```
19:12:30.0675 0x0ff4  TDSS rootkit removing tool 3.0.0.40 Jul 10 2014 12:37:58
19:12:30.0675 0x0ff4  UEFI system
19:12:40.0637 0x0ff4  ============================================================
19:12:40.0637 0x0ff4  Current date / time: 2014/08/08 19:12:40.0637
19:12:40.0637 0x0ff4  SystemInfo:
19:12:40.0637 0x0ff4
19:12:40.0637 0x0ff4  OS Version: 6.3.9600 ServicePack: 0.0
19:12:40.0637 0x0ff4  Product type: Workstation
19:12:40.0637 0x0ff4  ComputerName: PC-RIEKIE
19:12:40.0637 0x0ff4  UserName: Riekie
19:12:40.0637 0x0ff4  Windows directory: C:\WINDOWS
19:12:40.0638 0x0ff4  System windows directory: C:\WINDOWS
19:12:40.0638 0x0ff4  Running under WOW64
19:12:40.0638 0x0ff4  Processor architecture: Intel x64
19:12:40.0638 0x0ff4  Number of processors: 4
19:12:40.0638 0x0ff4  Page size: 0x1000
19:12:40.0638 0x0ff4  Boot type: Normal boot
19:12:40.0638 0x0ff4  ============================================================
19:12:40.0966 0x0ff4  KLMD registered as C:\WINDOWS\system32\drivers\14858670.sys
19:12:41.0630 0x0ff4  System UUID: {781A314D-91DE-8868-4A32-DD1EC289B3E1}
19:12:42.0811 0x0ff4  Drive \Device\Harddisk0\DR0 - Size: 0x747OC06000 ( 465.76
Gb ), SectorSize: 0x200, Cylinders: 0xED81, SectorsPerTrack: 0x3F,
TracksPerCylinder: 0xFF, Type 'K0', Flags 0x00000040
19:12:42.0849 0x0ff4  ============================================================
19:12:42.0849 0x0ff4  \Device\Harddisk0\DR0:
19:12:42.0849 0x0ff4  GPT partitions:
19:12:42.0850 0x0ff4  \Device\Harddisk0\DR0\Partition1: GPT, TypeGUID: {DE94BBA4-
06D1-4D40-A16A-BFD50179D6AC}, UniqueGUID: {09B9F2EF-9358-4C83-A999-0085A78655E9},
Name: Basic data partition, StartLBA 0x800, BlocksNum 0xC8000
19:12:42.0851 0x0ff4  \Device\Harddisk0\DR0\Partition2: GPT, TypeGUID: {C12A7328-
F81F-11D2-BA4B-00A0C93EC93B}, UniqueGUID: {250D5AD5-7D14-4CE8-B3D1-E7D43A12ACE2},
Name: EFI system partition, StartLBA 0xC8800, BlocksNum 0x96000
19:12:42.0851 0x0ff4  \Device\Harddisk0\DR0\Partition3: GPT, TypeGUID: {E3C9E316-
0B5C-4DB8-817D-F92DF00215AE}, UniqueGUID: {4BB1B154-9A86-45B0-B33F-C2A21684E6F9},
Name: Microsoft reserved partition, StartLBA 0x15E800, BlocksNum 0x40000
19:12:42.0851 0x0ff4  \Device\Harddisk0\DR0\Partition4: GPT, TypeGUID: {EBD0A0A2-
B9E5-4433-87C0-68B6B72699C7}, UniqueGUID: {99EA7AC0-6DFD-4684-9ECF-BB941675F707},
Name: Basic data partition, StartLBA 0x19E800, BlocksNum 0x37706000
19:12:42.0851 0x0ff4  \Device\Harddisk0\DR0\Partition5: GPT, TypeGUID: {DE94BBA4-
06D1-4D40-A16A-BFD50179D6AC}, UniqueGUID: {1F606DFA-9049-4AE4-BA93-15FE744B91FC},
Name:  , StartLBA 0x378A4800, BlocksNum 0xE1000
19:12:42.0852 0x0ff4  \Device\Harddisk0\DR0\Partition6: GPT, TypeGUID: {DE94BBA4-
06D1-4D40-A16A-BFD50179D6AC}, UniqueGUID: {E2BDA2A2-8EF8-4332-AE96-DE3CC2C9DF94},
Name: Basic data partition, StartLBA 0x37985800, BlocksNum 0x2A00800
19:12:42.0852 0x0ff4  MBR partitions:
19:12:42.0852 0x0ff4  ============================================================
19:12:42.0873 0x0ff4  C: <-> \Device\Harddisk0\DR0\Partition4
19:12:42.0874 0x0ff4  ============================================================
19:12:42.0874 0x0ff4  Initialize success
19:12:42.0874 0x0ff4  ============================================================
19:13:48.0598 0x1918  ============================================================
19:13:48.0598 0x1918  Scan started
19:13:48.0598 0x1918  Mode: Manual; SigCheck; TDLFS;
19:13:48.0598 0x1918  ============================================================
19:13:48.0598 0x1918  KSN ping started
19:13:51.0064 0x1918  KSN ping finished: true
19:13:51.0941 0x1918  ================ Scan system memory ========================
19:13:51.0941 0x1918  System memory - ok
19:13:51.0943 0x1918  ================ Scan services =============================
19:13:52.0128 0x1918  [ E1832BD9FD7E0FC2DC9FA5935DE3E8C1,
41FF7418887AFC8B9C96EF21C5950DD342CC9E3C0D87AFD60A05B988C1D6CC23 ] 1394ohci
C:\WINDOWS\System32\drivers\1394ohci.sys
19:13:52.0330 0x1918  1394ohci - ok
19:13:52.0365 0x1918  [ AD508A1A46EC21B740AB31C28EFDFDB1,
9B1046CF0B80723149BD359B55CC0B8B3ABBEAA9038469F542A4C345C503FB02 ] 3ware
C:\WINDOWS\system32\drivers\3ware.sys
19:13:52.0387 0x1918  3ware - ok
19:13:52.0444 0x1918  [ 9539F7917B4B6D92C90F0FAA6B86C605,
B4C284E8EECC2E7025053A3320EFDC9F47BCA9828853AD2A805DB826CA4AC27E ] ACPI
C:\WINDOWS\system32\drivers\ACPI.sys
19:13:52.0515 0x1918  ACPI - ok
19:13:52.0535 0x1918  [ AC8279D229398BCF05C3154ADCA86813,
083E86CBE53244D24C334DB1511C77025133AE7875191845764B890A8CA5AFA9 ] acpiex
C:\WINDOWS\system32\Drivers\acpiex.sys
19:13:52.0559 0x1918  acpiex - ok
19:13:52.0578 0x1918  [ A8970D9BF23CD309E0403978A1B58F3F,
```

```
9946C8477104EEC7DB197E2222F9905307F101C398CCED4B5FD0F86A5622C791 ] acpipagr
C:\WINDOWS\System32\drivers\acpipagr.sys
19:13:52.0613 0x1918  acpipagr - ok
19:13:52.0647 0x1918  [ 111A89C99C5B4F1A7BCE5F643DD86F65,
41A2E49FF443927D05F7EF6385181082278529 84E68D4663C8761178C0B84A45 ] AcpiPmi
C:\WINDOWS\System32\drivers\acpipmi.sys
19:13:52.0740 0x1918  AcpiPmi - ok
19:13:52.0755 0x1918  [ 5758387D68A20AE7D3245011B07E36E7,
77832E200E8B0D259552F6F60FE454A887E3EBBB9EA2F3590E6645289A04E293 ] acpitime
C:\WINDOWS\System32\drivers\acpitime.sys
19:13:52.0813 0x1918  acpitime - ok
19:13:52.0891 0x1918  [ B362181ED3771DC03B4141927C80F801,
69514E5177A0AEA89C27C2234712F9F82E8D8F99E1FD4273898C9324C6FF7472 ] AdobeARMservice
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
19:13:52.0911 0x1918  AdobeARMservice - ok
19:13:53.0009 0x1918  [ A6B6AB9502B63F43A9A56AE6AFB22078,
DD1F0BA3D8F3333F52A71EAE3719A001F6EF844D647FFABF0E4C56C6C764ACA7 ]
AdobeFlashPlayerUpdateSvc
C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
19:13:53.0037 0x1918  AdobeFlashPlayerUpdateSvc - ok
19:13:53.0108 0x1918  [ 7C1FDF1B48298CBA7CE4BDD4978951AD,
80F4D536E1231B30E836F72ADC8814AE6AA9FEC573FB5F3F965FAC8ABCCAF0F8 ] ADP80XX
C:\WINDOWS\system32\drivers\ADP80XX.SYS
19:13:53.0180 0x1918  ADP80XX - ok
19:13:53.0229 0x1918  [ 0F17D49BE041B7EFF1D33BF1414E7AC6,
F8B536B60903814DF88DAF535753288537EF0993E42AA4E734EDA8D68B24C7AB ] AeLookupSvc
C:\WINDOWS\System32\aelupsvc.dll
19:13:53.0325 0x1918  AeLookupSvc - ok
19:13:53.0396 0x1918  [ 374E27295F0A9DCAA8FC96370F9BEEA5,
51C394E0C2322D7D093941A1B8766171B5D1F47DF2FE0834209492891EA7D999 ] AFD
C:\WINDOWS\system32\drivers\afd.sys
19:13:53.0489 0x1918  AFD - ok
19:13:53.0521 0x1918  [ 7DFAEBA9AD62D20102B576D5CAC45EC8,
9FA5207335303D1E8E9A3C9E1FB82C09AD21B04382F69D777A67E48EE91D2093 ] agp440
C:\WINDOWS\system32\drivers\agp440.sys
19:13:53.0567 0x1918  agp440 - ok
19:13:53.0606 0x1918  [ 8E8E34B7BA059050EED827410D0697A2,
85B6684709F24729A6497563812A90A54068AC2DD9EEA03037CB1EEF5C85AAA9 ] ahcache
C:\WINDOWS\system32\DRIVERS\ahcache.sys
19:13:53.0700 0x1918  ahcache - ok
19:13:53.0742 0x1918  [ A91D8E1E433EFB32551BCE69037E1CE7,
41DFDD5B56918D19D09DFB3E4B07460AA85647A8647ABBBB906158D8D6653290 ] ALG
C:\WINDOWS\System32\alg.exe
19:13:53.0839 0x1918  ALG - ok
19:13:53.0869 0x1918  [ 7589DE749DB6F71A68489DCE04158729,
5F35EDD50737985595C9D6703237CA2ADE49AA5443331020899698EB5114A0FB ] AmdK8
C:\WINDOWS\System32\drivers\amdk8.sys
19:13:53.0958 0x1918  AmdK8 - ok
19:13:53.0984 0x1918  [ B46D2D89AFF8A9490FA8C98C7A5616E3,
BE0765B5423B690E0F097FECD9717FAA95BFDFFDC6CF1B93DE5A19A1B7797879 ] AmdPPM
C:\WINDOWS\System32\drivers\amdppm.sys
19:13:54.0060 0x1918  AmdPPM - ok
19:13:54.0085 0x1918  [ D2BF2F94A47D332814910FD47C6BBCD2,
FE273D77D119D958676E1197D9EA7B008E3B05C6192B1962A81D4223ED204C35 ] amdsata
C:\WINDOWS\system32\drivers\amdsata.sys
19:13:54.0127 0x1918  amdsata - ok
19:13:54.0160 0x1918  [ A8E04943C7BBA7219AA50400272C3C6E,
794C0BD12DF0392654E9A37AE4A24B5BE2D83F1F24F74DD48A1A0BF3AB8B1FF8 ] amdsbs
C:\WINDOWS\system32\drivers\amdsbs.sys
19:13:54.0194 0x1918  amdsbs - ok
19:13:54.0221 0x1918  [ CEA5F4F27CFC08E3A44D576811B35F50,
89DF64B81BD109BAABAE93A4603C1617241219F38DDAF325EFE6BD35FF6FD717 ] amdxata
C:\WINDOWS\system32\drivers\amdxata.sys
19:13:54.0238 0x1918  amdxata - ok
19:13:54.0296 0x1918  [ 968A4A0FD5BF07717F4E869875A4B149,
1AC58AD408E7FC8345E5CA7785321AE4B7FDE6776EA69280D0B05056517052F8 ] ApfiltrService
C:\WINDOWS\system32\DRIVERS\Apfiltr.sys
19:13:54.0351 0x1918  ApfiltrService - ok
19:13:54.0372 0x1918  [ 04951A9A937CBE28A2D3FEEA360B6D1F,
D8AAF000BE4FE4B203DC2EB2A64F780A542E5238CE3F9952FD03277379B11529 ] AppID
C:\WINDOWS\system32\drivers\appid.sys
19:13:54.0436 0x1918  AppID - ok
19:13:54.0476 0x1918  [ C0DC3F58214A227980AEB091CFD2F973,
0C3E8453C9F65ADA3E74C38C0E3AC3E0CBFD807B827097046265B38839E151E3 ] AppIDSvc
C:\WINDOWS\System32\appidsvc.dll
19:13:54.0549 0x1918  AppIDSvc - ok
```

19:13:54.0564 0x1918 [8D6F535461F6CFF75A8ADDF83024C904,
F2A97EC4A6284F28B685A3CE2D450F61E75EE8692D718A6AA352D5734BBBAD7B] Appinfo
C:\WINDOWS\System32\appinfo.dll
19:13:54.0653 0x1918 Appinfo - ok
19:13:54.0691 0x1918 [30E3850F303EAE5C364782EA78579CC9,
8C94E5A9052F6E794685194EEACB31A174A947D60246908B6A0DEFA081A747A3] Apple Mobile
Device C:\Program Files (x86)\Common Files\Apple\Mobile Device
Support\AppleMobileDeviceService.exe
19:13:54.0725 0x1918 Apple Mobile Device - ok
19:13:54.0774 0x1918 [CB12C47647D8BDAFAA94C0856B14128B,
5590C98095357C92563EF94800107D3611AA6ECA1A70BE463C03B279E618A6C4] AppReadiness
C:\WINDOWS\system32\AppReadiness.dll
19:13:54.0848 0x1918 AppReadiness - ok
19:13:54.0957 0x1918 [F7529BD3FFAC9C33D15F6DE3B7353B03,
8EF0A84C9687A246B60939A326E498121039E9CC617A7ABBA933EDD327F3467E] AppXSvc
C:\WINDOWS\system32\appxdeploymentserver.dll
19:13:55.0091 0x1918 AppXSvc - ok
19:13:55.0125 0x1918 [65045784366F7EC5FB4E71BCF923187B,
53C215C64FF12E44B097F7CB88E8482438CE0ACBD3C68D8FD38BA0D0D8747FAA] arcsas
C:\WINDOWS\system32\drivers\arcsas.sys
19:13:55.0148 0x1918 arcsas - ok
19:13:55.0171 0x1918 [D95E64416A4A3ED6986E0F474DA934BD,
DBB4A0DED0DABE1F8FF0DB8C0E9EC4EC906A85A45DC0AEC013A8744F9BF5D40E] aswHwid
C:\WINDOWS\system32\drivers\aswHwid.sys
19:13:55.0207 0x1918 aswHwid - ok
19:13:55.0222 0x1918 [D421F374BE2213E910CD133708DDE60E,
951C50BCDC24921F6D25D6704D3A8D054F89B30EFFB8E2A0E2826D8BCDAC9847] aswKbd
C:\WINDOWS\system32\drivers\aswKbd.sys
19:13:55.0245 0x1918 aswKbd - ok
19:13:55.0268 0x1918 [FF1E537A3632CBB9A0BF72B9FD0878D5,
B26E6A1F6E6FA5280A12861EFAD44D8F49353F47B21843EBA73E149CF613DCBC] aswMonFlt
C:\WINDOWS\system32\drivers\aswMonFlt.sys
19:13:55.0294 0x1918 aswMonFlt - ok
19:13:55.0311 0x1918 [A5757DE5F9C83AB40667A53D5126EA40,
58B72B1B126CF641188703CE82E26BEB0C41AD7587CFFCCCE9E3C64CC7AACC90] aswRdr
C:\WINDOWS\system32\drivers\aswRdr2.sys
19:13:55.0337 0x1918 aswRdr - ok
19:13:55.0357 0x1918 [645D97385F3F284FB5604F9B970F4D24,
15A9D7F0F4C1062210E4E744A9069B8645177D19F35B8740D74022639DC05F2E] aswRvrt
C:\WINDOWS\system32\drivers\aswRvrt.sys
19:13:55.0382 0x1918 aswRvrt - ok
19:13:55.0445 0x1918 [B8FDEDE963B82CFD23B3A53A3084666D,
3537E5B684FB6F0AA589A5FA7CD111E1744DF384AB1A266D4114100F104ED11B] aswSnx
C:\WINDOWS\system32\drivers\aswSnx.sys
19:13:55.0515 0x1918 aswSnx - ok
19:13:55.0587 0x1918 [0DEDC041DF594AEC2C3BD00417CFAF60,
0D3A8924503986546EE256D185225C0B080FDB6B0C8B0BED7516B07A7334371B] aswSP
C:\WINDOWS\system32\drivers\aswSP.sys
19:13:55.0630 0x1918 aswSP - ok
19:13:55.0668 0x1918 [48DED912CDE54FC0923B9858512366E1,
9B216B934408A7CB3CE2B41240B7EF01EAA3BC066211B784064FF8AC97A29B4E] aswStm
C:\WINDOWS\system32\drivers\aswStm.sys
19:13:55.0686 0x1918 aswStm - ok
19:13:55.0697 0x1918 [471A311745848B80339436688A8286E6,
E51C57236CEC19AC38E85D115DB97875517D837811188AD2E53FA49055B53890] aswVmm
C:\WINDOWS\system32\drivers\aswVmm.sys
19:13:55.0719 0x1918 aswVmm - ok
19:13:55.0730 0x1918 [3DB7721F06BC2FEDB25029EA23AB27DA,
221861148C66FE53E4D6EE49C6E656479AB5804A2D348A280A1CD8093E8AB788] AsyncMac
C:\WINDOWS\system32\DRIVERS\asyncmac.sys
19:13:55.0766 0x1918 AsyncMac - ok
19:13:55.0780 0x1918 [74B14192CF79A72F7536B27CB8814FBD,
0CF6BBB63FFE0C12777664D80B2797923844C8392D0FD81D7962EE5EE2C3C3D9] atapi
C:\WINDOWS\system32\drivers\atapi.sys
19:13:55.0823 0x1918 atapi - ok
19:13:55.0867 0x1918 [62A40F3DFF2B40915A1981285B14EFD4,
02F19978D153E816A6A879F6D0D67B2AB89F5964B86953F11B82D9970C3ED963] AthBTPort
C:\WINDOWS\system32\DRIVERS\btath_flt.sys
19:13:55.0907 0x1918 AthBTPort - ok
19:13:55.0965 0x1918 [69BF08F9B599117694600021AE1D6A59,
0CB72D0520DBD9EF3F477B73E6641F7CABDD24DBFC4FA9560A3AA15A53CBECC] AtherosSvc
C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\adminservice.exe
19:13:56.0000 0x1918 AtherosSvc - ok
19:13:56.0174 0x1918 [2C7676F892E88FD190F08D98048C7C6C,
44C13C103F61DA4D1A3823D37344F8C9465A611A9560808CE928925FB69604F7] athr
C:\WINDOWS\system32\DRIVERS\athw8x.sys

```
19:13:56.0388 0x1918  athr - ok
19:13:56.0435 0x1918  [ 886767FD022213F7885416134E9082E5,
E248D82210FBEBF62C23EBEC74A976B2D1A4E62D3B7638D95B2574B77BA05DD0 ]
AudioEndpointBuilder C:\WINDOWS\System32\AudioEndpointBuilder.dll
19:13:56.0516 0x1918  AudioEndpointBuilder - ok
19:13:56.0588 0x1918  [ 79B134ECE836B406B212E28C24011538,
1B875DD23CCAD8A2759DCDBCDCF3DE14231B9DB5EEC8E84FE081E41A52A047A1 ] Audiosrv
C:\WINDOWS\System32\Audiosrv.dll
19:13:56.0689 0x1918  Audiosrv - ok
19:13:56.0746 0x1918  [ 73F5C13B431915BAE35254B4E95DFB71,
393A045859382C44133C004598B1512048046BCC129FED2247A77FDBFCDB6DFF ] avast! Antivirus
C:\Program Files\AVAST Software\Avast\AvastSvc.exe
19:13:56.0784 0x1918  avast! Antivirus - ok
19:13:56.0830 0x1918  [ 96E8CAF20FC4B6C31CAD7816A801EB78,
E4870DB8FFBDCFEE98449338D0BDBF2DD0B5FEC75514E41C11A882BE6EB16833 ] AxInstSV
C:\WINDOWS\System32\AxInstSV.dll
19:13:56.0916 0x1918  AxInstSV - ok
19:13:56.0990 0x1918  [ A4A73F631FE2AA2826FBE4A399B04DEF,
973AACE8DC8DA669D0DF20F17EFDEEABB90AA046AC980948D16A62D39A606A79 ] b06bdrv
C:\WINDOWS\system32\drivers\bxvbda.sys
19:13:57.0062 0x1918  b06bdrv - ok
19:13:57.0099 0x1918  [ 8CC7F7E4AFCBA605921B137ED7992C68,
71406E6D6E9964740A6D90B05329D5492BB90AF40E0630CF2FBF4BA4BA14F2DD ] BasicDisplay
C:\WINDOWS\System32\drivers\BasicDisplay.sys
19:13:57.0175 0x1918  BasicDisplay - ok
19:13:57.0189 0x1918  [ 38A82F4EE8C416A6744B6D30381ED768,
9EAAE5F43BA0935913 0AC04B1DCA0F5D4DF32ED89C02DC5CEB640918948847F7 ] BasicRender
C:\WINDOWS\System32\drivers\BasicRender.sys
