GARRETT DISCOVERY

Report For

Dena Lewis-Bystrzycki

v.

City of Country Club Hills, Carl Pycz,

Joseph Ellington, and Roger Agpawa

Case ID - 2012 L 00916

Report on ESI Destruction

Prepared For: Dana Kurtz
Attorney at Law

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

Date: July 21, 2017

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 and ordered by the court to examine the computers that were in place during the time of employment of the plaintiff to report on the efforts to identify and collect ESI, possible destruction or withholding of ESI.

On May 18, 2017 I issued a 2,164 page report regarding the use of Country Club Hills computers to surf pornography.   This report was filed as a separate report and its findings and opinions stand alone and have no weight or bearing on this report.

3.0 Timeline of Events

I have written what I consider the importance of each of these events in **bold** and cited prior discovery materials as reference. Although, this is the best available information to show a timeline of events, the dates of the actual event may be on or about that date.

February 27, 2012	**Plaintiff files IDHR Charge**
April 13, 2012	**Defendant files appearance before the IDHR, and had received prior notice of preservation requirements from IDHR** See https://www.illinois.gov/dhr/FilingaCharge/Pages/Investigation.aspx
August 31, 2012	**Complaint Filed (See Attachment C)**
December 2013	**Plaintiff served initial discovery requests on Defendant**
April 15, 2013	**First Amended Complaint (See Attachment D)**
July 2, 2015	**Plaintiff served second supplemental discovery requests on defendants**
July 7 2015	**Plaintiff files Supplemental Complaint (See Attachment E)**

July 11, 2015 **Notice of Inspection (See Attachment F)**

"The computers for inspection and imaging using Encase Forensic software by Guidance Software or other comparable software, which located in (a) the classroom at Station 1, (b) the middle office across from the bathroom at Station 1, (c) the paramedic writing room computer at Station 2, and (d) the computer in the hallway by the engineers' office at Station 2; and This notice of inspection requires Defendants and Defendants' agents and employees to not alter in any way, shape, or form, any of the areas, documents, data, contents, and information to be inspected."

NOTE: AT THIS TIME THE COMPUTERS HAVE NOT BEEN UPGRADED OR SWAPPED OUT

July 17, 2015 **Defendant's Motion for Protective Order regarding Notice of Inspection**

August 18, 2015 **Plaintiff's Corrected Response to Protective Order (Attachment G)**

"Defendants erroneously claim that Plaintiff's Amended Notice of Inspection is overly broad, unduly burdensome, and irrelevant to issues in the case. In fact, all the areas Plaintiff has requested to inspect are relevant to Plaintiff's claims and the relevancy has been substantiated by testimony in this case.

Second, Plaintiff noticed the "[t]he computers for inspection and imaging" and the "the Televisions and cable boxes" due to evidence acquired during discovery that pornography is viewed at the Country Club Hills firehouses. There has been testimony on the record, during two separate depositions, that pornography is viewed by firefighters at the firehouse(s), including one Lieutenant who admitted *to watching pornography. (See Exhibit 2, Dep. Draft Transcript of Lt. Dangoy at 191-95 (excerpt only); Exhibit 3, Dep. Transcript of Defendant Pycz at 40 (excerpt only).)"*

August 20, 2015 **Country Club Hills Public Safety Director William A. Brown sends memorandum to all Department Personnel that an Investigation is underway. *(See Attachment H)***

"At the request of Fire Chief Roger Agpawa I am directing that an investigation into the use of cable TV in the station and Internet Services at the station using the city's wifi system be launched immediately. Investigators from the police department and personnel from the IT department will be conducting the investigation"

August 21, 2015 **Country Club Hills installs web filters to block pornography websites (See Attachment I)**

Wayne Werosh Country Club Hills IT consultant deposition of March 14, 2017 included:

"*Research and install DNS Web filtering at Station 1 and Station 2"* Page 143 Line 12-13 and when asked what it was for stated *"I believe it was both Chief Agpawa and Deputy Chief Kopec to look into installing filters into their computer networks to restrict access to objectional material: pornography, violence, things like that"*. **(See Attachment I at Page 143 Line 20-24**).

When asked if he had installed those filters in 2015 to prevent users from viewing that type of material he responded with "*yes*" **(See Attachment I Page 144 Line 6)** and was operational in August of 2015.

September 11, 2015 **Rudy Maybell (CCH IT Director) sends letter stating that computers were being monitored, no expectation of privacy and that there was no misuse of the computers and all internet history is being recorded. (See Attachment J)**

"The City regularly monitors and /or logs network activity with or without notice, including e-mail and all website communications, and therefore, users should have no reasonable expectation of privacy in the use of these resources.

- *a) City monitors logs network activity and all website communications*
- *b) There is no expectation of privacy for internet usage by employees*

1. *The following information reflects the Fire Department Internet and Software Audit started on 8/28-2015 and completed on 9/10/2015.*
   - *a) The city conducted a software audit*

2. *Review of inventoried equipment disclosed no irregularities or misuse of City equipment and policies based on our Country Club Hills Handbook of personnel, policies and procedures page 88 under {Acceptable Use of Technology Policy}.*
   - *a) No irregularities found*

3. *If deep forensic type hard drive discovery is required, we refer WTM Werosh Technology Management, located in Oak Forest, IL. As a vendor who can perform those services."*

August 21, 2016 **Wayne Werosh IT Consultant for Country Club Hills formats (wiped) drives on Network Attached Storage system. The network attached storage system holds backups and fire station files and is used as a fileserver and was wiped of its data. (See Attachment K)**

Wayne Werosh Deposition "*removed the network attached storage device from Station 1, I rebuilt it, and on 3/4/2016 I reinstalled it in the library in the network cabinet"* **(See Attachment I Page 115 Line 11-14)**

October 7, 2015 **Country Club Hills hires an outside Human Resources person, Marion Williams to conduct an investigation of the employees of the Country Club Hills regarding the use of the computers and tv based on allegations of employees watching pornography at work**. **(See Attachment L)**

November 9, 2015 **Country Club Hills Fire Chief Agpawa sends letter to Attorney Daniel Boddicker regarding an internal investigation regarding the use of the TV and computers to watch pornography and attached the IT Report and Williams HR Report. (See Attachment M)**

When Williams asked the employees: Carl Pycz, Glen McAuliff, Michael Kilburg, Raymond Bernadisius, Michelle Hullinger, Derek Dangoy, Nicholas Jula and Lawrenece Gillespie if they had any knowledge of employees watching porn while at the firehouse none of them admitted to surfing or seeing someone surf pornography websites.

My May 18, 2017 2,164 page report at page 12 – 16 clearly shows that Carl Pycz and Lawrence Gillespie were surfing and downloading large amounts of pornography on the computers contrary to their statements to Williams.

February 17, 2016 **CCleaner was ran on computer '6RW2GZ36' (See report below for more information)**

April 22, 2016 **Court Order, granting Plaintiff's Motion to Compel, and entered and continued Plaintiff's motion as to the computer imaging and inspection, and ordering the Parties' counsel, Plaintiff's expert, and Defendant's IT person to meet and confer to discuss search terms on other ESI issues.**

April 28, 2016 **Meet and confer per the Court's April 22, 2016 Order with Plaintiff's counsel, 4Discovery, Defendant's counsel and Rudy Maybell, regarding the existence and location of ESI, etc. No identification of the NAS server.**

March 4, 2016 **Wayne Werosh Installs the Rebuilt Network Attached Storage Device**

Wayne Werosh installed the Network Attached Storage device taken out of service on January 1, 2016 and testified that "to the best of my-my recollection the server, the training room computer, the computer in the lieutenant's office, and one of the computers in the library" **(Attachment I Page 116 Line15-18)** were being "imaged onto the NAS" **(Attachment I Page 116: Line 10-11)**

April 6, 2016 **Plaintiff filed Second Motion to Compel and for Sanctions (Attachment N)**

May 11, 2016 **CCleaner was ran on computer '6RW2GZ36' (See report below for more information)**

June 14, 2016 **Wayne Werosh IT Consultant for Country Club Hills received a call from Lt. Bernadisius authorizing fire station computers eligible for Windows 10 to be upgraded (Attachment O)**

The very computers that were subject of the litigation in the training room were being upgraded by Lt. Bernadisuis and not Wayne Werosh the night prior to Mr. Werosh arriving to upgrade the computers.

The two computers that were subject to this litigation are the two computers “across from the bathroom” and the room was identified to me by Mr. Maybell, Mr. Boddicker and Mr. Sachnoff as the training room and also called the library.

