GARRETT DISCOVERY

Report For

Algonquin Township Highway Department

Prepared For: Robert Hanlon
Attorney at Law
robert@robhanlonlaw.com

Prepared By: Andy Garrett
Garrett Discovery Inc
agarrett@garrettdiscovery.com

Date: January 15, 2018

Contents

1.0 Expert Background

I, Andrew Garrett am employed by Garrett Discovery Inc, an Illinois based computer forensics firm specializing in digital investigations and computer forensics. I was selected to review digital evidence and write an expert report. I have been performing computer forensics for the last ten years and was formerly a contractor and principal responsible for the largest computer forensics and electronic discovery facility at the Department of Defense. I have performed forensic analysis for private corporations, federal and state courts. I have processed more than five hundred cases. I have performed expert work by order for federal and state court cases in Tennessee, Wisconsin, Indiana, Delaware, Iowa, Illinois, Florida and Alabama.

I have received forensic training provided by Guidance Software and AccessData, whom are the leading forensic software companies in the United States. Additionally, I have been deemed an expert in multiple federal and state courts and have held numerous computer certifications. My CV (**Attachment A)** and case history **(Attachment B)** are attached.

2.0 Investigation Narrative

I was asked by counsel Robert Hanlon representing Algonquin Township Highway to examine the computers used prior to April 4th, 2017 for evidence of data destruction and alteration of files.

3.0 Timeline of Events

December 9, 2017	Discussion with Robert Hanlon
	Created forensic images of two computes on site and took possession of two computers and imaged off site
December 21, 2017	Obtained forensic images from Wavetek
December 26, 2017	Started forensic analysis of Forensic Images
January 15, 2018	Completed analysis of Server and issued report

4.0 Forensic Analysis Software

In order to process and analyze the forensic image of the server, the following forensic software was used:

- Magnet Forensics Axiom
- Guidance Software Encase

5.0 Evidence Analyzed

The following evidence was analyzed:

Device	**Size (Gigabyte) Logical**	**Hash of Files (MD5)**
Township Road File Server	6000	843b6d6cd7a9939626e79de85be31415

6.0 User Concepts

6.1 File Created Date

File created date is the date the file was created on that volume (C:\, D:\ E:\) and not the date the file was originally authored. For instance, when a file is downloaded from the internet and saved onto the computers local C: drive, the file created date would be the date of download. If the file is moved from the C: drive to the D: drive, the file created date of the file on the D drive would be the date the file was moved because it was 'created' on the D drive.

6.2 File Accessed Date

Anytime a user opens a file (whether or not the file is changed is irrelevant), the File Accessed Date changes to the current computer date. Anytime a file Created and Accessed dates are the same, it is interpreted that, after the file was saved to the volume on which it resides, the file has not been opened again.

6.3 Unallocated Space / Free Space

When a computer user saves a file on a computer many things happen, but important to this investigation is the file name and date properties are written to a pseudo spreadsheet called the Master File Table and the data is stored on the physical hard drive.

When a computer user deletes a file by either (Shift+Delete) or drags those files to the recycle bin and subsequently empties the recycle bin the entry in the Master File table is marked as deleted and eventually overwritten by new incoming data.

An easy way to think about data is a phone book. If I was to remove an entry from the phone book it doesn't destroy the house or business that exists. It only hinders me from finding the house or business. The Master File Table is like a phone book and without it a computer user using the operating system cannot locate a file as there is no reference to it.

We could talk about how a user could install specialized data recovery or forensic software and recover the file, but that would not be relevant to this analogy.

When a file is deleted using the methods described above, the data is still resident on the hard drive, but there is not reference to it from the operating system. It is essentially in a landfill of data that we often call 'unallocated space', because it is not allocated to a file name.

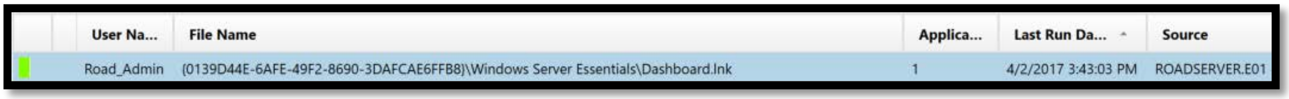
When a new file is stored on the computer the operating system finds an area on the drive that is unallocated and allocates it to the new file, therefore overwriting the previous data that existed.

Forensic software can recover files that were previously deleted by chaining back together the clusters on the hard drive that once was referenced only if those files have not been overwritten.

7.0 Forensic Analysis

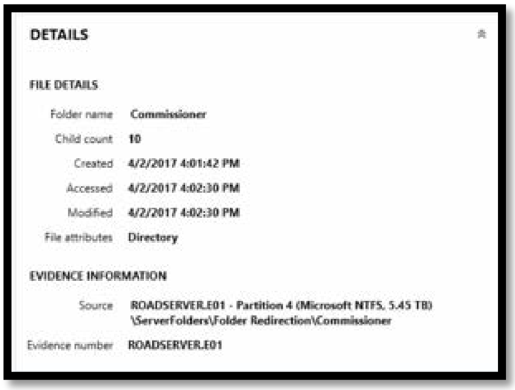
Based on the forensic analysis conduct I was able to determine that a person using two user names as login credentials 'road_admin' and 'commissioner' logged onto the server and performed the following tasks on April 2, 2017 at:

3:43 pm 'Road_Admin" Launched Server Dashboard – The Windows Server Essentials Dashboard is often configured to launch the dashboard. The Dashboard is comprised of applications that are used to administer the server.



		User Na...	File Name	Applica...	Last Run Da...	Source
🟩		Road_Admin	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Windows Server Essentials\Dashboard.lnk	1	4/2/2017 3:43:03 PM	ROADSERVER.E01

4:01 pm User Profile 'Commissioner', 'Manager', was deleted and rebuilt



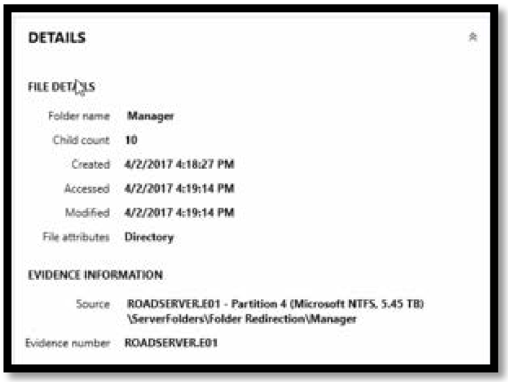
DETAILS

FILE DETAILS

Folder name	Commissioner
Child count	10
Created	4/2/2017 4:01:42 PM
Accessed	4/2/2017 4:02:30 PM
Modified	4/2/2017 4:02:30 PM
File attributes	Directory