19:13:57.0285 0x1918  BasicRender - ok
19:13:57.0333 0x1918  [ C1ABB0F7E3BEA48A0417BDF6FF14AB21,
1CAC63A1A0FB9855A27EE977794576A860F6650C9EF7667FFB27F2A2FF721857 ] bcmfn2
C:\WINDOWS\System32\drivers\bcmfn2.sys
19:13:57.0366 0x1918  bcmfn2 - ok
19:13:57.0409 0x1918  [ E07C80468D0C599BFF01D9D4EC7AEDC3,
F675F455924DEC3FF69AD816DFEB6E74C804AEC3D3BFF7515953DB9D79C9B2D0 ] BDESVC
C:\WINDOWS\System32\bdesvc.dll
19:13:57.0484 0x1918  BDESVC - ok
19:13:57.0517 0x1918  [ EC19013E4CF87609534165DF897274D6,
8ED45537CF2D58D759A587CCBFDADD5580C7447B0C3B172CF19ECC7585E073FC ] Beep
C:\WINDOWS\system32\drivers\Beep.sys
19:13:57.0605 0x1918  Beep - ok
19:13:57.0697 0x1918  [ 20FB137ADDE1255F15F265A7BD9579BE,
87B4D5C91EFEAD987AAC3491A4360F82824C46AFF958B6F4CAED7C12224EF159 ] BFE
C:\WINDOWS\System32\bfe.dll
19:13:57.0779 0x1918  BFE - ok
19:13:57.0875 0x1918  [ 15225081966C785A9192782401643FD4,
E2BA0C8D044556FDD9DD7A25F7F71553DE7A2924E78F9284413C2AC46F0BF4EB ] BITS
C:\WINDOWS\System32\qmgr.dll
19:13:57.0971 0x1918  BITS - ok
19:13:58.0011 0x1918  [ 6B4FFFDDC618FCF64473CAA86E305697,
29EA66071D5822920F5C50533673ADAB5204F8B25C11027AD27450D881F1142D ] bowser
C:\WINDOWS\system32\DRIVERS\bowser.sys
19:13:58.0090 0x1918  bowser - ok
19:13:58.0146 0x1918  [ F2559A492AF8D653D1F47ADABA4C3E97,
77347915FB433023769699DFC9511F54E69C7FC7AB75F57FDC1A58E64A7126DE ]
BrokerInfrastructure C:\WINDOWS\System32\bisrv.dll
19:13:58.0216 0x1918  BrokerInfrastructure - ok
19:13:58.0226 0x1918  [ D528D6A92D187777691993DD757AF19A,
2C79978310193431E5FC462368424A172858D5351C92D4815C2A7E35B5DDE50C ] Browser
C:\WINDOWS\System32\browser.dll
19:13:58.0273 0x1918  Browser - ok
19:13:58.0317 0x1918  [ 6BF12F3F3A5D3F2866E69B8B463BC0CD,
E6D3358ABCF16ED2E68A93171C5E84D797137898BB2231E26FF0E4A07B8ADB22 ] BTATH_A2DP
C:\WINDOWS\system32\drivers\btath_a2dp.sys
19:13:58.0340 0x1918  BTATH_A2DP - ok
19:13:58.0356 0x1918  [ DC7038090A369FE866B76DB18E356558,
6782DBDDA352FBF8C2F5F6A90591794B569F2897AA5BD901AF062E774E734E48 ] btath_avdt
C:\WINDOWS\system32\drivers\btath_avdt.sys
19:13:58.0371 0x1918  btath_avdt - ok
19:13:58.0400 0x1918  [ C6978F7EBA6F37D626482AC6B9390630,
B4BF939AB9962A61DE9518604C20347DC2A6FCDCEB3D8AEF295AF12E6F2CDCF3 ] BTATH_BUS
C:\WINDOWS\System32\drivers\btath_bus.sys
19:13:58.0413 0x1918  BTATH_BUS - ok
19:13:58.0446 0x1918  [ 4AF7C20F94DAC343C01ED671C82DCB99,
2AABD85D9D76461DE883E0F13F61C391BA81E6198FF88268B319474E25A196C8 ] BTATH_HCRP
C:\WINDOWS\System32\drivers\btath_hcrp.sys
```

```
19:13:58.0487 0x1918  BTATH_HCRP - ok
19:13:58.0508 0x1918  [ 785C38070043BEEE9E9D591DE4067244,
1C8D15B8A9E80A2799E7094C4AE111FEA9FBC6EAA4A61B13EFE59314C9794949 ] BTATH_LWFLT
C:\WINDOWS\system32\DRIVERS\btath_lwflt.sys
19:13:58.0533 0x1918  BTATH_LWFLT - ok
19:13:58.0553 0x1918  [ A6019537D6125099363F90D0C6D181F9,
CA0C46AABBF71E2A29C93A477A06D33E3CACC84978DD9D729BEFB339E50D7055 ] BTATH_RCP
C:\WINDOWS\System32\drivers\btath_rcp.sys
19:13:58.0581 0x1918  BTATH_RCP - ok
19:13:58.0648 0x1918  [ 239A81CC18170F3369D389DA65E74342,
5E26976176A6651B149784B1ED86ECCA133B7755EBB8B04361A8DDB705767AA3 ] BtFilter
C:\WINDOWS\system32\DRIVERS\btfilter.sys
19:13:58.0695 0x1918  BtFilter - ok
19:13:58.0724 0x1918  [ A8F23D453A424FF4DE04989C4727ECC7,
AE4A9081395C7379F1C947EF8243F7609F90C843E086B8E77E1A2C06E36D4381 ] BthAvrcpTg
C:\WINDOWS\System32\drivers\BthAvrcpTg.sys
19:13:58.0758 0x1918  BthAvrcpTg - ok
19:13:58.0775 0x1918  [ 131F1C8573E7BFB41C54FBF5309CCD94,
DAFE51E3BADBD82A33B580F212B2D6520A120877C23F6D675521FEA2F4BA5A1F ] BthEnum
C:\WINDOWS\system32\DRIVERS\BthEnum.sys
19:13:58.0859 0x1918  BthEnum - ok
19:13:58.0883 0x1918  [ 746B9F94214915AECDE4B7FEA5FF9664,
EA2877D49DB4B7B9CE61653D63E8776DFF1CBCCAB12C14DB1D20DA44B8F06357 ] BthHFEnum
C:\WINDOWS\System32\drivers\bthhfenum.sys
19:13:58.0956 0x1918  BthHFEnum - ok
19:13:58.0983 0x1918  [ 71FE2A48E4C93DDB9798C024880B6C07,
8E93DE29C61A5FA64216231228CB3C4A1A693FE87CAA2C070BCAD7BE2D8ED000 ] bthhfhid
C:\WINDOWS\System32\drivers\BthHFHid.sys
19:13:59.0041 0x1918  bthhfhid - ok
19:13:59.0069 0x1918  [ D30C67473A2E229662D21F27EAA9AAA5,
D009C4836B0DFE963D8E3DEEDE611068838F2BBCAB146E6D70692FAB838E11F1 ] BthLEEnum
C:\WINDOWS\system32\DRIVERS\BthLEEnum.sys
19:13:59.0147 0x1918  BthLEEnum - ok
19:13:59.0184 0x1918  [ 66B791F6B11DC4303DD18A224A501542,
502AE4D6FFC6B0FCED081B0E0F61F699F96F20DFEE737B53828F5DEE3BD0FCB1 ] BTHMODEM
C:\WINDOWS\System32\drivers\bthmodem.sys
19:13:59.0270 0x1918  BTHMODEM - ok
19:13:59.0292 0x1918  [ 3AFE71D80EDF5D4DE0C5731352905669,
3E370169B8C5D301954D1F1DA302F7A0DB2A034990E10B3D64458C48E569320 5 ] BthPan
C:\WINDOWS\system32\DRIVERS\bthpan.sys
19:13:59.0381 0x1918  BthPan - ok
19:13:59.0534 0x1918  [ 92370F46AF28D54B67C135FA8C2AFCFC,
B1C0DBF27D392DEA8786AB9479C6CCD5A5DBDF3BE25ABA5FC7C6DB6D3EEE739B ] BTHPORT
C:\WINDOWS\System32\Drivers\BTHport.sys
19:13:59.0684 0x1918  BTHPORT - ok
19:13:59.0725 0x1918  [ E5E48FEED73D463175EAB1542495191C,
0A8182F5BA7B694AB1DD3680F1194E4A568FE40DBA4BFDFF2EA09BAD045FFB29 ] bthserv
C:\WINDOWS\system32\bthserv.dll
19:13:59.0798 0x1918  bthserv - ok
19:13:59.0847 0x1918  [ 23E75BED9076F856B36F5F934BBD5795,
CCEB72B788522B7D52A6C07646005EBC68F9599D3714ECACF3A194CA47A1BE85 ] BTHUSB
C:\WINDOWS\System32\Drivers\BTHUSB.sys
19:13:59.0920 0x1918  BTHUSB - ok
19:14:00.0099 0x1918  [ D93FC9EF129C214D6E91DFE3DF98C38C,
96E079C2F46B382FA2F784AC35335673E4DA0ECBF65C44C3A25EE89DB4F4484F ] CCDMonitorService
C:\Program Files (x86)\Acer\Acer Cloud\CCDMonitorService.exe
19:14:00.0244 0x1918  CCDMonitorService - ok
19:14:00.0266 0x1918  [ 2FA6510E33F7DEFEC03658B74101A9B9,
61C8C8E3F09B427711464C974EE22E1E01C48E10DB54A4EC9901F482FC36C978 ] cdfs
C:\WINDOWS\system32\DRIVERS\cdfs.sys
19:14:00.0290 0x1918  cdfs - ok
19:14:00.0309 0x1918  [ C6796EA22B513E3457514D92DCDB1A3D,
2B893F3950C6B913B934C2089B69F3B0B77F229AE1820907E598455CBB78139C ] cdrom
C:\WINDOWS\System32\drivers\cdrom.sys
19:14:00.0350 0x1918  cdrom - ok
19:14:00.0391 0x1918  [ AB285CE3431FF3D2ACE669245874C1C7,
6AF4C3E86EFA51F7FB6F8492CB2CCB807C7775EAE0508B87F07134FDAC679BD7 ] CertPropSvc
C:\WINDOWS\System32\certprop.dll
19:14:00.0510 0x1918  CertPropSvc - ok
19:14:00.0526 0x1918  [ BE9936EDD3267FAAFF94A7835867F00B,
3CEEF2377D45ED38C7CD3CE4C746EC5EA7277EFEC728A5438F0EF5F62FC7C859 ] circlass
C:\WINDOWS\System32\drivers\circlass.sys
19:14:00.0571 0x1918  circlass - ok
19:14:00.0642 0x1918  [ 179A41249055D5F039F1B6703F3B6D2B,
886CF715D9E85DB5C9B991EBCB9B12E27AA0EEE52528E222C80CA5B5B0A7AF52 ] CLFS
C:\WINDOWS\system32\drivers\CLFS.sys
```

```
19:14:00.0720 0x1918  CLFS - ok
19:14:00.0884 0x1918  [ BAF12796292BDE195348C94BC53EDA09,
C0EF67BB6B11FFE149658BC269F2A692F04C2C2E27ECBAA6EF83D2E25CC6030B ] ClickToRunSvc
C:\Program Files\Microsoft Office 15\ClientX64\OfficeClickToRun.exe
19:14:00.0998 0x1918  ClickToRunSvc - ok
19:14:01.0058 0x1918  [ EF6EF85DADC3184A10D8F2F7159973CB,
42FCB286CED95A5DEBC5C0C894FCBC4818A2C818BB71087142FB51A08A0BE96B ] CmBatt
C:\WINDOWS\System32\drivers\CmBatt.sys
19:14:01.0156 0x1918  CmBatt - ok
19:14:01.0223 0x1918  [ 1CD3A907D64D08F49208DA00B69BF35E,
ABBD70FFCA0DE2274D855AFC08BF7BC0AA6D44EFC9FDBF7DF44B73CD5C210E28 ] CNG
C:\WINDOWS\system32\Drivers\cng.sys
19:14:01.0296 0x1918  CNG - ok
19:14:01.0335 0x1918  [ 03AAED827C36F35D70900558B8274905,
8E44A23C6013FFAE7769F99CAA3B1D6288DE00A38937F9056903AC265B503AFA ] CompositeBus
C:\WINDOWS\System32\drivers\CompositeBus.sys
19:14:01.0403 0x1918  CompositeBus - ok
19:14:01.0413 0x1918  COMSysApp - ok
19:14:01.0463 0x1918  [ A1FF7DFBFBE164CF92603C651D304DD2,
470ACE5A75E64FC62C950037201199857E974803625DC73BEDBCF6FA4DDD496C ] condrv
C:\WINDOWS\system32\drivers\condrv.sys
19:14:01.0540 0x1918  condrv - ok
19:14:01.0648 0x1918  [ 08F934092E0429BADF88E9F91DB0F61E,
6E9091C006FFFF261DC61C8E9A45219E47C351296E5355FC4B7242F30E1DDFE3 ] cphs
C:\WINDOWS\SysWow64\IntelCpHeciSvc.exe
19:14:01.0699 0x1918  cphs - ok
19:14:01.0735 0x1918  [ 0EFE4B5884A8032617826A4D76F80969,
083D296CC623C83D36A97AEE343ADF819B17E490F931DBE4D161BD1E8C289E02 ] CryptSvc
C:\WINDOWS\system32\cryptsvc.dll
19:14:01.0808 0x1918  CryptSvc - ok
19:14:01.0834 0x1918  [ 315BA4BC19316D72B2E037534E048B93,
69613635DB23E6A935673B1025C2010ED3E195473D25368CF74234C4C36910BE ] dam
C:\WINDOWS\system32\drivers\dam.sys
19:14:01.0874 0x1918  dam - ok
19:14:01.0932 0x1918  [ 81979817943D830BF24571B7C1B28A1A,
9584D8F1FB3E6CF17BD465670B208C723A8E8B06775A3DA44F75D7710404EEA6 ] DcomLaunch
C:\WINDOWS\system32\rpcss.dll
19:14:02.0100 0x1918  DcomLaunch - ok
19:14:02.0171 0x1918  [ AF3FF97AC2A73E70F8A8D11FB694175B,
3AA25BF9DED08056F52ACF246118C13C8816B5E8AA4D8606DB7DAB4E4E6A9169 ] defragsvc
C:\WINDOWS\System32\defragsvc.dll
19:14:02.0266 0x1918  defragsvc - ok
19:14:02.0330 0x1918  [ 8F387C2C99EE09C6E2AC316205F86A17,
EC9E8AE72A21992AA118964E17090BA4503EB051273AD18185C95172F57328CE ]
DeviceAssociationService C:\WINDOWS\system32\das.dll
19:14:02.0408 0x1918  DeviceAssociationService - ok
19:14:02.0496 0x1918  [ D06DB4200F9444B2386E6C0E68CD574A,
7266A22D6AF86813CF8AB13BE40384D20C24CE72EF75B0C467C5F88F5B058B1E ]
DeviceFastLaneService C:\Program Files\Acer\Acer Device Fast-
lane\DeviceFastLaneSvc.exe
19:14:02.0559 0x1918  DeviceFastLaneService - ok
19:14:02.0596 0x1918  [ BC6849C62DB407573C6AD8CB1A4D2628,
5BDE0D60F85E4C27CEAD1B301155B54D841FB773BD5BB8AC5DDAEE31F8E94627 ] DeviceInstall
C:\WINDOWS\system32\umpnpmgr.dll
19:14:02.0673 0x1918  DeviceInstall - ok
19:14:02.0699 0x1918  [ A03F362C5557E238CBFA914689C77248,
BAD0A1124E6A384C15028FBE121ADF650F7716442555AD3737B9EA1F58A69246 ] Dfsc
C:\WINDOWS\system32\Drivers\dfsc.sys
19:14:02.0776 0x1918  Dfsc - ok
19:14:02.0823 0x1918  [ 05DE04005CE0D84D0E6AD21CAEB369C6,
E6704A2A685BCFD560796D7C328F8E53DF0793DBDA590598A492D9070D109298 ] Dhcp
C:\WINDOWS\system32\dhcpcore.dll
19:14:02.0930 0x1918  Dhcp - ok
19:14:02.0977 0x1918  [ 4D40C9B33F738797CF50E77CB7C53E85,
7BA341342A47DEB15B51971C97A5237ACD8BDAD9033F63DF0000892BE43F8E13 ] disk
C:\WINDOWS\system32\drivers\disk.sys
19:14:03.0027 0x1918  disk - ok
19:14:03.0060 0x1918  [ EB70A894708D1BC176AFD690FF06085F,
0DD2A97F5E1B38D1F7C0D44E50F09EA222B18B3B074CC9C8CD25A7526CB1A112 ] dmvsc
C:\WINDOWS\System32\drivers\dmvsc.sys
19:14:03.0121 0x1918  dmvsc - ok
19:14:03.0175 0x1918  [ FE7656474448BE6A6C68E5C9BEB7CA94,
8B9F04CAA29A6EEFCA3D1E7BAFE340D5CCA8AF665474E69B1DF7E2A518B83A89 ] Dnscache
C:\WINDOWS\System32\dnsrslvr.dll
19:14:03.0267 0x1918  Dnscache - ok
19:14:03.0321 0x1918  [ 50288EA079BB520C2B8C8A154202D518,
```

8916A9180CA009D124FFDFB4CCF5FDFEF7FA2FD37CBCD49FAD4C68E051B4734D] dot3svc
C:\WINDOWS\System32\dot3svc.dll
19:14:03.0424 0x1918 dot3svc - ok
19:14:03.0465 0x1918 [281BEE07BA97E3E98D12A822D923D0D8,
6EB482B2D4D6048D145C3738B2B6FA27A90B5EA53E9167447820F9981B004E63] DPS
C:\WINDOWS\system32\dps.dll
19:14:03.0543 0x1918 DPS - ok
19:14:03.0553 0x1918 [DDC11A202207C0400CBE07315B8FDE5E,
3ED0CA3A714582D92001BA3BFF78BE082F4DC8021298D5A2632F3B2B0A1C09DC] drmkaud
C:\WINDOWS\system32\drivers\drmkaud.sys
19:14:03.0569 0x1918 drmkaud - ok
19:14:03.0619 0x1918 [D2BCDD6BBFCD068090C109854FCEE079,
6DC8C67713566ABD2CC7860359AC7ABDBA8B6949D8F7ED001730BB0D53010693] DsiWMIService
C:\Program Files (x86)\Launch Manager\dsiwmis.exe
19:14:03.0645 0x1918 DsiWMIService - ok
19:14:03.0670 0x1918 [5B074F14F5DD6418F46EE4CA2DEB7EA8,
B8223D73C3DE123759101F7D5D45C60BD12B221F09D349575A1044CE3F43CBC5] DsmSvc
C:\WINDOWS\System32\DeviceSetupManager.dll
19:14:03.0728 0x1918 DsmSvc - ok
19:14:03.0845 0x1918 [C7D252742946DD395670649742FBD73D,
333CC984CF318D36EA8C5867077A1732A214445EB6B7CF7AC2E8F1C8259CD9C7] DXGKrnl
C:\WINDOWS\System32\drivers\dxgkrnl.sys
19:14:03.0957 0x1918 DXGKrnl - ok
19:14:03.0978 0x1918 [6073537F250B45E1CB2A02E97F0FE1B2,
653F3F2F2019168EDF225944A88AFDBF8393B62AA076BD19980691778F3DB67D] Eaphost
C:\WINDOWS\System32\eapsvc.dll
19:14:04.0037 0x1918 Eaphost - ok
19:14:04.0215 0x1918 [114BCFDF367FF37C3F1B0A96AF542E4D,
D385BC1D91BC1406091C8C3691C07A90BD60EDE05B1384E5AA3506FCB909C857] ebdrv
C:\WINDOWS\system32\drivers\evbda.sys
19:14:04.0410 0x1918 ebdrv - ok
19:14:04.0441 0x1918 [F6F209DDB94959BA104FC8FC87C53759,
8E862D41F4332EABF64BD034E2C0E3CC8109C7990CB4112C2B2880E8E6EDF2D3] EFS
C:\WINDOWS\System32\lsass.exe
19:14:04.0488 0x1918 EFS - ok
19:14:04.0530 0x1918 [43531A5993380CC5113242C29D265FD9,
EE0076D96F7F3CF29884AC7A67C08A429115A7201354A1FB5DE45FD63ABB4960] EhStorClass
C:\WINDOWS\system32\drivers\EhStorClass.sys
19:14:04.0572 0x1918 EhStorClass - ok
19:14:04.0601 0x1918 [6F8E738A9505A388B1157FDDE7B3101B,
3696CA634102B41EEA11EB9DCA0B24439D8636AED4A7190C138C5E64A2EFB514] EhStorTcgDrv
C:\WINDOWS\system32\drivers\EhStorTcgDrv.sys
19:14:04.0633 0x1918 EhStorTcgDrv - ok
19:14:04.0728 0x1918 [5C5552BF36C443746A9808EB632B3947,
08969E5A04DECBF374C52A0A0A8DDB2188DFCDAE879D40943FE307971F03E027] ePowerSvc
C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe
19:14:04.0795 0x1918 ePowerSvc - ok
19:14:04.0810 0x1918 [DFFFAE1442BA4076E18EED5E406FA0D3,
329FC6FB8D14BEACDBE2A5D4C496EDEA485E838B1DF27566E278F8F8E0D8E82E] ErrDev
C:\WINDOWS\System32\drivers\errdev.sys
19:14:04.0838 0x1918 ErrDev - ok
19:14:04.0902 0x1918 [030CE75B7D8F75FAA7BA1EC6FD0EB5A3,
5264734F0572FAEDCCB008221C9982CCB7922C4FFC358605424EA413CDCDAE99] EventSystem
C:\WINDOWS\system32\es.dll
19:14:04.0999 0x1918 EventSystem - ok
19:14:05.0037 0x1918 [7729D294A555C7AEB281ED8E4D0E01E4,
7269E79D72CCE477AC108294D0DDFB59CF533B03C587599C5AB0507C43A0B6D4] exfat
C:\WINDOWS\system32\drivers\exfat.sys
19:14:05.0125 0x1918 exfat - ok
19:14:05.0161 0x1918 [7C4E0D5900B2A1D11EDD626D6DDB937B,
732F310F8F6016C56F432A81636B13CE0124A802FE8DD91287B618EED22C9A1D] fastfat
C:\WINDOWS\system32\drivers\fastfat.sys
19:14:05.0210 0x1918 fastfat - ok
19:14:05.0265 0x1918 [2BC8532ABF2B3756B78FA1DA54147DDE,
DF65EE2AB0255A2CF3221085A6BE7C37E3DB6BFEED3BCADCDD69BB1049F6DCB1] Fax
C:\WINDOWS\system32\fxssvc.exe
19:14:05.0338 0x1918 Fax - ok
19:14:05.0351 0x1918 [5D8402613E778B3BD45E687A8372710B,
EE9EA10805168D309A609B9019AEC5961EE46D18207B5E0EA2DE4064A5770AF8] fdc
C:\WINDOWS\System32\drivers\fdc.sys
19:14:05.0386 0x1918 fdc - ok
19:14:05.0418 0x1918 [DC1A78BCCCB7EE53D6FD3BD615A8E222,
