

# ComboFix

ComboFix 14-04-09.02 - srhutsell 04/10/2014 3:09.1.4 - x64  
 Microsoft Windows 7 Home Premium 6.1.7601.1.1252.1.1033.18.4863.2603 [GMT -4:00]  
 Running from: c:\users\srhutsell\Desktop\ComboFix.exe  
 AV: avast! Antivirus \*Disabled/Updated\* {17AD7D40-BA12-9C46-7131-94903A54AD8B}  
 SP: avast! Antivirus \*Disabled/Updated\* {ACCC9CA4-9C28-93C8-4B81-AFE241D3E736}  
 SP: Windows Defender \*Enabled/Updated\* {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}  
 \* Created a new restore point

(((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((( Other Deletions  
 ))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))

c:\install.exe

(((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((( Files Created from 2014-03-10 to 2014-04-10  
 ))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))

|                                                             |          |           |            |
|-------------------------------------------------------------|----------|-----------|------------|
| 2014-04-10 07:14 . 2014-04-10 07:14                         | -----    | d-----w-  |            |
| c:\users\Default\AppData\Local\temp                         |          |           |            |
| 2014-04-10 07:14 . 2014-04-10 07:14                         | -----    | d-----w-  |            |
| c:\users\ahutse112001\AppData\Local\temp                    |          |           |            |
| 2014-04-10 07:14 . 2014-04-10 07:14                         | -----    | d-----w-  |            |
| c:\users\Admin\AppData\Local\temp                           |          |           |            |
| 2014-04-10 06:20 . 2014-04-10 06:20                         | 75888    | -----a-w- |            |
| c:\programdata\Microsoft\Windows Defender\Definition        |          |           |            |
| Updates\{03D5D204-D9B6-4177-B9B2-95ED85032566}\offreg.dll   |          |           |            |
| 2014-04-09 09:03 . 2014-04-09 09:03                         | -----    | d-----w-  |            |
| c:\windows\LastGood                                         |          |           |            |
| 2014-04-09 08:59 . 2014-04-09 08:59                         | -----    | d-----w-  |            |
| c:\users\srhutsell\AppData\Local\ElevatedDiagnostics        |          |           |            |
| 2014-04-08 05:29 . 2013-11-11 14:58                         | 4900568  | -----a-w- |            |
| c:\programdata\cis26F0.exe                                  |          |           |            |
| 2014-04-06 08:54 . 2014-04-06 08:54                         | -----    | d-----w-  | c:\program |
| files (x86)\NirSoft                                         |          |           |            |
| 2014-04-06 07:53 . 2014-04-06 07:53                         | 43152    | -----a-w- |            |
| c:\windows\avastSS.scr                                      |          |           |            |
| 2014-04-04 05:59 . 2014-03-07 04:43                         | 10521840 | -----a-w- |            |
| c:\programdata\Microsoft\Windows Defender\Definition        |          |           |            |
| Updates\{03D5D204-D9B6-4177-B9B2-95ED85032566}\mpengine.dll |          |           |            |
| 2014-03-12 05:55 . 2014-02-04 02:32                         | 624128   | -----a-w- |            |
| c:\windows\system32\qedit.dll                               |          |           |            |
| 2014-03-12 05:55 . 2014-02-04 02:04                         | 509440   | -----a-w- |            |
| c:\windows\SysWow64\qedit.dll                               |          |           |            |
| 2014-03-12 05:55 . 2014-02-04 02:32                         | 1424384  | -----a-w- |            |
| c:\windows\system32\WindowsCodecs.dll                       |          |           |            |
| 2014-03-12 05:55 . 2014-02-04 02:04                         | 1230336  | -----a-w- |            |
| c:\windows\SysWow64\WindowsCodecs.dll                       |          |           |            |

(((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((( Find3M Report  
 ))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))

|                                           |        |           |  |
|-------------------------------------------|--------|-----------|--|
| 2014-04-06 08:14 . 2013-07-14 18:31       | 71048  | -----a-w- |  |
| c:\windows\SysWow64\FlashPlayerCPLApp.cp1 |        |           |  |
| 2014-04-06 08:14 . 2013-07-14 18:31       | 692616 | -----a-w- |  |
| c:\windows\SysWow64\FlashPlayerApp.exe    |        |           |  |
| 2014-04-06 07:53 . 2013-12-25 04:07       | 84816  | -----a-w- |  |
| c:\windows\system32\drivers\aswstm.sys    |        |           |  |
| 2014-04-06 07:53 . 2013-07-10 00:57       | 423240 | -----a-w- |  |

# ComboFix

```

c:\windows\system32\drivers\aswSP.sys
2014-04-06 07:53 . 2013-07-10 00:57 208928 ----a-w-
c:\windows\system32\drivers\aswVmm.sys
2014-04-06 07:53 . 2013-07-10 00:57 1039096 ----a-w-
c:\windows\system32\drivers\aswSnx.sys
2014-04-06 07:53 . 2013-07-10 00:57 65776 ----a-w-
c:\windows\system32\drivers\aswRvrt.sys
2014-04-06 07:53 . 2013-07-10 00:57 79184 ----a-w-
c:\windows\system32\drivers\aswMonFlt.sys
2014-04-06 07:53 . 2013-07-10 00:57 334648 ----a-w-
c:\windows\system32\aswBoot.exe
2014-04-06 07:53 . 2013-07-10 00:57 93568 ----a-w-
c:\windows\system32\drivers\aswRdr2.sys
2014-03-19 07:00 . 2013-07-10 04:03 90015360 ----a-w-
c:\windows\system32\MRT.exe

```

----- Sigcheck -----

Note: Unsigned files aren't necessarily malware.

```

[7] 2009-07-14 . 02062C0B390B7729EDC9E69C680A6F3C . 24128 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_mshdc.inf_31bf3856ad364e35_6.1.7600.16385_none_392d19c13b3ad
543\atapi.sys
[7] 2009-07-14 . 02062C0B390B7729EDC9E69C680A6F3C . 24128 . . [6.1.7600.16385] ..
c:\windows\system32\drivers\atapi.sys

[7] 2009-07-14 . 769765CE2CC62867468CEA93969B2242 . 23040 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-rasbase-asynctmac_31bf3856ad364e35_6.1.7600
.16385_none_804cc08a4e8a4516\asynctmac.sys
[7] 2009-07-14 . 769765CE2CC62867468CEA93969B2242 . 23040 . . [6.1.7600.16385] ..
c:\windows\system32\drivers\asynctmac.sys

[7] 2009-07-14 . BC02336F1CBA7DCC7D1213BB588A68A5 . 50768 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_keyboard.inf_31bf3856ad364e35_6.1.7600.16385_none_f3435f7ff2
a9f325\kbdclass.sys
[7] 2009-07-14 . BC02336F1CBA7DCC7D1213BB588A68A5 . 50768 . . [6.1.7601.17514] ..
c:\windows\system32\drivers\kbdclass.sys

[7] 2012-08-22 . 760E38053BF56E501D562B70AD796B88 . 950128 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-ndis_31bf3856ad364e35_6.1.7601.17939_none_
05dc9a6832ba428a\ndis.sys
[7] 2012-08-22 . 760E38053BF56E501D562B70AD796B88 . 950128 . . [6.1.7600.16385] ..
c:\windows\system32\drivers\ndis.sys

[7] 2013-04-12 . B98F8C6E31CD07B2E6F71F7F648E38C0 . 1656680 . . [6.1.7601.18127] ..
c:\windows\winsxs\amd64_microsoft-windows-ntfs_31bf3856ad364e35_6.1.7601.18127_none_
048f41be3390b0cf\ntfs.sys
[7] 2013-04-12 . B98F8C6E31CD07B2E6F71F7F648E38C0 . 1656680 . . [6.1.7600.16385] ..
c:\windows\system32\drivers\ntfs.sys

[7] 2009-07-13 . 9899284589F75FA8724FF3D16AED75C1 . 6144 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-null_31bf3856ad364e35_6.1.7600.16385_none_
055adf2434ae116e\null.sys
[7] 2009-07-13 . 9899284589F75FA8724FF3D16AED75C1 . 6144 . . [6.1.7600.16385] ..
c:\windows\system32\drivers\null.sys

[7] 2013-11-26 . F55B41AA6114568AC558ADBABDA85620 . 1897408 . . [6.1.7601.22525] ..
c:\windows\winsxs\amd64_microsoft-windows-tcpip-binaries_31bf3856ad364e35_6.1.7601.2
2525_none_11c3cc3c962abcc3\tcpip.sys
[7] 2013-09-08 . 40AF23633D197905F03AB5628C558C51 . 1903552 . . [6.1.7600.16385] ..
c:\windows\system32\drivers\tcpip.sys

[7] 2010-11-20 . DDAD5A7AB24D8B65F8D724F5C20FD806 . 119296 . . [6.1.7601.17514] ..

