OTL logfile created on: 4/6/2014 10:39:25 PM - Run 2
OTL by OldTimer - Version 3.2.69.0   Folder = C:\Users\srhutsell\Desktop\Cleanup Aisle 5
64bit- Home Premium Edition Service Pack 1 (Version = 6.1.7601) - Type = NTWorkstation
Internet Explorer (Version = 9.11.9600.16521)
Locale: 00000409 | Country: United States | Language: ENU | Date Format: M/d/yyyy

4.75 Gb Total Physical Memory | 2.95 Gb Available Physical Memory | 62.06% Memory free
9.50 Gb Paging File | 7.01 Gb Available in Paging File | 73.85% Paging File free
Paging file location(s): ?:\pagefile.sys [binary data]

%SystemDrive% = C: | %SystemRoot% = C:\Windows | %ProgramFiles% = C:\Program Files (x86)
Drive C: | 596.07 Gb Total Space | 534.71 Gb Free Space | 89.70% Space Free | Partition Type: NTFS
Drive D: | 228.50 Mb Total Space | 0.00 Mb Free Space | 0.00% Space Free | Partition Type: UDF

Computer Name: HUTSELL2S | User Name: srhutsell | Logged in as Administrator.
Boot Mode: Normal | Scan Mode: All users | Include 64bit Scans
Company Name Whitelist: Off | Skip Microsoft Files: Off | No Company Name Whitelist: On | File Age = 30 Days

[color=#E56717]========== Processes (SafeList) ==========[/color]

PRC - [2014/04/06 18:42:03 | 000,602,112 | ---- | M] (OldTimer Tools) -- C:\Users\srhutsell\Desktop\Cleanup Aisle 5\OTL.exe
PRC - [2014/04/06 03:53:17 | 003,854,640 | ---- | M] (AVAST Software) -- C:\Program Files\AVAST Software\Avast\AvastUI.exe
PRC - [2014/04/06 03:53:17 | 000,050,344 | ---- | M] (AVAST Software) -- C:\Program Files\AVAST Software\Avast\AvastSvc.exe
PRC - [2013/08/16 19:06:34 | 002,799,296 | ---- | M] (Sysinternals - www.sysinternals.com) -- C:\Users\srhutsell\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\procexp.exe
PRC - [2013/05/29 08:19:04 | 002,094,216 | ---- | M] () -- C:\Program Files (x86)\Comodo\Dragon\dragon_updater.exe

[color=#E56717]========== Modules (No Company Name) ==========[/color]

MOD - [2013/12/25 00:07:03 | 019,336,120 | ---- | M] () -- C:\Program Files\AVAST Software\Avast\libcef.dll

[color=#E56717]========== Services (SafeList) ==========[/color]

SRV:[b]64bit:[/b] - [2014/04/06 03:53:17 | 000,050,344 | ---- | M] (AVAST Software) [Auto | Running] -- C:\Program Files\AVAST Software\Avast\AvastSvc.exe -- (avast! Antivirus)
SRV:[b]64bit:[/b] - [2014/03/01 00:33:34 | 000,111,616 | ---- | M] (Microsoft Corporation) [On_Demand | Stopped] -- C:\Windows\SysNative\IEEtwCollector.exe -- (IEEtwCollectorService)
SRV:[b]64bit:[/b] - [2013/10/19 21:23:22 | 006,254,152 | ---- | M] (COMODO) [Auto | Running] -- C:\Program Files\COMODO\COMODO Internet Security\cmdagent.exe -- (cmdAgent)
SRV:[b]64bit:[/b] - [2013/09/24 06:53:30 | 000,164,056 | ---- | M] (COMODO) [On_Demand | Stopped] -- C:\Program Files\COMODO\COMODO Internet Security\cmdvirth.exe -- (cmdvirth)
SRV:[b]64bit:[/b] - [2013/05/27 01:50:47 | 001,011,712 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Defender\MpSvc.dll -- (WinDefend)