EE16B6853185AAE779D7135035983938009901658F76A8856AAC12EBA15BB34E] fdPHost
C:\WINDOWS\system32\fdPHost.dll
19:14:05.0503 0x1918 fdPHost - ok
19:14:05.0524 0x1918 [E5AD448F2DC84B1CF387FA7F2A3D1936,

BBB29C79A085C503F5EFFB5144596D5DEC48A4EB34A049A4E7B38B27F6D92E0A] FDResPub
C:\WINDOWS\system32\fdrespub.dll
19:14:05.0589 0x1918 FDResPub - ok
19:14:05.0613 0x1918 [0046E0BD031213D37123876B0D0FA61C,
A4FE17D56F0BAFB70D0D421ED9D1B6E50AF8ADAA4B59328A41AEC5B4C068A3CB] fhsvc
C:\WINDOWS\system32\fhsvc.dll
19:14:05.0691 0x1918 fhsvc - ok
19:14:05.0743 0x1918 [BCFD8B149B3ADF92D0DB1E909CAF0265,
002B085C1314736424500176B4B8359F3E5B04350AFB659B9C0F9EB587D1181E7] FileInfo
C:\WINDOWS\system32\drivers\fileinfo.sys
19:14:05.0789 0x1918 FileInfo - ok
19:14:05.0799 0x1918 [A1A66C4FDAFD6B0289523232AFB7D8AF,
0F5832F626BB62190D5F3A088CE6E048D8A400CCF9EA527F06973CAD96D3A81C] Filetrace
C:\WINDOWS\system32\drivers\filetrace.sys
19:14:05.0845 0x1918 Filetrace - ok
19:14:05.0897 0x1918 [BB0667B0171B632B97EA759515476F07,
07A123B2182D5813D2898928C231638353CF086606E9D5A5AF4A2A73E17CEC27] FLEXnet Licensing
Service C:\Program Files (x86)\Common Files\Macrovision Shared\FLEXnet
Publisher\FNPLicensingService.exe
19:14:05.0948 0x1918 FLEXnet Licensing Service - ok
19:14:05.0963 0x1918 [BE743083CF7063C486A4398E3AEFE59A,
85796D89943DD6FE3932C1ED6CF01470C1B4DFD243C390B07055FFDA3C231551] flpydisk
C:\WINDOWS\System32\drivers\flpydisk.sys
19:14:06.0001 0x1918 flpydisk - ok
19:14:06.0064 0x1918 [6592D192E2823C043EDBC010E7774053,
C025A0EC5517DC3BD5D6656DC0F0F19021FB3D2EE90EC6194E1BD74E638EBBDC] FltMgr
C:\WINDOWS\system32\drivers\fltmgr.sys
19:14:06.0123 0x1918 FltMgr - ok
19:14:06.0240 0x1918 [3FA6DC6B29717E32E211C1FD821F2C75,
E467F3775427C93CC2B87327B0A45669631A5FC460C558F6796BA26002A8BBFC] FontCache
C:\WINDOWS\system32\FntCache.dll
19:14:06.0394 0x1918 FontCache - ok
19:14:06.0492 0x1918 [1C52387BF5A127F5F3BFB31288F30D93,
90D13F60170CD74304F3036A90D596AA3E1E134455A780310BDF67AC7815F2E7] FontCache3.0.0.0
C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
19:14:06.0533 0x1918 FontCache3.0.0.0 - ok
19:14:06.0575 0x1918 [35005534E600E993A90B036E4E599F2B,
DA56FA3776FBD3D50276CB7410E0CB6F137DD8FCA84C0F3FEF8B1FEA5F6CA592] FsDepends
C:\WINDOWS\system32\drivers\FsDepends.sys
19:14:06.0613 0x1918 FsDepends - ok
19:14:06.0639 0x1918 [09F460AFEDCA03F3BF6E07D1CCC9AC42,
B832091BC9B2C2FE38A4BCA132ABB58251E851F21EC6F39636E73777AB9A5791] Fs_Rec
C:\WINDOWS\system32\drivers\Fs_Rec.sys
19:14:06.0667 0x1918 Fs_Rec - ok
19:14:06.0729 0x1918 [F152D55E497E1225629 0C43B31C7D0CE,
FFC54B14CCFBC1548948C07FB3866E40A11D0C05AC352BD000E71CEF053F6A6E] fvevol
C:\WINDOWS\system32\DRIVERS\fvevol.sys
19:14:06.0776 0x1918 fvevol - ok
19:14:06.0813 0x1918 [9591D0B9351ED489EAFD9D1CE52A8015,
AC64C236C3AE545FCE8ED44A4A87FB86265A453BA60026EC9A4DE2B631E99996] FxPPM
C:\WINDOWS\System32\drivers\fxppm.sys
19:14:06.0879 0x1918 FxPPM - ok
19:14:06.0904 0x1918 [FC3EF65EE20D39F8749C2218DBA681CA,
12980F1DE99B25E6920A33556F3ABDA5EC9BFE4757BE602130B5E939D8D25CE3] gagp30kx
C:\WINDOWS\system32\drivers\gagp30kx.sys
19:14:06.0944 0x1918 gagp30kx - ok
19:14:07.0026 0x1918 [9A0C359ACBB8D5A305A0235001B44DC9,
308351F614E7C1995C4C90CE7E38BFCD7ADF49E994844FDE46FAC50660D2AE06] Garmin Core
Update Service C:\Program Files (x86)\Garmin\Core Update
Service\Garmin.Cartography.MapUpdate.CoreService.exe
19:14:07.0101 0x1918 Garmin Core Update Service - ok
19:14:07.0141 0x1918 [0BF5CAD281E25F1418E5B8875DC5ADD1,
0929AD8437DD78234553D8B2CDF0D6838FD54ACDE1918AFEBE48684EB32A07A3] gencounter
C:\WINDOWS\System32\drivers\vmgencounter.sys
19:14:07.0204 0x1918 gencounter - ok
19:14:07.0252 0x1918 [EF3AE7773394DF49CE74AF78A1C8D23D,
CB12FF004C460A89F12AFF2467512B479A07CA10D4280CD4E624A5A9CDAB9C1B] GPIOClx0101
C:\WINDOWS\system32\Drivers\msgpioclx.sys
19:14:07.0300 0x1918 GPIOClx0101 - ok
19:14:07.0407 0x1918 [383DA813409316D69603C1D849834D24,
E1AAD3AB567457B00B8A378D5BA37ED653EE451FF79D071A8815FB8B1EB90DAF] gpsvc
C:\WINDOWS\System32\gpsvc.dll
19:14:07.0561 0x1918 gpsvc - ok
19:14:07.0649 0x1918 [506708142BC63DABA64F2D3AD1DCD5BF,
9C36A08D9E7932FF4DA7B5F24E6B42C92F28685B8ABE964C870E8D7670FD531A] gupdate
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe

```
19:14:07.0685 0x1918  gupdate - ok
19:14:07.0694 0x1918  [ 506708142BC63DABA64F2D3AD1DCD5BF,
9C36A08D9E7932FF4DA7B5F24E6B42C92F28685B8ABE964C870E8D7670FD531A ] gupdatem
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
19:14:07.0717 0x1918  gupdatem - ok
19:14:07.0744 0x1918  [ C1B577B2169900F4CF7190C39F085794,
73E104B96A48F4C80D8C37254ECB0891D15C0D2F0C251B57C168F90D60316447 ] gusvc
C:\Program Files (x86)\Google\Common\Google Updater\GoogleUpdaterService.exe
19:14:07.0782 0x1918  gusvc - ok
19:14:07.0809 0x1918  [ 498288DD5CA42C2D36D125893E968C53,
03B62FA51F9195D77170DCEFF3A93A6898AA96FB610044DDAE83767DA12745C5 ] HDAudBus
C:\WINDOWS\System32\drivers\HDAudBus.sys
19:14:07.0857 0x1918  HDAudBus - ok
19:14:07.0887 0x1918  [ 10A70BC1871CD955D85CD88372724906,
2480A74854D0A89FF028EE9BA41224D4B2F9B0863066BFC43097920794FEE08D ] HidBatt
C:\WINDOWS\System32\drivers\HidBatt.sys
19:14:07.0943 0x1918  HidBatt - ok
19:14:07.0982 0x1918  [ 1EA1B4FABB8CC348E73CA90DBA22E104,
5C18C6BD499272F216DD4626B5E8D38181AEAC9AD917FBEB614A75B70467B258 ] HidBth
C:\WINDOWS\System32\drivers\hidbth.sys
19:14:08.0057 0x1918  HidBth - ok
19:14:08.0085 0x1918  [ C241A8BAFBBFC90176EA0F5240EACC17,
571E20B87818618BE9179986177D55739A240F04D1F740B3C1B7809B9427B767 ] hidi2c
C:\WINDOWS\System32\drivers\hidi2c.sys
19:14:08.0155 0x1918  hidi2c - ok
19:14:08.0175 0x1918  [ 9BDDEE26255421017E161CCB9D5EDA95,
B766FD5E31708F29384F69418FC33C4BCC6E3064AA553D5B1D30EE0B8B1BFB40 ] HidIr
C:\WINDOWS\System32\drivers\hidir.sys
19:14:08.0245 0x1918  HidIr - ok
19:14:08.0271 0x1918  [ 449A20A674AA3FAA7F0DD4E33EE2DC20,
28B9BDA306456E8640C355718DE3477537B0FAF8C37F633C709129AAB64D9873 ] hidserv
C:\WINDOWS\system32\hidserv.dll
19:14:08.0342 0x1918  hidserv - ok
19:14:08.0372 0x1918  [ 8DB8EAB9D0C6A5DF0BDCADEA239220B4,
EDA23E6909EB83E5E148816DFB16CC29EA01BD6BD2F73AA46B3D820B85FB9C83 ] HidUsb
C:\WINDOWS\System32\drivers\hidusb.sys
19:14:08.0450 0x1918  HidUsb - ok
19:14:08.0495 0x1918  [ 7BF3ADCBD021D4F4A84CF40EB49C71B5,
5758A51FD2EBE67E6DBE3A298D714D351910F9E01C428D0C1359457C9242B298 ] hkmsvc
C:\WINDOWS\system32\kmsvc.dll
19:14:08.0572 0x1918  hkmsvc - ok
19:14:08.0611 0x1918  [ 6CD9C3819BE8C0A3DACC82AE5D3C4F18,
46BF4A968E506DE17CA401401D716B444CDC10A5C60EB081890DD4B886AEDF5F ] HomeGroupListener
C:\WINDOWS\system32\ListSvc.dll
19:14:08.0687 0x1918  HomeGroupListener - ok
19:14:08.0742 0x1918  [ 1A4DA1D6287B99033D144B436C23B656,
D4D1EEB372E61512EA36A33F095E68C225B8E6C72CC57ED8BD00533F88012F40 ] HomeGroupProvider
C:\WINDOWS\system32\provsvc.dll
19:14:08.0806 0x1918  HomeGroupProvider - ok
19:14:08.0839 0x1918  [ A6AACEA4C785789BDA5912AD1FEDA80D,
D197012A5DA6AB3F76FF298336DF0CF027C07ECC71267BAEF5912DE12893E096 ] HpSAMD
C:\WINDOWS\system32\drivers\HpSAMD.sys
19:14:08.0862 0x1918  HpSAMD - ok
19:14:08.0925 0x1918  [ 9DDCA7F18983C5410DEFF79F819DF93C,
CE97B4440377BFC5CA81BB600C3BD1DD9FB3951CA1EB70735F5E2050EBB74223 ] HTTP
C:\WINDOWS\system32\drivers\HTTP.sys
19:14:08.0998 0x1918  HTTP - ok
19:14:09.0025 0x1918  [ 90656C0B3864804B090434EFC582404F,
BDB60050B729AACB9E009AC7129BEBD6298BBD8A9DB14B817D02E8E13669BD6E ] hwpolicy
C:\WINDOWS\system32\drivers\hwpolicy.sys
19:14:09.0062 0x1918  hwpolicy - ok
19:14:09.0101 0x1918  [ 6D6F9E3BF0484967E52F7E846BFF1CA1,
C982966BDE6A3E6773D9441ADA7A3B08D13511DFC68D04DF303248B942423F38 ] hyperkbd
C:\WINDOWS\System32\drivers\hyperkbd.sys
19:14:09.0166 0x1918  hyperkbd - ok
19:14:09.0202 0x1918  [ 907C870F8C31F8DDD6F090857B46AB25,
308664A31717383D06185875E76C6612407A9F04E7DB28404F574A5706C6715D ] HyperVideo
C:\WINDOWS\system32\DRIVERS\HyperVideo.sys
19:14:09.0258 0x1918  HyperVideo - ok
19:14:09.0289 0x1918  [ 84CFC5EFA97D0C965EDE1D56F116A541,
0155EA62BF07D99D98D1C9B6559C8E3301B016A20D03DF1EF64B2FAB8C37403B ] i8042prt
C:\WINDOWS\System32\drivers\i8042prt.sys
19:14:09.0362 0x1918  i8042prt - ok
19:14:09.0380 0x1918  [ 5D90E32E36CE5D4C535D17CE08AEAF05,
976A463343E8C8308AFBE9E64DF56C430D2241DE002430D00318AB065EB72E4A ] iaLPSSi_GPIO
C:\WINDOWS\System32\drivers\iaLPSSi_GPIO.sys
```

```
19:14:09.0405 0x1918  iaLPSSi_GPIO - ok
19:14:09.0422 0x1918  [ DD05E7E80F52ADE9AEB292819920F32C,
E71AB6A50B0F90C8F94569CE89F66F915A0A4A00D4AC091B2E5E750D88CFC334 ] iaLPSSi_I2C
C:\WINDOWS\System32\drivers\iaLPSSi_I2C.sys
19:14:09.0459 0x1918  iaLPSSi_I2C - ok
19:14:09.0523 0x1918  [ 6C024B3AE192D72B216166802AF345DD,
67AEDBEF4A1C1EE1DA9B684BDEB3DB07715E12B766AA72B6684CC6C583A8DCC5 ] iaStorA
C:\WINDOWS\system32\drivers\iaStorA.sys
19:14:09.0560 0x1918  iaStorA - ok
19:14:09.0633 0x1918  [ 08BFE413B0B4AA8DFA4B5684CE06D3DC,
95DEEBB203E12EE6E191F5247A74C04AEC0E16DE981FADDC4D6C42EE41D8D079 ] iaStorAV
C:\WINDOWS\system32\drivers\iaStorAV.sys
19:14:09.0694 0x1918  iaStorAV - ok
19:14:09.0725 0x1918  [ A2200C3033FA4EF249FC096A7A7D02A2,
5819F5C2020DE2EEE339B0C08CD4B1E3490EAFBBEA1277CE649DB5A5150986B0 ] iaStorV
C:\WINDOWS\system32\drivers\iaStorV.sys
19:14:09.0766 0x1918  iaStorV - ok
19:14:09.0921 0x1918  [ 5AD5A7781BE907D6E2D75CA1DADAA97B,
355234ED6E49A1080CFFC9C18D185DA653A00C6B79B204368A971EACE5A416A9 ] IconMan_R
C:\Program Files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe
19:14:10.0087 0x1918  IconMan_R - ok
19:14:10.0092 0x1918  IEEtwCollectorService - ok
19:14:10.0324 0x1918  [ 8C44E6B688790E2AD3846C97661C54F1,
CB487D167EDA3C1E30BD5FB8F98C15EB9E75A6FB7930090C2F1BBCAAB4285F772 ] igfx
C:\WINDOWS\system32\DRIVERS\igdkmd64.sys
19:14:10.0653 0x1918  igfx - ok
19:14:10.0758 0x1918  [ DEA76F90F9777E3427D70E380222B23B,
B917BA423896A12E45623E3D494CA03317A6FC612CA433C62C897524DC3E756B ] IKEEXT
C:\WINDOWS\System32\ikeext.dll
19:14:10.0895 0x1918  IKEEXT - ok
19:14:11.0095 0x1918  [ DDC860724AEF8F8E42AC61E6585769C6,
62AD5772E8097B03E161E6F14582E2A4BBA0DFA1A1E7F664D881D464E136DBD2 ]
IntcAzAudAddService C:\WINDOWS\system32\drivers\RTKVHD64.sys
19:14:11.0308 0x1918  IntcAzAudAddService - ok
19:14:11.0347 0x1918  [ F5495B38BFB9149925F54F65AB40EFBF,
7CBB72C41E2343DACBFB967A39CA04788561EDECB289C41BC2D6A06B80882AC4 ] IntcDAud
C:\WINDOWS\system32\DRIVERS\IntcDAud.sys
19:14:11.0428 0x1918  IntcDAud - ok
19:14:11.0506 0x1918  [ C99F8E90DE4B8F0C7FE15BB1CBCD29DC,
F791EE101EEF8B9F48102B6C63A89B78F7C0041C750C4F4C0D16D54B583B7B5C ] Intel(R)
Capability Licensing Service Interface C:\Program Files\Intel\iCLS
Client\HeciServer.exe
19:14:11.0574 0x1918  Intel(R) Capability Licensing Service Interface - ok
19:14:11.0612 0x1918  [ 4E448FCFFD00E8D657CD9E48D3E47157,
4A958CF0BF8DAEAE5E008500BA67CE89B21388592811274331EE39CAC1043A00 ] intelide
C:\WINDOWS\system32\drivers\intelide.sys
19:14:11.0649 0x1918  intelide - ok
19:14:11.0682 0x1918  [ 139CFCDCD36B1B1782FD8C0014AC9B0E,
E0D7E0E9B46A8CECE138D689820023BFA650FB689E4FD62855BED37E04F2D9FF ] intelpep
C:\WINDOWS\system32\drivers\intelpep.sys
19:14:11.0710 0x1918  intelpep - ok
19:14:11.0733 0x1918  [ 47E74A8E53C7C24DCE38311E1451C1D9,
79B06E37A552C8A847404D4C572CDB8CF525354D8AE3BEBC06892B7C3B330761 ] intelppm
C:\WINDOWS\System32\drivers\intelppm.sys
19:14:11.0792 0x1918  intelppm - ok
19:14:11.0817 0x1918  [ 9DB76D7F9E4E53EFE5DD8C53DE837514,
07BA4EDA9BE9139A689A2C3EFC1D1A4F3D1216625ED145F313398292A2CD5703 ] IpFilterDriver
C:\WINDOWS\system32\DRIVERS\ipfltdrv.sys
19:14:11.0903 0x1918  IpFilterDriver - ok
19:14:12.0002 0x1918  [ DFC4050D58565ADBEE793A8D4AEBDAE6,
89B900408F030CD45753A11D6AE6CBAB87E8B0E3F8401402D2D8713C045BF488 ] iphlpsvc
C:\WINDOWS\System32\iphlpsvc.dll
19:14:12.0087 0x1918  iphlpsvc - ok
19:14:12.0120 0x1918  [ FD9C9E9E3F0ED51502C7E8C066BE26B9,
290E74380F1543DD22C9F3821513B3E2FB42E995724238D8779CBBCB4FC386C8 ] IPMIDRV
C:\WINDOWS\System32\drivers\IPMIDrv.sys
19:14:12.0203 0x1918  IPMIDRV - ok
19:14:12.0237 0x1918  [ B7342B3C58E91107F6E946A93D9D4EFD,
D5DA3C02C5C5A343785745EF6983CC9B5FBD3FB8D49FE9B450523E50212D1A32 ] IPNAT
C:\WINDOWS\system32\drivers\ipnat.sys
19:14:12.0331 0x1918  IPNAT - ok
19:14:12.0369 0x1918  [ AE44C526AB5F8A487D941CEB57B10C97,
A783A2EAF7A6FF450FB3F189A5930036FA60D125C42171AC44B6FE2E3DBD6F7A ] IRENUM
C:\WINDOWS\system32\drivers\irenum.sys
19:14:12.0442 0x1918  IRENUM - ok
19:14:12.0475 0x1918  [ 8AFEEA3955AA43616A60F133B1D25F21,
```

```
E99359A4F1D653790133F145CF7C9F97399FD75C5E135AA7E5F989BB660789AF ] isapnp
C:\WINDOWS\system32\drivers\isapnp.sys
19:14:12.0516 0x1918  isapnp - ok
19:14:12.0567 0x1918  [ D90AB68D0FAC9F357F663670FDBB511E,
A82AAA5DF1B38EFBDCF834535A0C520D1BB2D7A4A906C18CFDD22BCF16BDB97D ] iScsiPrt
C:\WINDOWS\System32\drivers\msiscsi.sys
19:14:12.0611 0x1918  iScsiPrt - ok
19:14:12.0724 0x1918  [ 3C4002D339491AF73D663FFC7F6E5ECB,
0B53047989BDB781572253BC3AA757912FE54366870C1955E687972CE210C285 ] jhi_service
C:\Program Files (x86)\Intel\Intel(R) Management Engine
Components\DAL\jhi_service.exe
19:14:12.0762 0x1918  jhi_service - ok
19:14:12.0778 0x1918  [ 8BE92376799B6B44D543E8D07CDCF885,
425B8BB1BAF62F735B3CB5A002E6055879F02E7207E55942BFD37F1784F5F368 ] kbdclass
C:\WINDOWS\System32\drivers\kbdclass.sys
19:14:12.0807 0x1918  kbdclass - ok
19:14:12.0824 0x1918  [ FB6E47E569D4872ABEB506BE03A45FBA,
5C4056CADA8F67587A119D9AE2A0EFAB30387CF6298F4019FF68AC92E2F6F54B ] kbdhid
C:\WINDOWS\System32\drivers\kbdhid.sys
19:14:12.0848 0x1918  kbdhid - ok
19:14:12.0857 0x1918  [ 813871C7D402A05F2E3A7075F9584A05,
FF0C2F87EB083F8CE74C679D80C845CDFBFBBC70BE818F899F3336BBB54A3FFB ] kdnic
C:\WINDOWS\system32\DRIVERS\kdnic.sys
19:14:12.0912 0x1918  kdnic - ok
19:14:12.0931 0x1918  [ F6F209DDB94959BA104FC8FC87C53759,
8E862D41F4332EABF64BD034E2C0E3CC8109C7990CB4112C2B2880E8E6EDF2D3 ] KeyIso
C:\WINDOWS\system32\lsass.exe
19:14:12.0976 0x1918  KeyIso - ok
19:14:12.0999 0x1918  [ ADDECBCC777665BD113BED437E602AB0,
B6283475A1219CE44E9F683DD3BEB8C42DA0943297E5C4699B22176AD8A6A7ED ] KSecDD
C:\WINDOWS\system32\Drivers\ksecdd.sys
19:14:13.0029 0x1918  KSecDD - ok
19:14:13.0061 0x1918  [ F88CC88F4A6D8476F1664E805CA18CC2,
2C61EE5EEA4FD45AA3FA927CC16E34EF90BD44324EAB14198AF65C3A27617991 ] KSecPkg
C:\WINDOWS\system32\Drivers\ksecpkg.sys