```

# ComboFix

```

c:\windows\winsxs\amd64_microsoft-windows-tdi-over-tcpip_31bf3856ad364e35_6.1.7601.1
7514_none_4863cdbaf2b532f8\tdx.sys
[7] 2009-07-13 . 079125C4B17B01FCAEEBCE0BCB290C0F . 99840 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-tdi-over-tcpip_31bf3856ad364e35_6.1.7600.1
6385_none_4632b9f2f5c6af5e\tdx.sys
[7] 2010-11-20 . DDAD5A7AB24D8B65F8D724F5C20FD806 . 119296 . . [6.1.7601.17514] ..
c:\windows\system32\drivers\tdx.sys
.
[7] 2012-07-04 . 00A7A2067E9822E4626DE846574ADA80 . 136704 . . [6.1.7600.21256] ..
c:\windows\winsxs\amd64_microsoft-windows-browserservice_31bf3856ad364e35_6.1.7600.2
1256_none_d5890aa5d0b400b5\browser.dll
[7] 2012-07-04 . 05F5A0D14A2EE1D8255C2AA0E9E8E694 . 136704 . . [6.1.7601.17887] ..
c:\windows\winsxs\amd64_microsoft-windows-browserservice_31bf3856ad364e35_6.1.7601.1
7887_none_d6c68344b4d406bf\browser.dll
[7] 2012-07-04 . 156768ABAE1DAF29BA0B0C05C21FEF09 . 136704 . . [6.1.7601.22044] ..
c:\windows\winsxs\amd64_microsoft-windows-browserservice_31bf3856ad364e35_6.1.7601.2
2044_none_d7783703cdd41e02\browser.dll
[7] 2012-07-04 . 6B054C67AAA87843504E8E3C09102009 . 136704 . . [6.1.7600.17056] ..
c:\windows\winsxs\amd64_microsoft-windows-browserservice_31bf3856ad364e35_6.1.7600.1
7056_none_d4ff6bf4b79663c4\browser.dll
[7] 2010-11-20 . 8EF0D5C41EC907751B8429162B1239ED . 136192 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-browserservice_31bf3856ad364e35_6.1.7601.1
7514_none_d70f2c28b49dffae\browser.dll
[7] 2009-07-14 . 94FBC06F294D58D02361918418F996E3 . 136192 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-browserservice_31bf3856ad364e35_6.1.7600.1
6385_none_d4de1860b7af7c14\browser.dll
[7] 2012-07-04 . 05F5A0D14A2EE1D8255C2AA0E9E8E694 . 136704 . . [6.1.7600.16385] ..
c:\windows\system32\browser.dll
.
[7] 2013-09-25 . F021DAFB1F87616FCEBA159C2ED7042F . 30720 . . [6.1.7601.22465] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7601.22465_none_0
4c503168cb026a0\lsass.exe
[7] 2013-09-25 . 4D71227301DD8D09097B9E4CC6527E5A . 30720 . . [6.1.7601.18270] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7601.18270_none_0
42b9307739f26ed\lsass.exe
[7] 2012-08-24 . 77119F1F9B492B260030C34F9BE327FA . 31232 . . [6.1.7601.22099] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7601.22099_none_0
4a88ce28cc4eb33\lsass.exe
[7] 2012-06-04 . 79C908CAA6F43021EB05F4C733A927D1 . 31232 . . [6.1.7601.22010] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7601.22010_none_0
4f609a88c8c279c\lsass.exe
[7] 2012-06-02 . BF63CE11A25F3509129888710D5111FC . 31232 . . [6.1.7600.21225] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7600.21225_none_0
309de288f695654\lsass.exe
[7] 2011-11-17 . 156F6159457D0AA7E59B62681B56EB90 . 31232 . . [6.1.7600.16915] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7600.16915_none_0
28b374176436a30\lsass.exe
[7] 2011-11-17 . 156F6159457D0AA7E59B62681B56EB90 . 31232 . . [6.1.7600.16915] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7600.17035_none_0
2756f8b7653d554\lsass.exe
[7] 2011-11-17 . D21BD47E528CD62E79311FB5DF0150E6 . 31232 . . [6.1.7600.21092] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7600.21092_none_0
2bb2a0a8fa4d398\lsass.exe
[7] 2011-11-17 . C118A82CD78818C29AB228366EBF81C3 . 31232 . . [6.1.7601.17725] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7601.17725_none_0
466c45b7371f20d\lsass.exe
[7] 2011-11-17 . C118A82CD78818C29AB228366EBF81C3 . 31232 . . [6.1.7601.17725] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7601.17856_none_0
44756c773895c5e\lsass.exe
[7] 2011-11-17 . C118A82CD78818C29AB228366EBF81C3 . 31232 . . [6.1.7601.17725] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7601.17940_none_0
44c26dd7386a58a\lsass.exe
[7] 2011-11-17 . 0A10B74FBB437FF9A23F1D5DE4446A83 . 31232 . . [6.1.7601.21861] ..

```

# ComboFix

```

c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7601.21861_none_0
4c1204e8cb39c3f\lsass.exe
[7] 2009-07-14 . 0793F40B9B8A1BDD266296409DBD91EA . 31232 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7600.16385_none_0
23f7c69767c3edd\lsass.exe
[7] 2009-07-14 . 0793F40B9B8A1BDD266296409DBD91EA . 31232 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7600.16484_none_0
23e7e05767d22ad\lsass.exe
[7] 2009-07-14 . 0793F40B9B8A1BDD266296409DBD91EA . 31232 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7600.20594_none_0
2bd4ae48fa2de68\lsass.exe
[7] 2009-07-14 . 0793F40B9B8A1BDD266296409DBD91EA . 31232 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-lsa_31bf3856ad364e35_6.1.7601.17514_none_0
4709031736ac277\lsass.exe
[7] 2013-09-25 . 4D71227301DD8D09097B9E4CC6527E5A . 30720 . . [6.1.7601.18270] ..
c:\windows\system32\lsass.exe

[7] 2009-07-14 . 847D3AE376C0817161A14A82C8922A9E . 360448 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-netman_31bf3856ad364e35_6.1.7600.16385_non
e_6bb20d3d6b80d9da\netman.dll
[7] 2009-07-14 . 847D3AE376C0817161A14A82C8922A9E . 360448 . . [6.1.7600.16385] ..
c:\windows\system32\netman.dll

[7] 2010-11-20 . 1EA7969E3271CBC59E1730697DC74682 . 849920 . . [7.5.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-bits-client_31bf3856ad364e35_6.1.7601.1751
4_none_81b6ca5c101195cd\qmgr.dll
[7] 2009-07-14 . 7F0C323FE3DA28AA4AA1BDA3F575707F . 848384 . . [7.5.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-bits-client_31bf3856ad364e35_6.1.7600.1638
5_none_7f85b69413231233\qmgr.dll
[7] 2010-11-20 . 1EA7969E3271CBC59E1730697DC74682 . 849920 . . [7.5.7600.16385] ..
c:\windows\system32\qmgr.dll

[7] 2010-11-20 . 5C627D1B1138676C0A7AB2C2C190D123 . 512000 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-com-base-qfe-rpcss_31bf3856ad364e35_6.1.76
01.17514_none_c7f0e16b547f887d\rpcss.dll
[7] 2009-07-14 . 7266972E86890E2B30C0C322E906B027 . 509440 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-com-base-qfe-rpcss_31bf3856ad364e35_6.1.76
00.16385_none_c5bfcd3579104e3\rpcss.dll
[7] 2010-11-20 . 5C627D1B1138676C0A7AB2C2C190D123 . 512000 . . [6.1.7601.17514] ..
c:\windows\system32\rpcss.dll

[7] 2009-07-14 . 24ACB7E5BE595468E3B9AA488B9B4FCB . 328704 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-s.s-servicecontroller_31bf3856ad364e35_6.
1.7600.16385_none_2b54b20ee6fa07b1\services.exe
[7] 2009-07-14 . 24ACB7E5BE595468E3B9AA488B9B4FCB . 328704 . . [6.1.7600.16385] ..
c:\windows\system32\services.exe

[7] 2012-02-11 . 85DAA09A98C9286D4EA2BA8D0E644377 . 559104 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-core_31bf3856ad364e35_6.1
.7601.17777_none_3433cdb2d8563d50\spoolsv.exe
[7] 2012-02-11 . 567977DC43CC13C4C35ED7084C0B84D5 . 559104 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-core_31bf3856ad364e35_6.1
.7600.16962_none_32533f26db2c36c0\spoolsv.exe
[7] 2012-02-11 . 807B5B0E287027F72AC37B0CDA9512DA . 559104 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-core_31bf3856ad364e35_6.1
.7600.21149_none_32f955f1f433834b\spoolsv.exe
[7] 2012-02-11 . B9D7A4858CF32A6A15D2763F1DE47E0E . 559616 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-core_31bf3856ad364e35_6.1
.7601.21921_none_34ed7a43f150b682\spoolsv.exe
[7] 2010-11-20 . B96C17B5DC1424D56EEA3A99E97428CD . 559104 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-core_31bf3856ad364e35_6.1
.7601.17514_none_3471a890d8284f57\spoolsv.exe
[7] 2010-08-21 . F8E1FA03CB70D54A9892AC88B91D1E7B . 558592 . . [6.1.7600.16385] ..