EVIDENCE INFORMATION

Source	ROADSERVER.E01 - Partition 4 (Microsoft NTFS, 5.45 TB) \ServerFolders\Folder Redirection\Commissioner
Evidence number	ROADSERVER.E01



DETAILS

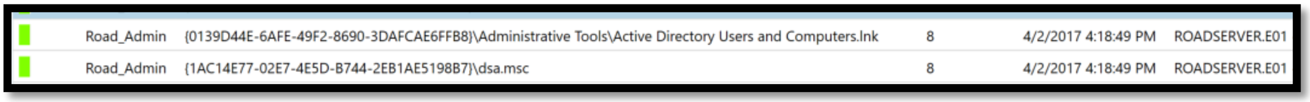
FILE DETAILS

Folder name	Manager
Child count	10
Created	4/2/2017 4:18:27 PM
Accessed	4/2/2017 4:19:14 PM
Modified	4/2/2017 4:19:14 PM
File attributes	Directory

EVIDENCE INFORMATION

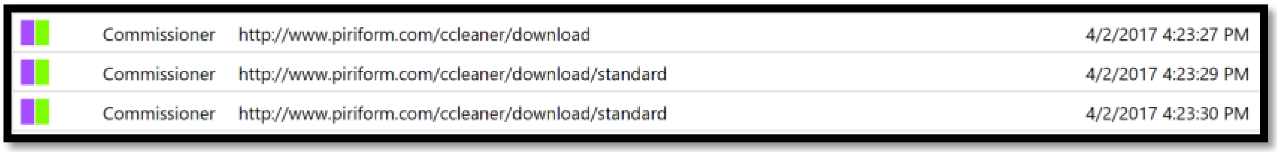
Source	ROADSERVER.E01 - Partition 4 (Microsoft NTFS, 5.45 TB) \ServerFolders\Folder Redirection\Manager
Evidence number	ROADSERVER.E01

4:18 pm ‘Road_Admin’ opened Active Directory Users and Computers (dsa.msc) which is used to maintain user profiles, add and remove users from access.

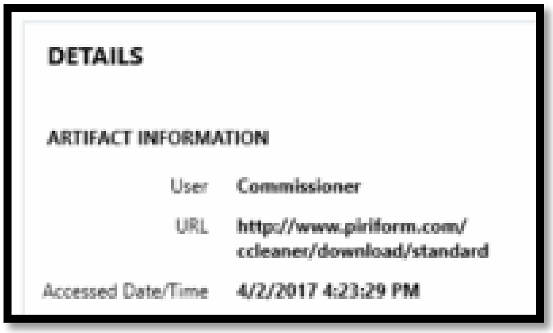


🟩	Road_Admin	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Administrative Tools\Active Directory Users and Computers.lnk	8	4/2/2017 4:18:49 PM	ROADSERVER.E01
🟩	Road_Admin	{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\dsa.msc	8	4/2/2017 4:18:49 PM	ROADSERVER.E01

4:23 pm ‘Commisioner’ browsed the internet for a program named CCleaner and subsequently downloaded the program



🟪🟩	Commissioner	http://www.piriform.com/ccleaner/download	4/2/2017 4:23:27 PM
🟪🟩	Commissioner	http://www.piriform.com/ccleaner/download/standard	4/2/2017 4:23:29 PM
🟪🟩	Commissioner	http://www.piriform.com/ccleaner/download/standard	4/2/2017 4:23:30 PM