19:14:13.0096 0x1918  KSecPkg - ok
19:14:13.0103 0x1918  [ 11AFB527AA370B1DAFD5C36F35F6D45F,
757AD234284467ADB826F7CA0251F58D48866B91995BC867DEA4BAF676947163 ] ksthunk
C:\WINDOWS\system32\drivers\ksthunk.sys
19:14:13.0149 0x1918  ksthunk - ok
19:14:13.0210 0x1918  [ 32B1A8351160F307A8C66BCB0F94A9C2,
52F1DEC2BBD4D5DDBB85ED20B99D96BBA7EB83304D76F183A11FDAFDA364E873 ] KtmRm
C:\WINDOWS\system32\msdtckrm.dll
19:14:13.0286 0x1918  KtmRm - ok
19:14:13.0312 0x1918  [ 50AECF8C21AB2A6428A6E1E10549D8E5,
6BC7C60CF5E8AFB9972619EE1C78357756E9C0A3EC783C3056CEB600DCBB1555 ] L1C
C:\WINDOWS\system32\DRIVERS\L1C63x64.sys
19:14:13.0339 0x1918  L1C - ok
19:14:13.0369 0x1918  [ 46378ECCB4A29AA81BF296641C2501EF,
5AB79BD824C00EF1338FDB8450692318AB14E0AE4145C30B37136767DFC1E4F9 ] LanmanServer
C:\WINDOWS\system32\srvsvc.dll
19:14:13.0438 0x1918  LanmanServer - ok
19:14:13.0471 0x1918  [ D0D9C2ECA4D03A8F06DCD91236B90C98,
E2D1144DC8040EA5FEB0602A20BA4CB920B4BC86AD5AD05FC0DF7D74DC95DC66 ] LanmanWorkstation
C:\WINDOWS\System32\wkssvc.dll
19:14:13.0547 0x1918  LanmanWorkstation - ok
19:14:13.0621 0x1918  [ 626D19F1771E1AE72208AE9A8F3082F7,
78FDB64545ED2EAE9F51C08120E21D2C3285208F6846BD8BBA08CAA839E7A0C4 ] lfsvc
C:\WINDOWS\System32\GeofenceMonitorService.dll
19:14:13.0713 0x1918  lfsvc - ok
19:14:13.0896 0x1918  [ 935E2093CEED8198C820B7F60BB63167,
7C8A7A0501BA31624143C576B0D8C6C74AF7869A9734E4AB142715B766F2B59D ] LiveUpdateSvc
C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
19:14:14.0043 0x1918  LiveUpdateSvc - ok
19:14:14.0055 0x1918  [ C09010B3680860131631F53E8FE7BAD8,
35F2A06D5F29478D22ABDCC20DA893EF9D96504C65594A0CEA674D1C21B04FF8 ] lltdio
C:\WINDOWS\system32\DRIVERS\lltdio.sys
19:14:14.0090 0x1918  lltdio - ok
19:14:14.0136 0x1918  [ 00E070FC0C673311AFD4B068D1242780,
50B0E0E625361145332C849709498FF444E46578DCAD2536E6D0289E0125580F ] lltdsvc
C:\WINDOWS\System32\lltdsvc.dll
19:14:14.0185 0x1918  lltdsvc - ok
19:14:14.0208 0x1918  [ D113FAD71A5E67AA94B32A0F8828D265,
08DDB4BBDB570C59926DBF5E27FCF46DCDF8B8212BB9251E97837E0504516FB3 ] lmhosts
C:\WINDOWS\System32\lmhsvc.dll
19:14:14.0247 0x1918  lmhosts - ok
```

19:14:14.0293 0x1918 [4269D44BB47A6DA5D80B11F4C8536458,
7A8FFC8F851DD9E5C43986BE0888831CB71D188138DF3CF7F787DADDA70915B0] LMS
C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe
19:14:14.0332 0x1918 LMS - ok
19:14:14.0380 0x1918 [C755AE4635457AA2A11F79C0DF857ABC,
E03D1ACAC155287291FE1BD0B653953ADC94279A74D0152088D698FAA796460F] LSI_SAS
C:\WINDOWS\system32\drivers\lsi_sas.sys
19:14:14.0419 0x1918 LSI_SAS - ok
19:14:14.0442 0x1918 [ADAC09CBE7A2040B7F68B5E5C9A75141,
7865DA7E91404F3642BC444B97F6B7AA42B9523D5EDD7F6365DA236B8EC3410F] LSI_SAS2
C:\WINDOWS\system32\drivers\lsi_sas2.sys
19:14:14.0473 0x1918 LSI_SAS2 - ok
19:14:14.0496 0x1918 [04D1274BB9BBCCF12BD12374002AA191,
4B9618F8D25F2278DE1610A70ACAADB074D171D162C3AF27D464F5DC800A8E60] LSI_SAS3
C:\WINDOWS\system32\drivers\lsi_sas3.sys
19:14:14.0524 0x1918 LSI_SAS3 - ok
19:14:14.0536 0x1918 [327469EEF3833D0C584B7E88A76AEC0C,
3D88B5A2D68F93F01B39C6E3D8D5C7A2A20686EFC756086E66AFFF1BC3019B85] LSI_SSS
C:\WINDOWS\system32\drivers\lsi_sss.sys
19:14:14.0556 0x1918 LSI_SSS - ok
19:14:14.0598 0x1918 [8EBB271E4588D835784A3FF7E80076A8,
A508BE95F6F5063A76F4C8726D9425BB1F00DE803EFE73A0BE145DD9AB82FF0A] LSM
C:\WINDOWS\System32\lsm.dll
19:14:14.0659 0x1918 LSM - ok
19:14:14.0698 0x1918 [DDEE191AB32DFC22C6465002ECDF5EE4,
190C3930A8449118F9FEDF43C482837EF1C255E6D67F9651156E66A1E2BC6553] luafv
C:\WINDOWS\system32\drivers\luafv.sys
19:14:14.0769 0x1918 luafv - ok
19:14:14.0840 0x1918 [C121367D21599367F2ADB9C11B7BABAA,
752993437AB2C797B5C0FFD397BC8FAC575886857C61BCCCCF169DA54BEE911C] McAfee
SiteAdvisor Service C:\Program Files\Common Files\McAfee\McSvcHost\McSvHost.exe
19:14:14.0886 0x1918 McAfee SiteAdvisor Service - ok
19:14:14.0919 0x1918 [EB5C03A070F30D64A6DF80E53B22F53F,
12051B6AEBDEE1E28F24364F25A52BA3A6E282ECF86D6290E34BD38E6D4E066D] megasas
C:\WINDOWS\system32\drivers\megasas.sys
19:14:14.0965 0x1918 megasas - ok
19:14:15.0023 0x1918 [F6F13533196DE7A582D422B0241E4363,
B3CD9B08937AFFF12141B38634AF3A56F5AC5FF3EF03941802B9841DEC559469] megasr
C:\WINDOWS\system32\drivers\megasr.sys
19:14:15.0096 0x1918 megasr - ok
19:14:15.0129 0x1918 [772A1DEEDFDBC244183B5C805D1B7D85,
7D821B8DF1F174E5414FFDEAB5207DB687740E9842F7203600AEBA086945AFC9] MEIx64
C:\WINDOWS\System32\drivers\HECIx64.sys
19:14:15.0165 0x1918 MEIx64 - ok
19:14:15.0205 0x1918 [FD788C2D96EA91469A3C1D13E80D7473,
7B14D4BFDE18CECC19FBFFAA5AFF5FD78BFB7FCDA6613990740A8A7DD9873D26] MMCSS
C:\WINDOWS\system32\mmcss.dll
19:14:15.0285 0x1918 MMCSS - ok
19:14:15.0304 0x1918 [8B38C44F69259987C95135C9627E2378,
E698B82D4EFFF56D66C7FC9866369BA5736FDBDBE2028CC421C51E70DEA74727] Modem
C:\WINDOWS\system32\drivers\modem.sys
19:14:15.0367 0x1918 Modem - ok
19:14:15.0401 0x1918 [601589000CC90F0DF8DA2CC254A3CCC9,
D1238A386C41B6C368D9A44B7C112C943995B5403E2A5B4B7346B266DDB0C5A0] monitor
C:\WINDOWS\System32\drivers\monitor.sys
19:14:15.0476 0x1918 monitor - ok
19:14:15.0529 0x1918 [CEAC6D40FE887CE8406C2393CF97DE06,
34E76908B802764FF0D7AB3AF89BE77BD35B44787983343FAD89891891C0A045] mouclass
C:\WINDOWS\System32\drivers\mouclass.sys
19:14:15.0573 0x1918 mouclass - ok
19:14:15.0582 0x1918 [02D98BF804084E9A0D69D1C69B02CCA9,
EC5BC5D87043DFFD035FD4DD27B3D94E03119063519E4151BCC3522B613E2D7F] mouhid
C:\WINDOWS\System32\drivers\mouhid.sys
19:14:15.0612 0x1918 mouhid - ok
19:14:15.0629 0x1918 [515549560D481138E6E21AF7C6998E56,
C7E4B38D8CCAF15B9BDA63C8C8209F6193AD220DA02E1264F1B687AACD8F409F] mountmgr
C:\WINDOWS\system32\drivers\mountmgr.sys
19:14:15.0650 0x1918 mountmgr - ok
19:14:15.0657 0x1918 [F170510BE94CF45E3C6274578F6204B2,
344C3DDE1D622607CA2ABECB2C47CB0166D2D258BD94A7960C45A5ADBB640566] mpsdrv
C:\WINDOWS\system32\drivers\mpsdrv.sys
19:14:15.0708 0x1918 mpsdrv - ok
19:14:15.0786 0x1918 [D186C5844393252147BE934F3871DB7A,
30160F8268B9F46E82C5CB536867E0CF280DC98074A481595072E3320200E343] MpsSvc
C:\WINDOWS\system32\mpssvc.dll
19:14:15.0886 0x1918 MpsSvc - ok

```
19:14:15.0942 0x1918  [ 1D55DADC22D21883A2F80297F5A5AE48,
B79DF4AFC2A9CBC54E74233596544D6E41C8CAA0516BD57CA695D051EC780265 ] MRxDAV
C:\WINDOWS\system32\drivers\mrxdav.sys
19:14:15.0998 0x1918  MRxDAV - ok
19:14:16.0047 0x1918  [ 7A1A3F213CDB3363D179D5014272025D,
6756F5B7D9FBF6839DB1FF4E94EA45B5499D7DF925E75581C96FBBA4BE131542 ] mrxsmb
C:\WINDOWS\system32\DRIVERS\mrxsmb.sys
19:14:16.0111 0x1918  mrxsmb - ok
19:14:16.0138 0x1918  [ 3E28B99198B514DFEB152EACF913025E,
6C1D8353DCD5F811F39C0C3CB5DF3D2457F0D17EE80FB06196AA169E3D19E9B2 ] mrxsmb10
C:\WINDOWS\system32\DRIVERS\mrxsmb10.sys
19:14:16.0208 0x1918  mrxsmb10 - ok
19:14:16.0249 0x1918  [ 5C42CEE3E2018E1DFC6E3E17240A432A,
7DFF61686167535125BA376A9BE3DD1C2AC7A2C13455E0FD8E83AAE88E52F987 ] mrxsmb20
C:\WINDOWS\system32\DRIVERS\mrxsmb20.sys
19:14:16.0336 0x1918  mrxsmb20 - ok
19:14:16.0380 0x1918  [ 4E888019078AC363076A5433E89AA4F8,
3DEBDA290230B3E83F956C902C960E39463B7EFE8643919952135676276 9FD91 ] MsBridge
C:\WINDOWS\system32\DRIVERS\bridge.sys
19:14:16.0447 0x1918  MsBridge - ok
19:14:16.0498 0x1918  [ A082C17D14D0790E27D064EA4B138AE1,
9A565ED885782D9D5135C8399C11C356DBF9EBF3B8EB4B4504BD2604AD0B45E6 ] MSDTC
C:\WINDOWS\System32\msdtc.exe
19:14:16.0584 0x1918  MSDTC - ok
19:14:16.0638 0x1918  [ D13329FBF8345B28AB30F44CC247DC08,
9C7EC2D4D65E6510EB5B9E61BB0D14F725D7E8FE98D65161C3971E43EF1AB6EB ] Msfs
C:\WINDOWS\system32\drivers\Msfs.sys
19:14:16.0708 0x1918  Msfs - ok
19:14:16.0730 0x1918  [ C6B474E46F9E543B875981ED3FFE6ADD,
E16687E52FB649C23D92159A1F036CB662202C1E58D961EECDAA528AA4FA669A ] msgpiowin32
C:\WINDOWS\System32\drivers\msgpiowin32.sys
19:14:16.0773 0x1918  msgpiowin32 - ok
19:14:16.0807 0x1918  [ 65C92EB9D08DB5C69F28C7FFD4E84E31,
D709BA4723225321F665B1157A33A4AE230420752308EF535DA9A41CAC164628 ] mshidkmdf
C:\WINDOWS\System32\drivers\mshidkmdf.sys
19:14:16.0863 0x1918  mshidkmdf - ok
19:14:16.0898 0x1918  [ 52299F086AC2DAFD100DD5DC4A8614BA,
B36BE0FC96798E5EB8C193C318970E3906961E3ABC3BFAAD73138C76D9A95B0B ] mshidumdf
C:\WINDOWS\System32\drivers\mshidumdf.sys
19:14:16.0964 0x1918  mshidumdf - ok
19:14:16.0981 0x1918  [ 36D92AF3343C3A3E57FEF11C449AEA4C,
ECC85AA1E530DF55B4A4545798219F87F0FCA66DDD2E37BCEF0850D3C9129DD2 ] msisadrv
C:\WINDOWS\system32\drivers\msisadrv.sys
19:14:17.0024 0x1918  msisadrv - ok
19:14:17.0069 0x1918  [ 810F8A0A0680662BB0CE44D0E2CEF90C,
5631B07911B7EF378CB1583A480A3C5715E59A5488B33A528F4D7A2F849B9113 ] MSiSCSI
C:\WINDOWS\system32\iscsiexe.dll
19:14:17.0140 0x1918  MSiSCSI - ok
19:14:17.0150 0x1918  msiserver - ok
19:14:17.0168 0x1918  [ A9BBBD2BAE6142253B9195E949AC2E8D,
599D2952D4E0B0B3E02D91E38A30F4900B1ADA330716B887B156A1CB9A3E6EE9 ] MSKSSRV
C:\WINDOWS\system32\drivers\MSKSSRV.sys
19:14:17.0226 0x1918  MSKSSRV - ok
19:14:17.0252 0x1918  [ 375E44168F2DFB91A68B8A3F619C5A7C,
AC243E02E9A39D0B4DE9571F196941700EE6EB5E94F5B0BA8994FB551E73A7A8 ] MsLldp
C:\WINDOWS\system32\DRIVERS\mslldp.sys
19:14:17.0320 0x1918  MsLldp - ok
19:14:17.0337 0x1918  [ 7B2128EB875DCBC006E6A913211006D6,
97BBD7FF770741FBFC0F181A609AD0954EA926DA203B742E8F08C89AD8FE476E ] MSPCLOCK
C:\WINDOWS\system32\drivers\MSPCLOCK.sys
19:14:17.0387 0x1918  MSPCLOCK - ok
19:14:17.0414 0x1918  [ 1E88171579B218115C7A772F8DE04BD8,
B9EAA835D0BF8F9C4DF8403D95EF1400E8AE38F28F9DBA87657DE2129FEF02D2 ] MSPQM
C:\WINDOWS\system32\drivers\MSPQM.sys
19:14:17.0480 0x1918  MSPQM - ok
19:14:17.0537 0x1918  [ BBE2A455053E63BECBF42C2F9B21FAE0,
7C5DF563499DF59DF9895A1581E47ADF5FD54C94ECEF6C886CDB60E5E95A6DAE ] MsRPC
C:\WINDOWS\system32\drivers\MsRPC.sys
19:14:17.0592 0x1918  MsRPC - ok
19:14:17.0606 0x1918  [ 8D6B7D515C5CBCDB75B928A0B73C3C5E,
1EB4DC3DD21D2627C78EC3F9931D9E5D033169087E43B5D7C17BF1FF2A0028CD ] mssmbios
C:\WINDOWS\System32\drivers\mssmbios.sys
19:14:17.0635 0x1918  mssmbios - ok
19:14:17.0658 0x1918  [ 115019AE01E0EB9C048530D2928AB4A2,
6E2275E85EACF2D0FC784792E0D72A165589D33CBAB3BCFA8E271CA09566C925 ] MSTEE
C:\WINDOWS\system32\drivers\MSTEE.sys
```

19:14:17.0702 0x1918 MSTEE - ok
19:14:17.0724 0x1918 [96D604A35070360F0DD4A7A8AF410B5E,
F94DD1A3566C7C8D0A76D6E1E2530552A9B7F99C5DA0DE11829325EAB9F8B7ED] MTConfig
C:\WINDOWS\System32\drivers\MTConfig.sys
19:14:17.0796 0x1918 MTConfig - ok
19:14:17.0812 0x1918 [619CA29326B82372621DB2C0964D8365,
4091F08E266DB45A6E33A4A8B1CE9FA78BB294B3111526AA9E3868620F30AFDF] Mup
C:\WINDOWS\system32\Drivers\mup.sys
19:14:17.0859 0x1918 Mup - ok
19:14:17.0890 0x1918 [B8C35C94DCB2DFEAF03BB42131F2F77F,
F0FCF367CA8F722D6ABCF7F363CD406D890D71452E91C3FC6677B47AD74D6324] mvumis
C:\WINDOWS\system32\drivers\mvumis.sys
19:14:17.0936 0x1918 mvumis - ok
19:14:18.0014 0x1918 [41A45D2A75494EABF2806EA051E00376,
EB2497561C8E33A4297C044604C717FF854C7F046882A9E4A400AE7679BF5467] napagent
C:\WINDOWS\system32\qagentRT.dll
19:14:18.0090 0x1918 napagent - ok
19:14:18.0142 0x1918 [78514B073CC5775800A65BFB82A0D66B,
DCD18E277569F23921E899F508860F89ABD417C74A7776152A4463284A989488] NativeWifiP
C:\WINDOWS\system32\DRIVERS\nwifi.sys
19:14:18.0238 0x1918 NativeWifiP - ok
19:14:18.0279 0x1918 [71E3C0100AA19D11373CCEB2F51A6008,
58FBF35F5FE19BEABE483C11E9996BE93D76721C8C34465350FA98B465CA3672] NcaSvc
C:\WINDOWS\System32\ncasvc.dll
19:14:18.0387 0x1918 NcaSvc - ok
19:14:18.0409 0x1918 [51DF09CAB2CAC64FEE3E371D9028ED01,
9B81604D0D0359AF8F54FED6DA7116FFD2F40407895028EAD99FF1D7CFDC2D14] NcbService
C:\WINDOWS\System32\ncbservice.dll
19:14:18.0510 0x1918 NcbService - ok
19:14:18.0536 0x1918 [2586C4C167499210DCBF3ECFD8CCE210,
D8129FEDE9918BF4FB0057CC58700D4E08457060E810B9CC25CA0F598506ADB8] NcdAutoSetup
C:\WINDOWS\System32\NcdAutoSetup.dll
19:14:18.0635 0x1918 NcdAutoSetup - ok
19:14:18.0738 0x1918 [F21B77B4D74092A543807D3CEB711A88,
5C3C17A10E990070FAB317C0C5333DE768E408CAF43EC4FA9D18116C6EE3B3DC] NDIS
C:\WINDOWS\system32\drivers\ndis.sys
19:14:18.0831 0x1918 NDIS - ok
19:14:18.0865 0x1918 [C6BB12BC35D1637CA17AE16D3A4725EB,
01C1D9FA738886A195166F88207EEB6715A1DE0608978ED6C5DC738AF5C02513] NdisCap
C:\WINDOWS\system32\DRIVERS\ndiscap.sys
19:14:18.0923 0x1918 NdisCap - ok
19:14:18.0948 0x1918 [9F1DA20E943BE7AA4ED5F3E1EBA78B37,
CCD99962917BBE256F64AE14CCC9FD12433C72B5DB98E0E57CA8F212A11B3C8F] NdisImPlatform
C:\WINDOWS\system32\DRIVERS\NdisImPlatform.sys
19:14:19.0023 0x1918 NdisImPlatform - ok
19:14:19.0046 0x1918 [9423421E735BD5394351E0C47C76BB92,
763E5D06F896C0EF8AD52515464F28BA85DB7A1560E451857AC9AA68FAFCBC66] NdisTapi
C:\WINDOWS\system32\DRIVERS\ndistapi.sys
19:14:19.0115 0x1918 NdisTapi - ok
19:14:19.0124 0x1918 [B832B35055BA2B7B4181861FF94D8E59,
2E60E5D503E88D27E35ECFEE265D51328E93A9C7B9B931F86D9CBC947636BB00] Ndisuio
C:\WINDOWS\system32\DRIVERS\ndisuio.sys
19:14:19.0160 0x1918 Ndisuio - ok
19:14:19.0177 0x1918 [1F58E48EF75F34C35D8E93A0DC535CFE,
D65619A6C4B1747F8B05DA08A44EF0E46B5CC384880E04E4755A2BA6CDB3C4EA] NdisVirtualBus
C:\WINDOWS\System32\drivers\NdisVirtualBus.sys
19:14:19.0245 0x1918 NdisVirtualBus - ok
19:14:19.0275 0x1918 [DEC29080202D4F9F17F55E18BCFCC41A,
F7E543741B1F4F637A99C40543D6AEC6EBF893F74359BBA769D1F882E0AFB571] NdisWan
C:\WINDOWS\system32\DRIVERS\ndiswan.sys
19:14:19.0341 0x1918 NdisWan - ok
19:14:19.0355 0x1918 [DEC29080202D4F9F17F55E18BCFCC41A,
F7E543741B1F4F637A99C40543D6AEC6EBF893F74359BBA769D1F882E0AFB571] NdisWanLegacy
C:\WINDOWS\system32\DRIVERS\ndiswan.sys
19:14:19.0390 0x1918 NdisWanLegacy - ok
19:14:19.0405 0x1918 [A5BD69A8812FA79D1A487691DD3FB244,
67B5EDE101943E0E8B8041DB2353D20C8B9F2D253E77964761CFE8F136C0BBC7] NDProxy
C:\WINDOWS\system32\drivers\NDProxy.sys
19:14:19.0446 0x1918 NDProxy - ok
19:14:19.0464 0x1918 [5A072F0B90C29C5233D78BE33EF5ED78,
B32ED76A674B1FC743361FB7BBD4C915A78B14132AB056AADD445D5995AD4F32] Ndu
C:\WINDOWS\system32\drivers\Ndu.sys
19:14:19.0504 0x1918 Ndu - ok
19:14:19.0517 0x1918 [A83D67D347A684F10B7D3019C8A6380C,
2B86832967981C8C786BF24C1CF8E13E01745ACE3333CF5C821DD93D623B96E4] NetBIOS
C:\WINDOWS\system32\DRIVERS\netbios.sys

```
19:14:19.0574 0x1918  NetBIOS - ok
19:14:19.0600 0x1918  [ 0217532E19A748F0E5D569307363D5FD,
C40C2E7AFA276057E7327A7BB173122689D6CEC9AE443C3850C3F94AF03DFBF5 ] NetBT
C:\WINDOWS\system32\DRIVERS\netbt.sys