```

# ComboFix

```

c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-core_31bf3856ad364e35_6.1.7600.16661_none_3252392adb2d25f4\spoolsv.exe
[7] 2010-08-20 . 8547491BE7086EE317163365D83A37D2 . 559104 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-core_31bf3856ad364e35_6.1.7600.20785_none_32ca3745f45762fc\spoolsv.exe
[7] 2009-07-14 . 89E8550C5862999FCF482EA562B0E98E . 558080 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-core_31bf3856ad364e35_6.1.7600.16385_none_324094c8db39cbbd\spoolsv.exe
[7] 2012-02-11 . 85DAA09A98C9286D4EA2BA8D0E644377 . 559104 . . [6.1.7600.16385] ..
c:\windows\system32\spoolsv.exe

[7] 2010-11-20 . 1151B1BAA6F350B1DB6598E0FEA7C457 . 390656 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-winlogon_31bf3856ad364e35_6.1.7601.17514_n
one_cde90685eb910636\winlogon.exe
[7] 2009-10-28 . A93D41A4D4B0D91C072D11DD8AF266DE . 389632 . . [6.1.7600.20560] ..
c:\windows\winsxs\amd64_microsoft-windows-winlogon_31bf3856ad364e35_6.1.7600.20560_n
one_cc522fd507b468f8\winlogon.exe
[7] 2009-10-28 . DA3E2A6FA9660CC75B471530CE88453A . 389632 . . [6.1.7600.16447] ..
c:\windows\winsxs\amd64_microsoft-windows-winlogon_31bf3856ad364e35_6.1.7600.16447_n
one_cbe534e7ee8042ad\winlogon.exe
[7] 2009-07-14 . 132328DF455B0028F13BF0ABEE51A63A . 389120 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-winlogon_31bf3856ad364e35_6.1.7600.16385_n
one_cbb7f2bdeea2829c\winlogon.exe
[7] 2010-11-20 . 1151B1BAA6F350B1DB6598E0FEA7C457 . 390656 . . [6.1.7601.17514] ..
c:\windows\system32\winlogon.exe

[7] 2012-06-02 . C1C03EA437EDDA8A7D4D8786E5AE6751 . 57880 . . [7.6.7600.256] ..
c:\windows\winsxs\amd64_microsoft-windows-w..wsupdateclient-core_31bf3856ad364e35_7.
6.7600.256_none_d5f513f25190f276\wuauclt.exe
[7] 2010-11-20 . 7FBFAA84FE176D9AE932ABC585AB68D5 . 51200 . . [7.5.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-w..wsupdateclient-core_31bf3856ad364e35_7.
5.7601.17514_none_1f3413afc64d10c5\wuauclt.exe
[7] 2009-07-14 . 0C12A2B863FEA45598134E3B6E379F88 . 51200 . . [7.3.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w..wsupdateclient-core_31bf3856ad364e35_7.
3.7600.16385_none_8ca5655e8bc7dae9\wuauclt.exe
[7] 2012-06-02 . C1C03EA437EDDA8A7D4D8786E5AE6751 . 57880 . . [7.6.7600.256] ..
c:\windows\system32\wuauclt.exe

[7] 2013-07-04 . 9028D1621C43DF8DFBD1C76860412A11 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.760
1.18201_none_97c9d703ee91c7f1\comctl32.dll
[7] 2013-07-04 . 9028D1621C43DF8DFBD1C76860412A11 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601
.18201_none_a4d3b9377117c3df\comctl32.dll
[7] 2013-07-04 . 4F3C5CE9EF990E1C62B7E7EBA0EBA1C2 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.760
1.22376_none_980cc5cd07e3aa05\comctl32.dll
[7] 2013-07-04 . 4F3C5CE9EF990E1C62B7E7EBA0EBA1C2 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601
.22376_none_a6ba9bf96e3dcd13\comctl32.dll
[7] 2010-11-20 . 14DFDEAF4E589ED3F1FF187A86B9408C . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.760
1.17514_none_97c2246fee970dbb\comctl32.dll
[7] 2010-11-20 . 14DFDEAF4E589ED3F1FF187A86B9408C . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601
.17514_none_a4d6a923711520a9\comctl32.dll
[7] 2010-11-20 . 7FA8FDC2C2A27817FD0F624E78D3B50C . 2030080 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.
17514_none_fa396087175ac9ac\comctl32.dll
[7] 2010-08-24 . B0CB1D2D5FFA6335DD94B1B531756412 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.760
0.20787_none_961cb3b90ac4540e\comctl32.dll
[7] 2010-08-24 . B0CB1D2D5FFA6335DD94B1B531756412 . 633856 . . [5.82] ..