“*I discussed the process with Lt. Bernadisius, who started the Training room Desktop the evening of 6/15/2016 with the agreement that we would start upgrading all devices in the morning on 6/16/2016.”*

June 24, 2016 **Court Order on Plaintiff’s Second Motion to Compel and for Sanctions, entering and continuing the motion for hearing on July 29, 2016, and ordering Defendants to answer questions from Forensic expert by July 8, 2016.**

July 19, 2016 Plaintiff’s 3rd Motion for Sanctions

Motion stated “Defendants and their counsel have violated and repeatedly ignored numerous Orders by this Court . . . Most recently on June 24, 2016, this Court entered an order requiring Defendants’ to answer the questions from Plaintiff’s forensic expert on the manner in which their electronic records (ESI) are kept and maintained by ***July 8, 2016.*** *. . . Defendants have failed to comply with this Court’s June 24, 2016 Order, and have not answered the forensic expert’s questions or so much as responded that they needed more time. They have simply ignored this Court’s order (like the many other orders that have been ignored by Defendants and their counsel).”*

July 25, 2016 **Disk Defragmenter was ran on computer ‘6RW2GZ36’ (see report below for more information)**

July 27, 2016 **Robert Kopec sent an email to CCH employees advising them that two computers were going to be replaced and to copy any data before they are taken out of service identified in this report as computer WCATR1278977 AND WCATR1278977(See Attachment P)**

July 27, 2016 **Wayne Werosh removed the two computers from service from the "training room" (the "room across from the bathroom") described by the plaintiff in the notice of inspection, and as being some of the computers used to surf pornography. These are the same two computers Werosh notified in two separate conversations Chief Roger Agpawa and Deputy Chief Kopec that they should be retained and left evidence tags on them.**

Wayne Werosh made a few assertions during his deposition regarding the removal of the two computers not previously identified by the defendants. At the time of the deposition I had not been told or informed that these computers were replaced with other computers from other areas in the firestation.

Werosh informed the Chief and Deputy Chief in two separate conversations that he took the two desktop computers out of service at Fire Station 1 and*"that they should probably keep them and not do anything with them"* Page 93 Line 6-11 and in another section of testimony commented as to why he had that conversation and responded with *"Because I had had the previous conversation with him about the forensic imaging and thought that it would probably be in his best interest if those were left alone"* **(Attachment I Page 99-100 Line 22-24)**.

	Mr. Werosh said both computers “*were left in the library on the floor up against the west wall”* **(Attachment I Page 99 Line 5-6**) and that *“There were only two computers – there were only two desktop computers in the library. And both of them were Windows XP machines that I previously stated I took out of service and left with tags on them”*
July 29, 2016	**Court Order, entering and continuing Plaintiff’s 3rd Motion for Sanctions, and Plaintiff’s 2nd Motion to Compel and for sanctions to August 31, 2016.**
August 1-14, 2016	**Disk Defragmenter was run on computer WCATR1278977 on August 1, 4, 11, 14. (See Report Below for more details)**
August 8, 2016	**Disk Defragmenter was run on computer ‘6RW2GZ36’ (See Report Below for more details)**
August 12, 2016	**Defendants answered 4Discovery questions that were generated from April 28, 2016 telephone call regarding ESI issues. No identification of the NAS server.**
August 12, 2016	**Disk Cleanup was run on computer ‘WCATR1278977’ (See Report Below for more details)**
August 31, 2016	**Court Order granting Plaintiff’s Second Motion to Compel as to the imaging of the four computers identified in the notice of inspection. The Court denied Plaintiff’s 3rd Motion for Sanctions without prejudice for reasons stated in the transcript.**

Report of Proceedings memorialized the courts intentions as to a forensic examination of the computers referenced by the Plaintiff. (See Attachment Q)

See transcript "Now, I thank you both for your patience in giving me time to look at everything again. After reviewing everything, I am granting the second motion to compel regarding plaintiff's request for a forensic examination regarding those computers in the classroom at station one, the middle office across from the bathroom at station one, the paramedic writing room computer at station two and the computer in the hallway by the engineer's office at station two.

"After reading the depositions, I have concluded this isn't a fishing expedition. The plaintiff was not wholly unable to come up with (inaudible) that she witnessed fellow employees watching porn. The problem is according to her the porn watching was pervasive. So, for example, every time she would worked with Larry, I don't know how to pronounce it, Giseppe --Giseppe? he was watching porn. And that applied to Mr. Marcus 65 percent of the time and Mr. Boyd 50 percent of the time. Again that is according to her testimony. When I couple that testimony with the defendants' witnesses' testimony that they admit witnessing firefighters watching porn or watching porn themselves, I conclude that the forensic examination requested may lead to discoverable evidence and does not constitute a fishing expedition."

"[As to Plaintiff's 3rd Motion for Sanctions, I am going to deny it. It is without prejudice. If due to your forensic analysis you discover that there are weighty documents that should have been produced that weren’t, I will reconsider sanctions.”

September 23, 2016

Wayne Werosh IT Consultant for Country Club Hills provided a *“Backup/Image Quote”* to Robert Kopec to provide three 2Terabyte USB drives an, image 10 workstation and provide a backup script. (Attachment R)

“Attached is a quote for three 2TB USB Drives, one for you, the Chief and the Assistant Chief, along with a script to replicate all documents, files, etc to the USB drives. Also included in the quote is setting up or verifying that five workstations at Station 2, and five workstations at Station 1 backup system images to the appropriate NAS drive”

November 2016

Daniel Boddicker called Wayne Werosh and asked if he could help with a forensic investigation and was told by Werosh that Werosh could not. (See Attachment I Page 34-35)

Counsel for the Defendants called CCH IT Consultant Wayne Werosh and asked if he *“could help with a forensic investigation” and “He contacted me to ask me if I could monitor whomever was doing the disc imaging.”* And *“I explained to Mr. Boddicker that I didn't feel like I had the experience in forensic imaging and investigation to be a competent expert witness in court.”*

January 16, 2017

Defendant’s refused Plaintiffs Expert access to forensically image computers at Fire Stations

Arrived at CCH Fire Station to forensically image computers pursuant to the ‘Fourth Amended Notice of Inspection’ and courts order of August 31, 2016.

I was directed to the computers in the library ("training room") by three uniformed unidentified firefighters. Within a few minutes, prior to getting started, I was told that I was not going to be doing the examination by Chief Agpawa.

I asked Chief Agpawa why or who made the decision not to proceed, so that I could report back and was told by that Mr. Boddicker said it was not going to happen today.

I asked to speak with Mr. Boddicker and was put on the phone with him and informed him that I had driven three hours to complete the forensic imaging of the computers and that even if protocols or keywords were still being worked out, that I could create the forensic images to preserve the data and leave it with the Fire Chief. I was told by Mr. Boddicker that it was not going to happen today. I asked when would be good time to return and he said he didn't know.

January 20, 2017 **Plaintiff's Motion to Show Cause and Sanctions regarding ESI Inspection**

"Defendants and Defendants' counsel has continued to evade the court's order granting the forensic imaging, including most recently cancelling the inspection the same morning only after the eDiscovery expert appeared at the fire station. In fact, the eDiscovery expert, Andrew Garrett was told to proceed by the staff on site prior to Defendant Chief Agpawa's and Defendants' counsel's subsequent cancellation of the inspection.

January 23, 2017 **Court order granting Plaintiff's motion for sanctions for violations of the Court's order regarding inspection of computers for pornographic material,**

and ordering the inspection and imaging to proceed on January 26, 2017, Defendants pay Plaintiff's Expert Fees (See Attachment S)

January 26, 2017

Court ordered imaging to proceed on this date. Defendants, in the presence of their counsel, directed Plaintiff's Expert to the wrong computers to be imaged because Defendants had removed the computers to be serviced and did not advise Plaintiff's expert or Plaintiff's counsel.

Arrived at the Fire station on 183rd street pursuant to the Emergency Motion and Courts Order and met Rudy Maybell (County Club Hills IT Department Head), Brent Sachnoff (Country Club Hills IT Consultant) and Daniel Boddicker (Counsel for the Defendants).

I asked Mr. Sachnoff to identify the computers used by the defendants that were referenced in the court order. Mr. Sachnoff looked at his mobile phone with Rudy Maybell preset and directed me to the middle office across from the bathroom identified as the training / library room as the first computers to forensically image. I was informed that by Mr. Sachnoff that he was directed to escort me to the computers I was to image and that I was only to image those computers. Mr. Boddicker arrived and oversaw part of the collection of the 'Library Computers'.

When powering down the computers, I noticed that the computers were networked on a domain. It is most typical that computers connected to a corporate network and joined to a domain have 'roaming profiles enabled'. Roaming Profiles redirect the users data to a centralized server. Therefore, the users usage data would reside on the workstation and other ESI such as documents stored in the My Documents folder could reside in the server.