DETAILS

ARTIFACT INFORMATION

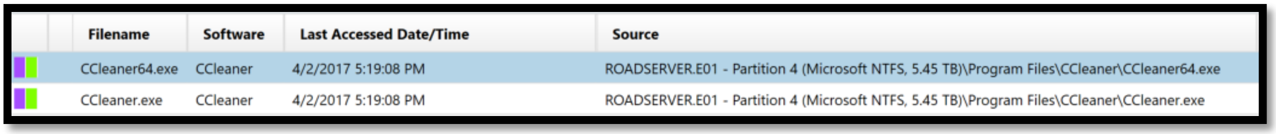
User Commissioner

URL http://www.piriform.com/ccleaner/download/standard

Accessed Date/Time 4/2/2017 4:23:29 PM

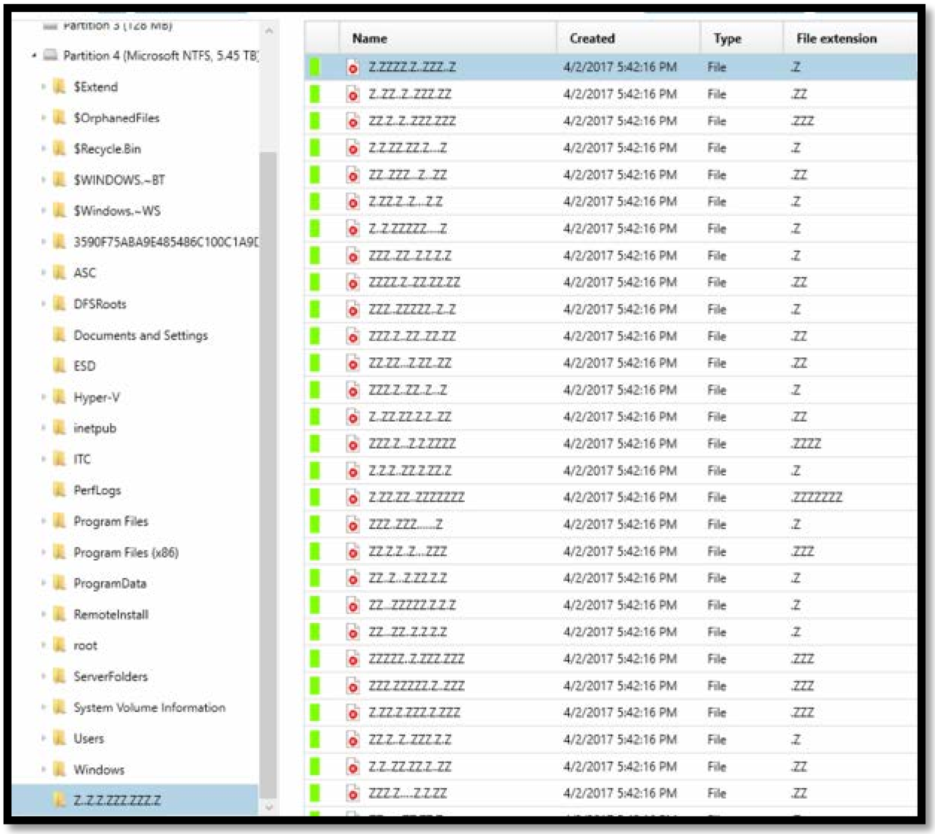
`

5:19 CCleaner was launched and ran on the computer



	Filename	Software	Last Accessed Date/Time	Source
🟪🟩	CCleaner64.exe	CCleaner	4/2/2017 5:19:08 PM	ROADSERVER.E01 - Partition 4 (Microsoft NTFS, 5.45 TB)\Program Files\CCleaner\CCleaner64.exe
🟪🟩	CCleaner.exe	CCleaner	4/2/2017 5:19:08 PM	ROADSERVER.E01 - Partition 4 (Microsoft NTFS, 5.45 TB)\Program Files\CCleaner\CCleaner.exe

5:42 Computer usage left evidence showing CCleaner overwrite the file names of some files with ZZZ’s and then failed at the subsequent deletion process.



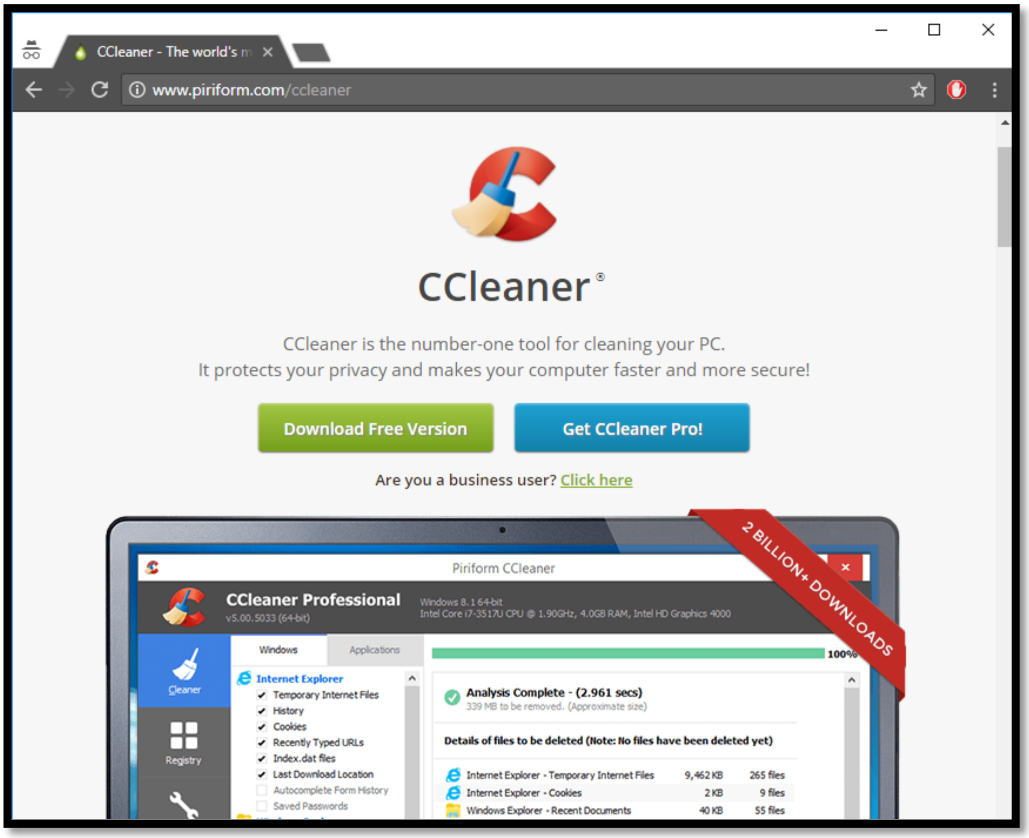
- Partition 3 (128 MB)
- Partition 4 (Microsoft NTFS, 5.45 TB)
  - $Extend
  - $OrphanedFiles
  - $Recycle.Bin
  - $WINDOWS.~BT
  - $Windows.~WS
  - 3590F75ABA9E485486C100C1A9D
  - ASC
  - DFSRoots
  - Documents and Settings
  - ESD
  - Hyper-V
  - inetpub
  - ITC
  - PerfLogs
  - Program Files
  - Program Files (x86)
  - ProgramData
  - RemoteInstall
  - root
  - ServerFolders
  - System Volume Information
  - Users
  - Windows
  - Z..Z.Z.ZZZ.ZZZ.Z

	Name	Created	Type	File extension
🟩	Z.ZZZZ.Z..ZZZ..Z	4/2/2017 5:42:16 PM	File	.Z
🟩	Z..ZZ..Z..ZZZ.ZZ	4/2/2017 5:42:16 PM	File	.ZZ
🟩	ZZ.Z..Z..ZZZ.ZZZ	4/2/2017 5:42:16 PM	File	.ZZZ
🟩	Z.Z.ZZ.ZZ.Z...Z	4/2/2017 5:42:16 PM	File	.Z
🟩	ZZ..ZZZ...Z...ZZ	4/2/2017 5:42:16 PM	File	.ZZ
🟩	Z.ZZ.Z..Z...Z.Z	4/2/2017 5:42:16 PM	File	.Z
🟩	Z..Z.ZZZZZ....Z	4/2/2017 5:42:16 PM	File	.Z
🟩	ZZZ..ZZ..Z.Z.Z.Z	4/2/2017 5:42:16 PM	File	.Z
🟩	ZZZZ.Z..ZZ.ZZ.ZZ	4/2/2017 5:42:16 PM	File	.ZZ
🟩	ZZZ..ZZZZZ..Z..Z	4/2/2017 5:42:16 PM	File	.Z
🟩	ZZZ.Z..ZZ..ZZ.ZZ	4/2/2017 5:42:16 PM	File	.ZZ
🟩	ZZ.ZZ...Z.ZZ..ZZ	4/2/2017 5:42:16 PM	File	.ZZ
🟩	ZZZ.Z..ZZ..Z...Z	4/2/2017 5:42:16 PM	File	.Z
🟩	Z..ZZ.ZZ.Z.Z..ZZ	4/2/2017 5:42:16 PM	File	.ZZ
🟩	ZZZ.Z...Z.Z.ZZZZ	4/2/2017 5:42:16 PM	File	.ZZZZ
🟩	Z.Z.Z..ZZ.Z.ZZ.Z	4/2/2017 5:42:16 PM	File	.Z
🟩	Z.ZZ.ZZ..ZZZZZZZ	4/2/2017 5:42:16 PM	File	.ZZZZZZZ
🟩	ZZZ..ZZZ......Z	4/2/2017 5:42:16 PM	File	.Z
🟩	ZZ.Z.Z..Z...ZZZ	4/2/2017 5:42:16 PM	File	.ZZZ
🟩	ZZ..Z...Z.ZZ.Z.Z	4/2/2017 5:42:16 PM	File	.Z
🟩	ZZ...ZZZZZ.Z.Z.Z	4/2/2017 5:42:16 PM	File	.Z
🟩	ZZ...ZZ..Z.Z.Z.Z	4/2/2017 5:42:16 PM	File	.Z
🟩	ZZZZZ..Z.ZZZ.ZZZ	4/2/2017 5:42:16 PM	File	.ZZZ
🟩	ZZZ.ZZZZZ.Z..ZZZ	4/2/2017 5:42:16 PM	File	.ZZZ
🟩	Z.ZZ.Z.ZZZ.Z.ZZZ	4/2/2017 5:42:16 PM	File	.ZZZ
🟩	ZZ.Z..Z..ZZZ.Z.Z	4/2/2017 5:42:16 PM	File	.Z
🟩	Z.Z..ZZ.ZZ.Z..ZZ	4/2/2017 5:42:16 PM	File	.ZZ
🟩	ZZZ.Z....Z.Z.ZZ	4/2/2017 5:42:16 PM	File	.ZZ