```

# ComboFix

```

c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7600
.20787_none_a6357652551c0c2c\comctl32.dll
[7] 2010-08-24 . 882C1C473BE598DF08730DA11C5B2B27 . 2030080 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.
20787_none_e3967e4730ab1731\comctl32.dll
[7] 2010-08-21 . BC052EFAD10ACA1AD69545B629F50D99 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.760
0.16661_none_95a2b509f19be458\comctl32.dll
[7] 2010-08-21 . BC052EFAD10ACA1AD69545B629F50D99 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7600
.16661_none_a44e1fc257f685f6\comctl32.dll
[7] 2010-08-21 . 113921FC4A80A3DDF646852998B836D0 . 2030080 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.
16661_none_fa62ad231704eab7\comctl32.dll
[7] 2009-07-14 . 7E8AB50AB7F2F81F30DCC8A98025B73A . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.760
0.16385_none_959110a7f1a88a21\comctl32.dll
[7] 2009-07-14 . 7E8AB50AB7F2F81F30DCC8A98025B73A . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7600
.16385_none_a44af8ec57f961cf\comctl32.dll
[7] 2009-07-14 . C093E7835C1372D6D70A6675EDAA97B5 . 2030080 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.
16385_none_fa645303170382f6\comctl32.dll
[7] 2013-07-04 . 9028D1621C43DF8DFBD1C76860412A11 . 633856 . . [5.82] ..
c:\windows\system32\comctl32.dll

[7] 2009-07-14 . 1A47D52E303B7543E4E6026595B95422 . 1297408 . . [2001.12.8530.16385]
..
c:\windows\winsxs\amd64_microsoft-windows-com-complus.res_31bf3856ad364e35_6.1.7600.
16385_none_88a5cc7effe2dfca\comres.dll
[7] 2009-07-14 . 1A47D52E303B7543E4E6026595B95422 . 1297408 . . [2001.12.8530.16385]
.. c:\windows\system32\comres.dll

[7] 2013-10-05 . 509D31797A4B8A3D6ED78A330B19A919 . 186880 . . [6.1.7601.22473] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.224
73_none_d46d4138cabe2596\cryptsvc.dll
[7] 2013-07-09 . 434CCE8E7150CD1324C5FAA088D1D061 . 186880 . . [6.1.7601.22380] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.223
80_none_d45f6e88cac8f85b\cryptsvc.dll
[7] 2013-07-09 . 6B400F211BEE880A37A1ED0368776BF4 . 184320 . . [6.1.7601.18205] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.182
05_none_d431528fb165f7bc\cryptsvc.dll
[7] 2013-05-13 . D8129C49798CBBFB2E4351D4B7B8EF9C . 184320 . . [6.1.7601.18151] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.181
51_none_d3f73fe5b19220ee\cryptsvc.dll
[7] 2013-05-11 . 8122252F0A4ACFA92FA0C1D50D18493B . 186880 . . [6.1.7601.22322] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.223
22_none_d4a24ea4ca968363\cryptsvc.dll
[7] 2013-05-10 . 7FDC4626B01106A8EF328C88C7C0DEE3 . 184320 . . [6.1.7601.18150] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.181
50_none_d3f63f9bb1930797\cryptsvc.dll
[7] 2013-05-10 . CA13C4F92BEE66DB48E58AB3223DDF6E . 186880 . . [6.1.7601.22321] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.223
21_none_d4a14e5aca976a0c\cryptsvc.dll
[7] 2012-06-04 . 7E7D2DACF65D750D466F36BD3D09AE20 . 186880 . . [6.1.7601.22010] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.220
10_none_d4ab184aca903d4f\cryptsvc.dll
[7] 2012-06-02 . 9C01375BE382E834CC26D1B7EAF2C4FE . 184320 . . [6.1.7601.17856] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.178
56_none_d3fc6569b18d7211\cryptsvc.dll
[7] 2012-06-02 . 456107D69D4EE850A559434F19EFEE65 . 183808 . . [6.1.7600.21225] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7600.212
25_none_d2beeccacd6d6c07\cryptsvc.dll

```

# ComboFix

```

[7] 2012-06-02 . BAF19B633933A9FB4883D27D66C39E9A . 182272 . . [6.1.7600.17035] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7600.170
35_none_d22a7e2db457eb07\cryptsvc.dll
[7] 2010-11-20 . 15597883FBE9B056F276ADA3AD87D9AF . 177152 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7601.175
14_none_d4259ed3b16ed82a\cryptsvc.dll
[7] 2009-07-14 . 8C57411B66282C01533CB776F98AD384 . 175104 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-dll_31bf3856ad364e35_6.1.7600.163
85_none_d1f48b0bb4805490\cryptsvc.dll
[7] 2013-07-09 . 6B400F211BEE880A37A1ED0368776BF4 . 184320 . . [6.1.7600.16385] ..
c:\windows\system32\cryptsvc.dll

[7] 2009-07-14 . 4166F82BE4D24938977DD1746BE9B8A0 . 402944 . . [2001.12.8530.16385]
..
c:\windows\winsxs\amd64_microsoft-windows-c..complus-eventsystem_31bf3856ad364e35_6.
1.7600.16385_none_68e290c46b6ea6d0\es.dll
[7] 2009-07-14 . 4166F82BE4D24938977DD1746BE9B8A0 . 402944 . . [2001.12.8530.16385]
.. c:\windows\system32\es.dll

[7] 2009-07-14 . AA2C08CE85653B1A0D2E4AB407FA176C . 167424 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-imm32_31bf3856ad364e35_6.1.7600.16385_none
_b84b0fbd941c03a9\imm32.dll
[7] 2009-07-14 . AA2C08CE85653B1A0D2E4AB407FA176C . 167424 . . [6.1.7600.16385] ..
c:\windows\system32\imm32.dll

[7] 2012-11-22 . BD5153969C41F697E23B9A43EF9228CE . 801280 . . [1.0626.7600.17174]
..
c:\windows\winsxs\amd64_microsoft-windows-usp_31bf3856ad364e35_6.1.7600.17174_none_0
8f91fc3722650e0\usp10.dll
[7] 2012-11-22 . E4ACCC7927A1478DF636534864E03666 . 801280 . . [1.0626.7601.22171]
..
c:\windows\winsxs\amd64_microsoft-windows-usp_31bf3856ad364e35_6.1.7601.22171_none_0
b661a9c886d0db8\usp10.dll
[7] 2012-11-22 . 77AD7076F8CF3CAB923F7FAE6DC9BDA8 . 800768 . . [1.0626.7600.21379]
..
c:\windows\winsxs\amd64_microsoft-windows-usp_31bf3856ad364e35_6.1.7600.21379_none_0
987bfe68b3f6c84\usp10.dll
[7] 2012-11-22 . DBF99FD9CAF75CA66D042BD8D050FF71 . 800768 . . [1.0626.7601.18009]
..
c:\windows\winsxs\amd64_microsoft-windows-usp_31bf3856ad364e35_6.1.7601.18009_none_0
b302f956f0f750f\usp10.dll
[7] 2010-11-20 . 2F8B1E3EE3545D3B5A8D56FA1AE07B65 . 800256 . . [1.0626.7601.17514]
..
c:\windows\winsxs\amd64_microsoft-windows-usp_31bf3856ad364e35_6.1.7601.17514_none_0
b207e7d6f1bea6f\usp10.dll
[7] 2009-07-14 . 5F2BDCA5FA0F20A6F452CF0EE2A2B18C . 801280 . . [1.0626.7600.16385]
..
c:\windows\winsxs\amd64_microsoft-windows-usp_31bf3856ad364e35_6.1.7600.16385_none_0
8ef6ab5722d66d5\usp10.dll
[7] 2012-11-22 . DBF99FD9CAF75CA66D042BD8D050FF71 . 800768 . . [1.0626.7601.18009]
.. c:\windows\system32\usp10.dll

[7] 2013-08-29 . 786D234A90FCAC72633AE6FC52653A49 . 1162240 . . [6.1.7601.22436] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.22436_n
one_f259cda386173c9c\kernel32.dll
[7] 2013-08-02 . C525D51A79B01342344F02E38866CF60 . 1162240 . . [6.1.7601.22411] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.22411_n
one_f26a6c09860b8607\kernel32.dll
[7] 2013-08-02 . D8973E71F1B35CD3F3DEA7C12D49D0F0 . 1161216 . . [6.1.7601.18229] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.18229_n
one_f1ddffbc6ceecfbf\kernel32.dll
[7] 2013-07-08 . 38E54D419A2962E24D35D868E4724AE7 . 1162240 . . [6.1.7601.22379] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.22379_n