SRV:[b]64bit:[/b] - [2012/11/02 22:43:00 | 000,112,224 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\WhsMcClient.exe -- (WhsMcClient)
SRV:[b]64bit:[/b] - [2012/11/02 22:07:28 | 000,080,504 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\Microsoft.HomeServer.Archive.TransferService.exe -- (arXfrSvc)
SRV:[b]64bit:[/b] - [2012/11/02 22:07:28 | 000,041,568 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\ProviderRegistryService.exe -- (ServiceProviderRegistry)
SRV:[b]64bit:[/b] - [2011/08/11 19:38:04 | 000,140,672 | ---- | M] (SUPERAntiSpyware.com) [Auto | Running] -- C:\Program Files\SUPERAntiSpyware\SASCore64.exe -- (!SASCORE)
SRV:[b]64bit:[/b] - [2011/06/30 00:42:32 | 000,204,288 | ---- | M] (AMD) [Auto | Running] -- C:\Windows\SysNative\atiesrxx.exe -- (AMD External Events Utility)
SRV:[b]64bit:[/b] - [2011/03/02 16:46:44 | 000,027,520 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\LANConfigSvc.exe -- (LANConfig)
SRV:[b]64bit:[/b] - [2011/03/02 16:46:40 | 000,030,592 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\SharedServiceHost.exe -- (WSS_ComputerBackupProviderSvc)
SRV:[b]64bit:[/b] - [2011/03/02 16:46:40 | 000,030,592 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\SharedServiceHost.exe -- (SqmProviderSvc)
SRV:[b]64bit:[/b] - [2011/03/02 16:46:40 | 000,030,592 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\SharedServiceHost.exe -- (providers_system)
SRV:[b]64bit:[/b] - [2011/03/02 16:46:40 | 000,030,592 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\SharedServiceHost.exe -- (NotificationsProviderSvc)
SRV:[b]64bit:[/b] - [2011/03/02 16:46:40 | 000,030,592 | ---- | M] (Microsoft Corporation) [Auto | Stopped] -- C:\Program Files\Windows Server\Bin\SharedServiceHost.exe -- (initMonitor)
SRV:[b]64bit:[/b] - [2011/03/02 16:46:40 | 000,030,592 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\SharedServiceHost.exe -- (HealthAlertsSvc)
SRV:[b]64bit:[/b] - [2011/03/02 16:46:34 | 000,228,736 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Program Files\Windows Server\Bin\WSConnectorUpdate.exe -- (WSConnectorUpdate)
SRV - [2014/04/06 04:31:57 | 000,119,408 | ---- | M] (Mozilla Foundation) [On_Demand | Stopped] -- C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe -- (MozillaMaintenance)
SRV - [2013/09/11 22:21:54 | 000,105,144 | ---- | M] (Microsoft Corporation) [Auto | Stopped] -- C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe -- (clr_optimization_v4.0.30319_32)
SRV - [2013/05/29 08:19:04 | 002,094,216 | ---- | M] () [Auto | Running] -- C:\Program Files (x86)\Comodo\Dragon\dragon_updater.exe -- (DragonUpdater)
SRV - [2009/06/10 17:23:09 | 000,066,384 | ---- | M] (Microsoft Corporation) [Disabled | Stopped] -- C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe -- (clr_optimization_v2.0.50727_32)

[color=#E56717]========== Driver Services (SafeList) ==========[/color]

DRV:[b]64bit:[/b] - [2014/04/06 03:53:27 | 001,039,096 | ---- | M] (AVAST Software) [File_System | System | Running] -- C:\Windows\SysNative\drivers\aswSnx.sys -- (aswSnx)
DRV:[b]64bit:[/b] - [2014/04/06 03:53:27 | 000,423,240 | ---- | M] (AVAST Software) [File_System | System | Running] -- C:\Windows\SysNative\drivers\aswSP.sys -- (aswSP)
DRV:[b]64bit:[/b] - [2014/04/06 03:53:27 | 000,208,928 | ---- | M] () [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\aswVmm.sys -- (aswVmm)
DRV:[b]64bit:[/b] - [2014/04/06 03:53:27 | 000,084,816 | ---- | M] (AVAST Software) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\aswstm.sys --