I was told by Mr. Sachnoff with Rudy Maybell present that the computers did not have roaming profiles. It was determined two hours later that day that the computers did have roaming profiles and Mr. Sachnoff agreed that there might be data that is relevant on the server. I asked to image the server and Mr. Sachnoff said no that was not going to happen. I asked to speak with Mr. Boddicker about it and Mr. Boddicker stated 'no' as well until I explained the likelihood of ESI being resident on the server due to roaming profiles. Mr. Boddicker agreed to imaging of the only server I was aware of at that time. At no time did the defendants disclose the Network attached storage system or the cloud as a source of ESI.

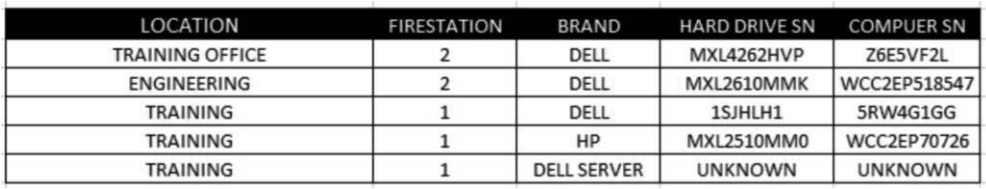
Mr. Sachnoff and Mr. Maybell both had a discussion with Chief Agpawa in the training room (across from the bathroom) and I could hear Chief Agpawa in a loud voice say "he is not copying the server" and then Mr. Sachnoff and Mr. Maybell returned to say that they think they are both going to be fired if I image the server. I was allowed the image the server pursuant to the agreement of Mr. Boddicker.

A copy of all forensic images were left with Mr. Sachnoff and Mr. Maybell.

Note: At the time of imaging, Defendants did not make me aware of the fact that the two computers from the library had been replaced and that the Network Attached Server contained backups of the workstations. As a result, neither the **original Library Computers (#2(b) to the notice of inspection and**

subject of the court's order) which were stored in a closet or the **Network Attached Storage System Server** were NOT imaged on this date. It was not until Wayne Werosh's Deposition that I was made aware of the existence of the two computers stored in a closet that were in service in the Library (or Training Office/Room) during the employment of the Plaintiff.

Below is a Matrix of the computer hard drives that were imaged.



LOCATION	FIRESTATION	BRAND	HARD DRIVE SN	COMPUER SN
TRAINING OFFICE	2	DELL	MXL4262HVP	Z6E5VF2L
ENGINEERING	2	DELL	MXL2610MMK	WCC2EP518547
TRAINING	1	DELL	1SJHLH1	5RW4G1GG
TRAINING	1	HP	MXL2510MM0	WCC2EP70726
TRAINING	1	DELL SERVER	UNKNOWN	UNKNOWN

February 6, 2017 **Court Order, ordering "the ESI/email imaging/retrieval shall occur [] by March 23, 2017."**

February 16, 2017 **Plaintiff's Emergency Motion to Preserve ESI**

"Plaintiff is concerned that Defendants have or will destroy other ESI and emails that are responsive to Plaintiff's discovery requests in this case, despite their ongoing obligations to preserve ESI."

February 17, 2017 **Court Order, granting Plaintiff's Motion to preserve ESI in part,** and ordering that the "imaging of Defs' email servers and google drive shall occur before 12:00 noon on February 18, 2017 with Defs' IT consultant, Brent Sachnoff [] present, Brent Sachnoff will maintain the imaging and ensure all data is preserved until further order of the court."

February 17, 2017 **I called IT Consultant for Country Club Hills, Brent Sachnoff, and arranged to meet at City Hall as previously arranged to collect the email pursuant to the courts order to be completed by Saturday February 18, 2017.**

When I arrived at City Hall I asked to see Rudy Maybell the IT Director for Country Club Hills and it was 5:02 pm. Five o'clock was the agreed time by Mr Sachnoff to meet as he was out of town and flying back to the area that afternoon. I was told by the Security Guard that Mr. Maybell had just left by direction of the Mayor and was told not to return until Monday.

I called Brent Sachnoff and informed him of the situation. He said he would call the mayor because the Mayor asked that he be directly in the loop on all matters going forward.

I received a call from Mr. Sachnoff with the Mayor on the phone whom proceeded to say "you are going to have to come back another time," and I explained that Mr. Sachnoff and I were ordered by the court to complete the imaging of the email. I asked that Mr. Boddicker be joined to the call for the conversation, and he was then joined in on the call. Upon merging the calls, Mr. Sachnoff's connection dropped from the call. Mr. Boddicker said he did not have his number with him, so I provided the number and he was brought back onto the line. Ms. Kurtz was also joined on this call. Mr. Boddicker said we would have to go back to court because he was not going to allow the imaging of the emails despite the court order. Mr. Kurtz said she would file another emergency motion to enforce the emergency motion and ask that the Mayor attend. After about 40 minutes of back and forth, I informed the Mayor of what the security guard had said when I arrived. The Mayor then agreed to calling Mr. Maybell back in to comply with the order.

Mr. Maybell provided me with access to the emails and then after about an hour of collecting, terminated my access and said that Brent Sachnoff was going to be collecting the emails. I again got Mr. Boddicker on the phone and let him know that I was there to follow the order, and if not allowed, I would leave. Mr. Boddicker agreed to allow me to continue and Mr. Maybell once again granted me access to the rest of the email boxes.

All emails were left on site on a portable hard drive with Mr. Sachnoff and to date have not been searched despite several attempts through correspondence from Plaintiff's counsel to Defendants' counsel.

March 14, 2017

Wayne Werosh was deposed pursuant to Plaintiff's subpoena. Werosh testified that the two computers in the room across from the bathroom were swapped out with two other computers from other areas in the fire station, and that he put evidence tags on them, and advised Chief Agpawa, Maybell, and Deputy Chief Kopec to preserve them because of the litigation, among other things. (See Attachment I)

Defendants never identified these computers that had been swapped out and evidence tags placed on them, until after being told that it appeared that the computers that were ordered by the Court to be imaged had been wiped based on the data contained on the computers.

March 22, 2017 **Ms. Kurtz emails Mr Boddicker, stating in part: “**I will be filing a motion for sanctions based on Defendants failure to produce the computers that were ordered by the Court for imaging relative to the issue of employees watching pornography in the Fire Stations. I will be seeking default judgment based on the history of non-compliance in this case and based upon the deliberate violations of the Court’s order(s) and failure to produce the computers as ordered by the Court.”

March 22, 2017 **Defendants’ counsel, Mr. Boddicker, responded via email regarding the computers, stating that they were located in a storage closet.**

April 12, 2017 **Plaintiff’s counsel email to Defendants’ counsel – regarding imaging 2 computers in the storage close without waiver.**

April 21, 2017 **Defendants’ counsel confirmed imaging of the 2 computers in the storage closet for April 24, 2017.**

April 24, 2017 **Imaged the two computers that were disclosed during the Werosh deposition and referenced in this report as computer hard drive ‘6RW2GZ36’ and ‘WCATR1278977’.**

May 18, 2017 **Delivered Report to Plaintiff regarding the Country Club Hills employees use of computer to surf pornography**

(See Attachment: Subject to Protective Order)

July 21, 2017 **Defendants forensic expert firm Sikich delivered a report concurring with Plaintiff’s expert and citing software to wipe data was found and ran.**

(See Attachment: Subject to a Protective Order)

5.0 Key Concepts and Terms

5.1 User Profile

In order for Microsoft Windows to separate one users information from another user profiles were created.

When a user establishes an account on a computer for the first time, he or she creates on that computer a registry key with the logged in name and a folder known as the user profile folder used to store data created by the user. At subsequent logons, the system loads the user's profile, and then other system components configure the user's environment according to the information in the profile.

For instance, when examining a computer and navigating to “C:\Users\” you may find multiple folders labeled the same as a users login name. If I had a user profile on the computer I was examining it would contain a folder at “C:\Users\” named ‘agarrett’ corresponding with my login name of ‘agarrett’.

It is the folders that are found in “C:\Users\username” that contain the web history of web sites visited, searches, web chat history, files and other pertinent information to show user actions and based on the name of the user profile it is a good indicator of whom performed the specific actions on the computer.

5.2 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.

5.3 User Assist Keys

The UserAssist Key artifacts allows users to easily see what application a user has run from their start menu, how many times they have executed that application and when the application was last run from the start menu.

5.4 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.

5.5 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.

