 379B349F65F453D2A6E75EA6B7448E49 ] vmbus
C:\windows\system32\DRIVERS\vmbus.sys
06:48:55.0697 4280 vmbus - ok
06:48:55.0728 4280 [ EC2BBAB4B84D0738C6C83D2234DC36FE ] VMBusHID
C:\windows\system32\DRIVERS\VMBusHID.sys
06:48:55.0728 4280 VMBusHID - ok
06:48:55.0744 4280 [ 384E5A2AA49934295171E499F86BA6F3 ] volmgr
C:\windows\system32\DRIVERS\volmgr.sys
06:48:55.0744 4280 volmgr - ok
06:48:55.0760 4280 [ B5BB72067DDDBBFB04B2F89FF8C3C87 ] volmgrx
C:\windows\system32\drivers\volmgrx.sys
06:48:55.0775 4280 volmgrx - ok
06:48:55.0806 4280 [ 59F06B4968E58BC83DFC56CA4517960E ] volsnap
C:\windows\system32\drivers\volsnap.sys
06:48:55.0822 4280 volsnap - ok
06:48:55.0822 4280 [ 33E74DF34753FCAAB06F6F2BDC8CABF5 ] vpcbus
C:\windows\system32\DRIVERS\vpchbus.sys
06:48:55.0838 4280 vpcbus - ok
06:48:55.0838 4280 [ 5F04362CEB5FB5901037E9D9EADD3760 ] vpcnfltr
C:\windows\system32\DRIVERS\vpchnfltr.sys
06:48:55.0853 4280 vpcnfltr - ok
06:48:55.0853 4280 [ 625088D6EE9EDE977FD03CF18D1CD5C5 ] vpcusb
C:\windows\system32\DRIVERS\vpusb.sys
06:48:55.0853 4280 vpcusb - ok
06:48:55.0884 4280 [ 1023C696D42268E9071BB376DBEC8396 ] vpcvmm
C:\windows\system32\drivers\vpvmm.sys
06:48:55.0900 4280 vpcvmm - ok
06:48:55.0931 4280 [ 9DFA0CC2F8855A04816729651175B631 ] vsmraid
C:\windows\system32\DRIVERS\vsraid.sys
06:48:55.0931 4280 vsmraid - ok
06:48:55.0978 4280 [ 7EA2BCD94D9CFAF4C556F5CC94532A6C ] VSS
C:\windows\system32\vssvc.exe
06:48:56.0009 4280 VSS - ok
06:48:56.0025 4280 [ 90567B1E658001E79D7C8BBD3DDE5AA6 ] vwifibus
C:\windows\system32\DRIVERS\vwifibus.sys
06:48:56.0025 4280 vwifibus - ok
06:48:56.0040 4280 [ 7090D3436EEB4E7DA3373090A23448F7 ] vwifflt
C:\windows\system32\DRIVERS\vwifflt.sys
06:48:56.0040 4280 vwifflt - ok

```