(aswStm)
DRV:[b]64bit:[/b] - [2014/04/06 03:53:27 | 000,079,184 | ---- | M] (AVAST Software) [File_System | Auto | Running] -- C:\Windows\SysNative\drivers\aswMonFlt.sys -- (aswMonFlt)
DRV:[b]64bit:[/b] - [2014/04/06 03:53:27 | 000,065,776 | ---- | M] () [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\aswRvrt.sys -- (aswRvrt)
DRV:[b]64bit:[/b] - [2014/04/06 03:53:26 | 000,093,568 | ---- | M] (AVAST Software) [Kernel | System | Running] -- C:\Windows\SysNative\drivers\aswRdr2.sys -- (aswRdr)
DRV:[b]64bit:[/b] - [2013/12/19 09:11:27 | 000,064,288 | ---- | M] (AVAST Software) [Kernel | System | Running] -- C:\Windows\SysNative\drivers\aswTdi.sys -- (aswTdi)
DRV:[b]64bit:[/b] - [2013/09/24 06:54:10 | 000,023,168 | ---- | M] (COMODO) [File_System | System | Running] -- C:\Windows\SysNative\drivers\cmderd.sys -- (cmderd)
DRV:[b]64bit:[/b] - [2012/11/22 02:18:37 | 000,011,576 | ---- | M] (Samsung Electronics) [Kernel | Auto | Running] -- C:\Windows\SysNative\drivers\SSPORT.SYS -- (SSPORT)
DRV:[b]64bit:[/b] - [2012/08/23 10:10:20 | 000,019,456 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\rdpvideominiport.sys -- (RdpVideoMiniport)
DRV:[b]64bit:[/b] - [2012/08/23 10:07:35 | 000,057,856 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\TsUsbFlt.sys -- (TsUsbFlt)
DRV:[b]64bit:[/b] - [2012/03/01 02:46:16 | 000,023,408 | ---- | M] (Microsoft Corporation) [Recognizer | Boot | Unknown] -- C:\Windows\SysNative\drivers\fs_rec.sys -- (Fs_Rec)
DRV:[b]64bit:[/b] - [2011/07/22 12:26:56 | 000,014,928 | ---- | M] (SUPERAdBlocker.com and SUPERAntiSpyware.com) [Kernel | System | Running] -- C:\Program Files\SUPERAntiSpyware\sasdifsv64.sys -- (SASDIFSV)
DRV:[b]64bit:[/b] - [2011/07/12 17:55:18 | 000,012,368 | ---- | M] (SUPERAdBlocker.com and SUPERAntiSpyware.com) [Kernel | System | Running] -- C:\Program Files\SUPERAntiSpyware\saskutil64.sys -- (SASKUTIL)
DRV:[b]64bit:[/b] - [2011/06/30 02:33:12 | 009,371,136 | ---- | M] (ATI Technologies Inc.) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\atikmdag.sys -- (amdkmdag)
DRV:[b]64bit:[/b] - [2011/06/30 00:00:50 | 000,309,760 | ---- | M] (Advanced Micro Devices, Inc.) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\atikmpag.sys -- (amdkmdap)
DRV:[b]64bit:[/b] - [2011/04/21 18:17:04 | 000,471,144 | ---- | M] (Realtek) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\Rt64win7.sys -- (RTL8167)
DRV:[b]64bit:[/b] - [2011/03/11 02:41:12 | 000,107,904 | ---- | M] (Advanced Micro Devices) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\amdsata.sys -- (amdsata)
DRV:[b]64bit:[/b] - [2011/03/11 02:41:12 | 000,027,008 | ---- | M] (Advanced Micro Devices) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\amdxata.sys -- (amdxata)
DRV:[b]64bit:[/b] - [2011/03/02 13:33:12 | 000,063,872 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\BackupReader.sys -- (BackupReader)
DRV:[b]64bit:[/b] - [2010/11/20 09:33:35 | 000,078,720 | ---- | M] (Hewlett-Packard Company) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\HpSAMD.sys -- (HpSAMD)
DRV:[b]64bit:[/b] - [2010/03/10 07:33:52 | 000,016,440 | ---- | M] (Advanced Micro Devices Inc.) [Kernel | Boot | Running] -- C:\Windows\SysNative\drivers\AtiPcie64.sys -- (AtiPcie)
DRV:[b]64bit:[/b] - [2009/07/13 21:52:20 | 000,194,128 | ---- | M] (AMD Technologies Inc.) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\amdsbs.sys -- (amdsbs)
DRV:[b]64bit:[/b] - [2009/07/13 21:48:04 | 000,065,600 | ---- | M] (LSI Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\lsi_sas2.sys -- (LSI_SAS2)
DRV:[b]64bit:[/b] - [2009/07/13 21:45:55 | 000,024,656 | ---- | M] (Promise Technology) [Kernel | On_Demand | Stopped] --

C:\Windows\SysNative\drivers\stexstor.sys -- (stexstor)
DRV:[b]64bit:[/b] - [2009/07/13 20:39:20 | 000,023,040 | ---- | M] (Microsoft Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\WSDPrint.sys -- (WSDPrintDevice)
DRV:[b]64bit:[/b] - [2009/06/10 17:01:06 | 001,146,880 | ---- | M] (LSI Corp) [Kernel | On_Demand | Running] -- C:\Windows\SysNative\drivers\agrsm64.sys -- (AGERESoftModem)
DRV:[b]64bit:[/b] - [2009/06/10 16:34:33 | 003,286,016 | ---- | M] (Broadcom Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\evbda.sys -- (ebdrv)
DRV:[b]64bit:[/b] - [2009/06/10 16:34:28 | 000,468,480 | ---- | M] (Broadcom Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\bxvbda.sys -- (b06bdrv)
DRV:[b]64bit:[/b] - [2009/06/10 16:34:23 | 000,270,848 | ---- | M] (Broadcom Corporation) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\b57nd60a.sys -- (b57nd60a)
DRV:[b]64bit:[/b] - [2009/06/10 16:31:59 | 000,031,232 | ---- | M] (Hauppauge Computer Works, Inc.) [Kernel | On_Demand | Stopped] -- C:\Windows\SysNative\drivers\hcw85cir.sys -- (hcw85cir)
DRV - [2009/10/12 21:24:56 | 000,007,408 | R--- | M] (SUPERAdBlocker.com and SUPERAntiSpyware.com) [Kernel | On_Demand | Stopped] -- C:\Program Files (x86)\SUPERAntiSpyware\SASENUM.SYS -- (SASENUM)
DRV - [2009/07/13 21:19:10 | 000,019,008 | ---- | M] (Microsoft Corporation) [File_System | On_Demand | Stopped] -- C:\Windows\SysWOW64\drivers\wimmount.sys -- (WIMMount)

[color=#E56717]========== Standard Registry (SafeList) ==========[/color]