7.1 Piriform Application CCleaner

CCleaner is a program that does not come pre-bundled with the Windows Operationg system. In order to obtain CCleaner a user would have to navigate to www.piriform.com/ccleaner website and download the application. The user of the Algonquin server downloaded, installed and ran CCleaner on April 2nd 2017.

A screenshot of the Piriform website showing CCleaner is below



CCleaner is the number-one tool for cleaning your PC.
It protects your privacy and makes your computer faster and more secure!

Are you a business user? Click here

Internet Explorer
☑ Temporary Internet Files
☑ History
☑ Cookies
☑ Recently Typed URLs
☑ Index.dat files
☑ Last Download Location
☐ Autocomplete Form History
☐ Saved Passwords

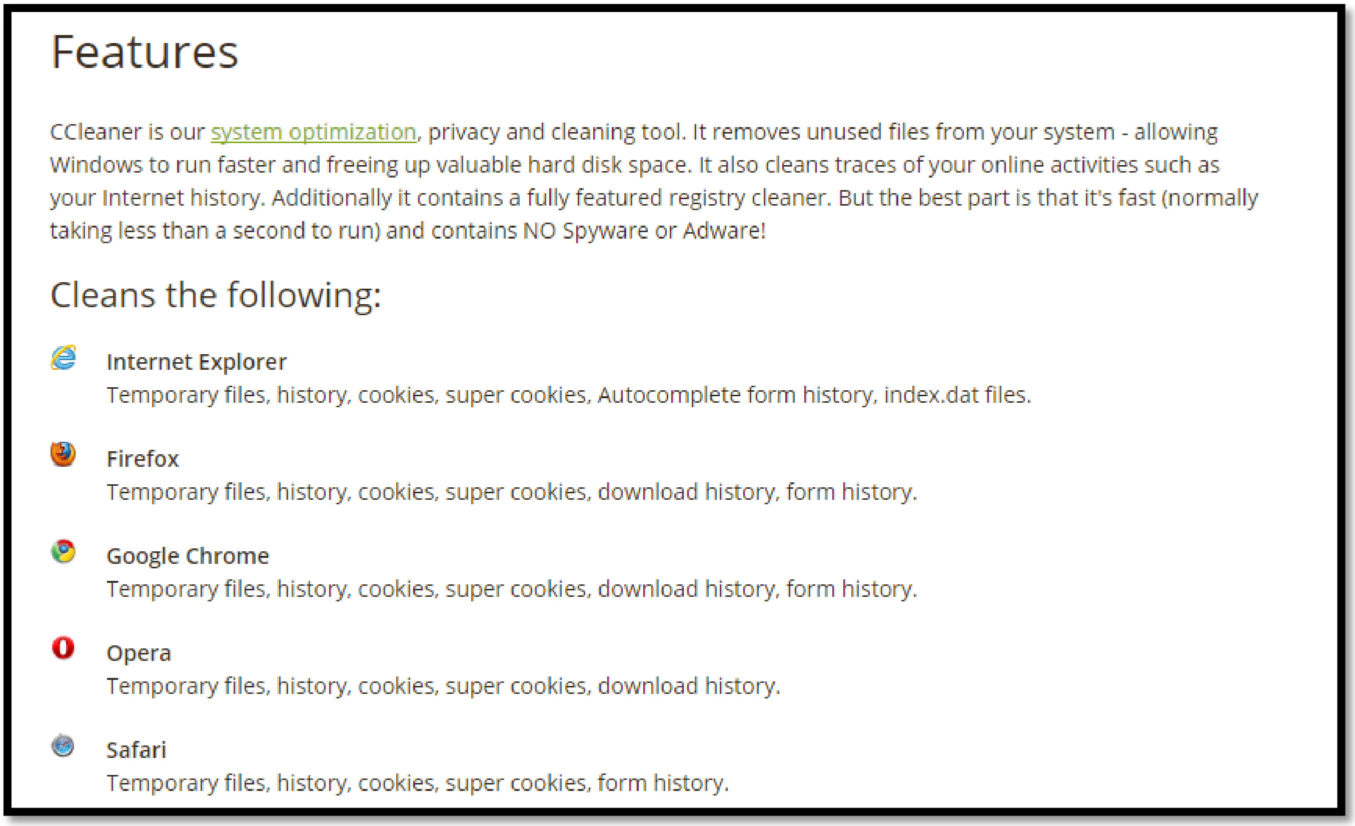
Analysis Complete - (2.961 secs)
339 MB to be removed. (Approximate size)

Details of files to be deleted (Note: No files have been deleted yet)

Internet Explorer - Temporary Internet Files	9,462 KB	265 files
Internet Explorer - Cookies	2 KB	9 files
Windows Explorer - Recent Documents	40 KB	55 files

The reader should notice the 'Download Free Version' and the 'Get CCleaner Pro'. CCleaner advertises that it is a 'cleaning tool' and cleans "traces of your online activities such as your Internet history" and "Additionally it contains a fully featured registry cleaner"

The free version of CCleaner allows a user to perform functions such as those listed on the CCleaner website (see graphic below).