19:14:19.0672 0x1918  NetBT - ok
19:14:19.0686 0x1918  [ F6F209DDB94959BA104FC8FC87C53759,
8E862D41F4332EABF64BD034E2C0E3CC8109C7990CB4112C2B2880E8E6EDF2D3 ] Netlogon
C:\WINDOWS\system32\lsass.exe
19:14:19.0712 0x1918  Netlogon - ok
19:14:19.0781 0x1918  [ B7AD851A21FEBA3BA214972627614207,
29605320CCC3DAAD062CAECF0009DACBC2F6D28ED4E8AF7CE76132129F5572A0 ] Netman
C:\WINDOWS\System32\netman.dll
19:14:19.0866 0x1918  Netman - ok
19:14:20.0076 0x1918  [ F0F0A372C2EF6358399C4936F91B6131,
CE596C71EB4D1A5E104D3148F2D0D8789882C59FD198DCF33CCAC7A08B50E4EE ] netprofm
C:\WINDOWS\System32\netprofmsvc.dll
19:14:20.0264 0x1918  netprofm - ok
19:14:20.0325 0x1918  [ 1092B3190E69E0C5ECBCE90F171DE047,
C16106EEFC324EE80E5F659CB71A5DD69FA800D36D829F5B0E6AD3393BD1BAF7 ] NetTcpPortSharing
C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
19:14:20.0400 0x1918  NetTcpPortSharing - ok
19:14:20.0445 0x1918  [ 70414DB660BFBB7BD58FCE8EA4364E1B,
6DFB3897CD55E22BA1EDF0AE672F4D7A6A1F512F8A0A26AF106765E6B1CF65AC ] netvsc
C:\WINDOWS\system32\DRIVERS\netvsc63.sys
19:14:20.0513 0x1918  netvsc - ok
19:14:20.0572 0x1918  [ 3A280F3B3C7A46E29C404ACD46ECBF5E,
81C3367A2A212DBCC65B8A0166FD092E3205AB31A146B4B737061335CEC51F9D ] NlaSvc
C:\WINDOWS\System32\nlasvc.dll
19:14:20.0629 0x1918  NlaSvc - ok
19:14:20.0649 0x1918  [ 8F44A2F57C9F1A19AC9C6288C10FB351,
310274DDBAC0FE4BE54ECD3B90C97D82A0F9F5CFCA7A35711A36164DE4B94074 ] Npfs
C:\WINDOWS\system32\drivers\Npfs.sys
19:14:20.0729 0x1918  Npfs - ok
19:14:20.0765 0x1918  [ CBDB4F0871C88DF930FC0E8588CA67FC,
7E4AA3EA81A9D532F236FD7896744F07ED07CA9B37A9F18A9778BCCCC67490F2 ] npsvctrig
C:\WINDOWS\System32\drivers\npsvctrig.sys
19:14:20.0844 0x1918  npsvctrig - ok
19:14:20.0859 0x1918  [ 6E2271ED0C3E95B8E29F3752B91B9E84,
44026AD9757EA82967D7F7578455802FAD7FE0057EAC088E0AE207C15F594B86 ] nsi
C:\WINDOWS\system32\nsisvc.dll
19:14:20.0909 0x1918  nsi - ok
19:14:20.0917 0x1918  [ E490B459978CB87779E84C761D22B827,
1E5CA38626E41618E4CA16DD0C70EB2FA86E986F0CF21A749BDE2A17015DEEC6 ] nsiproxy
C:\WINDOWS\system32\drivers\nsiproxy.sys
19:14:20.0956 0x1918  nsiproxy - ok
19:14:21.0116 0x1918  [ 1C80517BE6836A812F6A9B99B8321351,
7DBED4633820E201C9C242D961EF6F25BA2B1D5593BA60F707CC71A4014C2D4B ] Ntfs
C:\WINDOWS\system32\drivers\Ntfs.sys
19:14:21.0272 0x1918  Ntfs - ok
19:14:21.0330 0x1918  [ A9AE582FE2240E7FB0E9C11E1CC762A0,
60297CBEE5638E4E5EEF1098B2391A72DE75DC72B1DD812277758BEF770D6C71 ] NTI IScheduleSvc
C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe
19:14:21.0375 0x1918  NTI IScheduleSvc - ok
19:14:21.0406 0x1918  [ EE3BA1024594D5D09E314F206B94069E,
34C8EC3DF1C3088D8A0442CAA4F5506665AFB2DF016709457ED2AB7DA45F53A6 ] NTIDrvr
C:\Windows\system32\drivers\NTIDrvr.sys
19:14:21.0428 0x1918  NTIDrvr - ok
19:14:21.0464 0x1918  [ EF1B290FC9F0E47CC0B537292BEE5904,
DBC07BBC54EBC2D2E576B23A4CE116B3DA988577AD0D96CB7289A6748A60F9EA ] Null
C:\WINDOWS\system32\drivers\Null.sys
19:14:21.0511 0x1918  Null - ok
19:14:21.0537 0x1918  [ BC6B5942AFF25EBAF62DE43C3807EDF8,
CB0FA194084B8C309039D571B5760FDA800E9531B8660C499B4F9977BA5C36D5 ] nvraid
C:\WINDOWS\system32\drivers\nvraid.sys
19:14:21.0592 0x1918  nvraid - ok
19:14:21.0622 0x1918  [ 1F43ABFFAC3D6CA356851D517392966E,
6FD7621F67BA94B0E1D8F43BEC2951DBCDEEA1E848BB265AC169E27C01DA68F2 ] nvstor
C:\WINDOWS\system32\drivers\nvstor.sys
19:14:21.0672 0x1918  nvstor - ok
19:14:21.0695 0x1918  [ 6934A936A7369DFE37B7DBA93F5E5E49,
0900FEEB0CE8D09F0FC60630B5B986034A8BCD3882ED66E47170810C32492892 ] nv_agp
C:\WINDOWS\system32\drivers\nv_agp.sys
19:14:21.0728 0x1918  nv_agp - ok
19:14:21.0782 0x1918  [ 30B5F9FB0C35AE6B4A0851D24CE2EE8B,
0340E77E8EC2ADC21B8DDD9C9CC95B3F4BCAFD54618A333C72D7D9587D593B83 ] ose
C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE
```

```
19:14:21.0833 0x1918  ose - ok
19:14:21.0897 0x1918  [ E287F157F7A0011D93179C64EF8ADCF2,
C16FB92C7B18D634BB1344238D35B3111494C243FBD5853F05376F5051480D83 ] p2pimsvc
C:\WINDOWS\system32\pnrpsvc.dll
19:14:21.0962 0x1918  p2pimsvc - ok
19:14:21.0993 0x1918  [ 2A57A937BC5B1B2D6AFE6A8C5925F50B,
00D84EFED5A7129AAD8694594003047479590 5C32D65CBD5B1A3EBADCED8F873 ] p2psvc
C:\WINDOWS\system32\p2psvc.dll
19:14:22.0079 0x1918  p2psvc - ok
19:14:22.0133 0x1918  [ 764B1121867B2D9B31C491668AC72B2B,
32C04B6FCE1DDD09697B81473A23BDCED8BEEFBCD0D2D58DDC9A11A33C756967 ] Parport
C:\WINDOWS\System32\drivers\parport.sys
19:14:22.0210 0x1918  Parport - ok
19:14:22.0238 0x1918  [ EF0C1749C9A8CEE9A457473D433CC00F,
A5FDAB5AD47471640D697C6CFBA6C67730878ABBA47D394EAA47C9733EDCE1F3 ] partmgr
C:\WINDOWS\system32\drivers\partmgr.sys
19:14:22.0288 0x1918  partmgr - ok
19:14:22.0342 0x1918  [ 9A5309EF92F39346CFD5A4C2C3D1BFAD,
5908E0C9562F9CB24784491BD9AE7983A33A6BDF81AFA0A08045518A0C9BB2B1 ] PcaSvc
C:\WINDOWS\System32\pcasvc.dll
19:14:22.0427 0x1918  PcaSvc - ok
19:14:22.0449 0x1918  [ 275AFE3FA35E8D78BE97695DF49817C6,
447CEBB16285AE073B4251D2DA71399306EF2DCB7F56286ABE2F0BD6C83EB489 ] pci
C:\WINDOWS\system32\drivers\pci.sys
19:14:22.0486 0x1918  pci - ok
19:14:22.0504 0x1918  [ 346E38FCC6859A727DD28AFAD1F0AFF4,
FF3DA26F79B3BC3A5B8A8AA0B9139B9EF70297F4EA1203B1E68FB5A212C3AA58 ] pciide
C:\WINDOWS\system32\drivers\pciide.sys
19:14:22.0520 0x1918  pciide - ok
19:14:22.0541 0x1918  [ 4D3BDCC1C7B40C9D7B6AD990E6DEC397,
27A7AF2127B699F4579CB77936F38DC102211E26E5E2947DB808756FE06FC98E ] pcmcia
C:\WINDOWS\system32\drivers\pcmcia.sys
19:14:22.0562 0x1918  pcmcia - ok
19:14:22.0568 0x1918  [ BF28771D1436C88BE1D297D3098B0F7D,
5F7630916A76A8CF31289E9C577F522B999C74C39E541CD40E62BD53004BEF74 ] pcw
C:\WINDOWS\system32\drivers\pcw.sys
19:14:22.0587 0x1918  pcw - ok
19:14:22.0595 0x1918  [ B9D968D8E2B0F9C6301CEB39CFC9B9E4,
83F32831B0727F18B56DC3CAF37E45A3523D2BBCD54D1421F0DE5A0179D8A404 ] pdc
C:\WINDOWS\system32\drivers\pdc.sys
19:14:22.0619 0x1918  pdc - ok
19:14:22.0687 0x1918  [ 0ECEE590F2E2EF969FB74A6FC583A1E6,
1C611D9225C863CF32125F684B324C58BDE1942F4F283F5674133200AC505D44 ] PEAUTH
C:\WINDOWS\system32\drivers\peauth.sys
19:14:22.0764 0x1918  PEAUTH - ok
19:14:22.0851 0x1918  [ 8E3C640FFF5A963F570233AE99C0FFF3,
3DE978B005BF2E88BA858CE37D9E27BD3584642B8412E22C300A1E739743838A ] PerfHost
C:\WINDOWS\SysWow64\perfhost.exe
19:14:22.0943 0x1918  PerfHost - ok
19:14:23.0105 0x1918  [ 928061178CD9856CA6B67FFFCE6BA766,
71DE3C7CA7F83EAAA550CD8A68FB67DE042B0AE51BFACB1ECB8852D502E11F50 ] pla
C:\WINDOWS\system32\pla.dll
19:14:23.0263 0x1918  pla - ok
19:14:23.0302 0x1918  [ BC6849C62DB407573C6AD8CB1A4D2628,
5BDE0D60F85E4C27CEAD1B301155B54D841FB773BD5BB8AC5DDAEE31F8E94627 ] PlugPlay
C:\WINDOWS\system32\umpnpmgr.dll
19:14:23.0361 0x1918  PlugPlay - ok
19:14:23.0378 0x1918  [ 045EB4F260606A03BE340D09DEAF3BA4,
6F34B8D414F7F69F4388F2F8A86E0F3AD179E423126990AF3E1EC4DCCB8E7693 ] PNRPAutoReg
C:\WINDOWS\system32\pnrpauto.dll
19:14:23.0444 0x1918  PNRPAutoReg - ok
19:14:23.0495 0x1918  [ E287F157F7A0011D93179C64EF8ADCF2,
C16FB92C7B18D634BB1344238D35B3111494C243FBD5853F05376F5051480D83 ] PNRPsvc
C:\WINDOWS\system32\pnrpsvc.dll
19:14:23.0565 0x1918  PNRPsvc - ok
19:14:23.0622 0x1918  [ C16097D77A232A288D65F299E2E01105,
5CE4B44B06FD26569C0F92FF1D3991D0128D8444AE7BC9EBEF5A33811D721BE8 ] PolicyAgent
C:\WINDOWS\System32\ipsecsvc.dll
19:14:23.0703 0x1918  PolicyAgent - ok
19:14:23.0734 0x1918  [ 00E08B30E7F7C13ECE2CDF4F46A77311,
1807C0A64C1794E572C86730816C01DCF4D8F773ADE9CAEA3AC0658F7BD71A4E ] Power
C:\WINDOWS\system32\umpo.dll
19:14:23.0803 0x1918  Power - ok
19:14:23.0841 0x1918  [ E075CC071022BD4E9BE7C024717C0E0A,
BE65A8C1082AE8DF8C37CA06B2BCC521478AC153EA7388B03F7FAE3913920E75 ] PptpMiniport
C:\WINDOWS\system32\DRIVERS\raspptp.sys
```

```
19:14:23.0906 0x1918  PptpMiniport - ok
19:14:24.0137 0x1918  [ B7DB57A000D46D4DE75BC0C563E58072,
8183EB09DC4D44DFF027CA0AAA8C09921A14F088C1BC427B6ACA42340AAF69E6 ] PrintNotify
C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll
19:14:24.0285 0x1918  PrintNotify - ok
19:14:24.0331 0x1918  [ ECD373F9571C745894367CC2635EA44F,
E08B2A1017DAE1BF10B986DAFAD14BDE20D79703E0EF3A8C700A3753908C1392 ] Processor
C:\WINDOWS\System32\drivers\processr.sys
19:14:24.0382 0x1918  Processor - ok
19:14:24.0430 0x1918  [ B2A890D96C05E33FDD2BF3F3D4D0DF92,
3A29E17424429A5654D906E420D938148F09F57457356EFA72DA003B73F2D81E ] ProfSvc
C:\WINDOWS\system32\profsvc.dll
19:14:24.0512 0x1918  ProfSvc - ok
19:14:24.0546 0x1918  [ AF038FA3D3748B7595FE7096AD803696,
55263B2424BE1F59F16050C8A0A3B16B2A3A4C212051170DE8A49AC387BE1386 ] Ps2Kb2Hid
C:\WINDOWS\System32\drivers\aPs2Kb2Hid.sys
19:14:24.0562 0x1918  Ps2Kb2Hid - ok
19:14:24.0595 0x1918  [ 8528BB05E4D4E25945F78B00B2555FB7,
FF8E0D4580F93CD348080967F52FE6C2C68B56DAEACAE2EAEF04E19412A953AE ] Psched
C:\WINDOWS\system32\DRIVERS\pacer.sys
19:14:24.0634 0x1918  Psched - ok
19:14:24.0677 0x1918  [ AF90BB44C99D6820BE52C9BBAA523283,
9772D9CC1666959EC8EE4ED740A5179473CE4F38762109F1123DD68010D20EA1 ] QWAVE
C:\WINDOWS\system32\qwave.dll
19:14:24.0734 0x1918  QWAVE - ok
19:14:24.0763 0x1918  [ 3FB466684609A4329858CF2EBD62E0FD,
CFC8FBAB1436948F9D34CE6A2D6DE2F86F3E93E50B86851CED979C8CCE609798 ] QWAVEdrv
C:\WINDOWS\system32\drivers\qwavedrv.sys
19:14:24.0789 0x1918  QWAVEdrv - ok
19:14:24.0891 0x1918  [ 000D82CC258E2D341605A6F350C4D1E6,
59EC5BA95D8B9EC739BC7D0BBE0E244CA2AE2DF01A8B65BFF7741DFBE38C2940 ]
RapportCerberus_59849
C:\ProgramData\Trusteer\Rapport\store\exts\RapportCerberus\baseline\RapportCerberus6
4_59849.sys
19:14:24.0962 0x1918  RapportCerberus_59849 - ok
19:14:24.0998 0x1918  [ B6DD1E631D51250A07ECA001B6D62CB9,
D0561FC19CB1761607B569549C4427B4960100F40B61BF45BDCA6370708853D5 ] RapportEI64
C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportEI64.sys
19:14:25.0031 0x1918  RapportEI64 - ok
19:14:25.0046 0x1918  [ C375A3B45F320D91584746A39220561B,
C5C702040B25C16080F1AA0A6A875E7BEE01CC1C8C18394A78C88A0F4E6AE76D ] RapportHades64
C:\WINDOWS\system32\Drivers\RapportHades64.sys
19:14:25.0071 0x1918  RapportHades64 - ok
19:14:25.0100 0x1918  [ DD4C7AAAE0DBDE3A0091B2D552F3785E,
A149F7A70BCC07DEAA8B77BCAA76C553B3069DC8ED3D059BA46EF6DA5D13ADE0 ] RapportKE64
C:\WINDOWS\system32\Drivers\RapportKE64.sys
19:14:25.0126 0x1918  RapportKE64 - ok
19:14:25.0230 0x1918  [ 074E46476AB4427B36DC324629AA7A89,
3E86F32E9F344A8082F757B8068916CA859FEAA0D2F40C6C57F6135E1C0E25DC ]
RapportMgmtService C:\Program Files
(x86)\Trusteer\Rapport\bin\RapportMgmtService.exe
19:14:25.0310 0x1918  Suspicious file ( Forged ): C:\Program Files
(x86)\Trusteer\Rapport\bin\RapportMgmtService.exe. Real md5:
074E46476AB4427B36DC324629AA7A89, sha256:
3E86F32E9F344A8082F757B8068916CA859FEAA0D2F40C6C57F6135E1C0E25DC, fake md5:
E6826101399705281721 5A0A066A7900, fake sha256:
861EF2ECF460C7BAD8A809C3832BEB6E2E937BD6CC5C3186CAA6992A167F012A
19:14:25.0314 0x1918  RapportMgmtService - detected ForgedFile.Multi.Generic ( 1 )
19:14:25.0390 0x1918  RapportMgmtService ( ForgedFile.Multi.Generic ) - warning
19:14:25.0391 0x1918  Force sending object to P2P due to detect: RapportMgmtService
19:14:27.0970 0x1918  Object send P2P result: true
19:14:30.0454 0x1918  [ 6CAB58F6D357DE682B2075B1312708E9,
3FA41B333E5C742904F233E1940D9E3B1BF48D908A89A9D4B43DD7EBEBBAAB5F ] RapportPG64
C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportPG64.sys
19:14:30.0505 0x1918  RapportPG64 - ok
19:14:30.0540 0x1918  [ 2C56F0EE27E4EF70CA4B4983D3638905,
AFFDD686886CE982424B644D9168D61C6F86A5244FF97BC644DF75B321E415E5 ] RasAcd
C:\WINDOWS\system32\DRIVERS\rasacd.sys
19:14:30.0603 0x1918  RasAcd - ok
19:14:30.0647 0x1918  [ 674A4702E4E144E8710ED1A2EC6DD049,
613A921101A6815C9185D5EF3E251A592604E56FADE945BB7E256885CAD473BC ] RasAgileVpn
C:\WINDOWS\system32\DRIVERS\AgileVpn.sys
19:14:30.0717 0x1918  RasAgileVpn - ok
19:14:30.0753 0x1918  [ 5F061AC45266841A2860C1858ED863B8,
9E0D52BAC8A50225C32D0397C35350601B996443E2481C808CC59D3B0763FEF0 ] RasAuto
C:\WINDOWS\System32\rasauto.dll
```

```
19:14:30.0846 0x1918  RasAuto - ok
19:14:30.0866 0x1918  [ BBB6272B7F46C4640A8CDB8A70C3450F,
4266C3ABD0D1D0219F715EA0F155744F7C1E3A7B722BE863831B57AE785419A2 ] Rasl2tp
C:\WINDOWS\system32\DRIVERS\rasl2tp.sys
19:14:30.0934 0x1918  Rasl2tp - ok
19:14:31.0005 0x1918  [ 5C7B86EE33505E36026AFAAB62DA6364,
903BB1A355AC746BF09C2A7C87B068168648DB79DEF39AB1DC710B6A7A5F6556 ] RasMan
C:\WINDOWS\System32\rasmans.dll
19:14:31.0108 0x1918  RasMan - ok
19:14:31.0127 0x1918  [ 5247F308C4103CDC4FE12AE1D235800A,
E567CD33CA1897D53795E071B7AFBAF98B2C8F725F8BED0BA90F5EF611520E48 ] RasPppoe
C:\WINDOWS\system32\DRIVERS\raspppoe.sys
19:14:31.0172 0x1918  RasPppoe - ok
19:14:31.0197 0x1918  [ 2B0F1677CDD08967005F34488559BC6F,
FFF168EBD171C0B85A448AD1A04F66534E889AE1DC128F68EA3F35D5996C8D39 ] RasSstp
C:\WINDOWS\system32\DRIVERS\rassstp.sys
19:14:31.0267 0x1918  RasSstp - ok
19:14:31.0298 0x1918  [ A1A5E79C0D1352AFDC08328A623DA051,
01546DDE6F1FF159A7EB7F2BF104910445D3D863F1F37DEA695579BA60D84280 ] rdbss
C:\WINDOWS\system32\DRIVERS\rdbss.sys
19:14:31.0386 0x1918  rdbss - ok
19:14:31.0415 0x1918  [ 6B21EBF892CD8CACB71669B35AB5DE32,
0AD8E14FEF16FB2559F5FC8AFBC9D49E4E24F43CF65F480DBF9FAB593269B419 ] rdpbus
C:\WINDOWS\System32\drivers\rdpbus.sys
19:14:31.0490 0x1918  rdpbus - ok
19:14:31.0528 0x1918  [ 680C1DAE268B6FB67FA21B389A8B79EF,
856911F77BDD8830C3D683EBE8AF399FB3A54C7D8D0B34EA37D903377F0A39BD ] RDPDR
C:\WINDOWS\system32\drivers\rdpdr.sys
19:14:31.0595 0x1918  RDPDR - ok
19:14:31.0634 0x1918  [ 858776908AF838E3790F3261B799CDA6,
5BE4658540382D1B2F46E503CE175D74E3870FE492B8B8F37C3CFB34FF8E2DA8 ] RdpVideoMiniport
C:\WINDOWS\system32\drivers\rdpvideominiport.sys
19:14:31.0660 0x1918  RdpVideoMiniport - ok
19:14:31.0691 0x1918  [ A26AEC49F318FEE141DDDB2C5F99B3E6,
246AD79FF27E79DEDCB0AAA7C22A8EA6349DEDAC863413A1E378E68FD94C9C4F ] rdyboost
C:\WINDOWS\system32\drivers\rdyboost.sys
19:14:31.0742 0x1918  rdyboost - ok
19:14:31.0832 0x1918  [ E515A287C8FAE901EB8FB42F168E14F2,
9AE8D608587713FD18BB728BADD402C86FFF06A67359B22ED9431705522BC310 ] ReFS
C:\WINDOWS\system32\drivers\ReFS.sys
19:14:31.0904 0x1918  ReFS - ok
19:14:31.0945 0x1918  [ BFFB40FBE6D2C3469F8D06EE5E4934AB,
5B6763F973A740DCD53CEA75156926457BED8B075965033C484877DDA8B97F39 ] RemoteAccess
C:\WINDOWS\System32\mprdim.dll