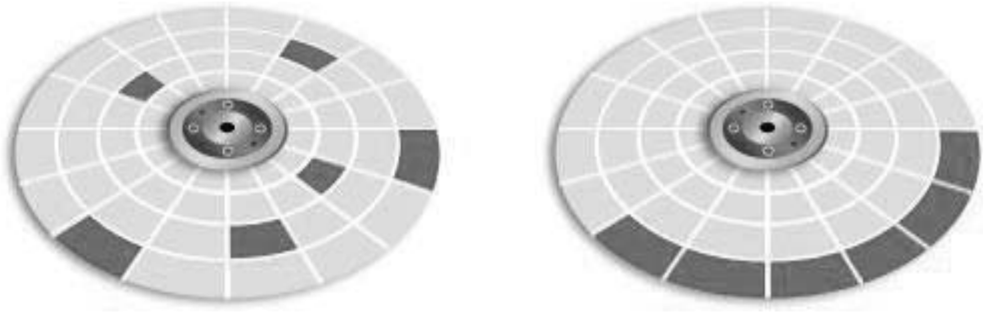
6.0 Applications used as Anti-Forensic Tools

6.1 Windows Application - Disk Defragmenter

As part of eDiscovery training I have attended with Guidance Software the manufacturers of the most used eDiscovery platform to date, I was required to read the and understand landmark cases for study. One such case Victor Stanley v Creative Pipe (MJG-06-2662) **(See Attachment T)** in the District of Maryland best described what Disk Defragmenters use as tool of spoliation and I will quote the courts description:

> "Disk Defragmenter, Microsoft Window's disk defragmentation program, is a system utility that "consolidates fragmented files and folders on [a] computer's hard disk, so that each occupies a single, contiguous space" in the system. http://www.microsoft.com/resources/documentation /windows/xp/all/proddocs/en-us/snap_defrag.mspx?mfr=true. To consolidate fragmented files, the program moves the file fragments together by "overwriting all those places" where space in the system was occupied by deleted files. As a result, "the ability to recover deleted items virtually . . . disappears" because the same is occupied by other files. (Dec. 1, 2009 Hr'g Tr. 43:1 – 44:18 (Spruill Test.).) Cutting through all the techno-speak, it is foreseeable that the running of a disk defragmentation program, colloquially referred to as "defragging," can result in the loss of files that were recoverable before the defragmentation occurred."

The graphic below shows how fragmented data is moved by Disk Defragmenter.



I can offer another explanation of what Disk Defragmenter does as "it moves around files on a hard drive to areas that make it easier for the hard drive to retrieve data. The side effect of this process is that it moves the files to areas that may have occupied a previously deleted file, therefore, overwriting the data that could have been recoverable.

The forensic community has classified the use of Disk Defragmenter as a tool that can be used for anti-forensic measures. SANS institute one of the world's leading forensic training schools has written papers on the use of Disk Defragmenter as a anti forensic tool.

6.2 Disk Defragmenter Usage

By examining the User Assist Keys, Prefetch Folder and Prefetch entries, I was able to recover entries that show when disk defragmenter was ran and in some cases who ran it.   Some of the entries were recovered from the unallocated space of the computer indicating that the entries had been deleted and unreferenced prior to my examination. Without the aid of forensic tools the recovery of these entries would not have been possible.

I was able to determine that on multiple occasions disk defragmenter was run on both computers containing hard drives 'WCATR1278977' and 'GRWZGZ36'. Below is a chart of dates that Disk Defragmenter was ran and for most of the entries the user name was not able to be recovered. When the Defragmenter is run a user selecting and running it only the DFRGNTFS.exe entry in Prefetch is updated and the Defrag.exe is not.

Although there are legitimate reasons to run Disk Defragmenter on a computer, there is not when data on the computer is subject to litigation. The software was ran on a computer just prior to taking the computers out of service by direction of Firehouse Management*"Please be advised the two desktop computers at Station 1 in the large office are scheduled to be removed. The replacement units are already in place. Anyone who has been saving documents, photos or other files to the local hard drive should copy or move them to their share folder if they want to keep them. I recommend that this be done prior to the week of August 8th, when the old desktops would be placed in storage."* ***(See Attachment P)***

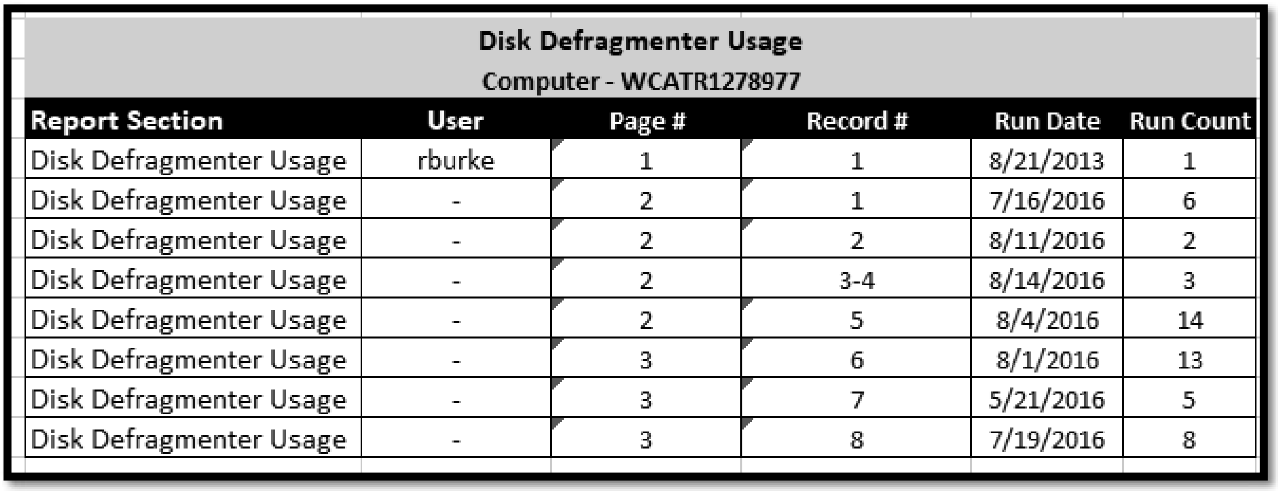
On August 8, 2016 the computers were to be taken out of service by Wayne Werosh the IT contractor for CCH and according to his deposition he placed them to the side of the room with an evidence tag on it.

Werosh stated that he notified Chief Agpawa and Deputy Chief Kopec that he would highly recommend they retain those computers as they are part of court case.

6.2 Disk Defragmenter Usage on Computer WCATR1278977

Reference: See Attachment U

Disk Defragmenter appears to be run on the computer WCATR1278977. The computer keeps track of the amount of times Disk Defragmenter has been run. I was not able to find any information that would support the consistent use of Disk Defragmenter. I was able to determine that Disk Defragmenter was run just before and many times after the computer was allegedly taken out of service indicating that after Wayne Werosh IT Contractor for CCH's disconnected the computer, that someone reconnected it to power.



Disk Defragmenter Usage
Computer - WCATR1278977

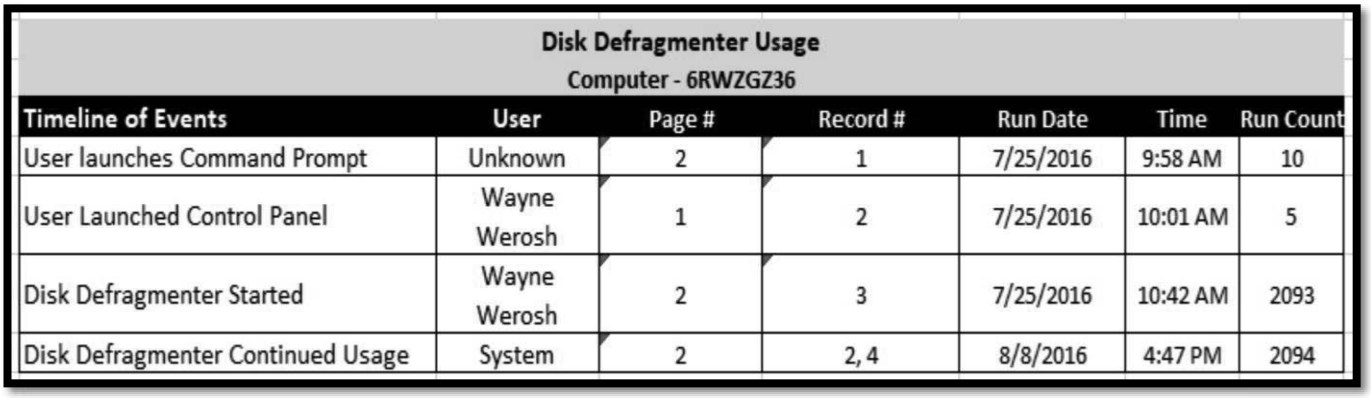
Report Section	User	Page #	Record #	Run Date	Run Count
Disk Defragmenter Usage	rburke	1	1	8/21/2013	1
Disk Defragmenter Usage	-	2	1	7/16/2016	6
Disk Defragmenter Usage	-	2	2	8/11/2016	2
Disk Defragmenter Usage	-	2	3-4	8/14/2016	3
Disk Defragmenter Usage	-	2	5	8/4/2016	14
Disk Defragmenter Usage	-	3	6	8/1/2016	13
Disk Defragmenter Usage	-	3	7	5/21/2016	5
Disk Defragmenter Usage	-	3	8	7/19/2016	8

6.3 Disk Defragmenter Usage on Computer 6RWZGZ36

Reference: See Attachment V

Disk Defragmenter appears to be set to run on a schedule on the computer 6RWZGZ36. The computer keeps track of the amount of times Disk Defragmenter has been ran and considering it has been run an excess of 2000 times it appears to be ran consistently. I was not able to find any information that would support the suspension of this task created to run Disk Defragmenter.