```

# ComboFix

```

one_f2318ceb8634fb3e\kernel32.dll
[7] 2013-01-04 . 9DD828EFBD17246275E8A74D58E836AC . 1162752 . . [6.1.7600.21416] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7600.21416_n
one_f0890ca988e09e80\kernel32.dll
[7] 2013-01-04 . B844114B247D8EF1E5E4E93A282D2E6F . 1162240 . . [6.1.7601.22209] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.22209_n
one_f27d3a7985fc3a80\kernel32.dll
[7] 2013-01-04 . 43DB3433F141F01E53D1C5AA0F434098 . 1161216 . . [6.1.7600.17206] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7600.17206_n
one_f00a3de46fbae59e\kernel32.dll
[7] 2012-11-30 . B3BEA6420D482356E53B7C728E05C637 . 1163264 . . [6.1.7601.22177] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.22177_n
one_f22f888b8636ce42\kernel32.dll
[7] 2012-11-30 . E3BC37881D92EB59EE0BA3B854A54D1E . 1161216 . . [6.1.7600.17179] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7600.17179_n
one_efc18d686ff0f813\kernel32.dll
[7] 2012-11-30 . 65C113214F7B05820F6D8A65B1485196 . 1161216 . . [6.1.7601.18015] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.18015_n
one_f1e4cab46cea5424\kernel32.dll
[7] 2012-11-30 . B6B1AB98BA656BA1D8E0CA03F59DED51 . 1162752 . . [6.1.7600.21386] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7600.21386_n
one_f03d5b4f891964f0\kernel32.dll
[7] 2012-10-04 . 1DC3504CA4C57900F1557E9A3F01D272 . 1161216 . . [6.1.7601.17965] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.17965_n
one_f1aee2f66d12ac97\kernel32.dll
[7] 2012-10-04 . F3C594D0DA3ACFA6C7B781A490AB4282 . 1162240 . . [6.1.7601.22125] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.22125_n
one_f263979386100fdf\kernel32.dll
[7] 2012-10-04 . 1DDCACAB8DA5399E5521051923016B18 . 1161216 . . [6.1.7600.17135] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7600.17135_n
one_efe8cbf06fd422f3\kernel32.dll
[7] 2012-10-04 . 6EED0D77C20137948979EA47360A890B . 1162752 . . [6.1.7600.21335] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7600.21335_n
one_f0726aa188f1bfe4\kernel32.dll
[7] 2010-11-20 . B6326D96D53048FDEC542DF23D875A0 . 1161216 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7601.17514_n
one_f1e3eab06ceb12ef\kernel32.dll
[7] 2009-07-14 . 5B4B379AD10DEDA4EDA01B8C6961B193 . 1162240 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7600.16385_n
one_efb2d6e86ffc8f55\kernel32.dll
[7] 2013-08-02 . D8973E71F1B35CD3F3DEA7C12D49D0F0 . 1161216 . . [6.1.7601.18015] ..
c:\windows\system32\kernel32.dll

[7] 2009-07-14 . A0A65D306A5490D2EB8E7DE66898ECFD . 29696 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-linkinfo_31bf3856ad364e35_6.1.7600.16385_n
one_945a23c3bf051859\linkinfo.dll
[7] 2009-07-14 . A0A65D306A5490D2EB8E7DE66898ECFD . 29696 . . [6.1.7600.16385] ..
c:\windows\system32\linkinfo.dll

[7] 2013-06-06 . 796B47A4B82EF1C39F13435B88834C48 . 41472 . . [6.1.7601.18177] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7601.18177_none_0
7bb20dd7154003d\lpk.dll
[7] 2013-06-06 . 22FC61B8E1EBA296FF416C3678E26DD3 . 41472 . . [6.1.7601.22350] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7601.22350_none_0
8535d608a67b3eb\lpk.dll
[7] 2012-12-16 . 838BF2634A38B344B27AC080D76B28C2 . 41472 . . [6.1.7600.21402] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7600.21402_none_0
6a50ea48d16f1d1\lpk.dll
[7] 2009-07-14 . D20223587518B13D72D68937B7E3F70 . 41984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7600.16385_none_0
5c80a1f743763f3\lpk.dll
[7] 2009-07-14 . D20223587518B13D72D68937B7E3F70 . 41984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7600.16402_none_0

```

# ComboFix

```

61b8a8773f9358d\lpk.dll
[7] 2009-07-14 . D20223587518B13D72D68937B7E3F70 . 41984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7600.16444_none_0
5f24b6b7417d7ff\lpk.dll
[7] 2009-07-14 . D20223587518B13D72D68937B7E3F70 . 41984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7600.17194_none_0
5bc1f55744085e0\lpk.dll
[7] 2009-07-14 . D20223587518B13D72D68937B7E3F70 . 41984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7600.20498_none_0
649d7dc8d5a6bb3\lpk.dll
[7] 2009-07-14 . D20223587518B13D72D68937B7E3F70 . 41984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7600.20553_none_0
67018008d3e7a63\lpk.dll
[7] 2009-07-14 . D20223587518B13D72D68937B7E3F70 . 41984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7601.17514_none_0
7f91de77125e78d\lpk.dll
[7] 2009-07-14 . D20223587518B13D72D68937B7E3F70 . 41984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7601.18032_none_0
7e15d357138149f\lpk.dll
[7] 2009-07-14 . D20223587518B13D72D68937B7E3F70 . 41984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7601.22195_none_0
82d1b568a83a814\lpk.dll
[7] 2013-06-06 . 796B47A4B82EF1C39F13435B88834C48 . 41472 . . [6.1.7601.18177] ..
c:\windows\system32\lpk.dll

[7] 2009-07-14 . 3B367397320C26DBA890B260F80D1B1B . 424448 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-i..ectionssharingconfig_31bf3856ad364e35_6.
1.7600.16385_none_0c2b375bae4a8d38\hnetcfg.dll
[7] 2009-07-14 . 3B367397320C26DBA890B260F80D1B1B . 424448 . . [6.1.7600.16385] ..
c:\windows\system32\hnetcfg.dll

[7] 2014-03-01 . 4E0709D9BB951AD1C22E4FF519B90839 . 23133696 . . [11.00.9600.16428]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_11.2.960
0.16521_none_f58ff536373f154c\mshtml.dll
[7] 2014-02-06 . D016F5092E4FFC41147E8555A71D2DDE . 23170048 . . [11.00.9600.16428]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_11.2.960
0.16518_none_f58e55743740af5c\mshtml.dll
[7] 2013-12-03 . D233E1A32CE6AF918C9DE1BC44AFEB2A . 23212032 . . [11.00.9600.16428]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_11.2.960
0.16428_none_f59a25aa3737acc2\mshtml.dll
[7] 2013-11-26 . 16B0A65F52531B769B891DC251ECC6C0 . 23183360 . . [11.00.9600.16428]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_11.2.960
0.16476_none_f59f54ac3732f833\mshtml.dll
[7] 2013-10-12 . 25C356A79B7002E0A20AAF592ED59DE4 . 19269632 . . [10.00.9200.16736]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_10.2.920
0.16736_none_91079aba92acea3d\mshtml.dll
[7] 2013-10-12 . BED01C981AA5D47941F6BAF30B6FE12C . 19510784 . . [10.00.9200.20848]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_10.2.920
0.20848_none_7a2ff6ecac5bb27c\mshtml.dll
[7] 2013-09-22 . 9958430CE5BFC43D693D6138C31788CC . 19494912 . . [10.00.9200.20831]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_10.2.920
0.20831_none_7a2f961aac5be5be\mshtml.dll
[7] 2013-09-22 . F026C6F104758D0EB215B017016FAE27 . 19252224 . . [10.00.9200.16721]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_10.2.920
0.16721_none_91070c5892ad50c1\mshtml.dll