[color=#E56717]========== Internet Explorer ==========[/color]

IE:[b]64bit:[/b] - HKLM\..\SearchScopes,DefaultScope = {0633EE93-D776-472f-A0FF-E1416B8B2E3A}
IE:[b]64bit:[/b] - HKLM\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://search.live.com/results.aspx?q={searchTerms}&src={referrer:source?}
IE:[b]64bit:[/b] - HKLM\..\SearchScopes\{CF739809-1C6C-47C0-85B9-569DBB141420}: "URL" = http://toolbar.ask.com/toolbarv/askRedirect?o=10587&gct=&gc=1&q={searchTerms}&crm=1
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page = C:\Windows\SysWOW64\blank.htm
IE - HKLM\..\SearchScopes,DefaultScope = {0633EE93-D776-472f-A0FF-E1416B8B2E3A}
IE - HKLM\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/search?q={searchTerms}&FORM=IE8SRC

IE - HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0

IE - HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0

IE - HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0

IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Search_URL = http://www.google.com/ie
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\SOFTWARE\Microsoft\Internet Explorer\Main,Search Bar = http://www.google.com/ie
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://www.google.com
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\SOFTWARE\Microsoft\Internet

Explorer\Main,Start Page = http://www.msn.com/
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\SOFTWARE\Microsoft\Internet Explorer\Search,Default_Search_URL = http://www.google.com/ie
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\SOFTWARE\Microsoft\Internet Explorer\Search,SearchAssistant = http://www.google.com/ie
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\..\SearchScopes,DefaultScope = {6A1806CD-94D4-4689-BA73-E35EA1EA9990}
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/search?q={searchTerms}&src=IE-SearchBox&FORM=IE11SR
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\..\SearchScopes\{6A1806CD-94D4-4689-BA73-E35EA1EA9990}: "URL" = http://www.google.com/search?q={searchTerms}&rls=com.microsoft:{language}
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\..\SearchScopes\{CF739809-1C6C-47C0-85B9-569DBB141420}: "URL" = http://toolbar.ask.com/toolbarv/askRedirect?o=10587&gct=&gc=1&q={searchTerms}&crm=1
IE - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0

[color=#E56717]========== FireFox ==========[/color]

FF - prefs.js..browser.startup.homepage: "http://www.msn.com/"
FF - prefs.js..extensions.enabledAddons: %7B73a6fe31-595d-460b-a920-fcc0f8843232%7D:2.6.8.19
FF - prefs.js..extensions.enabledAddons: %7B972ce4c6-7e08-4474-a285-3208198ce6fd%7D:28.0
FF - user.js - File not found

FF:[b]64bit:[/b] - HKLM\Software\MozillaPlugins\@adobe.com/FlashPlayer: C:\Windows\system32\Macromed\Flash\NPSWF64_12_0_0_77.dll File not found
FF:[b]64bit:[/b] - HKLM\Software\MozillaPlugins\@microsoft.com/GENUINE: disabled File not found
FF - HKLM\Software\MozillaPlugins\@adobe.com/FlashPlayer: C:\Windows\SysWOW64\Macromed\Flash\NPSWF32_12_0_0_77.dll ()
FF - HKLM\Software\MozillaPlugins\@foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/pdf: C:\Program Files (x86)\Foxit Software\Foxit Reader\plugins\npFoxitReaderPlugin.dll (Foxit Corporation)
FF - HKLM\Software\MozillaPlugins\@foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/vnd.fdf: C:\Program Files (x86)\Foxit Software\Foxit Reader\plugins\npFoxitReaderPlugin.dll (Foxit Corporation)
FF - HKLM\Software\MozillaPlugins\@google.com/npPicasa3,version=3.0.0: C:\Program Files (x86)\Google\Picasa3\npPicasa3.dll (Google, Inc.)
FF - HKLM\Software\MozillaPlugins\@microsoft.com/GENUINE: disabled File not found
FF - HKLM\Software\MozillaPlugins\@videolan.org/vlc,version=2.0.7: C:\Program Files (x86)\VideoLAN\VLC\npvlc.dll (VideoLAN)

FF - HKEY_LOCAL_MACHINE\software\mozilla\Firefox\Extensions\\wrc@avast.com: C:\Program Files\AVAST Software\Avast\WebRep\FF [2014/04/06 03:53:29 | 000,000,000 | ---D | M]
FF - HKEY_LOCAL_MACHINE\software\mozilla\Mozilla Firefox 28.0\extensions\\Components: C:\Program Files (x86)\Mozilla Firefox\components
FF - HKEY_LOCAL_MACHINE\software\mozilla\Mozilla Firefox 28.0\extensions\\Plugins: C:\Program Files (x86)\Mozilla Firefox\plugins
FF - HKEY_CURRENT_USER\software\mozilla\Mozilla Firefox 28.0\extensions\\Components: C:\Program Files (x86)\Mozilla Firefox\components
FF - HKEY_CURRENT_USER\software\mozilla\Mozilla Firefox 28.0\extensions\\Plugins: C:\Program Files (x86)\Mozilla Firefox\plugins