I was able to recover artifacts that suggest Wayne Werosh on July 25, 2017 used a program named Command Prompt and launched the System Control Panel (controls settings in the computer) and subsequently Disk Defragmenter was ran within 41 minutes of these actions. Additionally, Disk Defragmenter was ran the same day the computers were to be taken out of service according to emails produced.



Disk Defragmenter Usage
Computer - 6RWZGZ36

Timeline of Events	User	Page #	Record #	Run Date	Time	Run Count
User launches Command Prompt	Unknown	2	1	7/25/2016	9:58 AM	10
User Launched Control Panel	Wayne Werosh	1	2	7/25/2016	10:01 AM	5
Disk Defragmenter Started	Wayne Werosh	2	3	7/25/2016	10:42 AM	2093
Disk Defragmenter Continued Usage	System	2	2, 4	8/8/2016	4:47 PM	2094

6.4 Windows Application – Disk Cleanup

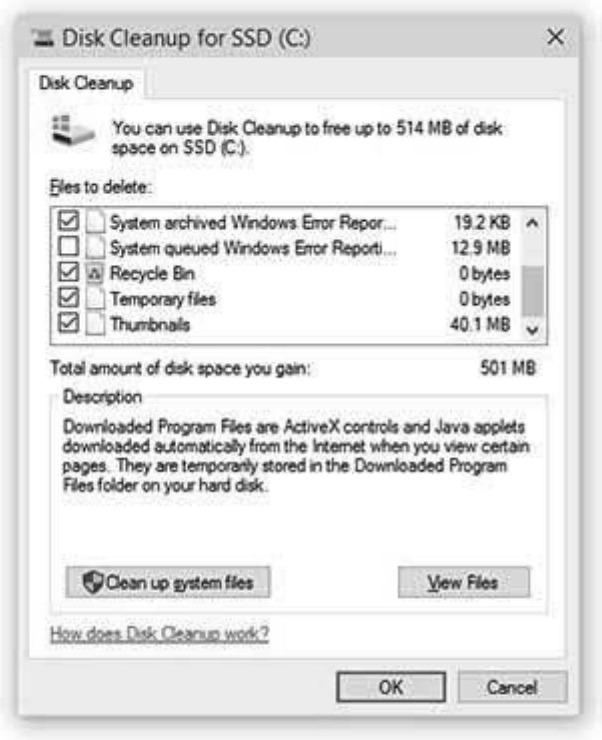
Reference: See Attachment W

Microsoft Windows operating system contains a Disk Cleanup tool. Microsoft states on its website that the *"The Disk Cleanup tool helps you free up space on your hard disk by searching your disk for files that you can safely delete. You can choose to delete some or all of the files. Use Disk Cleanup to perform any of the following tasks to free up space on your hard disk:*

- Remove temporary Internet files"
- Examiner Note: Temporary Internet Files are files downloaded as part of a webpage (pictures)
- "Remove downloaded program files
- For example, ActiveX controls and Java applets that are downloaded from the Internet
- Empty the Recycle Bin
- Remove Windows temporary files "

  Note: This removes system restore points that can be used to examine the computer forensically and recover old data
- "Remove optional Windows components that you are not using
- Remove installed programs that you no longer use"

Disk Cleanup Wizard does not run on a schedule and has to be launched manually \every time the user needs to clean up their disk.



You can use Disk Cleanup to free up to 514 MB of disk space on SSD (C:).

Files to delete:

☑	System archived Windows Error Repor...	19.2 KB
□	System queued Windows Error Reporti...	12.9 MB
☑	Recycle Bin	0 bytes
☑	Temporary files	0 bytes
☑	Thumbnails	40.1 MB

Total amount of disk space you gain: 501 MB

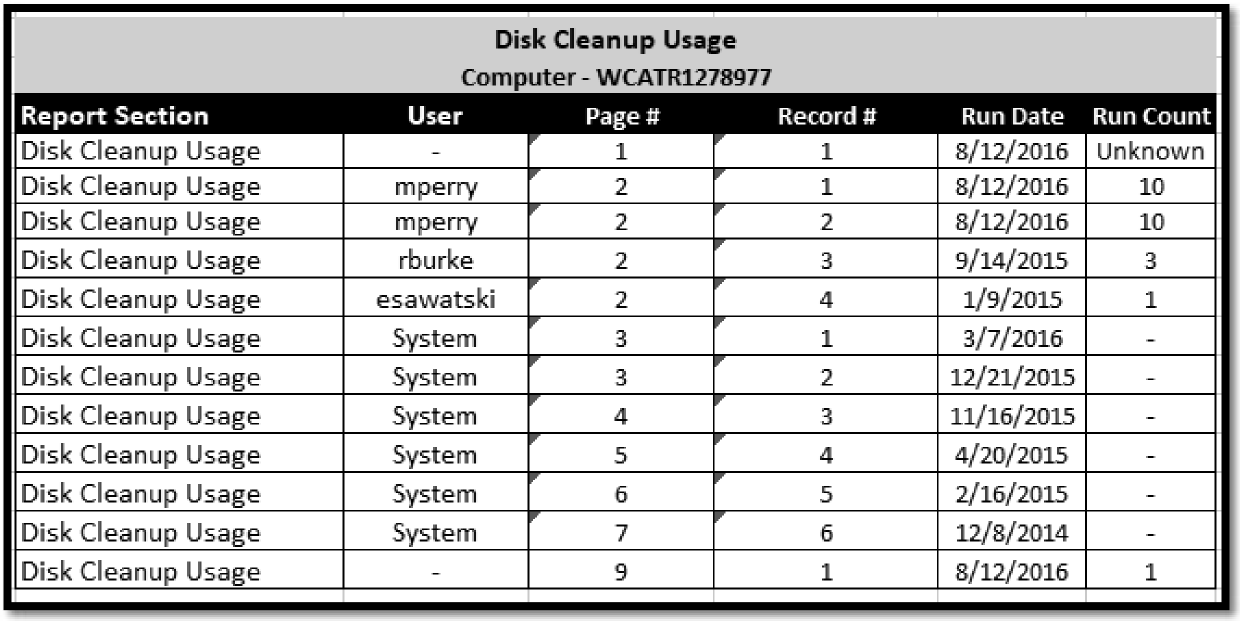
Description

Downloaded Program Files are ActiveX controls and Java applets downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.

6.5 Disk Cleanup Usage on WCATR1278977

Reference: See Attachment X

Below is a graphic showing the dates and times Disk Cleanup was run on the computer hard drive ‘WCATR1278977’.



Disk Cleanup Usage
Computer - WCATR1278977

Report Section	User	Page #	Record #	Run Date	Run Count
Disk Cleanup Usage	-	1	1	8/12/2016	Unknown
Disk Cleanup Usage	mperry	2	1	8/12/2016	10
Disk Cleanup Usage	mperry	2	2	8/12/2016	10
Disk Cleanup Usage	rburke	2	3	9/14/2015	3
Disk Cleanup Usage	esawatski	2	4	1/9/2015	1
Disk Cleanup Usage	System	3	1	3/7/2016	-
Disk Cleanup Usage	System	3	2	12/21/2015	-
Disk Cleanup Usage	System	4	3	11/16/2015	-
Disk Cleanup Usage	System	5	4	4/20/2015	-
Disk Cleanup Usage	System	6	5	2/16/2015	-
Disk Cleanup Usage	System	7	6	12/8/2014	-
Disk Cleanup Usage	-	9	1	8/12/2016	1