```

06:48:56.0072 4280 [ 55187FD710E27D5095D10A472C8BAF1C ] w32Time
C:\windows\system32\w32time.dll
06:48:56.0087 4280 w32Time - ok
06:48:56.0118 4280 [ 427A8BC96F16C40DF81C2D2F4EDD32DD ] wacomousefilter
C:\windows\system32\DRIVERS\wacomousefilter.sys
06:48:56.0118 4280 wacomousefilter - ok
06:48:56.0134 4280 [ DE3721E89C653AA281428C8A69745D90 ] WacomPen
C:\windows\system32\DRIVERS\wacompen.sys
06:48:56.0134 4280 WacomPen - ok
06:48:56.0181 4280 [ 846B58EA44BF8C92E4B59F4E2252C4C0 ] wacomvhid
C:\windows\system32\DRIVERS\wacomvhid.sys
06:48:56.0181 4280 wacomvhid - ok
06:48:56.0196 4280 [ C497C0A80BAD225244B1CA6C86FA3463 ] WacomVTHid
C:\windows\system32\DRIVERS\wacomVTHid.sys
06:48:56.0196 4280 WacomVTHid - ok
06:48:56.0212 4280 [ 692A712062146E96D28BA0B7D75DE31B ] WANARP
C:\windows\system32\DRIVERS\wanarp.sys
06:48:56.0212 4280 WANARP - ok
06:48:56.0228 4280 [ 692A712062146E96D28BA0B7D75DE31B ] wanarpv6
C:\windows\system32\DRIVERS\wanarp.sys
06:48:56.0228 4280 wanarpv6 - ok
06:48:56.0274 4280 [ 353A04C273EC58475D8633E75CCD5604 ] WatAdminSvc
C:\windows\system32\wat\watAdminSvc.exe
06:48:56.0290 4280 WatAdminSvc - ok
06:48:56.0337 4280 [ 7790B77FE1E5EE47DCC66247095BB4C9 ] wbengine
C:\windows\system32\wbengine.exe
06:48:56.0384 4280 wbengine - ok
06:48:56.0399 4280 [ 9614B5D29DC76AC3C29F6D2D3AA70E67 ] WbioSrv
C:\windows\System32\wbiosrv.dll
06:48:56.0415 4280 WbioSrv - ok
06:48:56.0430 4280 [ 6D9B75275C3E3A5F51AEF81AFFADB2B6 ] WcnSvc
C:\windows\System32\WcnSvc.dll
06:48:56.0446 4280 WcnSvc - ok
06:48:56.0462 4280 [ 5D930B6357A6D2AF4D7653BDABBF352F ] WcsPlugInService
C:\windows\System32\WcsPlugInService.dll
06:48:56.0477 4280 WcsPlugInService - ok
06:48:56.0477 4280 [ 1112A9BADACB47B7C0BB0392E3158DFF ] Wd
C:\windows\system32\DRIVERS\Wd.sys
06:48:56.0477 4280 Wd - ok
06:48:56.0524 4280 [ A840213F1ACDCC175B4D1D5AAEAC0D7A ] Wdf01000
C:\windows\system32\drivers\Wdf01000.sys
06:48:56.0555 4280 Wdf01000 - ok
06:48:56.0571 4280 [ 46EF9DC96265FD0B423DB72E7C38C2A5 ] WdiServiceHost
C:\windows\system32\Wdi.dll
06:48:56.0586 4280 WdiServiceHost - ok
06:48:56.0602 4280 [ 46EF9DC96265FD0B423DB72E7C38C2A5 ] WdiSystemHost
C:\windows\system32\Wdi.dll
06:48:56.0618 4280 WdiSystemHost - ok
06:48:56.0649 4280 [ BB5EC38F8D4600119B4720BC5D4211F1 ] WebClient
C:\windows\System32\WebClient.dll
06:48:56.0649 4280 WebClient - ok
06:48:56.0696 4280 [ 760F0AFE937A77CFF27153206534F275 ] WecSvc
C:\windows\system32\WecSvc.dll
06:48:56.0711 4280 WecSvc - ok
06:48:56.0727 4280 [ AC804569BB2364FB6017370258A4091B ] Wercplsupport
C:\windows\System32\Wercplsupport.dll
06:48:56.0742 4280 Wercplsupport - ok
06:48:56.0758 4280 [ 08E420D873E4FD85241EE2421B02C4A4 ] Wersvc
C:\windows\System32\Wersvc.dll
06:48:56.0774 4280 Wersvc - ok
06:48:56.0774 4280 [ 8B9A943F3B53861F2BFAF6C186168F79 ] WfpLwf
C:\windows\system32\DRIVERS\WfpLwf.sys
06:48:56.0789 4280 WfpLwf - ok
06:48:56.0805 4280 [ 5CF95B35E59E2A38023836FFF31BE64C ] WIMMount
C:\windows\system32\drivers\WIMMount.sys
06:48:56.0805 4280 WIMMount - ok
06:48:56.0852 4280 [ 3FAE8F94296001C32EAB62CD7D82E0FD ] WinDefend
C:\Program Files\windows Defender\mpsvc.dll