[2013/07/14 17:40:04 | 000,000,000 | ---D | M] (No name found) --

C:\Users\srhutsell\AppData\Roaming\Mozilla\Extensions
[2014/04/06 04:16:41 | 000,000,000 | ---D | M] (No name found) -- C:\Users\srhutsell\AppData\Roaming\Mozilla\Firefox\Profiles\gzywid7h.default\extensions
[2014/04/06 04:16:41 | 000,537,316 | ---- | M] () (No name found) -- C:\Users\srhutsell\AppData\Roaming\Mozilla\Firefox\Profiles\gzywid7h.default\extensions\{73a6fe31-595d-460b-a920-fcc0f8843232}.xpi
[2014/04/06 04:31:45 | 000,000,000 | ---D | M] (No name found) -- C:\Program Files (x86)\Mozilla Firefox\browser\extensions
[2014/04/06 04:31:59 | 000,000,000 | ---D | M] (Default) -- C:\Program Files (x86)\Mozilla Firefox\browser\extensions\{972ce4c6-7e08-4474-a285-3208198ce6fd}

O1 HOSTS File: ([2009/06/10 17:00:26 | 000,000,824 | ---- | M]) - C:\Windows\SysNative\drivers\etc\hosts
O2:[b]64bit:[/b] - BHO: (avast! Online Security) - {8E5E2654-AD2D-48bf-AC2D-D17F00898D06} - C:\Program Files\AVAST Software\Avast\aswWebRepIE64.dll (AVAST Software)
O2 - BHO: (avast! Online Security) - {8E5E2654-AD2D-48bf-AC2D-D17F00898D06} - C:\Program Files\AVAST Software\Avast\aswWebRepIE.dll (AVAST Software)
O3:[b]64bit:[/b] - HKLM\..\Toolbar: (no name) - {318A227B-5E9F-45bd-8999-7F8F10CA4CF5} - No CLSID value found.
O3:[b]64bit:[/b] - HKLM\..\Toolbar: (no name) - {CC1A175A-E45B-41ED-A30C-C9B1D7A0C02F} - No CLSID value found.
O4:[b]64bit:[/b] - HKLM..\Run: [COMODO Internet Security] C:\Program Files\COMODO\COMODO Internet Security\cistray.exe (COMODO)
O4:[b]64bit:[/b] - HKLM..\Run: [Launchpad] C:\Program Files\Windows Server\Bin\Launchpad.exe (Microsoft Corporation)
O4 - HKLM..\Run: [APSDaemon] C:\Program Files (x86)\Common Files\Apple\Apple Application Support\APSDaemon.exe (Apple Inc.)
O4 - HKLM..\Run: [AvastUI.exe] C:\Program Files\AVAST Software\Avast\AvastUI.exe (AVAST Software)
O4 - HKLM..\Run: [StartCCC] C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLIStart.exe (Advanced Micro Devices, Inc.)
O4 - HKLM..\Run: [tvncontrol] "C:\Program Files (x86)\Common Files\COMODO\GeekBuddyRSP.exe" -controlservice -slave File not found
O4 - HKU\S-1-5-19..\Run: [Sidebar] C:\Program Files (x86)\Windows Sidebar\Sidebar.exe (Microsoft Corporation)
O4 - HKU\S-1-5-20..\Run: [Sidebar] C:\Program Files (x86)\Windows Sidebar\Sidebar.exe (Microsoft Corporation)
O4 - HKU\S-1-5-21-3455503661-4230816971-2044476751-1022..\Run: [SUPERAntiSpyware] C:\Program Files\SUPERAntiSpyware\SUPERANTISPYWARE.EXE (SUPERAntiSpyware)
O4 - HKU\.DEFAULT..\RunOnce: [SPReview] "C:\Windows\System32\SPReview\SPReview.exe" /sp:1 /errorfwlink:"http://go.microsoft.com/fwlink/?LinkID=122915" /build:7601 File not found
O4 - HKU\S-1-5-18..\RunOnce: [SPReview] "C:\Windows\System32\SPReview\SPReview.exe" /sp:1 /errorfwlink:"http://go.microsoft.com/fwlink/?LinkID=122915" /build:7601 File not found
O4 - HKU\S-1-5-19..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe File not found
O4 - HKU\S-1-5-20..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe File not found
O4 - Startup: C:\Users\srhutsell\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\procexp.exe (Sysinternals - www.sysinternals.com)
O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer: NoActiveDesktop = 1
O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer: NoActiveDesktopChanges = 1
O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System: ConsentPromptBehaviorAdmin = 5
O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System: ConsentPromptBehaviorUser = 3
O8:[b]64bit:[/b] - Extra context menu item: Add to Google Photos Screensa&ver - res://C:\Windows\system32\GPhotos.scr/200 File not found