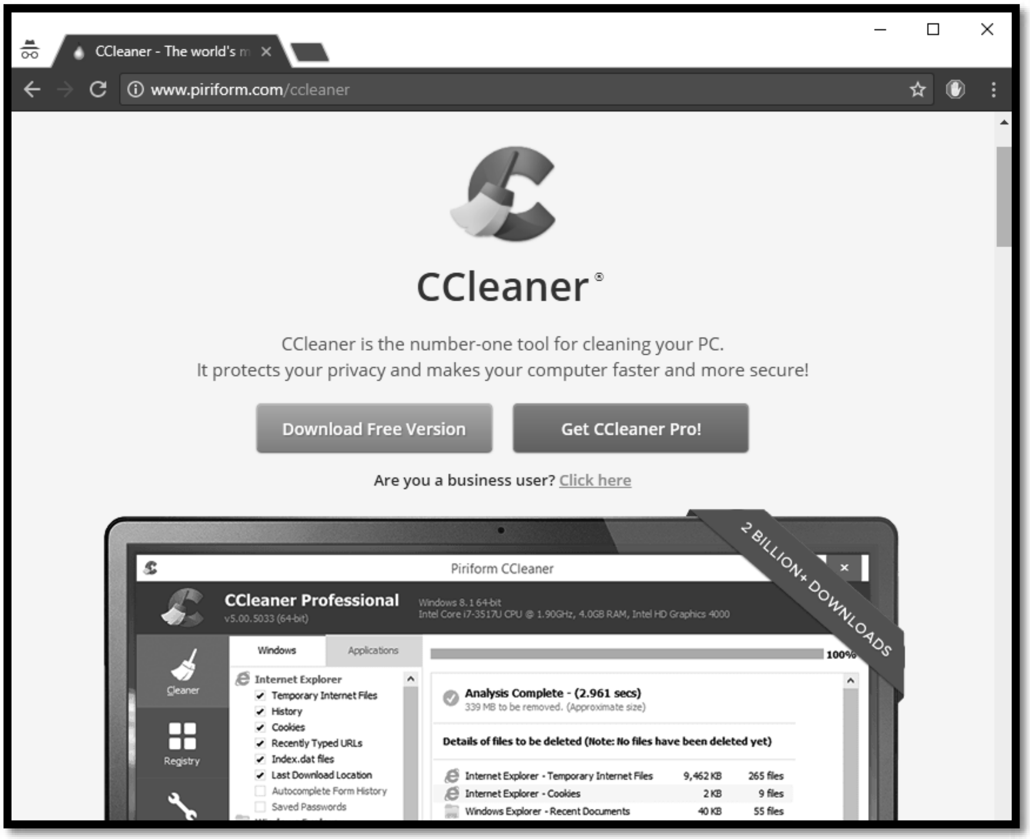
Multiple users have run Disk Cleanup multiple times and the most recent was on August 12, 2016.

6.6 Piriform Application CCleaner

Reference – See Attachment Y

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.

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

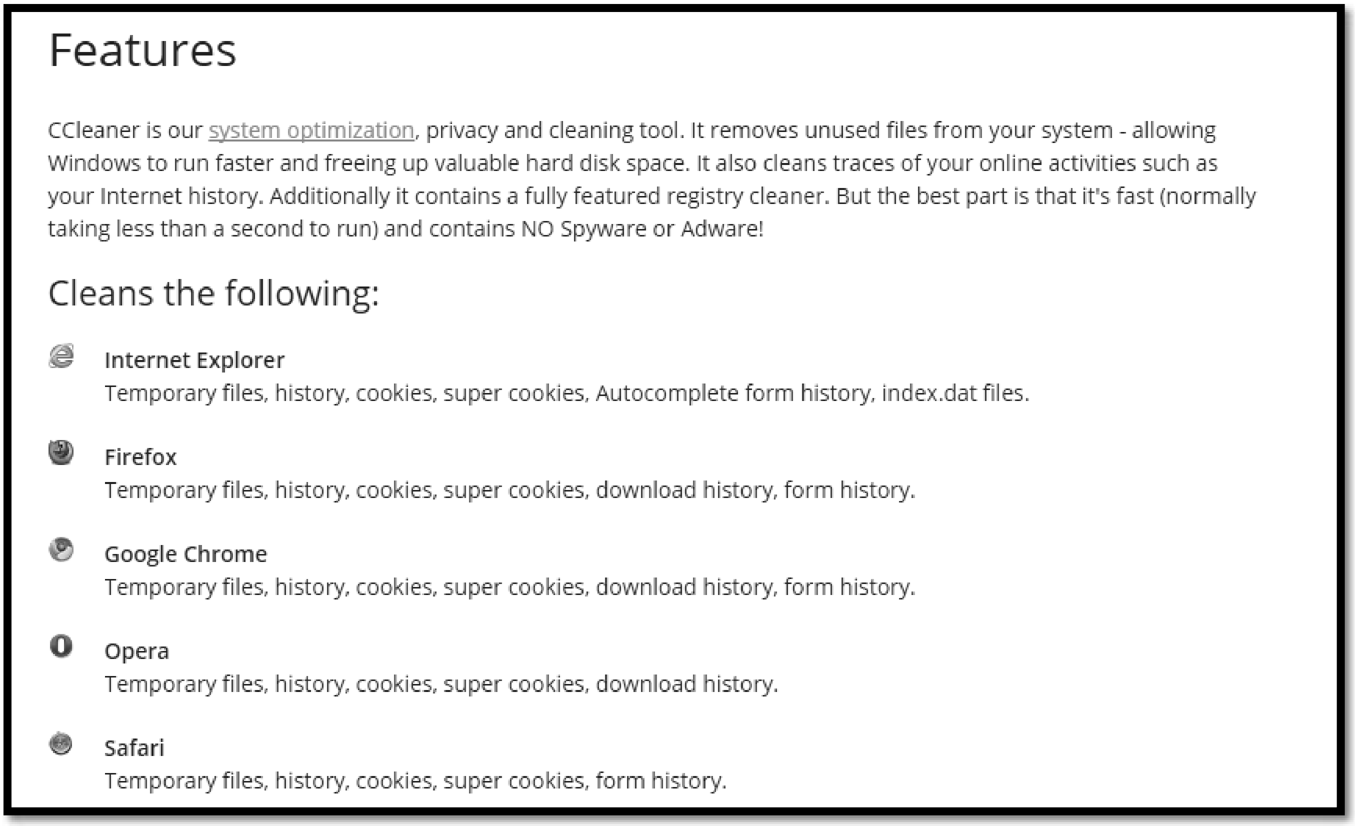
Analysis Complete - (2.961 secs)
339 MB to be removed. (Approximate size)

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:

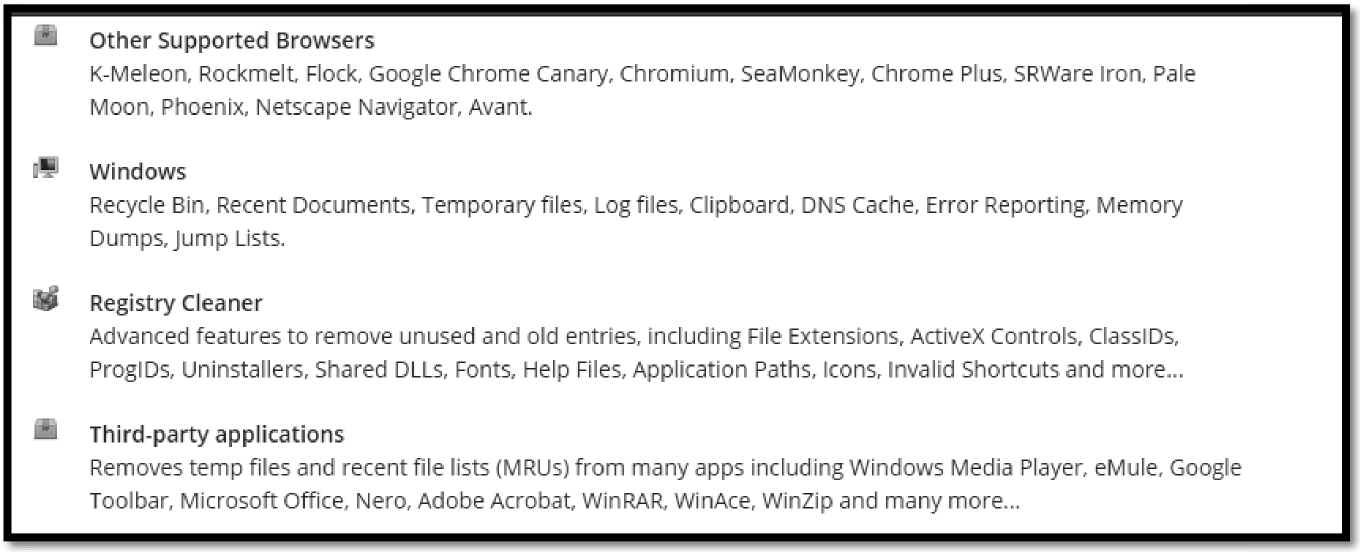
Internet Explorer
Temporary files, history, cookies, super cookies, Autocomplete form history, index.dat files.