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt

```

06:48:56.0883 4280 winDefend - ok
06:48:56.0898 4280 winHttpAutoProxySvc - ok
06:48:56.0945 4280 [ F62E510B6AD4C21EB9FE8668ED251826 ] winmgmt
C:\windows\system32\wbem\WMIsvc.dll
06:48:56.0961 4280 winmgmt - ok
06:48:57.0008 4280 [ C4F5D3901D1B41D602DDC196E0B95B51 ] winRM
C:\windows\system32\wsmSvc.dll
06:48:57.0039 4280 winRM - ok
06:48:57.0054 4280 [ B5BA3CC19D00F2EBA92F1CFBEBB5D650 ] winUSB
C:\windows\system32\DRIVERS\winUSB.sys
06:48:57.0070 4280 winUSB - ok
06:48:57.0086 4280 [ FF17B6A01A9FEB2A8D322BF369D36C96 ] wisdpen
C:\windows\system32\DRIVERS\wisdpen.sys
06:48:57.0086 4280 wisdpen - ok
06:48:57.0117 4280 [ 16935C98FF639D185086A3529B1F2067 ] wlansvc
C:\windows\System32\wlansvc.dll
06:48:57.0148 4280 wlansvc - ok
06:48:57.0210 4280 [ 5144AE67D60EC653F97DDF3FEED29E77 ] wlidsvc
C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDSVC.EXE
06:48:57.0257 4280 wlidsvc - ok
06:48:57.0273 4280 [ 0217679B8FCA58714C3BF2726D2CA84E ] wmiAcpi
C:\windows\system32\DRIVERS\wmiacpi.sys
06:48:57.0273 4280 wmiAcpi - ok
06:48:57.0320 4280 [ 6EB6B66517B048D87DC1856DDF1F4C3F ] wmiApSrv
C:\windows\system32\wbem\WmiApSrv.exe
06:48:57.0320 4280 wmiApSrv - ok
06:48:57.0382 4280 [ 77FBD400984CF72BA0FC4B3489D65F74 ] WMPNetworkSvc
C:\Program Files\windows Media Player\wmpnetwk.exe
06:48:57.0413 4280 WMPNetworkSvc - ok
06:48:57.0444 4280 [ A2F0EC770A92F2B3F9DE6D518E11409C ] WPCSvc
C:\windows\System32\wpcsvc.dll
06:48:57.0444 4280 WPCSvc - ok
06:48:57.0460 4280 [ B7F658A2EBC07129538AD9AB35212637 ] WPDBusEnum
C:\windows\system32\wpdbusenum.dll
06:48:57.0476 4280 WPDBusEnum - ok
06:48:57.0491 4280 [ 6DB3276587B853BF886B69528FDB048C ] ws2ifs1
C:\windows\system32\drivers\ws2ifs1.sys
06:48:57.0507 4280 ws2ifs1 - ok
06:48:57.0507 4280 [ A661A76333057B383A06E65F0073222F ] wscsvc
C:\windows\System32\wscsvc.dll
06:48:57.0522 4280 wscsvc - ok
06:48:57.0522 4280 wSearch - ok
06:48:57.0569 4280 [ 8A9ECBFB1B822EC2D9E140DF0DA21BA3 ] WTouchService
C:\Program Files\WTouch\WTouchService.exe
06:48:57.0569 4280 WTouchService - ok
06:48:57.0647 4280 [ FC3EC24FCE372C89423E015A2AC1A31E ] wuauerv
C:\windows\system32\wuaueng.dll
06:48:57.0678 4280 wuauerv - ok
06:48:57.0725 4280 [ 06E6F32C8D0A3F66D956F57B43A2E070 ] wudfPf
C:\windows\system32\drivers\wudfPf.sys
06:48:57.0725 4280 wudfPf - ok
06:48:57.0741 4280 [ 867C301E8B790040AE9CF6486E8041DF ] WUDFRd
C:\windows\system32\DRIVERS\WUDFRd.sys
06:48:57.0741 4280 WUDFRd - ok
06:48:57.0772 4280 [ FE47B7BC8EA320C2D9B5E5BF6E303765 ] wudfsvc
C:\windows\System32\WUDFSvc.dll
06:48:57.0772 4280 wudfsvc - ok
06:48:57.0788 4280 [ FF2D745B560F7C71B31F30F4D49F73D2 ] wwanSvc
C:\windows\System32\wwansvc.dll
06:48:57.0788 4280 wwanSvc - ok
06:48:57.0803 4280 ===== Scan global =====
06:48:57.0834 4280 [ 9A595DF601070DA78C40481120DD2C06 ]
C:\windows\system32\basesrv.dll
06:48:57.0866 4280 [ 8531AAF69394EFB93BC653916C46D245 ]
C:\windows\system32\winsrv.dll
06:48:57.0897 4280 [ 8531AAF69394EFB93BC653916C46D245 ]
C:\windows\system32\winsrv.dll
06:48:57.0928 4280 [ 364455805E64882844EE9ACB72522830 ]

```

```

TDSSkiller.2.8.16.0_30.03.2013_06.47.17_log.txt
C:\windows\system32\svchost.exe
06:48:57.0959 4280 [ 5F1B6A9C35D3D5CA72D6D6FDEF9747D6 ]
C:\windows\system32\services.exe
06:48:57.0975 4280 [Global] - ok
06:48:57.0990 4280 ===== Scan MBR =====
06:48:57.0990 4280 [ A36C5E4F47E84449FF07ED3517B43A31 ] \Device\Harddisk0\DR0
06:48:58.0396 4280 \Device\Harddisk0\DR0 - ok
06:48:58.0396 4280 ===== Scan VBR =====
06:48:58.0412 4280 [ 8CBB78C18728ED4B40486C51DA75EAA9 ]
\Device\Harddisk0\DR0\Partition1
06:48:58.0412 4280 \Device\Harddisk0\DR0\Partition1 - ok
06:48:58.0427 4280 [ 8C3EE3CBE82BA2D5CC0DD2DC8A9731CA ]
\Device\Harddisk0\DR0\Partition2
06:48:58.0427 4280 \Device\Harddisk0\DR0\Partition2 - ok
06:48:58.0474 4280 [ D09097A1C75BB9B87169F378D7C8541F ]
\Device\Harddisk0\DR0\Partition3
06:48:58.0490 4280 \Device\Harddisk0\DR0\Partition3 - ok
06:48:58.0552 4280 [ C22C4B1B501C2CF8EA1F7E7712D8DB9D ]
\Device\Harddisk0\DR0\Partition4
06:48:58.0568 4280 \Device\Harddisk0\DR0\Partition4 - ok
06:48:58.0568 4280 =====
06:48:58.0568 4280 Scan finished
06:48:58.0568 4280 =====
06:48:58.0583 8132 Detected object count: 0
06:48:58.0583 8132 Actual detected object count: 0
06:49:02.0171 4224 Deinitialize success

```