19:14:31.0978 0x1918  RemoteAccess - ok
19:14:32.0009 0x1918  [ 4DCCABE03D06955ED61BABBD8EF9F30F,
531CD60315AAF283B73E0F6CF77D4DE093B809E73C44D2AC43B7247500B3485E ] RemoteRegistry
C:\WINDOWS\system32\regsvc.dll
19:14:32.0067 0x1918  RemoteRegistry - ok
19:14:32.0092 0x1918  [ CF59781FCB68F859EB6C835ED285211D,
E979014C07BF45F4F27E4433ED6B8FA618E4416CB01075FBF52CB2536EC63984 ]
RfButtonDriverService C:\Windows\RfBtnSvc64.exe
19:14:32.0111 0x1918  RfButtonDriverService - ok
19:14:32.0135 0x1918  [ 0527EF6E23B9FAB37DDCBC479C6CFA28,
C004CE6000074AC434F8B24A3383F8C0ACFA5476D9E3B1493B40911C78B028D64 ] RFCOMM
C:\WINDOWS\system32\DRIVERS\rfcomm.sys
19:14:32.0161 0x1918  RFCOMM - ok
19:14:32.0189 0x1918  [ D894CBD7DA753C881EE8D5E33B583225,
DA4472A85F10A3DF8CE969F731E67FE7C75EE6095908AB8AC2C44851DC5A3F8B ] RpcEptMapper
C:\WINDOWS\System32\RpcEpMap.dll
19:14:32.0255 0x1918  RpcEptMapper - ok
19:14:32.0293 0x1918  [ 5CAE8F47B31D5CFC322B5B898C19E0FE,
FDB5F0B6EA36403E031D9147AB0519011FAAD3AC8190DE5B1F17FB5472D79D47 ] RpcLocator
C:\WINDOWS\system32\locator.exe
19:14:32.0365 0x1918  RpcLocator - ok
19:14:32.0434 0x1918  [ 81979817943D830BF24571B7C1B28A1A,
9584D8F1FB3E6CF17BD465670B208C723A8E8B06775A3DA44F75D7710404EEA6 ] RpcSs
C:\WINDOWS\system32\rpcss.dll
19:14:32.0491 0x1918  RpcSs - ok
19:14:32.0547 0x1918  [ B868B9C46B11067A809987415E8A08A0,
8139EF76613DD7F2A002E48A593B2B01C5AD38630B9E9E454EB271F8754D511B ] RSPCIESTOR
C:\WINDOWS\system32\DRIVERS\RtsPStor.sys
19:14:32.0598 0x1918  RSPCIESTOR - ok
19:14:32.0632 0x1918  [ 2D05A5508F4685412F2B89E8C2189ABC,
82F12B4E0E73411A121EFD35FBD3B44CBBC0AE96ACFBB45D8C3C3777E2EA320D ] rspndr
C:\WINDOWS\system32\DRIVERS\rspndr.sys
```

```
19:14:32.0712 0x1918  rspndr - ok
19:14:32.0737 0x1918  [ 1A06373OF221B2746FFOO457AE17E4FO,
39A3C258CBFE3BC566C63528C9O2OA3BC9409736AE5289CO8A7BA471D8409263 ] s3cap
C:\WINDOWS\System32\drivers\vms3cap.sys
19:14:32.0802 0x1918  s3cap - ok
19:14:32.0837 0x1918  [ F6F2O9DDB94959BA104FC8FC87C53759,
8E862D41F4332EABF64BDO34E2COE3CC8109C799OCB4112C2B288OE8E6EDF2D3 ] SamSs
C:\WINDOWS\system32\lsass.exe
19:14:32.0885 0x1918  SamSs - ok
19:14:32.0928 0x1918  [ C624A1B32211C3166EDB3F4AB02A3OB7,
6B2A4607DB52D74242787ED9DF9067058983D310431D8612D2BO236E6201E681 ] sbp2port
C:\WINDOWS\system32\drivers\sbp2port.sys
19:14:32.0977 0x1918  sbp2port - ok
19:14:33.0019 0x1918  [ 47C497FA4DDEA908633CAA60CEBE6805,
4DF5742D4C99D3F7B6A5671AEDB1E5E47D3399D36B28BA19C105FA604D8D5A1C ] SCardSvr
C:\WINDOWS\System32\SCardSvr.dll
19:14:33.0074 0x1918  SCardSvr - ok
19:14:33.0086 0x1918  [ E76C4E98302AE39CC6FA5D20FC8B5438,
B6B6B59CF427515087689285797F4A5763103440EBE5D87A61FA74F80F895BDO ] ScDeviceEnum
C:\WINDOWS\System32\ScDeviceEnum.dll
19:14:33.0138 0x1918  ScDeviceEnum - ok
19:14:33.0152 0x1918  [ ABDO237B15DBD2B4695F4B7D734A58F7,
D6831921FOCD3E03CBF1CA3ED5824EE0C75127842D12D4E897E74EC72BO792EB ] scfilter
C:\WINDOWS\system32\DRIVERS\scfilter.sys
19:14:33.0203 0x1918  scfilter - ok
19:14:33.0273 0x1918  [ A95838FFFAEAA75OO263D491575F7E0C,
FEB79ECAE6D9AB0C29D9AFE12F60502A8357B3A382C0FACF4C6DA4852B6ECFA4 ] Schedule
C:\WINDOWS\system32\schedsvc.dll
19:14:33.0384 0x1918  Schedule - ok
19:14:33.0428 0x1918  [ AB285CE3431FF3D2ACE669245874C1C7,
6AF4C3E86EFA51F7FB6F8492CB2CCB807C7775EAE0508B87F07134FDAC679BD7 ] SCPolicySvc
C:\WINDOWS\System32\certprop.dll
19:14:33.0464 0x1918  SCPolicySvc - ok
19:14:33.0508 0x1918  [ FDEC5799BA499D18AFA3A540538866E7,
551EE0945FE4EC213FFF623E52450OB57531EFEA2D76FA7ED1D2D605E7E2168F ] sdbus
C:\WINDOWS\System32\drivers\sdbus.sys
19:14:33.0542 0x1918  sdbus - ok
19:14:33.0592 0x1918  [ 0B1E929D11A8E358106955603FAC65E8,
A5EC91BFC0873EC6AB1D0DB4E91654BD35339BD680E7E82DA2DC64996B4AE515 ] sdstor
C:\WINDOWS\System32\drivers\sdstor.sys
19:14:33.0618 0x1918  sdstor - ok
19:14:33.0651 0x1918  [ 3EA8A16169C26AFBEB544E0E48421186,
34BBB0459C96B3DE94CCB0D73461562935C583D7BF93828DA4E20A6BC9B7301D ] secdrv
C:\WINDOWS\system32\drivers\secdrv.sys
19:14:33.0724 0x1918  secdrv - ok
19:14:33.0790 0x1918  [ C49009F897BA4F2F4F31043663AA1485,
48C8BE1E3A4F150662AD012AF4E0357ABA792AD1147AB90EFF6CB2630E2501B6 ] seclogon
C:\WINDOWS\system32\seclogon.dll
19:14:33.0903 0x1918  seclogon - ok
19:14:33.0932 0x1918  [ A88882E64BDC1D8E8D6E727B71CCCC53,
12D2235F54D0CEEED8AA268C17CDE44020269F4FEFC70CE957DBBF99AF7F553D ] SENS
C:\WINDOWS\System32\sens.dll
19:14:34.0013 0x1918  SENS - ok
19:14:34.0058 0x1918  [ E66A7C8CE7ED22DED6DF1CA479FB4790,
ADEB076F131E7A8C3AD96022B09BB33EB9AB26C9C831503B8C6960AA763B8975 ] SensrSvc
C:\WINDOWS\system32\sensrsvc.dll
19:14:34.0114 0x1918  SensrSvc - ok
19:14:34.0150 0x1918  [ DB2FF24CE0BDD15FE75870AFE312BA89,
7DB0D978C92CD0A0A81F7AB46FE323B4929CEA01585B0F330921E6DFA7DE1B85 ] SerCx
C:\WINDOWS\system32\drivers\SerCx.sys
19:14:34.0206 0x1918  SerCx - ok
19:14:34.0243 0x1918  [ 0044B31F93946D5D41982314381FE431,
95B8A94BA9EF770F29ACD5B23D447EC2B6CF1CB3D0030343BA1550AC31F6E2A5 ] SerCx2
C:\WINDOWS\system32\drivers\SerCx2.sys
19:14:34.0283 0x1918  SerCx2 - ok
19:14:34.0299 0x1918  [ 3CD600C089C1251BEEB4CD4CD5164F9E,
D9F81951B4454B24E821E33ACA53A851A61F3135E8EC6FBE6761A1A3E1CDCBE2 ] Serenum
C:\WINDOWS\System32\drivers\serenum.sys
19:14:34.0338 0x1918  Serenum - ok
19:14:34.0355 0x1918  [ D864381BC9C725FAB01D94C060660166,
132FED95222BBE3B0B25B3F1F0EFC5903D04564BD047BA4D2042AD51E3FDA724 ] Serial
C:\WINDOWS\System32\drivers\serial.sys
19:14:34.0382 0x1918  Serial - ok
19:14:34.0415 0x1918  [ 0BD2B65DCE756FDE95A2E5CCCBF7705D,
F13FAFEC8FCF3E796196562717C433CE359A74A3E5876AB070647C717AF74028 ] sermouse
C:\WINDOWS\System32\drivers\sermouse.sys
```

```
19:14:34.0462 0x1918  sermouse - ok
19:14:34.0514 0x1918  [ D5C3776CBD8BC307DCCA3FD4CE667A37,
98E4253B770C25914C91A6148E2EA15ED0EF37ADCB042A47252DBA135972BF74 ] SessionEnv
C:\WINDOWS\system32\sessenv.dll
19:14:34.0574 0x1918  SessionEnv - ok
19:14:34.0597 0x1918  [ 472B7A5AC181C050888DB454663DD764,
C950A8615D57BFD455E18880398350642B2E1D6B951EC9754FD8D429F3418835 ] sfloppy
C:\WINDOWS\System32\drivers\sfloppy.sys
19:14:34.0636 0x1918  sfloppy - ok
19:14:34.0748 0x1918  [ F4414F57DF2CECB8FC969AA43A6B0D50,
AD09A6E1294721507DD6BE82B91F2EEB0FF0151B9BC14A75840CD657DBFDECEC ] SharedAccess
C:\WINDOWS\System32\ipnathlp.dll
19:14:34.0852 0x1918  SharedAccess - ok
19:14:34.0977 0x1918  [ 0D190D8B4B20446BE6299AC734DFADF1,
6551095971F99820BBFC5FED8FAB9591A3F8ABFA0F027887F3B71B79325FF6D9 ] ShellHWDetection
C:\WINDOWS\System32\shsvcs.dll
19:14:35.0062 0x1918  ShellHWDetection - ok
19:14:35.0095 0x1918  [ 2F518D13DD6F3053837FE606F1A2EA1F,
64109296CE95BD233525688A350D575CF97B9464659AA07CF78B307B6ADBC835 ] SiSRaid2
C:\WINDOWS\system32\drivers\SiSRaid2.sys
19:14:35.0117 0x1918  SiSRaid2 - ok
19:14:35.0134 0x1918  [ 1AC9A200A9C49C4508F04AAFFCA34A3F,
972BCB2A39169155F74111FAC74ACCD8F50E34EADCF087833B0980827627BBF4 ] SiSRaid4
C:\WINDOWS\system32\drivers\sisraid4.sys
19:14:35.0155 0x1918  SiSRaid4 - ok
19:14:35.0186 0x1918  [ 587ACA15210D1B01FBF272E07A08F91A,
1F3C13C218C5EA329C6E33E4AE7CFE88DAD59DA40F59FDE09D733AFD2E489000 ] smphost
C:\WINDOWS\System32\smphost.dll
19:14:35.0230 0x1918  smphost - ok
19:14:35.0269 0x1918  [ 49EEB92DE930B8566EF615D600781DB4,
0B7C929D24FAFC34F95BB4AA77DCBA29DDD8F1977EB42713B64228677D1FBFD3 ] SNMPTRAP
C:\WINDOWS\System32\snmptrap.exe
19:14:35.0298 0x1918  SNMPTRAP - ok
19:14:35.0393 0x1918  [ 33977549C2CED09936E05BEE7659EAFF,
EB95C72ED0EAC59A50E6882B2501049191A796542C42414FAF0028907C669B21 ] spaceport
C:\WINDOWS\system32\drivers\spaceport.sys
19:14:35.0449 0x1918  spaceport - ok
19:14:35.0501 0x1918  [ F337BE11071818FC3F5DC2940B6BDE34,
D5CFF00E5DF37045F71AEE101AC9B270EBB29F372F404757B58600E9966C7E4D ] SpbCx
C:\WINDOWS\system32\drivers\SpbCx.sys
19:14:35.0548 0x1918  SpbCx - ok
19:14:35.0723 0x1918  [ FE0CB40F36D3FCDD3A1B312EF72C38D5,
42EA50869752164764DFE8CE7E1C247BE8342A0C15F39158DC808E8A692C460F ] Spooler
C:\WINDOWS\System32\spoolsv.exe
19:14:35.0845 0x1918  Spooler - ok
19:14:36.0276 0x1918  [ C993A0B97BECD3AAF5158E3869878465,
8B86F37DEFCBE55DE507D830EC4980EBB39B3CCA30C2B3E76B588AAB282A50FC ] sppsvc
C:\WINDOWS\system32\sppsvc.exe
19:14:36.0699 0x1918  sppsvc - ok
19:14:36.0798 0x1918  [ 2B78788A1485F9B99A578A299DF42C02,
A87183A9B13585C9E850437A45237105D39D7F3212ADB079D6AB430B67A59643 ] srv
C:\WINDOWS\system32\DRIVERS\srv.sys
19:14:36.0870 0x1918  srv - ok
19:14:37.0007 0x1918  [ FD163F487CBA9C98AFFEB546C80F49A2,
18DAAD173C0517F7BBF5D0C914302D98931E3BA6DAA36DC91D8DB0743EC40563 ] srv2
C:\WINDOWS\system32\DRIVERS\srv2.sys
19:14:37.0106 0x1918  srv2 - ok
19:14:37.0131 0x1918  [ 716059F37BCCB1ABEDE99EBE82E8E362,
05F27B0FABBBC0E324F06D20ABEF51EDA3316C9F7F85C1AD24639CD6DE1BC8AC ] srvnet
C:\WINDOWS\system32\DRIVERS\srvnet.sys
19:14:37.0178 0x1918  srvnet - ok
19:14:37.0262 0x1918  [ BB9ED3EDD8E85008215A7250D325A72E,
D3404E31B7706B25CDEA7CB4260C343B5F090E8CCB9A5FA203B0F94A9112F1B3 ] SSDPSRV
C:\WINDOWS\System32\ssdpsrv.dll
19:14:37.0349 0x1918  SSDPSRV - ok
19:14:37.0386 0x1918  [ 0211AB46B73A2623B86C1CFCB30579AB,
7CC9BA2DF7B9EA6BB17EE342898EDD7F54703B93B6DED6A819E83A7EE9F938B4 ] SSPORT
C:\WINDOWS\system32\Drivers\SSPORT.sys
19:14:37.0408 0x1918  SSPORT - ok
19:14:37.0490 0x1918  [ 3911418AFDE10EA6823B7799E4815524,
A73517C4C1271E666B2B3A747756070098E923742B41572AA16573170440AA07 ] SstpSvc
C:\WINDOWS\system32\sstpsvc.dll
19:14:37.0577 0x1918  SstpSvc - ok
19:14:37.0632 0x1918  [ 366DEA74BBA65B362BCCFC6FC2ADFD8B,
4D28122AB9D8DAB724021E6513B4474BD34FCEDF47769B1D27AC7551FCA002F8 ] stexstor
C:\WINDOWS\system32\drivers\stexstor.sys
```

19:14:37.0717 0x1918 stexstor - ok
19:14:37.0808 0x1918 [D638904FE86A5FE542A1BA13A9D68E5C,
89A956F932316BC50DD99B54BAF4E2809DCAA084DBB04CB84D11E5470BEAF251] stisvc
C:\WINDOWS\System32\wiaservc.dll
19:14:37.0900 0x1918 stisvc - ok
19:14:37.0922 0x1918 [0ED2E318ABB68C1A35A8B8038BDB4C90,
5C3ABC245F4BCFE64E646D9C0E2F5E211244956C84D03084C71FF6A7E0CDED30] storahci
C:\WINDOWS\system32\drivers\storahci.sys
19:14:37.0945 0x1918 storahci - ok
19:14:37.0977 0x1918 [7A08CEE1535F5A448215634C5EA74E50,
41529CDC08A3956F8FE9D5759B147E2E56E3305149EA415EB200249F7CD32094] storflt
C:\WINDOWS\system32\DRIVERS\vmstorfl.sys
19:14:38.0015 0x1918 storflt - ok
19:14:38.0059 0x1918 [6B06E2D11E604BE2B1A406C4CB3B90DE,
2DDEA1568A85AD64FCE5D10D348304FCD9BE6E96C2313353EF70A2933306D188] stornvme
C:\WINDOWS\system32\drivers\stornvme.sys
19:14:38.0109 0x1918 stornvme - ok
19:14:38.0149 0x1918 [3118058E3D07021A55324A943C6D722B,
0B255DF1977DADD2B9766EEEA814B464F0ABFA34D6439F3C453083850C121F16] StorSvc
C:\WINDOWS\system32\storsvc.dll
19:14:38.0226 0x1918 StorSvc - ok
19:14:38.0253 0x1918 [548759755BC73DAD663250239D7E0B9F,
D31A05A8CE800B539420B6E545F1F4BF6E4B02EAF8366DE89CAF13A83C6CA48D] storvsc
C:\WINDOWS\system32\drivers\storvsc.sys
19:14:38.0305 0x1918 storvsc - ok
19:14:38.0345 0x1918 [D8E1AE075AB3E8AD56F69C44AA978596,
CAFF5116DE7F0EEFFEBE38724BCEE7D11B44153AD35EE43E314C56D5E210758A] svsvc
C:\WINDOWS\system32\svsvc.dll
19:14:38.0438 0x1918 svsvc - ok
19:14:38.0465 0x1918 [84E0F5D41C138C5CC975137A2A98F6D3,
1E36CED05E4F4365C2AB020CAF920E3959995D7F89F3FABD7B2FB05985F85F38] swenum
C:\WINDOWS\System32\drivers\swenum.sys
19:14:38.0482 0x1918 swenum - ok
19:14:38.0560 0x1918 [850EBB87584484DC16F917E7B6F4A304,
C253D1DFFCDFB018432063602FB01DBCBDDD6E03458E5C366AABD4670F114B0C] swprv
C:\WINDOWS\System32\swprv.dll
19:14:38.0673 0x1918 swprv - ok
19:14:38.0864 0x1918 [3DA26652B12E9AB43FD04976AC6DFD33,
DEFE220D86197949E97342FE3487CD6A07DD2FFAF6D17A7C65419C2C1B9D1AB5] SysMain
C:\WINDOWS\system32\sysmain.dll
19:14:39.0024 0x1918 SysMain - ok
19:14:39.0080 0x1918 [D65B1C952AEB864C2BAC7A770B17ECCE,
3EFAAFFF73390D9CB660E0F42B305512396CF66ED06E4A20ED67E8722FB4355B]
SystemEventsBroker C:\WINDOWS\System32\SystemEventsBrokerServer.dll
19:14:39.0157 0x1918 SystemEventsBroker - ok
19:14:39.0218 0x1918 [BA6DD39266A5E15515C8C14DA2DA3E5C,
5BC917BA4E7281A67CC6CEF2F4D1972DF04DECBEFB6DED0B08FFBD06E15D4B4F]
TabletInputService C:\WINDOWS\System32\TabSvc.dll
19:14:39.0297 0x1918 TabletInputService - ok
19:14:39.0326 0x1918 [B517410F157693043DACA21B19B258A6,
2224EECEB575CEA811036C43BB5B0A408DE5F59BC97235AB948968E4C3E438F2] TapiSrv
C:\WINDOWS\System32\tapisrv.dll
19:14:39.0388 0x1918 TapiSrv - ok
19:14:39.0590 0x1918 [25AC0B50A71938890970E1508F107196,
6FAFBA2DFFFF9916CC304AE7E6AD0F6CE1D6F4AAE6B2C113202D78310EFEBC58] Tcpip
C:\WINDOWS\system32\drivers\tcpip.sys
19:14:39.0752 0x1918 Tcpip - ok
19:14:39.0903 0x1918 [25AC0B50A71938890970E1508F107196,
6FAFBA2DFFFF9916CC304AE7E6AD0F6CE1D6F4AAE6B2C113202D78310EFEBC58] TCPIP6
C:\WINDOWS\system32\DRIVERS\tcpip.sys
19:14:40.0011 0x1918 TCPIP6 - ok
19:14:40.0043 0x1918 [41CF802064F72E55F50CA0A221FD36D4,
70ABCDF9E96611E8C83042C581575E26649FE479475E8E118CD3FF6CB1C84C3F] tcpipreg
C:\WINDOWS\system32\drivers\tcpipreg.sys
19:14:40.0121 0x1918 tcpipreg - ok
19:14:40.0183 0x1918 [FFF28F9F6823EB1756C60F1649560BBF,
208DFF8BF0329D0D4761C7E31527AEED7FF5F3C36C5005953D01477F35408D5C] tdx
C:\WINDOWS\system32\DRIVERS\tdx.sys
19:14:40.0263 0x1918 tdx - ok
19:14:40.0598 0x1918 [0F2A43DB0A4A70EF400295F413527293,
D67D78CFB47E9EA1C1D9B37BFFFB44320A6ECC2D0C029768517C64F3A1882E19] TeamViewer8
C:\Program Files (x86)\TeamViewer\Version8\TeamViewer_Service.exe
19:14:40.0857 0x1918 TeamViewer8 - ok
19:14:40.0892 0x1918 [232D185D2337F141311D0CF1983E1431,
02EB56D3F26174AF1741C1A444CE30DE84D5BAF583C1A52C7A953BCC52445547] terminpt
C:\WINDOWS\System32\drivers\terminpt.sys

```
19:14:40.0930 0x1918  terminpt - ok
19:14:41.0000 0x1918  [ 3D748E5558FD9A9F03182CB2330698DC,
70B2069AB7912EB49AB3ABD18D4B42CB94AC99CA6DE3F63F4888B8EAAC78AAA2 ] TermService
C:\WINDOWS\System32\termsrv.dll
19:14:41.0103 0x1918  TermService - ok
19:14:41.0143 0x1918  [ 05FBE1F7C13E87AF7A414CDF288B1F62,
24079E1A6B2E33A1A8E76A77F73473B93DD6B379E44C982CE50D6CEED9747838 ] Themes
C:\WINDOWS\system32\themeservice.dll
19:14:41.0236 0x1918  Themes - ok
19:14:41.0277 0x1918  [ FD788C2D96EA91469A3C1D13E80D7473,
7B14D4BFDE18CECC19FBFFAA5AFF5FD78BFB7FCDA6613990740A8A7DD9873D26 ] THREADORDER
C:\WINDOWS\system32\mmcss.dll
19:14:41.0338 0x1918  THREADORDER - ok
19:14:41.0382 0x1918  [ 347A3E49CE18402305B8119A6EC7CFEB,