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...

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

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 operating systems file system. This is called ‘unallocated / free space”

5. CCleaner Wipe Free Space option is ran against the hard drive and the file that still existed is overwrites the unallocated / free space with 0’s, therefore wiping the data from the computer

6. The files can no longer be recovered

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.

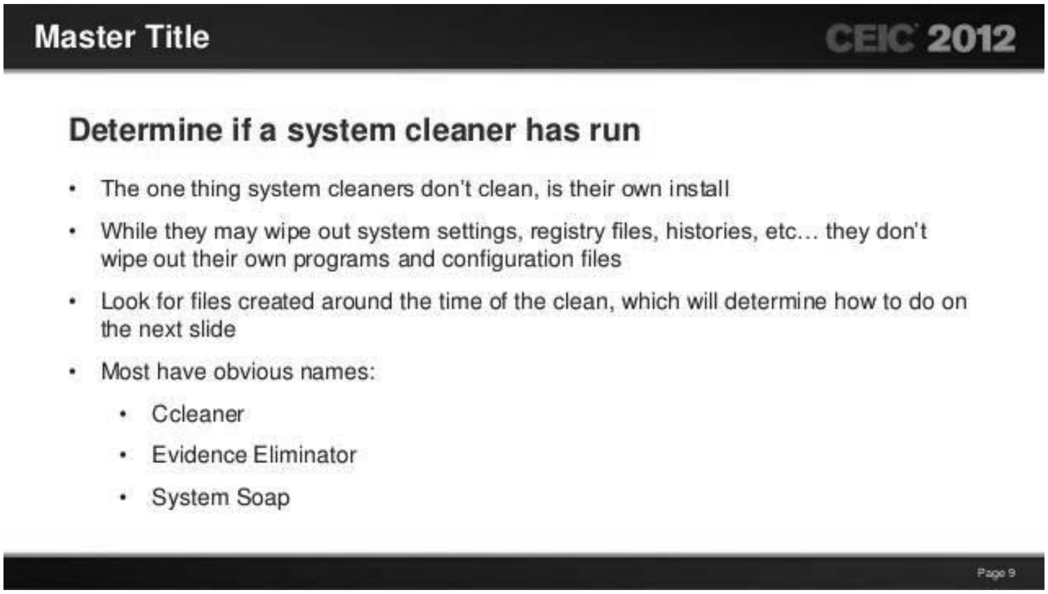
CCleaner touts its ability to wipe out files permanently on its website at https://www.piriform.com/docs/ccleaner/using-ccleaner/wiping-free-disk-space.

“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. For privacy and security reasons, you can set CCleaner to wipe the free areas of your hard disk so that deleted files can never be recovered."

As far as wiping out internet website history the process is completely different and CCleaner has many flaws. These failures of other parts of the program leave behind many artifacts that can be recovered by forensic software. For instance, there are files that are part of the operating system or part of an internet browser that if deleted the program may not function anymore. In those cases, CCleaner opens the file and attempts to flush out the data within the file. There are many reasons that CCleaner fails when attempting to flush out data within a file, which should not be confused with the process of overwriting a previously deleted file. For instance, if a user has the internet browser open while CCleaner is open, the index.dat file containing the internet history can be locked by the operating system preventing CCleaner from flushing out the data.

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

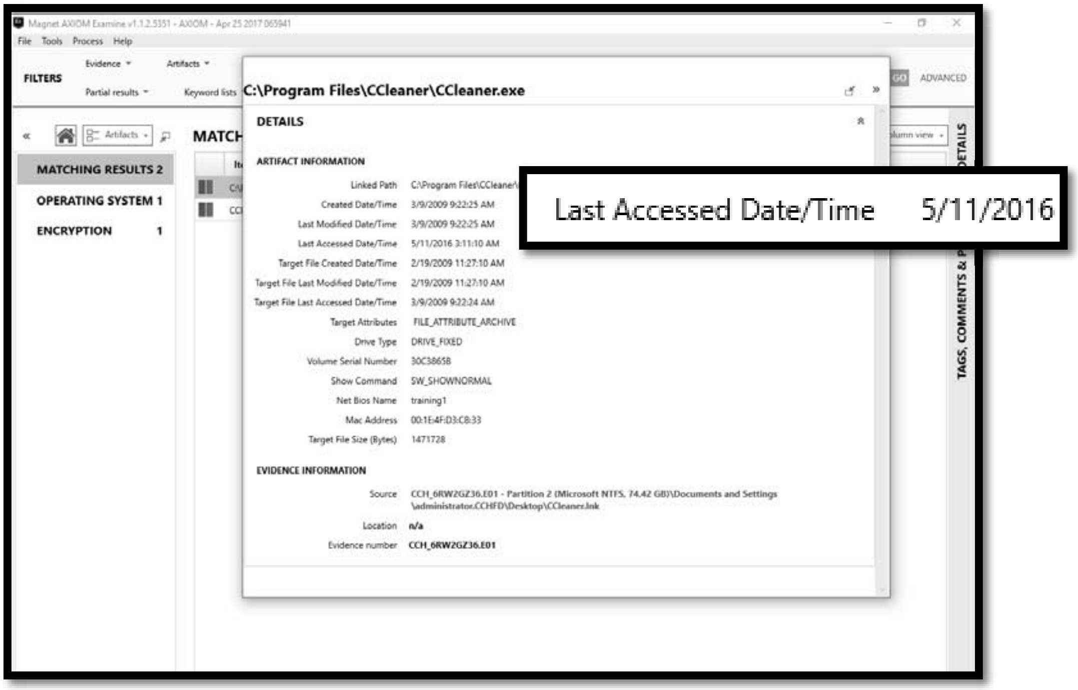
Page 9

6.7 Application CCleaner Usage

Reference: See Attachment Z

On February 17, 2016 and May 11, 2016, a user logged into the computer '6RW2GZ36' using the administrator account and launched the program CCleaner.

The report generated by the Defense Expert states *"Link files on the image showed that the administrator.CCHFD user account accessed the CCleaner software on February 17, 2016 and May 11, 2016. It is unknown how the administrator.CCHFD user account utilized the CCleaner software or which artifacts (if any) were deleted." (See Report Filed under Seal)*



C:\Program Files\CCleaner\CCleaner.exe

DETAILS

ARTIFACT INFORMATION

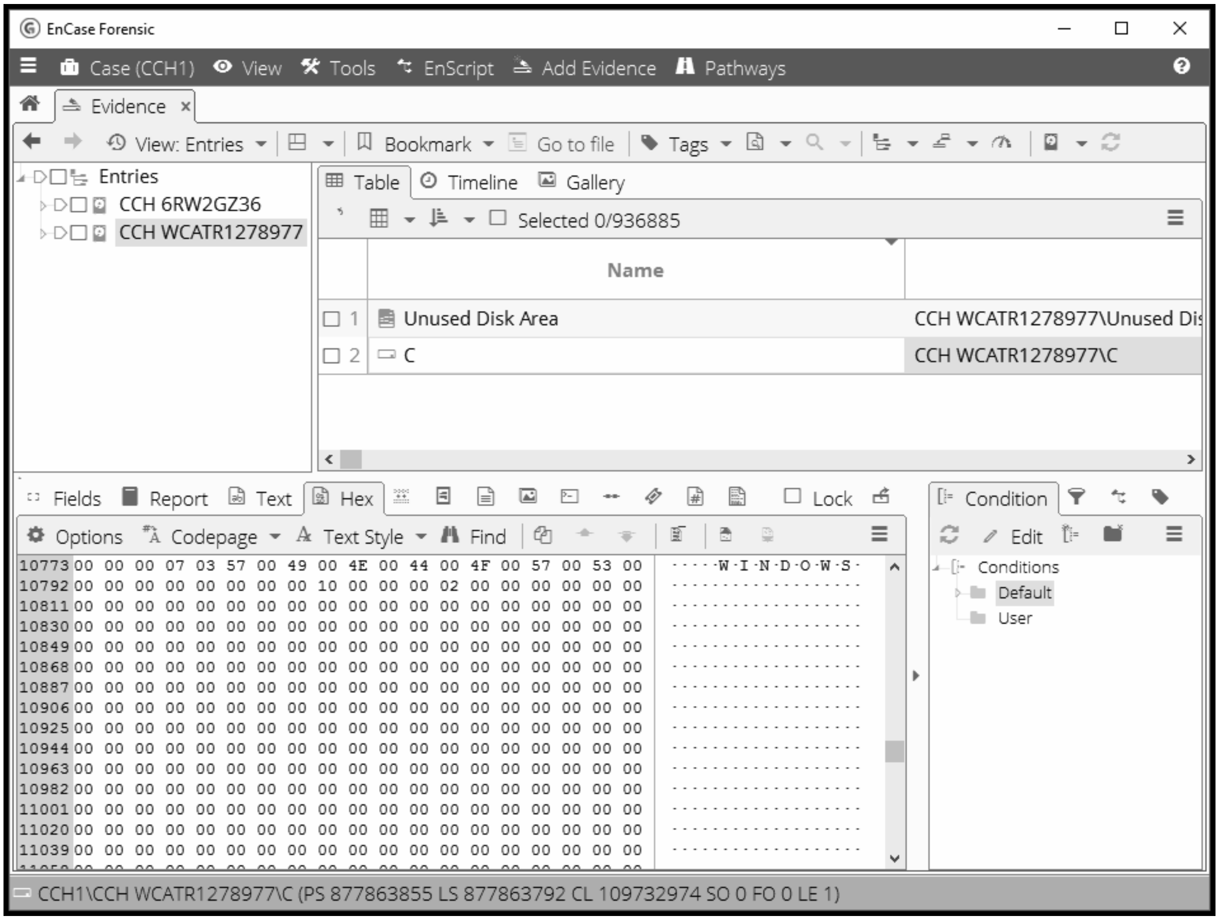
Linked Path	C:\Program Files\CCleaner\
Created Date/Time	3/9/2009 9:22:25 AM
Last Modified Date/Time	3/9/2009 9:22:25 AM
Last Accessed Date/Time	5/11/2016 3:11:10 AM
Target File Created Date/Time	2/19/2009 11:27:10 AM
Target File Last Modified Date/Time	2/19/2009 11:27:10 AM
Target File Last Accessed Date/Time	3/9/2009 9:22:24 AM
Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Drive Type	DRIVE_FIXED
Volume Serial Number	30C3865B
Show Command	SW_SHOWNORMAL
Net Bios Name	training1
Mac Address	00:1E:4F:D3:C8:33
Target File Size (Bytes)	1471728