```

# ComboFix

```

[7] 2013-08-10 . CC4AE7E2ECAEE7612B3C0D3AB302375C . 19246592 . . [10.00.9200.16686]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_10.2.920
0.16686_none_91176c1892a04cff\mshtml.dll
[7] 2013-08-10 . C2793FDC1EDB82635C538630FE192CC9 . 19488768 . . [10.00.9200.20794]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_10.2.920
0.20794_none_7a40236aac4eaeba\mshtml.dll
[7] 2013-07-26 . 396889142BD839DB8A055A0BE0AD2F79 . 19239424 . . [10.00.9200.16660]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_10.2.920
0.16660_none_9115f43492a1808b\mshtml.dll
[7] 2013-07-26 . 865EB4E69DAF2DE052E8D020F4F7D313 . 19482112 . . [10.00.9200.20768]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_10.2.920
0.20768_none_7a3cc76cac51c939\mshtml.dll
[7] 2013-07-13 . 9586EC4E1CC39CCBA26A5E7DFE774C9E . 19238912 . . [10.00.9200.16635]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_10.2.920
0.16635_none_9112816e92a4b4ab\mshtml.dll
[7] 2013-07-10 . 34426D52FBA4F3E31739DB840D2601AD . 17829376 . . [9.00.8112.16496]
..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_9.4.8112
.16496_none_879aa2dbf5018011\mshtml.dll
[7] 2013-03-04 . 23FF9EA25842DB24427A7993CC192D8F . 9382400 . . [8.00.7600.21484] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_8.0.7600
.21484_none_8a7ad133cbfb1a54\mshtml.dll
[7] 2013-03-02 . 7C91A589EC32A0D183D9BDA19D45274F . 9059328 . . [8.00.7601.18106] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_8.0.7601
.18106_none_8c301162afc1399c\mshtml.dll
[7] 2013-03-02 . 633B37E7AB84DF5E0A95173A9C33938F . 9377280 . . [8.00.7600.17267] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_8.0.7600
.17267_none_8a09d338b2ca9186\mshtml.dll
[7] 2013-03-02 . 01A3EE0DB86FD44D7E0BFC7269F18405 . 9061888 . . [8.00.7601.22272] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_8.0.7601
.22272_none_8c69fd91c91b37a1\mshtml.dll
[7] 2010-11-20 . 1C8B787BAA52DEAD1A6FEC1502D652F0 . 8988160 . . [8.00.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_8.0.7601
.17514_none_8c235f42afcafd4a\mshtml.dll
[7] 2009-07-14 . 12C3F25EA578DAA752024E1918D59313 . 9271296 . . [8.00.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-htmlrendering_31bf3856ad364e35_8.0.7600
.16385_none_89f24b7ab2dc7a40\mshtml.dll
[7] 2014-03-01 . 4E0709D9BB951AD1C22E4FF519B90839 . 23133696 . . [11.00.9600.16428]
.. c:\windows\system32\mshtml.dll
.
[7] 2011-12-16 . C391FC68282A000CDF953F8B6B55D2EF . 634880 . . [7.0.7601.17744] ..
c:\windows\winsxs\amd64_microsoft-windows-msvcrt_31bf3856ad364e35_6.1.7601.17744_non
e_2f5acf97b59df60f\msvcrt.dll
[7] 2011-12-16 . 579F6AFC6A6561951FA2202EFC3FE485 . 634368 . . [7.0.7600.16930] ..
c:\windows\winsxs\amd64_microsoft-windows-msvcrt_31bf3856ad364e35_6.1.7600.16930_non
e_2d7b4155b87308d6\msvcrt.dll
[7] 2011-12-16 . F9A4C695C86CC32048FE2C987A0BD387 . 634880 . . [7.0.7601.21878] ..
c:\windows\winsxs\amd64_microsoft-windows-msvcrt_31bf3856ad364e35_6.1.7601.21878_non
e_2fc7fdc6ced04f08\msvcrt.dll
[7] 2011-12-16 . 7D8B505E35AB89D3C3E9AE54A2C95DD2 . 634880 . . [7.0.7600.21108] ..
c:\windows\winsxs\amd64_microsoft-windows-msvcrt_31bf3856ad364e35_6.1.7600.21108_non
e_2e2d2856d17152c7\msvcrt.dll
[7] 2009-07-14 . 7319BB10FA1F86E49E3DCF4136F6C957 . 634880 . . [7.0.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-msvcrt_31bf3856ad364e35_6.1.7600.16385_non
e_2d4a27c7b8972454\msvcrt.dll
[7] 2011-12-16 . C391FC68282A000CDF953F8B6B55D2EF . 634880 . . [7.0.7601.17744] ..
c:\windows\system32\msvcrt.dll
.

```

# ComboFix

```

[7] 2013-09-08 . 9A9F9F1A77D6A80EE28B57664F00013E . 327168 . . [6.1.7601.18254] ..
c:\windows\winsxs\amd64_microsoft-windows-w.-infrastructure-bsp_31bf3856ad364e35_6.
1.7601.18254_none_16e26ee85d215bbf\mswsock.dll
[7] 2013-09-07 . BDD81FD258B92DEE00F222D3304B5D9C . 327168 . . [6.1.7601.22444] ..
c:\windows\winsxs\amd64_microsoft-windows-w.-infrastructure-bsp_31bf3856ad364e35_6.
1.7601.22444_none_16e26ee85d215bbf\mswsock.dll
[7] 2010-11-20 . 1D5185A4C7E6695431AE4B55C3D7D333 . 326144 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-w.-infrastructure-bsp_31bf3856ad364e35_6.
1.7601.17514_none_16795c7543eb48cf\mswsock.dll
[7] 2009-07-14 . FC76FE3C1E1FDB761244D4F74EF560FD . 320000 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w.-infrastructure-bsp_31bf3856ad364e35_6.
1.7600.16385_none_144848ad46fcc535\mswsock.dll
[7] 2013-09-08 . 9A9F9F1A77D6A80EE28B57664F00013E . 327168 . . [6.1.7600.16385] ..
c:\windows\system32\mswsock.dll
.
[7] 2010-11-20 . AA339DD8BB128EF66660DFBBB59043D3 . 695808 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-security-netlogon_31bf3856ad364e35_6.1.760
1.17514_none_5bddbcb24e997298\netlogon.dll
[7] 2009-07-14 . 956D030D375F207B22FB111E06EF9C35 . 692736 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-security-netlogon_31bf3856ad364e35_6.1.760
0.16385_none_59aca8ea51aaeefe\netlogon.dll
[7] 2010-11-20 . AA339DD8BB128EF66660DFBBB59043D3 . 695808 . . [6.1.7600.16385] ..
c:\windows\system32\netlogon.dll
.
[7] 2009-07-14 . 716175021BDA290504CE434273F666BC . 167424 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-userpowermanagement_31bf3856ad364e35_6.1.7
600.16385_none_ff0e900816896618\powrprof.dll
[7] 2009-07-14 . 716175021BDA290504CE434273F666BC . 167424 . . [6.1.7600.16385] ..
c:\windows\system32\powrprof.dll
.
[7] 2010-11-20 . ED78427259134C63ED69804D2132B86C . 232960 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-s..urationengineclient_31bf3856ad364e35_6.
1.7601.17514_none_9633e7caefbaf953\scecli.dll
[7] 2009-07-14 . 398712DDDAEFB85EDF61DF6A07B65C79 . 232448 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-s..urationengineclient_31bf3856ad364e35_6.
1.7600.16385_none_9402d402f2cc75b9\scecli.dll
[7] 2010-11-20 . ED78427259134C63ED69804D2132B86C . 232960 . . [6.1.7600.16385] ..
c:\windows\system32\scecli.dll
.
[7] 2009-07-14 . C6DCD1D11ED6827F05C00773C3E7053C . 3072 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-sfc_31bf3856ad364e35_6.1.7600.16385_none_0
32ab4f375e2ac1f\sfc.dll
[7] 2009-07-14 . C6DCD1D11ED6827F05C00773C3E7053C . 3072 . . [6.1.7600.16385] ..
c:\windows\system32\sfc.dll
.
[7] 2009-07-14 . C78655BC80301D76ED4FEF1C1EA40A7D . 27136 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-services-svchost_31bf3856ad364e35_6.1.7600
.16385_none_11b04b481efec48c\svchost.exe
[7] 2009-07-14 . C78655BC80301D76ED4FEF1C1EA40A7D . 27136 . . [6.1.7600.16385] ..
c:\windows\system32\svchost.exe
.
[7] 2010-11-20 . 40F0849F65D13EE87B9A9AE3C1DD6823 . 316928 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-tapiservice_31bf3856ad364e35_6.1.7601.1751
4_none_4162de4afb9222c0\tapisrv.dll
[7] 2009-07-14 . 884264AC597B690C5707C89723BB8E7B . 316416 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-tapiservice_31bf3856ad364e35_6.1.7600.1638
5_none_3f31ca82fea39f26\tapisrv.dll
[7] 2010-11-20 . 40F0849F65D13EE87B9A9AE3C1DD6823 . 316928 . . [6.1.7600.16385] ..
c:\windows\system32\tapisrv.dll
.
[7] 2010-11-20 . FE70103391A64039A921DBFFF9C7AB1B . 1008128 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-user32_31bf3856ad364e35_6.1.7601.17514_non
e_2b5e71b083fc0973\user32.dll