Features

CCleaner is our system optimization, privacy and cleaning tool. It removes unused files from your system - allowing Windows to run faster and freeing up valuable hard disk space. It also cleans traces of your online activities such as your Internet history. Additionally it contains a fully featured registry cleaner. But the best part is that it's fast (normally taking less than a second to run) and contains NO Spyware or Adware!

Cleans the following:

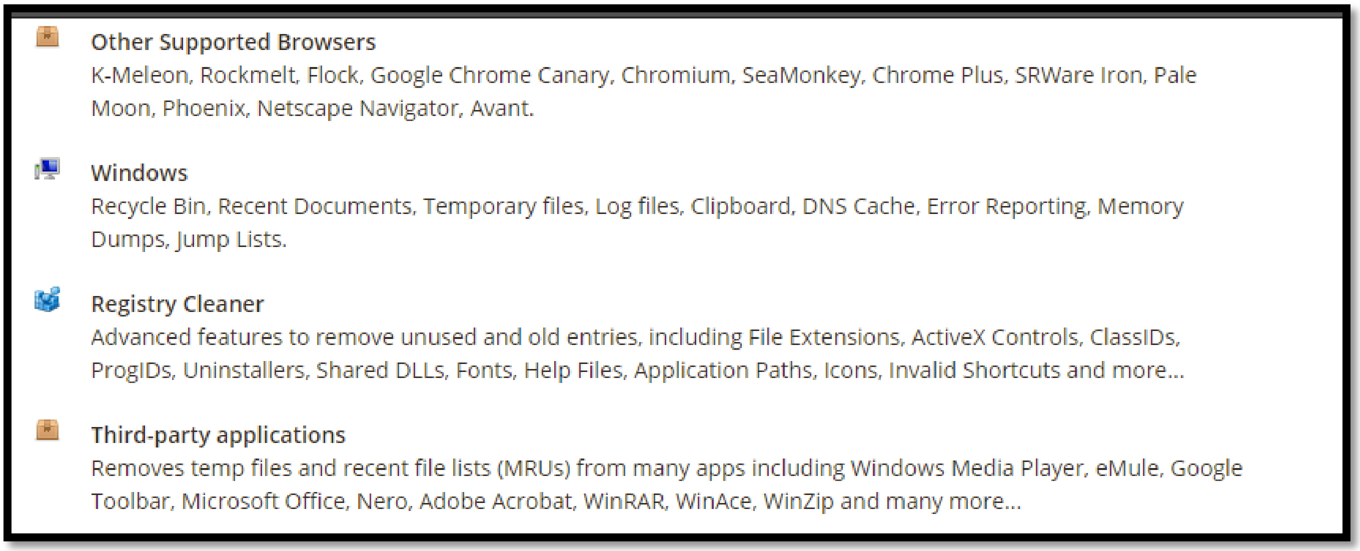
Internet Explorer
Temporary files, history, cookies, super cookies, Autocomplete form history, index.dat files.

Firefox
Temporary files, history, cookies, super cookies, download history, form history.

Google Chrome
Temporary files, history, cookies, super cookies, download history, form history.

Opera
Temporary files, history, cookies, super cookies, download history.

Safari
Temporary files, history, cookies, super cookies, form history.



Other Supported Browsers
K-Meleon, Rockmelt, Flock, Google Chrome Canary, Chromium, SeaMonkey, Chrome Plus, SRWare Iron, Pale Moon, Phoenix, Netscape Navigator, Avant.

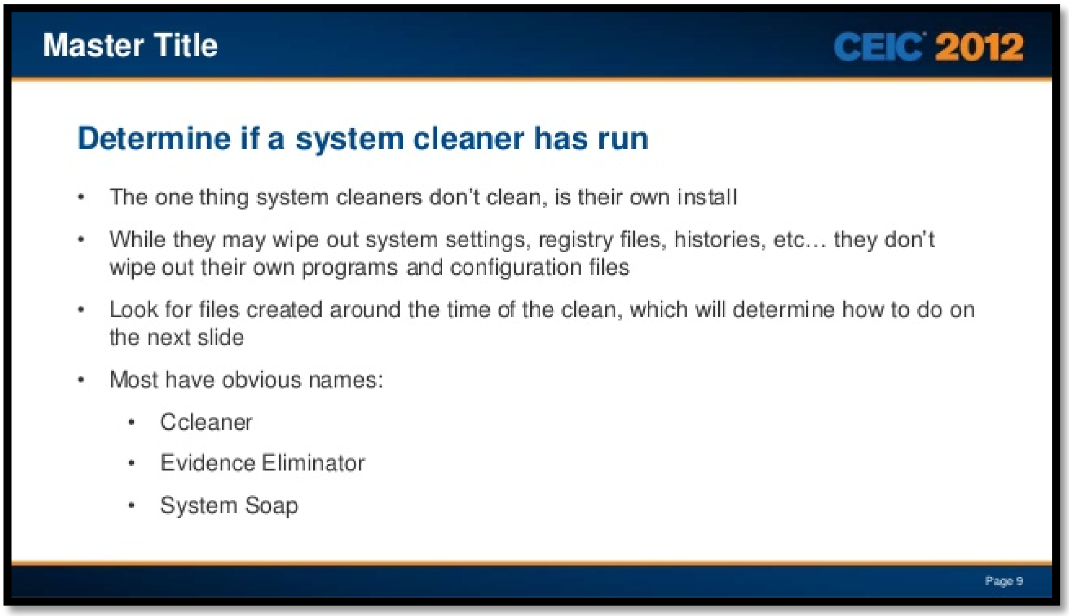
Windows
Recycle Bin, Recent Documents, Temporary files, Log files, Clipboard, DNS Cache, Error Reporting, Memory Dumps, Jump Lists.

Registry Cleaner
Advanced features to remove unused and old entries, including File Extensions, ActiveX Controls, ClassIDs, ProgIDs, Uninstallers, Shared DLLs, Fonts, Help Files, Application Paths, Icons, Invalid Shortcuts and more...

Third-party applications
Removes temp files and recent file lists (MRUs) from many apps including Windows Media Player, eMule, Google Toolbar, Microsoft Office, Nero, Adobe Acrobat, WinRAR, WinAce, WinZip and many more...