O8 - Extra context menu item: Add to Google Photos Screensa&ver - C:\Windows\SysWow64\GPhotos.scr (Google Inc.)
O13[b]64bit:[/b] - gopher Prefix: missing
O13 - gopher Prefix: missing
O18:[b]64bit:[/b] - Protocol\Handler\msdaipp - No CLSID value found
O18:[b]64bit:[/b] - Protocol\Handler\msdaipp\0x00000001 - No CLSID value found
O18:[b]64bit:[/b] - Protocol\Handler\msdaipp\oledb - No CLSID value found
O18:[b]64bit:[/b] - Protocol\Handler\ms-itss - No CLSID value found
O18:[b]64bit:[/b] - Protocol\Handler\mso-offdap - No CLSID value found
O18:[b]64bit:[/b] - Protocol\Handler\mso-offdap11 - No CLSID value found
O18 - Protocol\Handler\msdaipp\0x00000001 {E1D2BF42-A96B-11d1-9C6B-0000F875AC61} - C:\Program Files (x86)\Common Files\System\Ole DB\MSDAIPP.DLL (Microsoft Corporation)
O18 - Protocol\Handler\msdaipp\oledb {E1D2BF40-A96B-11d1-9C6B-0000F875AC61} - C:\Program Files (x86)\Common Files\System\Ole DB\MSDAIPP.DLL (Microsoft Corporation)
O18:[b]64bit:[/b] - Protocol\Filter\text/xml - No CLSID value found
O20:[b]64bit:[/b] - HKLM Winlogon: Shell - (explorer.exe) - C:\Windows\explorer.exe (Microsoft Corporation)
O20:[b]64bit:[/b] - HKLM Winlogon: UserInit - (C:\Windows\system32\userinit.exe) - C:\Windows\SysNative\userinit.exe (Microsoft Corporation)
O20 - HKLM Winlogon: Shell - (explorer.exe) - C:\Windows\SysWow64\explorer.exe (Microsoft Corporation)
O20 - HKLM Winlogon: UserInit - (userinit.exe) - C:\Windows\SysWow64\userinit.exe (Microsoft Corporation)
O20 - Winlogon\Notify\!SASWinLogon: DllName - (C:\Program Files (x86)\SUPERAntiSpyware\SASWINLO.dll) - C:\Program Files (x86)\SUPERAntiSpyware\SASWINLO.dll (SUPERAntiSpyware.com)
O21:[b]64bit:[/b] - SSODL: WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} - No CLSID value found.
O21 - SSODL: WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} - No CLSID value found.
O28 - HKLM ShellExecuteHooks: {5AE067D3-9AFB-48E0-853A-EBB7F4A000DA} - C:\Program Files (x86)\SUPERAntiSpyware\SASSEH.DLL (SuperAdBlocker.com)
O32 - HKLM CDRom: AutoRun - 1
O34 - HKLM BootExecute: (autocheck autochk *)
O35:[b]64bit:[/b] - HKLM\..comfile [open] -- "%1" %*
O35:[b]64bit:[/b] - HKLM\..exefile [open] -- "%1" %*
O35 - HKLM\..comfile [open] -- "%1" %*
O35 - HKLM\..exefile [open] -- "%1" %*
O37:[b]64bit:[/b] - HKLM\...com [@ = comfile] -- "%1" %*
O37:[b]64bit:[/b] - HKLM\...exe [@ = exefile] -- "%1" %*
O37 - HKLM\...com [@ = comfile] -- "%1" %*
O37 - HKLM\...exe [@ = exefile] -- "%1" %*
O38 - SubSystems\\Windows: (ServerDll=winsrv:UserServerDllInitialization,3)
O38 - SubSystems\\Windows: (ServerDll=winsrv:ConServerDllInitialization,2)
O38 - SubSystems\\Windows: (ServerDll=sxssrv,4)

[color=#E56717]========== Files/Folders - Created Within 30 Days ==========[/color]

[2014/04/06 22:37:44 | 000,000,000 | ---D | C] -- C:\Users\srhutsell\Desktop\Cleanup Aisle 5
[2014/04/06 04:54:55 | 000,000,000 | ---D | C] -- C:\Users\srhutsell\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\NirSoft SmartSniff
[2014/04/06 04:54:55 | 000,000,000 | ---D | C] -- C:\Program Files (x86)\NirSoft
[2014/04/06 04:31:45 | 000,000,000 | ---D | C] -- C:\Program Files (x86)\Mozilla Firefox
[2014/04/06 03:53:24 | 000,043,152 | ---- | C] (AVAST Software) -- C:\Windows\avastSS.scr
[2014/03/12 02:00:49 | 000,032,768 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\iernonce.dll
[2014/03/12 02:00:48 | 000,004,096 | ---- | C] (Microsoft Corporation) --