```

# ComboFix

```

[7] 2009-07-14 . 72D7B3EA16946E8F0CF7458150031CC6 . 1008640 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-user32_31bf3856ad364e35_6.1.7600.16385_non
e_292d5de8870d85d9\user32.dll
[7] 2010-11-20 . FE70103391A64039A921DBFFF9C7AB1B . 1008128 . . [6.1.7601.17514] ..
c:\windows\system32\user32.dll

[7] 2010-11-20 . BAFE84E637BF7388C96EF48D4D3FDD53 . 30720 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-userinit_31bf3856ad364e35_6.1.7601.17514_n
one_3a4ebf84e84f824c\userinit.exe
[7] 2009-07-14 . 6F8F1376A13114CC10C0E69274F5A4DE . 30208 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-userinit_31bf3856ad364e35_6.1.7600.16385_n
one_381dabbceb60feb2\userinit.exe
[7] 2010-11-20 . BAFE84E637BF7388C96EF48D4D3FDD53 . 30720 . . [6.1.7600.16385] ..
c:\windows\system32\userinit.exe

[7] 2014-03-01 . DF79CE9B950C62677D232154E93A81C7 . 2334208 . . [11.00.9600.16521]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_11
.2.9600.16521_none_e435d617b6e8ac16\wininet.dll
[7] 2014-02-06 . 263B6E451526A90FF8B1CEC759F22956 . 2334208 . . [11.00.9600.16518]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_11
.2.9600.16518_none_e4343655b6ea4626\wininet.dll
[7] 2013-12-03 . E6CB36B85BE59095337427E853A5B65A . 2332160 . . [11.00.9600.16428]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_11
.2.9600.16428_none_e440068bb6e1438c\wininet.dll
[7] 2013-11-26 . 9B6678DB9C6A232C5A84D2FDFFF8B0E1 . 2334208 . . [11.00.9600.16476]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_11
.2.9600.16476_none_e445358db6dc8efd\wininet.dll
[7] 2013-10-12 . 9706C99DAEBE3FEAC811B239617E98C4 . 2241536 . . [10.00.9200.16736]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_10
.2.9200.16736_none_7fad7b9c12568107\wininet.dll
[7] 2013-10-12 . 7E7F32C588DA6A4554046804D8EEAC55 . 2249216 . . [10.00.9200.20848]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_10
.2.9200.20848_none_68d5d7ce2c054946\wininet.dll
[7] 2013-09-22 . 1377A310439639A610097ED56975AE19 . 2248704 . . [10.00.9200.20830]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_10
.2.9200.20831_none_68d576fc2c057c88\wininet.dll
[7] 2013-09-22 . D28B35DE88D27EFB27DF4B1E8319E3C0 . 2241024 . . [10.00.9200.16720]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_10
.2.9200.16721_none_7faced3a1256e78b\wininet.dll
[7] 2013-08-10 . AAFA952E774DDDB0956D3BDFAE5B5B99 . 2241024 . . [10.00.9200.16686]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_10
.2.9200.16686_none_7fbd4cfa1249e3c9\wininet.dll
[7] 2013-08-10 . 0A380C8E396975463E3F643E88AE8BDF . 2248704 . . [10.00.9200.20794]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_10
.2.9200.20794_none_68e6044c2bf84584\wininet.dll
[7] 2013-07-26 . AC155DD9BD1E6D3B740826A4D1C68AAE . 2241024 . . [10.00.9200.16660]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_10
.2.9200.16660_none_7fbbd516124b1755\wininet.dll
[7] 2013-07-26 . 5C49F5A791B944AD8247473ABD35602D . 2248704 . . [10.00.9200.20768]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_10
.2.9200.20768_none_68e2a84e2bfb6003\wininet.dll

```

# ComboFix

```

[7] 2013-07-13 . FAF6EC2460AD5FBBBD38D8E1AE28B0D77 . 2241024 . . [10.00.9200.16635]
..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_10
.2.9200.16635_none_7fb86250124e4b75\wininet.dll
[7] 2013-07-10 . 5536F6E7B74DA37D3EDBB509DE9CE3F5 . 1392128 . . [9.00.8112.16496] ..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_9.
4.8112.16496_none_764083bd74ab16db\wininet.dll
[7] 2013-03-04 . 3BD77CF56FF4B03BA390379F67259258 . 1198080 . . [8.00.7600.21484] ..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_8.
0.7600.21484_none_7920b2154ba4b11e\wininet.dll
[7] 2013-03-02 . 9E7687984107C81B859200C9BD570AFF . 1188864 . . [8.00.7601.18106] ..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_8.
0.7601.18106_none_7ad5f2442f6ad066\wininet.dll
[7] 2013-03-02 . 8523338F749AC8C5300C125BC4B08275 . 1198080 . . [8.00.7600.17267] ..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_8.
0.7600.17267_none_78afb41a32742850\wininet.dll
[7] 2013-03-02 . 6E8A768CEA17C6542E3031812745AC3F . 1189888 . . [8.00.7601.22272] ..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_8.
0.7601.22272_none_7b0fde7348c4ce6b\wininet.dll
[7] 2010-12-21 . E71DB117DBDA6B33646F37936C17D226 . 1197056 . . [8.00.7600.16723] ..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_8.
0.7600.16723_none_78d712e832572b52\wininet.dll
[7] 2010-12-21 . 1D3466E7E9D63F8B2B84A8AD5E833C29 . 1198080 . . [8.00.7600.20862] ..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_8.
0.7600.20862_none_79346fb94b962189\wininet.dll
[7] 2010-11-20 . F6C5302E1F4813D552F41A0AC82455E5 . 1188864 . . [8.00.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_8.
0.7601.17514_none_7ac940242f7494a4\wininet.dll
[7] 2009-07-14 . B1037F0131C9A010D611F6914E03CD92 . 1193472 . . [8.00.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-i..tocolimplementation_31bf3856ad364e35_8.
0.7600.16385_none_78982c5c3286110a\wininet.dll
[7] 2014-03-01 . DF79CE9B950C62677D232154E93A81C7 . 2334208 . . [11.00.9600.16428]
.. c:\windows\system32\wininet.dll

[7] 2010-11-20 . 4BBFA57F594F7E8A8EDC8F377184C3F0 . 297984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w..nfrastructure-ws232_31bf3856ad364e35_6.
1.7601.17514_none_50ddb631e4f59005\ws2_32.dll
[7] 2009-07-14 . 7083F463788CB34FCC42F565D56F89E8 . 296448 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w..nfrastructure-ws232_31bf3856ad364e35_6.
1.7600.16385_none_4eaca269e8070c6b\ws2_32.dll
[7] 2010-11-20 . 4BBFA57F594F7E8A8EDC8F377184C3F0 . 297984 . . [6.1.7600.16385] ..
c:\windows\system32\ws2_32.dll

[7] 2009-07-14 . 8396C6C26AADD5FE4590CCEFOF419B6B7 . 4608 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w..nfrastructure-other_31bf3856ad364e35_6.
1.7600.16385_none_6079f415110c0210\ws2help.dll
[7] 2009-07-14 . 8396C6C26AADD5FE4590CCEFOF419B6B7 . 4608 . . [6.1.7600.16385] ..
c:\windows\system32\ws2help.dll

[7] 2010-11-20 . 6C60B5ACA7442EFB794082CDACFC001C . 2086912 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-com-base-qfe-ole32_31bf3856ad364e35_6.1.76
01.17514_none_0a43accb08f0eac5\ole32.dll
[7] 2010-06-29 . AC8F79017C5C1FB316930EDEAD0AF517 . 2085376 . . [6.1.7600.16624] ..
c:\windows\winsxs\amd64_microsoft-windows-com-base-qfe-ole32_31bf3856ad364e35_6.1.76
00.16624_none_08527df30bd29da3\ole32.dll
[7] 2010-06-29 . 49401892E8305914A9E7F64C7000D6A6 . 2085376 . . [6.1.7600.20744] ..
c:\windows\winsxs\amd64_microsoft-windows-com-base-qfe-ole32_31bf3856ad364e35_6.1.76
00.20744_none_08c67ae62500754f\ole32.dll
[7] 2009-07-14 . 4B25DDE615AC2CABAB73169CA7DA96E6 . 2084352 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-com-base-qfe-ole32_31bf3856ad364e35_6.1.76
00.16385_none_081299030c02672b\ole32.dll
[7] 2010-11-20 . 6C60B5ACA7442EFB794082CDACFC001C . 2086912 . . [6.1.7600.16385] ..
c:\windows\system32\ole32.dll