6768B20EE577880B0353FE84B980D4A18D323929A63FAE41F7A55123BBFC8DBA ] TimeBroker
C:\WINDOWS\System32\TimeBrokerServer.dll
19:14:41.0463 0x1918  TimeBroker - ok
19:14:41.0490 0x1918  [ 82F909359600D3603FE852DB7F135626,
2EB2BB9D81AC9A2E432B2628E296B7B21F1C82EAE8009300EEF1B8596A9F418D ] TPM
C:\WINDOWS\system32\drivers\tpm.sys
19:14:41.0536 0x1918  TPM - ok
19:14:41.0564 0x1918  [ C97E14BB6A196B0554D6EB67D8818175,
C00588C94988F10507F84584DFA4C0A43B8648AD1AD35E9BAE14CDD21FCF7B90 ] TrkWks
C:\WINDOWS\System32\trkwks.dll
19:14:41.0624 0x1918  TrkWks - ok
19:14:41.0681 0x1918  [ 887CC44830D3F367CAD17A0CA7CCA5C8,
D4022A76433A11FD66D0F41A1EB4D6893BC5B22317E7E9E021739109EB493B44 ] TrustedInstaller
C:\WINDOWS\servicing\TrustedInstaller.exe
19:14:41.0755 0x1918  TrustedInstaller - ok
19:14:41.0779 0x1918  [ BF8F54CA37E9C9D6582C31C5761F8C93,
337C566792F6FB9B7FD5D1D4384B767CFE4CF5DBB2E4688CCC36CBB018A0DD0F ] TsUsbFlt
C:\WINDOWS\system32\drivers\tsusbflt.sys
19:14:41.0844 0x1918  TsUsbFlt - ok
19:14:41.0868 0x1918  [ E0088068DCE2EE82897027DDB8E05254,
FA9C201D3C885DAD2ABE6A23343EDCC83CFB342EFF9E3005FA50B1D88B21D203 ] TsUsbGD
C:\WINDOWS\System32\drivers\TsUsbGD.sys
19:14:41.0926 0x1918  TsUsbGD - ok
19:14:41.0954 0x1918  [ C8E0E78B5D284C2FF59BDFFDAF997242,
BA1576C491A1246EF9866762426D110F4570F9DB42A68C174943C7D5020FE3E2 ] tunnel
C:\WINDOWS\system32\DRIVERS\tunnel.sys
19:14:42.0010 0x1918  tunnel - ok
19:14:42.0044 0x1918  [ F6EEAD052943B5A3104C1405BB856C54,
FE422813E6C1012E9F392EFF2AE4C6D3A4DBD9CB2BD5E6A5CAB57D4E89A29468 ] uagp35
C:\WINDOWS\system32\drivers\uagp35.sys
19:14:42.0075 0x1918  uagp35 - ok
19:14:42.0099 0x1918  [ FE6067B1FD4E63650C667B33D080565B,
2C330ED00E49BA55E25564230E0DFB8A35F2B5320EB18D4AF7CAACFA9A449044 ] UASPStor
C:\WINDOWS\System32\drivers\uaspstor.sys
19:14:42.0132 0x1918  UASPStor - ok
19:14:42.0156 0x1918  [ A17D5E1A6DF4EAB0A480F2C490DE4C9D,
1EA835F172B6BF3D7F496E079DF1CDF00122B2110C08D61427582BC9405D2B7B ] UBHelper
C:\Windows\system32\drivers\UBHelper.sys
19:14:42.0186 0x1918  UBHelper - ok
19:14:42.0228 0x1918  [ B034A41891A36457B994307DFA772293,
CA5E6500764A9777AE0E15B2AFB6F05982C90F01374E3F6DDC6DF3852282C66B ] UCX01000
C:\WINDOWS\System32\drivers\ucx01000.sys
19:14:42.0265 0x1918  UCX01000 - ok
19:14:42.0330 0x1918  [ 1EC649F112896FAE33250F0B97AC5D0B,
0C0A1C2C7615DEB298AD3073340FD1BF91FEBE611F133E3B48D994A6EAA8369F ] udfs
C:\WINDOWS\system32\DRIVERS\udfs.sys
19:14:42.0411 0x1918  udfs - ok
19:14:42.0427 0x1918  [ 9578691F297E1B1F519970FE6D47CB21,
080C352AAF22A16A4F3C4AB4DCEA5BFA656457C73F735CEBA30516FDACCF6301 ] UEFI
C:\WINDOWS\System32\drivers\UEFI.sys
19:14:42.0455 0x1918  UEFI - ok
19:14:42.0496 0x1918  [ 320878AFECDBBD61BBE98624A6CAAC08,
15C090EA32A24D976B5FCB1373B1281DCC2295C075299C814345D694AEB47CB9 ] UIODetect
C:\WINDOWS\system32\UIODetect.exe
19:14:42.0565 0x1918  UIODetect - ok
19:14:42.0615 0x1918  [ 5EAB5117DDB24FC4D39E6FFFCF1837B9,
2BC709240867F161E94BE6625A04F478EAAA3EEE7BC7C37ED0DFA9EEA5928E98 ] uliagpkx
C:\WINDOWS\system32\drivers\uliagpkx.sys
19:14:42.0662 0x1918  uliagpkx - ok
19:14:42.0678 0x1918  [ DA34C39A18E60E7C3FA0630566408034,
2F162504214053894C72760D9933D01DBF3578609FE5E2376C3272818599FE32 ] umbus
C:\WINDOWS\System32\drivers\umbus.sys
```

```
19:14:42.0729 0x1918  umbus - ok
19:14:42.0753 0x1918  [ AE8294875E5446E359B1E8035D40C05E,
AE0357BAB47C07C3576BC76951CD258C009BC5A1B93259D2122A841BD9CDA8FA ] UmPass
C:\WINDOWS\System32\drivers\umpass.sys
19:14:42.0808 0x1918  UmPass - ok
19:14:42.0868 0x1918  [ E3DDF7D43E05784FAA5E042605EEE528,
8E20E880FAB09AF4FF5C438BF9EAE9970D46C05167870110869B744E498FD761 ] UmRdpService
C:\WINDOWS\System32\umrdp.dll
19:14:42.0936 0x1918  UmRdpService - ok
19:14:42.0987 0x1918  [ 9DC07E73A4ABB9ACF692113B36A5009F,
CA7176FC219515D58DCFA66EC61880ECE5617275C9B83701BB74D8B60E733D34 ] UnlockerDriver5
C:\Program Files\Unlocker\UnlockerDriver5.sys
19:14:43.0003 0x1918  UnlockerDriver5 - ok
19:14:43.0162 0x1918  [ DBE2E6388379D5CC78099650541E9566,
1914BC929F109A49FB18ED31F239A9813A010B0A3914BC8CD0D6A94A67A072D7 ] UNS
C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe
19:14:43.0202 0x1918  UNS - ok
19:14:43.0275 0x1918  [ 4A2FFDAC45F317E17DF642C7160EB633,
F1AB762912FAA5F469F322407DA37C91556086C42D1643AD27516C12A84F74D0 ] upnphost
C:\WINDOWS\System32\upnphost.dll
19:14:43.0368 0x1918  upnphost - ok
19:14:43.0444 0x1918  [ 433ECDE01A52691FA7ACA51C10C09B70,
B896296A3F8EF2AF3AC5F0091B9848156608586F1E10A95D70700BAB51E8062A ] usbccgp
C:\WINDOWS\System32\drivers\usbccgp.sys
19:14:43.0495 0x1918  usbccgp - ok
19:14:43.0542 0x1918  [ B3D6457D841A0CAEF4C52D88621715F2,
CBDD76A8A28379B107B1FB530757B477B8AB74CD01F9F3CEDC7B1BA0C6E5A990 ] usbcir
C:\WINDOWS\System32\drivers\usbcir.sys
19:14:43.0591 0x1918  usbcir - ok
19:14:43.0628 0x1918  [ 48BA326A3DBA5B5BEB5F2777F4618696,
B9EC8155F11A3A7644BD9DC8910681B46AE44AE3BF53F052DF50E9C5555E3229 ] usbehci
C:\WINDOWS\System32\drivers\usbehci.sys
19:14:43.0649 0x1918  usbehci - ok
19:14:43.0730 0x1918  [ 93435654DCA210298BA0F986EB51C679,
926313A0499100EA5C49C5EC44BB8FE5F8F2A7F57F3EA56D59DA694F8396A409 ] usbhub
C:\WINDOWS\System32\drivers\usbhub.sys
19:14:43.0791 0x1918  usbhub - ok
19:14:43.0834 0x1918  [ 83C9C45D59C72FEFDAE9A5686BE31FEA,
12FC2C3C3C5CD5F2EFBAA11A1AD06FDD7DDB6EECF6F2684BBAAF88198D976316 ] USBHUB3
C:\WINDOWS\System32\drivers\UsbHub3.sys
19:14:43.0870 0x1918  USBHUB3 - ok
19:14:43.0993 0x1918  [ 3019097FB6C985EF24C058090FF3BDBD,
24AC518D34E338D94BF3D5B3F72E53F8A1369BAA7F32FEA3EDBCF928C4FF1D17 ] usbohci
C:\WINDOWS\System32\drivers\usbohci.sys
19:14:44.0060 0x1918  usbohci - ok
19:14:44.0089 0x1918  [ 4D655E3B684BE9B0F7FFD8A2935C348C,
3A7FC1748C5AEA8CFE0E7C22ADC77E3DCA475455FC16D9C6A5C16EB5E949A516 ] usbprint
C:\WINDOWS\System32\drivers\usbprint.sys
19:14:44.0149 0x1918  usbprint - ok
19:14:44.0187 0x1918  [ F04D164C4168701A4E7835607722E5F1,
6F743CF2CF73945B4A4B1C4402744BC2FE1624F1346C194493AD2F7110F9EB35 ] usbscan
C:\WINDOWS\system32\DRIVERS\usbscan.sys
19:14:44.0248 0x1918  usbscan - ok
19:14:44.0328 0x1918  [ EA23453240137F6773174E0D93F61A69,
579AD09FB428C2BB8B4055128620A7AADD1B606C1EA44B87A01D69A84232A5D9 ] USBSTOR
C:\WINDOWS\System32\drivers\USBSTOR.SYS
19:14:44.0381 0x1918  USBSTOR - ok
19:14:44.0423 0x1918  [ 064260B3A5868AC894A4943543BC7AB7,
D3534E98B34C4AC9A430D7E0AB301A0E5E1511E3117C2FEA392636B0DE2C38E2 ] usbuhci
C:\WINDOWS\System32\drivers\usbuhci.sys
19:14:44.0489 0x1918  usbuhci - ok
19:14:44.0559 0x1918  [ 18F744E8CCEB2670040EBAF7AD77B8C6,
C5E2DF4EA0D946B4DA67DE29FA9D0F079DED35EC59B98E532C4C2D5F8E86DA0A ] usbvideo
C:\WINDOWS\System32\Drivers\usbvideo.sys
19:14:44.0615 0x1918  usbvideo - ok
19:14:44.0686 0x1918  [ 48430B0313FC1CFE3D2400553F1A93CD,
92994DE6B131E904AFF2C9C4FBB4E6B0D58525A1539763327373DA18C9F08193 ] USBXHCI
C:\WINDOWS\System32\drivers\USBXHCI.SYS
19:14:44.0738 0x1918  USBXHCI - ok
19:14:44.0762 0x1918  [ F6F209DDB94959BA104FC8FC87C53759,
8E862D41F4332EABF64BD034E2C0E3CC8109C7990CB4112C2B2880E8E6EDF2D3 ] VaultSvc
C:\WINDOWS\system32\lsass.exe
19:14:44.0781 0x1918  VaultSvc - ok
19:14:44.0789 0x1918  [ FEB26E3B8345A7E8D62F945C4AE86562,
3AAFE87C402FC8E92542DFE60EC9540559863065F88D429A16D7B1BF829223FF ] vdrvroot
C:\WINDOWS\system32\drivers\vdrvroot.sys
```

```
19:14:44.0806 0x1918  vdrvroot - ok
19:14:44.0879 0x1918  [ E3EF58D4123B5AA29C8E19825AF84A5E,
FB1046722BC643E955DBC3B1459DBF2A6D575EBA2BCF7B20A0FA51E3993835E2 ] vds
C:\WINDOWS\System32\vds.exe
19:14:45.0020 0x1918  vds - ok
19:14:45.0030 0x1918  [ A026EDEAA5EECAE0B08E2748B616D4BD,
2525A54DC7F49DDFBB999C22BF3FAB6D9E9F70C0806E58D81E90AC59F9F46089 ] VerifierExt
C:\WINDOWS\system32\drivers\VerifierExt.sys
19:14:45.0055 0x1918  VerifierExt - ok
19:14:45.0091 0x1918  [ 52E483A3701A5A61A75A06993720347D,
689E812755E485DF6960D1E049740FBAFB812467D23B673DCAA40C03FEBB544F ] vhdmp
C:\WINDOWS\System32\drivers\vhdmp.sys
19:14:45.0136 0x1918  vhdmp - ok
19:14:45.0150 0x1918  [ 06D38968028E9AB19DE9B618C7B6D199,
62022297A47F440D1C82CA0B0E57C0C8E9D5033D83DD3B40492B218DF65EBF68 ] viaide
C:\WINDOWS\system32\drivers\viaide.sys
19:14:45.0168 0x1918  viaide - ok
19:14:45.0184 0x1918  [ C6305BDFC4F7CE51F72BB072C03D4ACE,
73E62869CA3104F48CC3B0C45E69CE9BF4F8D7D06E29C2F049B9347ABB50554D ] vmbus
C:\WINDOWS\system32\drivers\vmbus.sys
19:14:45.0205 0x1918  vmbus - ok
19:14:45.0222 0x1918  [ DA40BEA0A863CE768C940CA9723BF81F,
567C0C3F422325635808B0CF76E05D3B6187F96845C33F85F92F98C9FE53A5B8 ] VMBusHID
C:\WINDOWS\System32\drivers\VMBusHID.sys
19:14:45.0255 0x1918  VMBusHID - ok
19:14:45.0316 0x1918  [ 9067880BBB1C18703DBFF27D731D7ECA,
0044246249F4B945D72BBC0FEF9BF3C31E62F57CBF77615A95213B36A29F0C71 ]
vmicguestinterface C:\WINDOWS\System32\ICSvc.dll
19:14:45.0395 0x1918  vmicguestinterface - ok
19:14:45.0414 0x1918  [ 9067880BBB1C18703DBFF27D731D7ECA,
0044246249F4B945D72BBC0FEF9BF3C31E62F57CBF77615A95213B36A29F0C71 ] vmicheartbeat
C:\WINDOWS\System32\ICSvc.dll
19:14:45.0451 0x1918  vmicheartbeat - ok
19:14:45.0470 0x1918  [ 9067880BBB1C18703DBFF27D731D7ECA,
0044246249F4B945D72BBC0FEF9BF3C31E62F57CBF77615A95213B36A29F0C71 ] vmickvpexchange
C:\WINDOWS\System32\ICSvc.dll
19:14:45.0503 0x1918  vmickvpexchange - ok
19:14:45.0520 0x1918  [ 9067880BBB1C18703DBFF27D731D7ECA,
0044246249F4B945D72BBC0FEF9BF3C31E62F57CBF77615A95213B36A29F0C71 ] vmicrdv
C:\WINDOWS\System32\ICSvc.dll
19:14:45.0554 0x1918  vmicrdv - ok
19:14:45.0570 0x1918  [ 9067880BBB1C18703DBFF27D731D7ECA,
0044246249F4B945D72BBC0FEF9BF3C31E62F57CBF77615A95213B36A29F0C71 ] vmicshutdown
C:\WINDOWS\System32\ICSvc.dll
19:14:45.0605 0x1918  vmicshutdown - ok
19:14:45.0624 0x1918  [ 9067880BBB1C18703DBFF27D731D7ECA,
0044246249F4B945D72BBC0FEF9BF3C31E62F57CBF77615A95213B36A29F0C71 ] vmictimesync
C:\WINDOWS\System32\ICSvc.dll
19:14:45.0665 0x1918  vmictimesync - ok
19:14:45.0695 0x1918  [ 9067880BBB1C18703DBFF27D731D7ECA,
0044246249F4B945D72BBC0FEF9BF3C31E62F57CBF77615A95213B36A29F0C71 ] vmicvss
C:\WINDOWS\System32\ICSvc.dll
19:14:45.0730 0x1918  vmicvss - ok
19:14:45.0754 0x1918  [ 55D7D963DE85162F1C49721E502F9744,
5AD34D6DB707EF3E5242BD8CA67B21D6258EE7E7FC477D5227BD15500AE7F45F ] volmgr
C:\WINDOWS\system32\drivers\volmgr.sys
19:14:45.0772 0x1918  volmgr - ok
19:14:45.0789 0x1918  [ CCB9E901F7254BF96D28EB1B0E5329B7,
F0E3CA4EFA544CDAEF4092284CF3EC7DF07F806A770285E281816457AD8813F5 ] volmgrx
C:\WINDOWS\system32\drivers\volmgrx.sys
19:14:45.0821 0x1918  volmgrx - ok
19:14:45.0851 0x1918  [ 4BB9BC49DEE1A319EC58274A7BBED663,
624491089623A5B68C01A6A000E60D450E8E467619ACEBB90C6FDED0CF670F95 ] volsnap
C:\WINDOWS\system32\drivers\volsnap.sys
19:14:45.0878 0x1918  volsnap - ok
19:14:45.0917 0x1918  [ 01355C98B5C3ED1EC446743CDA848FCE,
B9FCF558C20E05DD0F53FFB70BBEF873EA57801E13A16701E636128D625C4B67 ] vpci
C:\WINDOWS\System32\drivers\vpci.sys
19:14:45.0964 0x1918  vpci - ok
19:14:45.0993 0x1918  [ 4539F45F9F4C9757A86A56C949421E07,
DEC362314B2C66414F39354AFE79C02B18BF4EEF90787FB58307F6EB62237E2C ] vsmraid
C:\WINDOWS\system32\drivers\vsmraid.sys
19:14:46.0030 0x1918  vsmraid - ok
19:14:46.0123 0x1918  [ E369C59F2C0852DDD090C07E0DDE0051,
4FAC94458EAAEED4F84A86FBAB8FBB332D0AF85BD528E63C0C058A2DA8E3011D ] VSS
C:\WINDOWS\system32\vssvc.exe
```

```
19:14:46.0273 0x1918  VSS - ok
19:14:46.0311 0x1918  [ 0849B7260F26FE05EA56DED0672E2F4B,
7EAC0E7988F45CB4133A15932955B7B03CE715C967A3BAC9999D81543EBCAEC5 ] VSTXRAID
C:\WINDOWS\system32\drivers\vstxraid.sys
19:14:46.0368 0x1918  VSTXRAID - ok
19:14:46.0402 0x1918  [ BE970C369E43B509C1EDA2B8FA7CECB0,
18951F2AA842A0795AA79A4E164EE925A35E6270EBE4C4CDB19D0A891830E383 ] vwifibus
C:\WINDOWS\System32\drivers\vwifibus.sys
19:14:46.0472 0x1918  vwifibus - ok
19:14:46.0510 0x1918  [ 35BF5C5F5E3C9902C98978C7640574DA,
C61E50B04000DCEC72365723F0C0725C2E005529DAF2777A59E624C14DA29E55 ] vwififlt
C:\WINDOWS\system32\DRIVERS\vwififlt.sys
19:14:46.0573 0x1918  vwififlt - ok
19:14:46.0597 0x1918  [ 65ED7B9CFEA893DF7748D5FF692690DE,
73AB9D8BB928B3247BDFC7BB47AD7FCA763B375DC250C251DB4E0573531040E8 ] vwifimp
C:\WINDOWS\system32\DRIVERS\vwifimp.sys
19:14:46.0652 0x1918  vwifimp - ok
19:14:46.0705 0x1918  [ 7599E582CA3A6AAA95A18FFE1172D339,
A0410778FBBC4302EA91CF24B944427410B4706535F1192504D4F34C3ED4503E ] W32Time
C:\WINDOWS\system32\w32time.dll
19:14:46.0763 0x1918  W32Time - ok
19:14:46.0801 0x1918  [ 0910AB9ED404C1434E2D0376C2AD5D8B,
62585CA5F1375BDA440D28D5DF1ADDC9DE3DDFA196D49BBFF3456A5A09EE1C6B ] WacomPen
C:\WINDOWS\System32\drivers\wacompen.sys
19:14:46.0864 0x1918  WacomPen - ok
19:14:46.0919 0x1918  [ AFCD4054D61BD708B82991348ED1C763,
EBDAC0E218F1DFC405DB3C8A2F014D20A17B0690EA381C750BED5C2AFCDFEBE3 ] WANARP
C:\WINDOWS\system32\DRIVERS\wanarp.sys
19:14:46.0974 0x1918  WANARP - ok
19:14:46.0982 0x1918  [ AFCD4054D61BD708B82991348ED1C763,
EBDAC0E218F1DFC405DB3C8A2F014D20A17B0690EA381C750BED5C2AFCDFEBE3 ] Wanarpv6
C:\WINDOWS\system32\DRIVERS\wanarp.sys
19:14:47.0011 0x1918  Wanarpv6 - ok
19:14:47.0127 0x1918  [ 61692DB39AD3DF2F29392D68EAA7BB93,
854D4B9C7DD1676968598ED973500650ECEC02C420E44C0B3957C24F073AA5FB ] wbengine
C:\WINDOWS\system32\wbengine.exe
19:14:47.0276 0x1918  wbengine - ok
19:14:47.0337 0x1918  [ 3BC1D1D56637A32CD91C8AE08E2484AA,
9EE1BD3FB0D289E25F3DDD0D8F67DC1C701A6B1D5418FADF348D0E642B1DEBEB ] WbioSrvc
C:\WINDOWS\System32\wbiosrvc.dll
19:14:47.0436 0x1918  WbioSrvc - ok
19:14:47.0478 0x1918  [ A07CFC4B593D15B6BF06813C3B5B33BF,
B57BD918E2AFF9943B51A24B95E0C4D3482B4DF73C0E2421E8CC67C2BC7A4C70 ] Wcmsvc
C:\WINDOWS\System32\wcmsvc.dll
19:14:47.0563 0x1918  Wcmsvc - ok
19:14:47.0620 0x1918  [ D2726823DF7E19F213F4805A9D6D145F,
A7F582C99918D204264D3B374F70D75984BDA5805203041E3DECB8153D16E102 ] wcncsvc
C:\WINDOWS\System32\wcncsvc.dll
19:14:47.0711 0x1918  wcncsvc - ok
19:14:47.0727 0x1918  [ 846C02A8B48CBD921A3D6AB521AA0DC4,
B07573A774A6C65D24E5718DC25DF378270EB5B40221CA5A53B21D47838381D3 ] WcsPlugInService
C:\WINDOWS\System32\WcsPlugInService.dll
19:14:47.0784 0x1918  WcsPlugInService - ok
19:14:47.0830 0x1918  [ F5D4FA3E1F4879C361FFF3855259D2C2,
48C60FE4AAB011E2250157506FF0624031BFA346F8F2F8C6DFDF6F3CAA4F3F42 ] WdBoot
C:\WINDOWS\system32\drivers\WdBoot.sys
19:14:47.0874 0x1918  WdBoot - ok