7.2 CCleaner – Anti-Forensic Tool

CCleaner is listed as one of the top Anti Forensic tools by the forensic community. A presentation was given at the largest computer forensic conference in the world Computer Enterprise Investigations Conference (CEIC) put on by Guidance Software the tool used by over 90% of law enforcement labs. See below slide showing CCleaner.



Master Title

CEIC 2012

Determine if a system cleaner has run

- The one thing system cleaners don't clean, is their own install
- While they may wipe out system settings, registry files, histories, etc… they don't wipe out their own programs and configuration files
- Look for files created around the time of the clean, which will determine how to do on the next slide
- Most have obvious names:
  - Ccleaner
  - Evidence Eliminator
  - System Soap

Page 9

7.3 CCleaner – Wiping Free Space (Unallocated)

CCleaner also has a feature that wipes out previously deleted data. This option is called "Wipe Free Space" and overwrites data. You may think that if CCleaner is ran on a computer, that there should be no previously deleted data recovered.

An example of how this can wipe out data is below:

1. User downloads 1000 pictures from the internet over 2 years

2. User moves all of the downloaded pictures into the recycle bin or clicks shift + delete

3. User Empties the Windows Recycle Bin

4. The user can no longer see the files using the operating system, but forensic programs can recover the files from the spaces on the hard drive that are no longer allocated to the file system. This is called ‘unallocated / free space”

5. CCleaners Wipe Free Space option is ran against the hard drive and the file that could have been recovered are overwritten through a process of renaming the files with ZZZ’s, deleting them and then overwriting the free space with all 0’s.

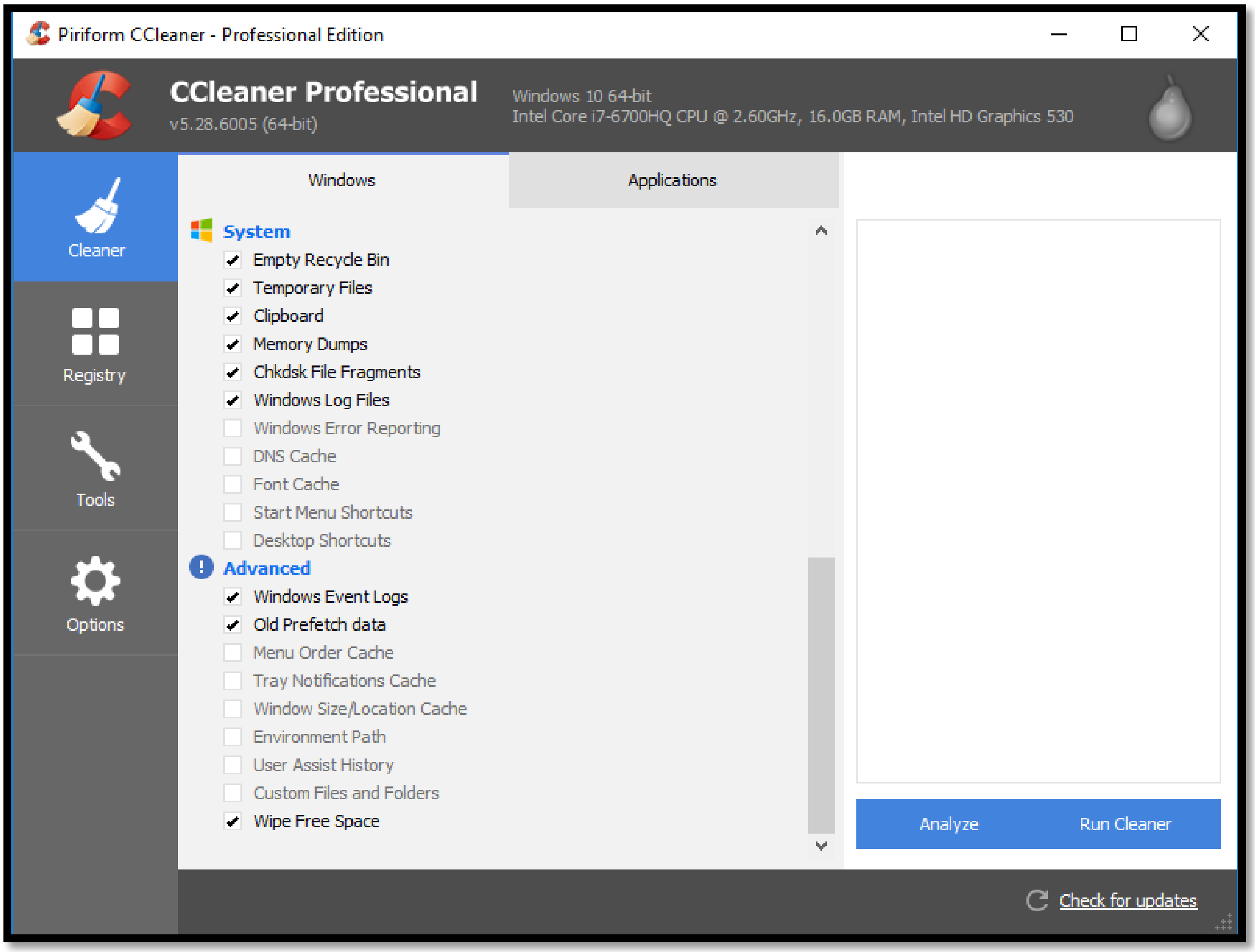
6. The files can no longer be recovered using any method

This option may work for pictures that were downloaded, but have no bearing on things such as internet history containing within databases or files that are not deleted.   Deleting internet website history is not the same process.

CCleaner touts its ability to wipe out files permanently on its website at https://www.piriform.com/docs/ccleaner/using-ccleaner/wiping-free-disk-space.

“When you delete a file, Windows removes the reference to that file, but doesn't delete the actual data that made up the file on your hard drive. Over time, this data will be overwritten as Windows writes new files to that area of the drive.