C:\Windows\SysNative\ieetwcollectorres.dll
[2014/03/12 02:00:47 | 000,051,200 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\ieetwproxystub.dll
[2014/03/12 02:00:45 | 001,964,032 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\inetcpl.cpl
[2014/03/12 02:00:45 | 000,553,472 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\jscript9diag.dll
[2014/03/12 02:00:45 | 000,061,952 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\iesetup.dll
[2014/03/12 02:00:45 | 000,033,792 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\iernonce.dll
[2014/03/12 02:00:44 | 000,440,832 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\ieui.dll
[2014/03/12 02:00:44 | 000,048,640 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\ieetwproxystub.dll
[2014/03/12 02:00:43 | 000,627,200 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\msfeeds.dll
[2014/03/12 02:00:42 | 000,218,624 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\ie4uinit.exe
[2014/03/12 02:00:42 | 000,066,048 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\iesetup.dll
[2014/03/12 02:00:41 | 002,041,856 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\inetcpl.cpl
[2014/03/12 02:00:40 | 000,703,488 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\ieapfltr.dll
[2014/03/12 02:00:40 | 000,112,128 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\ieUnatt.exe
[2014/03/12 02:00:39 | 000,164,864 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\msrating.dll
[2014/03/12 02:00:39 | 000,111,616 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\ieetwcollector.exe
[2014/03/12 02:00:38 | 000,708,608 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\jscript9diag.dll
[2014/03/12 02:00:38 | 000,574,976 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\ieui.dll
[2014/03/12 02:00:38 | 000,139,264 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\ieUnatt.exe
[2014/03/12 02:00:37 | 005,768,704 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\jscript9.dll
[2014/03/12 02:00:37 | 000,817,664 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\ieapfltr.dll
[2014/03/12 02:00:36 | 000,195,584 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\msrating.dll
[2014/03/12 02:00:34 | 000,940,032 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\MsSpellCheckingFacility.exe
[2014/03/12 02:00:12 | 000,484,864 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\wer.dll
[2014/03/12 02:00:12 | 000,381,440 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\wer.dll
[2014/03/12 01:55:34 | 000,624,128 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\qedit.dll
[2014/03/12 01:55:33 | 000,509,440 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysWow64\qedit.dll
[2014/03/12 01:55:30 | 001,424,384 | ---- | C] (Microsoft Corporation) --
C:\Windows\SysNative\WindowsCodecs.dll

[color=#E56717]========== Files - Modified Within 30 Days ==========[/color]

[2014/04/06 22:37:37 | 000,015,008 | -H-- | M] () --
C:\Windows\SysNative\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-81
15-601632D005A0
[2014/04/06 22:37:37 | 000,015,008 | -H-- | M] () --
C:\Windows\SysNative\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-81

15-601632D005A0
[2014/04/06 22:35:58 | 000,782,470 | ---- | M] () --
C:\Windows\SysNative\PerfStringBackup.INI
[2014/04/06 22:35:58 | 000,662,384 | ---- | M] () --
C:\Windows\SysNative\perfh009.dat
[2014/04/06 22:35:58 | 000,122,252 | ---- | M] () --
C:\Windows\SysNative\perfc009.dat
[2014/04/06 22:29:56 | 000,067,584 | --S- | M] () -- C:\Windows\bootstat.dat
[2014/04/06 22:29:54 | 3824,656,384 | -HS- | M] () -- C:\hiberfil.sys
[2014/04/06 09:34:46 | 000,000,518 | ---- | M] () --
C:\Windows\tasks\SUPERAntiSpyware Scheduled Task
501d43ed-97cc-46be-93a8-bfa21dc4efab.job
[2014/04/06 04:14:12 | 000,692,616 | ---- | M] (Adobe Systems Incorporated) --
C:\Windows\SysWow64\FlashPlayerApp.exe
[2014/04/06 04:14:12 | 000,071,048 | ---- | M] (Adobe Systems Incorporated) --
C:\Windows\SysWow64\FlashPlayerCPLApp.cpl
[2014/04/06 03:54:09 | 000,001,966 | ---- | M] () -- C:\Users\Public\Desktop\avast!
Free Antivirus.lnk
[2014/04/06 03:53:27 | 001,039,096 | ---- | M] (AVAST Software) --
C:\Windows\SysNative\drivers\aswSnx.sys
[2014/04/06 03:53:27 | 000,423,240 | ---- | M] (AVAST Software) --
C:\Windows\SysNative\drivers\aswSP.sys
[2014/04/06 03:53:27 | 000,334,648 | ---- | M] (AVAST Software) --
C:\Windows\SysNative\aswBoot.exe
[2014/04/06 03:53:27 | 000,208,928 | ---- | M] () --
C:\Windows\SysNative\drivers\aswVmm.sys
[2014/04/06 03:53:27 | 000,084,816 | ---- | M] (AVAST Software) --
C:\Windows\SysNative\drivers\aswstm.sys
[2014/04/06 03:53:27 | 000,079,184 | ---- | M] (AVAST Software) --
C:\Windows\SysNative\drivers\aswMonFlt.sys
[2014/04/06 03:53:27 | 000,065,776 | ---- | M] () --
C:\Windows\SysNative\drivers\aswRvrt.sys
[2014/04/06 03:53:26 | 000,093,568 | ---- | M] (AVAST Software) --
C:\Windows\SysNative\drivers\aswRdr2.sys
[2014/04/06 03:53:24 | 000,043,152 | ---- | M] (AVAST Software) --
C:\Windows\avastSS.scr
[2014/04/05 02:00:00 | 000,000,518 | ---- | M] () --
C:\Windows\tasks\SUPERAntiSpyware Scheduled Task
53e97ced-da88-404b-9dde-635c877baa69.job
[2014/03/12 03:19:04 | 000,417,392 | ---- | M] () --
C:\Windows\SysNative\FNTCACHE.DAT