19:14:47.0975 0x1918  [ CB6C63FF8342B467E2EF76E98D5B934D,
BE017CE91E3BAB293DE6ECF143797CCE3F33CC63024437472B4E38C6961AD884 ] Wdf01000
C:\WINDOWS\system32\drivers\Wdf01000.sys
19:14:48.0055 0x1918  Wdf01000 - ok
19:14:48.0086 0x1918  [ 019CC610AD95FF47EAD7C08B7A683B96,
BB9D42F8ED90ECA2E7B8C906E06A1EA859FAD9BD1B3492BB1E28C0D00004812A ] WdFilter
C:\WINDOWS\system32\drivers\WdFilter.sys
19:14:48.0137 0x1918  WdFilter - ok
19:14:48.0154 0x1918  [ 40C67D1A4891120874767F6E6604D6C5,
4D9DD658566DE711ADF4D6C33FCB31DA351EE050E3ED188664D04526CCAAEEF5 ] WdiServiceHost
C:\WINDOWS\system32\wdi.dll
19:14:48.0222 0x1918  WdiServiceHost - ok
19:14:48.0237 0x1918  [ 40C67D1A4891120874767F6E6604D6C5,
4D9DD658566DE711ADF4D6C33FCB31DA351EE050E3ED188664D04526CCAAEEF5 ] WdiSystemHost
C:\WINDOWS\system32\wdi.dll
19:14:48.0306 0x1918  WdiSystemHost - ok
19:14:48.0323 0x1918  [ 6CC1BB8F6851A262E2E824F0E92D5EEF,
45A88A984179BBA38C1F4434C4D6C2823C1FE6AFBE8CB0F656DAE0092D1D5611 ] WdNisDrv
C:\WINDOWS\system32\Drivers\WdNisDrv.sys
```

```
19:14:48.0346 0x1918  WdNisDrv - ok
19:14:48.0376 0x1918  WdNisSvc - ok
19:14:48.0414 0x1918  [ D261A12A43D33122CB90E70D3BC1CC68,
1B5237909CDD5DC4982599E94C2AAC37FEA6B1C282249DEB13E84A826C6E4B01 ] WebClient
C:\WINDOWS\System32\webclnt.dll
19:14:48.0511 0x1918  WebClient - ok
19:14:48.0570 0x1918  [ 3274312F263882B51B964329FAF49734,
99A020377ACF0762BE5ECD2D68EB5E1497B9D59963247E725F7F96FB5DF41FAD ] Wecsvc
C:\WINDOWS\system32\wecsvc.dll
19:14:48.0650 0x1918  Wecsvc - ok
19:14:48.0674 0x1918  [ 7CDD84E0023A0C5C230B06A7965EC65E,
6EC7DC18C76D66CF9A893C3DD20F9BE3ADD76546F9A9BA42CE4F24854709F9D9 ] WEPHOSTSVC
C:\WINDOWS\system32\wephostsvc.dll
19:14:48.0724 0x1918  WEPHOSTSVC - ok
19:14:48.0742 0x1918  [ 959534ACF085C137D2D094384EF89C45,
D029F440789FE170A1C46217C6DE6D78DC0188A5CF33FCCC17FA65D3BC80C2B7 ] wercplsupport
C:\WINDOWS\System32\wercplsupport.dll
19:14:48.0787 0x1918  wercplsupport - ok
19:14:48.0808 0x1918  [ 82BCCF5FBE47AC9E8CBA2020994DFB3F,
EA96C6BD98A701B465D0780EC10BDA92E45FE636D60C1385813AA3B456D8B931 ] WerSvc
C:\WINDOWS\System32\WerSvc.dll
19:14:48.0852 0x1918  WerSvc - ok
19:14:48.0897 0x1918  [ BFBE1C5F57FE7A885673A1962D5532B7,
F0BD05B257108699FE6AB32EF11F927C31932F27062A705B3FEFA4F5B4C0D8C3 ] WFPLWFS
C:\WINDOWS\system32\DRIVERS\wfplwfs.sys
19:14:48.0945 0x1918  WFPLWFS - ok
19:14:48.0970 0x1918  [ E06AFE2F94BA7CFA2FE4FD2A449E60E2,
99A81E16366E9E77905D873B0246E4C11B383FE1E99E0E1D9A07FAD4E52EA9E4 ] WiaRpc
C:\WINDOWS\System32\wiarpc.dll
19:14:49.0013 0x1918  WiaRpc - ok
19:14:49.0045 0x1918  [ 867BCC69ED9C31C501465EB0E8BA9DFA,
678B7FF4D4E86245143019560DA7FB451159BBFC83FF2E4E5E7DADAE3C7AB2EC ] WIMMount
C:\WINDOWS\system32\drivers\wimmount.sys
19:14:49.0073 0x1918  WIMMount - ok
19:14:49.0079 0x1918  WinDefend - ok
19:14:49.0156 0x1918  [ DD079EC8F44DCA3A176B345C6ADEFB66,
6CD9371B83EA23D2181891FAE1DB285BC111A78C35F374E57666ED09860C91A9 ]
WinHttpAutoProxySvc C:\WINDOWS\system32\winhttp.dll
19:14:49.0242 0x1918  WinHttpAutoProxySvc - ok
19:14:49.0295 0x1918  [ 9DB490F3E823C5C3C070644B96CB9D59,
81937D0B331E43C7C61514E60B3AD51370C5201F7B4D12F8534840D91EDC32DD ] Winmgmt
C:\WINDOWS\system32\wbem\WMIsvc.dll
19:14:49.0379 0x1918  Winmgmt - ok
19:14:49.0548 0x1918  [ C8D6344BDE2691A196E61C0D3372EAB7,
FF8EB79D8A7E298343C22B83276FF68293D08A9DA438BB22600BEFC4CA93A91D ] WinRM
C:\WINDOWS\system32\WsmSvc.dll
19:14:49.0714 0x1918  WinRM - ok
19:14:49.0854 0x1918  [ EF252510DB6C3511E30418BD2AC95A2D,
75B496F5C611129D9D19B382503830FDB0E2E61D4880D2821AE381DF578C5E56 ] WlanSvc
C:\WINDOWS\System32\wlansvc.dll
19:14:49.0999 0x1918  WlanSvc - ok
19:14:50.0130 0x1918  [ 5F56C0DE776C7AE43AF749845BFAA1EF,
837993C5853B7E682C7FB8401B7F5D951FFD15E5659EBB1B01DC3F5719ACEE19 ] wlidsvc
C:\WINDOWS\system32\wlidsvc.dll
19:14:50.0278 0x1918  wlidsvc - ok
19:14:50.0319 0x1918  [ 2834D9D3B4F554A39C72F00EA3F0E128,
D10124343C67FE9A0B711AD569BB8080495FCEA0ECEF9AC3F3FBD6865F436A44 ] WmiAcpi
C:\WINDOWS\System32\drivers\wmiacpi.sys
19:14:50.0390 0x1918  WmiAcpi - ok
19:14:50.0440 0x1918  [ 7AFAC828F52D62F304A911EC32F42EEE,
4EDCF4149069413A166169F2E23F7505F47B39B7EC319E1EF6D2C46CD140AA24 ] wmiApSrv
C:\WINDOWS\system32\wbem\WmiApSrv.exe
19:14:50.0501 0x1918  wmiApSrv - ok
19:14:50.0526 0x1918  WMPNetworkSvc - ok
19:14:50.0569 0x1918  [ 7FC5667DF73D4B04AA457CC3A4180E09,
CB7B014945DCA16B6D120DBE0E5876C4C867A4ACD3C3536AEADC14B908613D4E ] Wof
C:\WINDOWS\system32\drivers\Wof.sys
19:14:50.0619 0x1918  Wof - ok
19:14:50.0745 0x1918  [ 5071E71CC05346D88C5A08EB8B5A05E3,
EA2B14130EDD1846B2E25D310B0D49253CFB43C22D3DC7B3179DF7349CC4AEFB ] workfolderssvc
C:\WINDOWS\system32\workfolderssvc.dll
19:14:50.0907 0x1918  workfolderssvc - ok
19:14:50.0934 0x1918  [ 182561A14F2E93E81E66FE3700D17A5A,
FB9A06058A8BCCEDCDC5BF8899D9B2FBA5752C262C5FC6D2B8338884F3303D12 ] wpcfltr
C:\WINDOWS\system32\DRIVERS\wpcfltr.sys
19:14:50.0965 0x1918  wpcfltr - ok
```

```
19:14:51.0005 0x1918  [ 4E6A0F60DA7EF050D3D26417CD4D24E9,
E6B3BFB007B641D41F8532ED086F92CB3D86E210023DBFAA9AD8152A9FD33CCA ] WPCSvc
C:\WINDOWS\System32\wpcsvc.dll
19:14:51.0054 0x1918  WPCSvc - ok
19:14:51.0073 0x1918  [ D27491CFCE452C154CECFA155AD0EBC8,
1F3F74C253E3B07DE7EFE27C34DD9AF08617C7B03BB44C2902F69BA9DA3F21F2 ] WPDBusEnum
C:\WINDOWS\system32\wpdbusenum.dll
19:14:51.0114 0x1918  WPDBusEnum - ok
19:14:51.0153 0x1918  [ 9F2904B55F6CECCD1A8D986B5CE2609A,
E19ED4DD3CEF3A22C058FC324824604FB3FC98A029C94E6C2A3389F938D680B6 ] WpdUpFltr
C:\WINDOWS\system32\drivers\WpdUpFltr.sys
19:14:51.0185 0x1918  WpdUpFltr - ok
19:14:51.0226 0x1918  [ AE072B0339D0A18E455DC21666CAD572,
AB1DAEA25E2C7AD610818D4B4783F6D4190D85EBB3963BBAD410E8CEA7899EDB ] ws2ifsl
C:\WINDOWS\system32\drivers\ws2ifsl.sys
19:14:51.0290 0x1918  ws2ifsl - ok
19:14:51.0331 0x1918  [ 9654DE19551093CD73874281E1573C94,
5E3513EC0CB180D90904BE8970AB64A4434279E8C467AE2CF693254E47B1D11E ] wscsvc
C:\WINDOWS\System32\wscsvc.dll
19:14:51.0414 0x1918  wscsvc - ok
19:14:51.0424 0x1918  WSearch - ok
19:14:51.0546 0x1918  [ 95B6670E6933E1DEE19686C55BE709A0,
4B9EB8F1712B7959A71F6DA445D29BD09B25EEFC6B30D736EFE30163D79B233E ] WSService
C:\WINDOWS\System32\WSService.dll
19:14:51.0712 0x1918  WSService - ok
19:14:51.0884 0x1918  [ E66AC3CA92FC471BFE69F61549193A64,
E2DD7EA4ED164EE8FB07546896BE743734B04DE4C9480E84231901CB2C63F31C ] wuauserv
C:\WINDOWS\system32\wuaueng.dll
19:14:52.0147 0x1918  wuauserv - ok
19:14:52.0183 0x1918  [ D537815E450A149752C15868392AD1F3,
8788CE493349299DB36E409C8CC3C6EA08301FA492C95D9D556E00BC13A05F13 ] WudfPf
C:\WINDOWS\system32\drivers\WudfPf.sys
19:14:52.0252 0x1918  WudfPf - ok
19:14:52.0295 0x1918  [ 7CCBBCEE408A5DBE3FE47297DB5A6CFC,
FB44B65B37B1C1A12C618E16BEF195EF861A87179B9216E43024C671C3AE052C ] WUDFRd
C:\WINDOWS\System32\drivers\WUDFRd.sys
19:14:52.0374 0x1918  WUDFRd - ok
19:14:52.0396 0x1918  [ 7CCBBCEE408A5DBE3FE47297DB5A6CFC,
FB44B65B37B1C1A12C618E16BEF195EF861A87179B9216E43024C671C3AE052C ] WUDFSensorLP
C:\WINDOWS\system32\DRIVERS\WUDFRd.sys
19:14:52.0443 0x1918  WUDFSensorLP - ok
19:14:52.0456 0x1918  [ 9CDC2059A23E3C9B57696178508777E7,
B680A2E2EDA5C8C6A547E7D9B2F2F8E6407C3EA0A01B82A4B88D48A27913A597 ] wudfsvc
C:\WINDOWS\System32\WUDFSvc.dll
19:14:52.0505 0x1918  wudfsvc - ok
19:14:52.0524 0x1918  [ 7CCBBCEE408A5DBE3FE47297DB5A6CFC,
FB44B65B37B1C1A12C618E16BEF195EF861A87179B9216E43024C671C3AE052C ] WUDFWpdFs
C:\WINDOWS\system32\DRIVERS\WUDFRd.sys
19:14:52.0570 0x1918  WUDFWpdFs - ok
19:14:52.0643 0x1918  [ 2FA9794CA36147756F3FDFD6CA29B46F,
4B86DC38C2411C281686E9A4E64DA6FB2992E39391371F78E012D6D8BB85123F ] WwanSvc
C:\WINDOWS\System32\wwansvc.dll
19:14:52.0707 0x1918  WwanSvc - ok
19:14:52.0729 0x1918  ================ Scan global ================================
19:14:52.0757 0x1918  [ C89780A6F58D113C28A96D85D1261DC5,
185114F33A60916C7904E4A0F278CA43258454343E614F01F0DAFA98BAC981B1 ]
C:\WINDOWS\system32\basesrv.dll
19:14:52.0800 0x1918  [ 00DD4D2ACC2E72155A8AAA82018BEC0D,
9D7CA68B4A81240477FCC85A3CC11EF986093F9D6228A6C5AC608EDAD664068C ]
C:\WINDOWS\system32\winsrv.dll
19:14:52.0855 0x1918  [ 9C1833ABD62876856836C5AE55C7CE86,
0A21E2C8B2FF3B0438C86DA7151A548F9C6F5C62CD402CBBEDB435994C8508F1 ]
C:\WINDOWS\system32\sxssrv.dll
19:14:52.0933 0x1918  [ 067CB90C277DB4A737D5DEABA3055972,
C681BF013170F2D92A3FC4D783FC3F200CDC0C8173373B7ECC27FCF32A03CCBD ]
C:\WINDOWS\system32\services.exe
19:14:52.0974 0x1918  [ Global ] - ok
19:14:52.0976 0x1918  ================ Scan MBR ===================================
19:14:52.0992 0x1918  [ 5FB38429D5D77768867C76DCBDB35194 ] \Device\Harddisk0\DR0
19:14:53.0096 0x1918  \Device\Harddisk0\DR0 - ok
19:14:53.0098 0x1918  ================ Scan VBR ===================================
19:14:53.0134 0x1918  [ A4F1353F78116103346169DEF2E303F4 ]
\Device\Harddisk0\DR0\Partition1
19:14:53.0155 0x1918  \Device\Harddisk0\DR0\Partition1 - ok
19:14:53.0174 0x1918  [ 574B8917774FC73C2B5574488C70B4D5 ]
\Device\Harddisk0\DR0\Partition2
```

```
19:14:53.0192 0x1918  \Device\Harddisk0\DR0\Partition2 - ok
19:14:53.0209 0x1918  [ A3A70E1C29475B441BF40BDA5866EAE7 ]
\Device\Harddisk0\DR0\Partition3
19:14:53.0210 0x1918  \Device\Harddisk0\DR0\Partition3 - ok
19:14:53.0219 0x1918  [ EDF67D28A20E5EDEE18025069AFD5481 ]
\Device\Harddisk0\DR0\Partition4
19:14:53.0233 0x1918  \Device\Harddisk0\DR0\Partition4 - ok
19:14:53.0269 0x1918  [ AE06EE77B33416824F52F2BB1F8EA968 ]
\Device\Harddisk0\DR0\Partition5
19:14:53.0283 0x1918  \Device\Harddisk0\DR0\Partition5 - ok
19:14:53.0298 0x1918  [ 4F51520F3996DEDADED0DBB11500B9EF ]
\Device\Harddisk0\DR0\Partition6
19:14:53.0314 0x1918  \Device\Harddisk0\DR0\Partition6 - ok
19:14:53.0316 0x1918  ================ Scan generic autorun ======================
19:14:53.0370 0x1918  [ 28062B17191C9450BF6C6C3EF8C7EB27,
4859C5708DFD119021F7B7FFB38F0B316675E1E4D5D51A10D4265F712CF8CDB6 ]
C:\WINDOWS\system32\igfxtray.exe
19:14:53.0413 0x1918  IgfxTray - ok
19:14:53.0444 0x1918  [ 28FC280487F0BAAE5E8119257C4EEF8C,
F574BC70B79B77912FC683B3EB0BE6929E7758284ED5B47008E18B0E4A4A09FD ]
C:\WINDOWS\system32\hkcmd.exe
19:14:53.0476 0x1918  HotKeysCmds - ok
19:14:53.0505 0x1918  [ F29BEA821C753E4F00177690F70CDC13,
0EDB40F4A4C23553C0288E6E3AD65E7B523F6764C87C6C36C3ECB0C1940C5176 ]
C:\WINDOWS\system32\igfxpers.exe
19:14:53.0530 0x1918  Persistence - ok
19:14:53.0619 0x1918  [ 24F37B2CB893109EE4654BBE62E82C5F,
77EA72014B2100BF50DCA81FAFCA7A17952E5A0D56564E5D5406BAC62A31F05B ] C:\Program
Files\Apoint2K\Apoint.exe
19:14:53.0659 0x1918  Apoint - ok
19:14:54.0173 0x1918  [ B0666DF6D554879AE8A7C91E26A5972F,
81112CFA81E26C388D36F0472A4983728AFE4C4C04910849AF22C191E206CF39 ] C:\Program
Files\Realtek\Audio\HDA\RAVCpl64.exe
19:14:54.0613 0x1918  RtHDVCpl - ok
19:14:54.0662 0x1918  [ 5E53A66C680A06E26B1234CB0C3CD99B,
D782E724FF487459704BFA2BC5BA5E6E7E85BC9D71ECF68BE78F9C74449EB207 ] C:\Program
Files\Realtek\Audio\HDA\RAVBg64.exe
19:14:54.0736 0x1918  RtHDVBg_Dolby - ok
19:14:54.0788 0x1918  [ 59D8F3E319A61E98EED5362FEAFED7EF,
54FEE193634F35A5B3B144CDF32E1FBDC79DA9645603356A8C7F5681FA243D12 ] C:\Program Files
(x86)\Qualcomm Atheros\Bluetooth Suite\BtPreLoad.exe
19:14:54.0820 0x1918  BtPreLoad - ok
19:14:54.0891 0x1918  [ 564765F1F68BBFA26CAC8F89662F106B,
AA7A3CD8C3515E824DE10390852538BAAF998421ABA4F1E4CA967CC451DE493D ] C:\Program
Files\Common Files\Common Desktop Agent\CDASrv.exe
19:14:54.0942 0x1918  CDAServer - detected UnsignedFile.Multi.Generic ( 1 )
19:14:54.0942 0x1918  CDAServer ( UnsignedFile.Multi.Generic ) - warning
19:14:57.0423 0x1918  [ 50D1476C84446135A990F4939DC2DC1D,
D062F92863E32EC075BD672F3C185CE8C9329F8B679D5508C396131B1DB30EF7 ] C:\Dolby
PCEE4\pcee4.exe
19:14:57.0465 0x1918  Dolby Home Theater v4 - ok
19:14:57.0564 0x1918  [ 61E4289E91E88C90478D7F4BEB10DCF7,
1D0F4034E0111CF5758F470C15A22A0A28EB8269CB5BF07222C9C0FB07A15C55 ] C:\Program Files
(x86)\Common Files\Apple\Apple Application Support\APSDaemon.exe
19:14:57.0601 0x1918  APSDaemon - ok
19:14:57.0856 0x1918  [ 048EA4B978851788E9F5E8E4F081DF7A,
EB62719AC0DCC18FF056F2CD84438BF14B61E38F0619617C81961C6257BDFCEC ] C:\Program Files
(x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
19:14:57.0915 0x1918  Adobe ARM - ok
19:14:58.0431 0x1918  [ 26B558B2D31C7425B455B00E562EAD93,
B64D128A2F1FC42BA4376F8EB08D70F4B705745CB983D0631DB45851BF34BBDF ] C:\Program
Files\AVAST Software\Avast\AvastUI.exe
19:14:58.0802 0x1918  AvastUI.exe - ok
19:14:59.0737 0x1918  [ 5D38814FF2F1A79F5BB41056C82FA3C3,
8A82A2C82286E32DF72E956A74058A7B32F130DEF481A9BF58209C08B2BD94F5 ] C:\Program
Files\Start Menu X\StartMenuX.exe
19:14:59.0941 0x1918  StartMenuX - ok
19:15:00.0203 0x1918  [ AEA1A710A52E3990FC1FD38ABAAFA77D,
A7EB15929856874CA2CB24937AC34904F338971AD94AD84E738A8509D39B18AC ] C:\Program Files
(x86)\Garmin\Express Tray\ExpressTray.exe
19:15:00.0269 0x1918  GarminExpressTrayApp - ok
19:15:00.0340 0x1918  AV detected via SS2: McAfee Antivirus en antispyware,
C:\Program Files\McAfee.com\Agent\mcupdate.exe (  ), 0x50000 ( disabled : updated )
19:15:00.0405 0x1918  AV detected via SS2: Windows Defender, C:\Program
Files\Windows Defender\MSASCui.exe ( 4.5.218.0 ), 0x60100 ( disabled : updated )
19:15:00.0416 0x1918  AV detected via SS2: avast! Antivirus, C:\Program Files\AVAST
```

```
Software\Avast\VisthAux.exe ( 9.0.2021.515 ), 0x41000 ( enabled : updated )
19:15:00.0420 0x1918  FW detected via SS2: McAfee Firewall, C:\Program
Files\McAfee.com\Agent\mcupdate.exe (  ), 0x50010 ( disabled )
19:15:00.0429 0x1918  Win FW state via NFP2: enabled
19:15:02.0792 0x1918  ============================================================
19:15:02.0792 0x1918  Scan finished
19:15:02.0792 0x1918  ============================================================
19:15:02.0812 0x0aec  Detected object count: 2
19:15:02.0812 0x0aec  Actual detected object count: 2
19:20:44.0332 0x0aec  RapportMgmtService ( ForgedFile.Multi.Generic ) - skipped by
user
19:20:44.0332 0x0aec  RapportMgmtService ( ForgedFile.Multi.Generic ) - User select
action: Skip
19:20:44.0333 0x0aec  CDAServer ( UnsignedFile.Multi.Generic ) - skipped by user
19:20:44.0333 0x0aec  CDAServer ( UnsignedFile.Multi.Generic ) - User select action:
Skip
```