This means that, given the right software, someone could reconstruct all, or parts of files that you've deleted. By default, CCleaner does not wipe free space. A user of the software must select the option to run the wiping of free space. See graphic below:



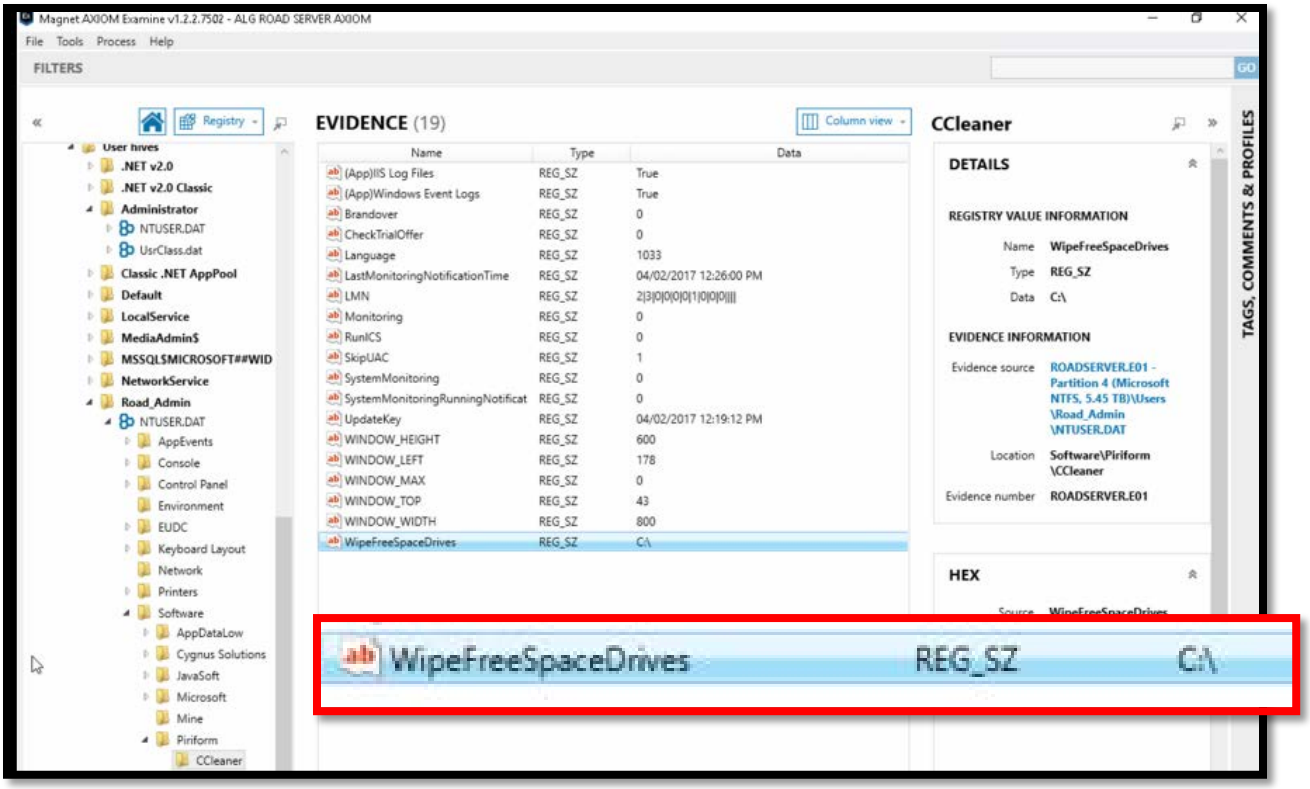
System

- ☑ Empty Recycle Bin
- ☑ Temporary Files
- ☑ Clipboard
- ☑ Memory Dumps
- ☑ Chkdsk File Fragments
- ☑ Windows Log Files
- □ Windows Error Reporting
- □ DNS Cache
- □ Font Cache
- □ Start Menu Shortcuts
- □ Desktop Shortcuts

Advanced

- ☑ Windows Event Logs
- ☑ Old Prefetch data
- □ Menu Order Cache
- □ Tray Notifications Cache
- □ Window Size/Location Cache
- □ Environment Path
- □ User Assist History
- □ Custom Files and Folders
- ☑ Wipe Free Space

When a user selects the ‘Wipe Free Space’ option the operating system memorizes this selection by setting a registry key. I was able to examine the registry for user ‘Road_Admin’ and based on the registry key ‘Wipe Free Space’ was an option selected as C:\ and therefore would wipe out files that have been previously deleted on the drive C:\.



EVIDENCE (19)

Name	Type	Data
(App)IIS Log Files	REG_SZ	True
(App)Windows Event Logs	REG_SZ	True
Brandover	REG_SZ	0
CheckTrialOffer	REG_SZ	0
Language	REG_SZ	1033
LastMonitoringNotificationTime	REG_SZ	04/02/2017 12:26:00 PM
LMN	REG_SZ	2|3|0|0|0|0|1|0|0|0|||
Monitoring	REG_SZ	0
RunICS	REG_SZ	0
SkipUAC	REG_SZ	1
SystemMonitoring	REG_SZ	0
SystemMonitoringRunningNotificat	REG_SZ	0
UpdateKey	REG_SZ	04/02/2017 12:19:12 PM
WINDOW_HEIGHT	REG_SZ	600
WINDOW_LEFT	REG_SZ	178
WINDOW_MAX	REG_SZ	0
WINDOW_TOP	REG_SZ	43
WINDOW_WIDTH	REG_SZ	800
WipeFreeSpaceDrives	REG_SZ	C:\