EVIDENCE INFORMATION

Source	CCH_6RW2GZ36.E01 - Partition 2 (Microsoft NTFS, 74.42 GB)\Documents and Settings \administrator.CCHFD\Desktop\CCleaner.lnk
Location	n/a
Evidence number	CCH_6RW2GZ36.E01

Last Accessed Date/Time 5/11/2016

A screen shot of the forensic tool Encase which is used by the majority of law enforcement forensic labs is below showing that over one third of the hard drive ‘6RW2GZ36’ was partially wiped. By overwriting previously deleted data it prevents forensic applications from recovering items such as downloaded pictures.



	Name	
□ 1	Unused Disk Area	CCH WCATR1278977\Unused Di
□ 2	C	CCH WCATR1278977\C

```
10773 00 00 00 07 03 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00   ·····W·I·N·D·O·W·S·
10792 00 00 00 00 00 00 00 00 10 00 00 00 02 00 00 00 00 00 00   ···················
10811 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
10830 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
10849 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
10868 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
10887 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
10906 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
10925 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
10944 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
10963 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
10982 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
11001 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
11020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
11039 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ···················
```

CCH1\CCH WCATR1278977\C (PS 877863855 LS 877863792 CL 109732974 SO 0 FO 0 LE 1)

When a forensic examiner looks at the surface of the hard drive would show data written and in the middle of the data would see a string of 0's. This is an indication that a wiping utility has been used.

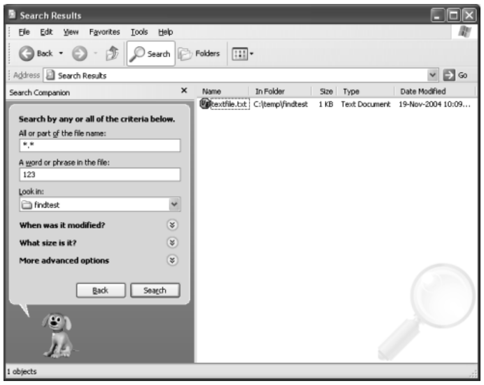
One may make an argument that the drive was simply just not written to yet. That could be true if the drive was a newer drive, but since the drive was manufactured and has been in use for over 6 years it would not be possible and data should exist throughout the drive. In addition, in my experience consumer grade hard drive manufacturers in the early 2000’s did not zero fill their hard drives.

The only way to put the files together without random data between the files is the run disk defragmenter and then additionally run ccleaner or another wiping tool that zero’s out sections of the hard drive.

The problem with doing that often tools designed to wipe free space/unallocated/prior deleted files are not perfect and do not destroy all othe prior deleted data.

7.0 Defendants Search of Desktop Computers

When a computer user searches within a Windows computer that search is recorded in users NTuser.dat file within the users profile. The search history is recorded in the same file whether or not the operating system is Windows XP (graphic below on the left) and Windows 7 (graphic below on the right). You can see from the graphics below the search pane within Windows is very simple to use.



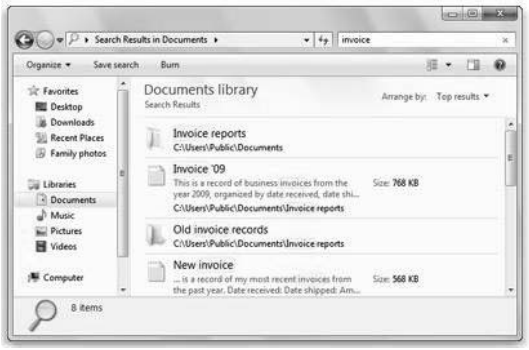
All or part of the file name: *.*

A word or phrase in the file: 123

Look in: findtest

Name	In Folder	Size	Type	Date Modified
textfile.txt	C:\temp\findtest	1 KB	Text Document	19-Nov-2004 10:09...

1 objects



invoice

Documents library
Search Results

Invoice reports
C:\Users\Public\Documents

Invoice '09
This is a record of business invoices from the year 2009, organized by date received, date shi... Size: 768 KB
C:\Users\Public\Documents\Invoice reports

Old invoice records
C:\Users\Public\Documents\Invoice reports

New invoice
... is a record of my most recent invoices from the past year. Date received: Date shipped: Am... Size: 568 KB

8 items

I was able to extract what has been search from each of the computers imaged since beginning of 2013. It is apparent that no one has used the Windows Search to conduct a search relevant to this litigation. (**See Attachment ZA)** for the listing of searches conducted on the computers and corresponding dates.

8.0 Conclusion

Based on the totality of the evidence, defendants took many actions between the initiation of Plaintiff's IDHR charge and litigation hold obligations, including throughout this case, to the time they actually allowed for examination of the computers. Below are some of the actions taken by the defendants after the filing of the suit and well after the time notified to not allow for destruction of data. I will not opine as to whether or not the actions were willful or intentional as those are legal conclusions. I can only offer what is in evidence as facts and based on the facts I think that one could make their own conclusion at to the conduct and actions of the defendants.

1. IT Web Filters were installed to prevent pornography usage
2. An investigation was started
3. Defendants wiped the Network Attached Storage Drive of all data that held computer backups
4. Defendants used anti forensic tool CCleaner on one computer

5. Defendants state they had sent a litigation hold letter to employees long after this litigation started
6. Defendants used Disk Cleanup on multiple computers (used to destroy data beyond recovery including web history)
7. Defendants used Disk Defragmenter on a computer (can be used as an Anti Forensic Tool)
8. Defendants swapped out the two computers identified by the Plaintiff
9. HR Firm conducted an investigation stating there was no pornography usage on the computers
10. IT Department conducted an investigation saying there was no pornography usage on the computer
11. Defendants testified in depositions contrary to evidence found by the Plaintiff's and Defendant's experts
12. Defendants were asked and failed to identify the hidden from sight computers until confronted with the deposition of Wayne Werosh IT Consultant for Defendants and possibly the email from Plaintiff's counsel
13. Defendants refused to allow entry despite order for Plaintiff's expert to examine computers and were sanctioned
14. The use of anti-forensic tools on the computers destroyed web history, electronic data and files.
15. Defendants wiped drives on the Network Attached Storage System and then used the Network Attached Storage system to store new files

16. Defendants did not identify as a source of data the backups created by Wayne Werosh stored on the newly wiped drives of the Network Attached Storage System
17. Defendants did not identify as a source of data the cloud storage system
18. Defendants did not identify as a source of data the network attached storage system in station 1 and 2 that contain the images of 10 computers identified by the plaintiff
19. Plaintiff's and Defendant's expert both filed reports showing that anti forensic tools were launched on a computer after the initiation of the litigation and after Defendants' obligation to preserve such data
20. Plaintiff and Defendants expert both filed reports showing the usage of computers to surf pornography contrary to defendants HR Investigation results, IT Investigation results, and testimony at deposition of the defendants

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

_______________________________ July 21, 2017

Andy Garrett Date