[color=#E56717]========== Files Created - No Company Name ==========[/color]

[2014/01/11 19:49:40 | 000,000,057 | ---- | C] () -- C:\ProgramData\Ament.ini
[2013/11/30 13:19:58 | 000,216,064 | ---- | C] () --
C:\Windows\SysWow64\gcapi_dll.dll
[2013/08/18 17:28:28 | 000,007,680 | ---- | C] () --
C:\Users\srhutsell\AppData\Local\DCBC2A71-70D8-4DAN-EHR8-E0D61DEA3FDF.ini
[2013/07/22 23:43:31 | 003,566,434 | ---- | C] () --
C:\Windows\SysWow64\fun_avcodec.dll
[2013/07/22 23:43:31 | 000,827,392 | ---- | C] () --
C:\Windows\SysWow64\Mpeg4System.dll
[2013/07/22 23:43:31 | 000,167,936 | ---- | C] () --
C:\Windows\SysWow64\Mpeg4Tools.dll
[2013/07/22 23:43:31 | 000,122,880 | ---- | C] () --
C:\Windows\SysWow64\Mpeg4DSF.dll
[2013/07/22 23:43:31 | 000,042,108 | ---- | C] () --
C:\Windows\SysWow64\fun_avutil.dll
[2013/07/22 23:43:30 | 000,241,664 | ---- | C] () -- C:\Windows\SysWow64\AMR.dll
[2013/07/22 23:43:30 | 000,057,344 | ---- | C] () --
C:\Windows\SysWow64\EvrcDecDll.dll
[2013/07/22 23:43:30 | 000,057,344 | ---- | C] () -- C:\Windows\SysWow64\AMRDSF.dll

[2013/07/14 18:36:06 | 000,000,376 | ---- | C] () -- C:\Windows\ODBC.INI
[2013/07/13 13:07:28 | 000,774,592 | ---- | C] () -- C:\Windows\SysWow64\PerfStringBackup.INI
[2013/07/10 01:07:50 | 000,000,000 | ---- | C] () -- C:\Windows\ativpsrm.bin
[2013/07/09 22:55:14 | 000,003,929 | ---- | C] () -- C:\Windows\SysWow64\atipblag.dat
[2010/11/15 22:50:17 | 000,001,024 | ---- | C] () -- C:\Users\srhutsell\.rnd.old

[color=#E56717]========== ZeroAccess Check ==========[/color]

[2009/07/14 00:55:00 | 000,000,227 | RHS- | M] () -- C:\Windows\assembly\Desktop.ini

[HKEY_CURRENT_USER\Software\Classes\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32] /64

[HKEY_CURRENT_USER\Software\Classes\Wow6432node\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32]

[HKEY_CURRENT_USER\Software\Classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InProcServer32] /64

[HKEY_CURRENT_USER\Software\Classes\Wow6432node\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InProcServer32]

[HKEY_LOCAL_MACHINE\Software\Classes\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32] /64
"" = C:\Windows\SysNative\shell32.dll -- [2013/07/25 22:24:57 | 014,172,672 | ---- | M] (Microsoft Corporation)
"ThreadingModel" = Apartment

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Classes\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32]
"" = %SystemRoot%\system32\shell32.dll -- [2013/07/25 21:55:59 | 012,872,704 | ---- | M] (Microsoft Corporation)
"ThreadingModel" = Apartment

[HKEY_LOCAL_MACHINE\Software\Classes\clsid\{5839FCA9-774D-42A1-ACDA-D6A79037F57F}\InProcServer32] /64
"" = C:\Windows\SysNative\wbem\fastprox.dll -- [2009/07/13 21:40:51 | 000,909,312 | ---- | M] (Microsoft Corporation)
"ThreadingModel" = Free

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Classes\clsid\{5839FCA9-774D-42A1-ACDA-D6A79037F57F}\InProcServer32]
"" = %systemroot%\system32\wbem\fastprox.dll -- [2010/11/20 08:19:02 | 000,606,208 | ---- | M] (Microsoft Corporation)
"ThreadingModel" = Free

[HKEY_LOCAL_MACHINE\Software\Classes\clsid\{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}\InProcServer32] /64
"" = C:\Windows\SysNative\wbem\wbemess.dll -- [2009/07/13 21:41:56 | 000,505,856 | ---- | M] (Microsoft Corporation)
"ThreadingModel" = Both

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Classes\clsid\{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}\InProcServer32]

< End of report >