CCleaner

DETAILS

REGISTRY VALUE INFORMATION

Name WipeFreeSpaceDrives
Type REG_SZ
Data C:\

EVIDENCE INFORMATION

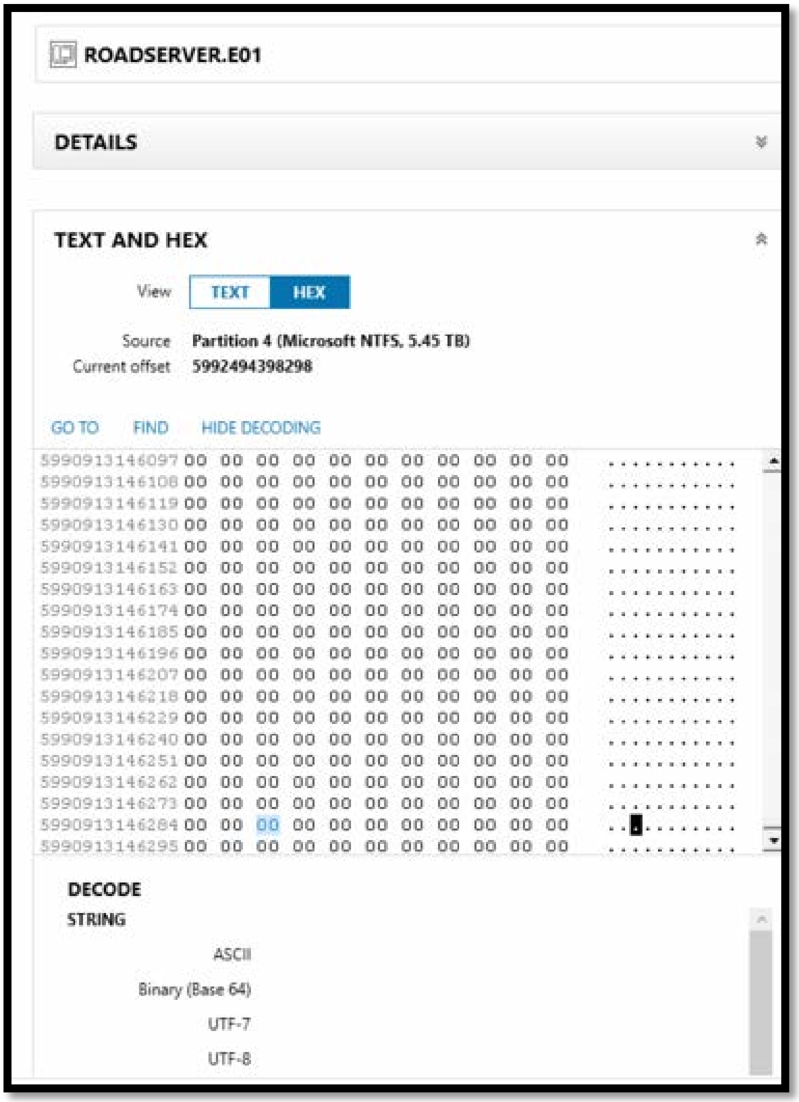
Evidence source ROADSERVER.E01 - Partition 4 (Microsoft NTFS, 5.45 TB)\Users\Road_Admin\NTUSER.DAT
Location Software\Piriform\CCleaner
Evidence number ROADSERVER.E01

HEX

Source WipeFreeSpaceDrives

WipeFreeSpaceDrives REG_SZ C:\

I have performed many examinations and testified at trials involving the user of CCleaner. One of the most telling aspects of its use is that it wipes out the unallocated / free space of a hard drive by overwriting it with all 0's, therefore hindering the ability to recover deleted files. This is very obvious when looking at the surface of a disk using forensic tools. Below is a graphic showing the surface of servers disk drive showing that about 40% of the drive has been wiped using CCleaners wipe free space tool.



ROADSERVER.E01

DETAILS

TEXT AND HEX

View TEXT HEX

Source Partition 4 (Microsoft NTFS, 5.45 TB)
Current offset 5992494398298

GO TO FIND HIDE DECODING

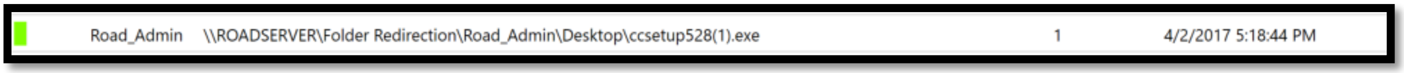
```
5990913146097 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146108 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146119 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146130 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146141 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146152 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146163 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146174 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146185 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146196 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146207 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146218 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146229 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146240 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146251 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146262 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146273 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146284 00  00  00  00  00  00  00  00  00  00  00    ...........
5990913146295 00  00  00  00  00  00  00  00  00  00  00    ...........
```

DECODE
STRING

ASCII
Binary (Base 64)
UTF-7
UTF-8

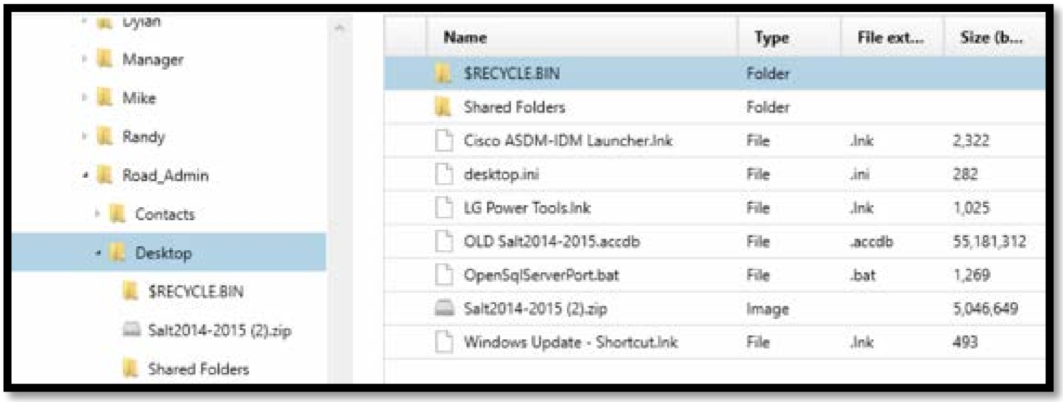
7.4 CCleaner removal from computer

By examining the location in which CCleaner was downloaded and saved to it (see below)



🟩 Road_Admin \\ROADSERVER\Folder Redirection\Road_Admin\Desktop\ccsetup528(1).exe 1 4/2/2017 5:18:44 PM

I was able to determine that the setup file was subsequently removed from the computer by both deleting it from the desktop, but also removing it from the recycle bin.



Name	Type	File ext...	Size (b...
$RECYCLE.BIN	Folder		
Shared Folders	Folder		
Cisco ASDM-IDM Launcher.lnk	File	.lnk	2,322
desktop.ini	File	.ini	282
LG Power Tools.lnk	File	.lnk	1,025
OLD Salt2014-2015.accdb	File	.accdb	55,181,312
OpenSqlServerPort.bat	File	.bat	1,269
Salt2014-2015 (2).zip	Image		5,046,649
Windows Update - Shortcut.lnk	File	.lnk	493

8.0 Conclusion

It is my conclusion based on the totality of the evidence a user logged onto the server on April 2, 2017 and installed an anti-forensic software package designed to delete and destroy data, executed that program and destroyed beyond recover many files.

Additionally, a user took action to remove the user profile of ‘commissioner’ and ‘manager’ from the profile redirection folders including all files within those folders essentially deleting all user created data that was stored in those profiles and even deleted the local server login profile for those usernames.

After deletion of the folders and profiles the profiles were rebuilt and gives the appearance that they have never been deleted, except that no user created data is present in those profiles.

9.0 Declaration

I declare under penalty and perjury under the laws of the State of Illinois that the information provided is true and correct.

Andy Garrett

_______________________________ January 15, 2018

Andy Garrett Date