```

# ComboFix

```

[7] 2009-07-14 . 86FE1B1F8FD42CD0DB641AB1CDB13093 . 18944 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cngaudit-dll_31bf3856ad364e35_6.1.7600.163
85_none_4458dccc49458461\cngaudit.dll
[7] 2009-07-14 . 86FE1B1F8FD42CD0DB641AB1CDB13093 . 18944 . . [6.1.7600.16385] ..
c:\windows\system32\cngaudit.dll
.
[7] 2009-07-14 . 94355C28C1970635A31B3FE52EB7CEBA . 129024 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-wininit_31bf3856ad364e35_6.1.7600.16385_no
ne_8ce7aa761e01ad49\wininit.exe
[7] 2009-07-14 . 94355C28C1970635A31B3FE52EB7CEBA . 129024 . . [6.1.7600.16385] ..
c:\windows\system32\wininit.exe
.
[7] 2009-07-14 . 42B6A94DD747DF2B5F628A2752E62A98 . 9728 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-t..cesframework-ctfmon_31bf3856ad364e35_6.
1.7600.16385_none_f9257e7aaa4290ce\ctfmon.exe
[7] 2009-07-14 . 42B6A94DD747DF2B5F628A2752E62A98 . 9728 . . [6.1.7600.16385] ..
c:\windows\system32\ctfmon.exe
.
[7] 2010-11-20 . AAF932B4011D14052955D4B212A4DA8D . 370688 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-shsvcs_31bf3856ad364e35_6.1.7601.17514_non
e_2b566299338d2123\shsvcs.dll
[7] 2009-07-14 . 0298AC45D0EFFFFB2DB4BAA7DD186E7BF . 369664 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-shsvcs_31bf3856ad364e35_6.1.7600.16385_non
e_29254ed1369e9d89\shsvcs.dll
[7] 2010-11-20 . AAF932B4011D14052955D4B212A4DA8D . 370688 . . [6.1.7600.16385] ..
c:\windows\system32\shsvcs.dll
.
[7] 2009-07-14 . E4D94F24081440B5FC5AA556C7C62702 . 159232 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-remoteregistry-service_31bf3856ad364e35_6.
1.7600.16385_none_e55af7609d2857a8\regsvc.dll
[7] 2009-07-14 . E4D94F24081440B5FC5AA556C7C62702 . 159232 . . [6.1.7600.16385] ..
c:\windows\system32\regsvc.dll
.
[7] 2010-11-20 . 262F6592C3299C005FD6BEC90FC4463A . 1110016 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-taskscheduler-service_31bf3856ad364e35_6.1
.7601.17514_none_8d272400ada202f9\schedsvc.dll
[7] 2010-11-02 . 5269A787C24D968D291B22F7ED4955B1 . 1114624 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-taskscheduler-service_31bf3856ad364e35_6.1
.7600.20830_none_8bb0c2c5c9ad095d\schedsvc.dll
[7] 2010-11-02 . 624D0F5FF99428BB90A5B8A4123E918E . 1114624 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-taskscheduler-service_31bf3856ad364e35_6.1
.7600.16699_none_8aef4726b0b7f821\schedsvc.dll
[7] 2009-07-14 . EC56B171F85C7E855E7B0588AC503EEA . 1104384 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-taskscheduler-service_31bf3856ad364e35_6.1
.7600.16385_none_8af61038b0b37f5f\schedsvc.dll
[7] 2010-11-20 . 262F6592C3299C005FD6BEC90FC4463A . 1110016 . . [6.1.7600.16385] ..
c:\windows\system32\schedsvc.dll
.
[7] 2009-07-14 . 51B52FBD583CDE8AA9BA62B8B4298F33 . 193024 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-upnpssdp_31bf3856ad364e35_6.1.7600.16385_n
one_dbbe6492eae9505c\ssdpsrv.dll
[7] 2009-07-14 . 51B52FBD583CDE8AA9BA62B8B4298F33 . 193024 . . [6.1.7600.16385] ..
c:\windows\system32\ssdpsrv.dll
.
[7] 2010-11-20 . 2E648163254233755035B46DD7B89123 . 680960 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-t..teconnectionmanager_31bf3856ad364e35_6.
1.7601.17514_none_ecc547376ae3a1a3\termsrv.dll
[7] 2009-07-14 . 0F05EC2887BFE197AD82A13287D2F404 . 706560 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-t..teconnectionmanager_31bf3856ad364e35_6.
1.7600.16385_none_ea94336f6df51e09\termsrv.dll
[7] 2010-11-20 . 2E648163254233755035B46DD7B89123 . 680960 . . [6.1.7601.17514] ..
c:\windows\system32\termsrv.dll

```

# ComboFix

```
.
[7] 2013-08-29 . C842D8DC6E5BCD750FA50E4083CBBEB . 5552064 . . [6.1.7601.22436] ..
c:\windows\winsxs\amd64_microsoft-windows-os-kernel_31bf3856ad364e35_6.1.7601.22436_
none_cacc4a02e3eec656\ntoskrnl.exe
[7] 2013-08-29 . 5B9A6A310326D9C438F2C19FBBE97C97 . 5549504 . . [6.1.7601.18247] ..
c:\windows\system32\ntoskrnl.exe

[7] 2009-07-14 . 8560FFFC8EB3A806DCD4F82252CFC8C6 . 5120 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-d..tshow-kernel-support_31bf3856ad364e35_6.
1.7600.16385_none_43f68e03b0fd4b38\ksuser.dll
[7] 2009-07-14 . 8560FFFC8EB3A806DCD4F82252CFC8C6 . 5120 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-d..tshow-kernel-support_31bf3856ad364e35_6.
1.7601.17514_none_4627a1cbadebcd2\ksuser.dll
[7] 2009-07-14 . 8560FFFC8EB3A806DCD4F82252CFC8C6 . 5120 . . [6.1.7600.16385] ..
c:\windows\system32\ksuser.dll

[7] 2009-07-14 . E424B3EF666B184CEE0B6871AAA8C9F6 . 8192 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi-painting_31bf3856ad364e35_6.1.7600.163
85_none_d360c9c235bd1868\msimg32.dll
[7] 2009-07-14 . E424B3EF666B184CEE0B6871AAA8C9F6 . 8192 . . [6.1.7600.16385] ..
c:\windows\system32\msimg32.dll

[7] 2013-07-04 . 700BD5A6AA5381D1D8ADC4045149DBF6 . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.7601.
22376_none_3bee2a494f8638cf\comctl32.dll
[7] 2013-07-04 . 700BD5A6AA5381D1D8ADC4045149DBF6 . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.2
2376_none_ee67d2d082b9f619\comctl32.dll
[7] 2013-07-04 . 75F5E1FE8D55CF8E577E0EC5F2290D3F . 530432 . . [5.82] ..
c:\windows\SysWOW64\comctl32.dll
[7] 2013-07-04 . 75F5E1FE8D55CF8E577E0EC5F2290D3F . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.7601.
18201_none_3bab3b80363456bb\comctl32.dll
[7] 2013-07-04 . 75F5E1FE8D55CF8E577E0EC5F2290D3F . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.1
8201_none_ec80f00e8593ece5\comctl32.dll
[7] 2010-11-20 . BDAC1AA64495D0F7E1FF810EBBF1F018 . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.7601.
17514_none_3ba388ec36399c85\comctl32.dll
[7] 2010-11-20 . BDAC1AA64495D0F7E1FF810EBBF1F018 . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.1
7514_none_ec83dffa859149af\comctl32.dll
[7] 2010-11-20 . 352B3DC62A0D259A82A052238425C872 . 1680896 . . [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17
514_none_41e6975e2bd6f2b2\comctl32.dll
[7] 2010-08-21 . BF5D71B4A40687A90C8B47F776758A6F . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.7600.
20787_none_39fe18355266e2d8\comctl32.dll
[7] 2010-08-21 . BF5D71B4A40687A90C8B47F776758A6F . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7600.2
0787_none_e2ad2969983532\comctl32.dll
[7] 2010-08-21 . 70EF5DFEF7069164EACF7140C2CC6344 . 1680896 . . [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.20
787_none_2b43b51e45274037\comctl32.dll
[7] 2010-08-21 . D3EAD1CF16BA729A7F7C9A5D94AA7C05 . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft-windows-shell-comctl32-v5_31bf3856ad364e35_6.1.7600.
16661_none_39841986393e7322\comctl32.dll
[7] 2010-08-21 . D3EAD1CF16BA729A7F7C9A5D94AA7C05 . 530432 . . [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7600.1
6661_none_ebfb56996c72aefc\comctl32.dll
[7] 2010-08-21 . 4B8DD8541C0E26602005DD0137333615 . 1680896 . . [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16
661_none_420fe3fa2b8113bd\comctl32.dll
```