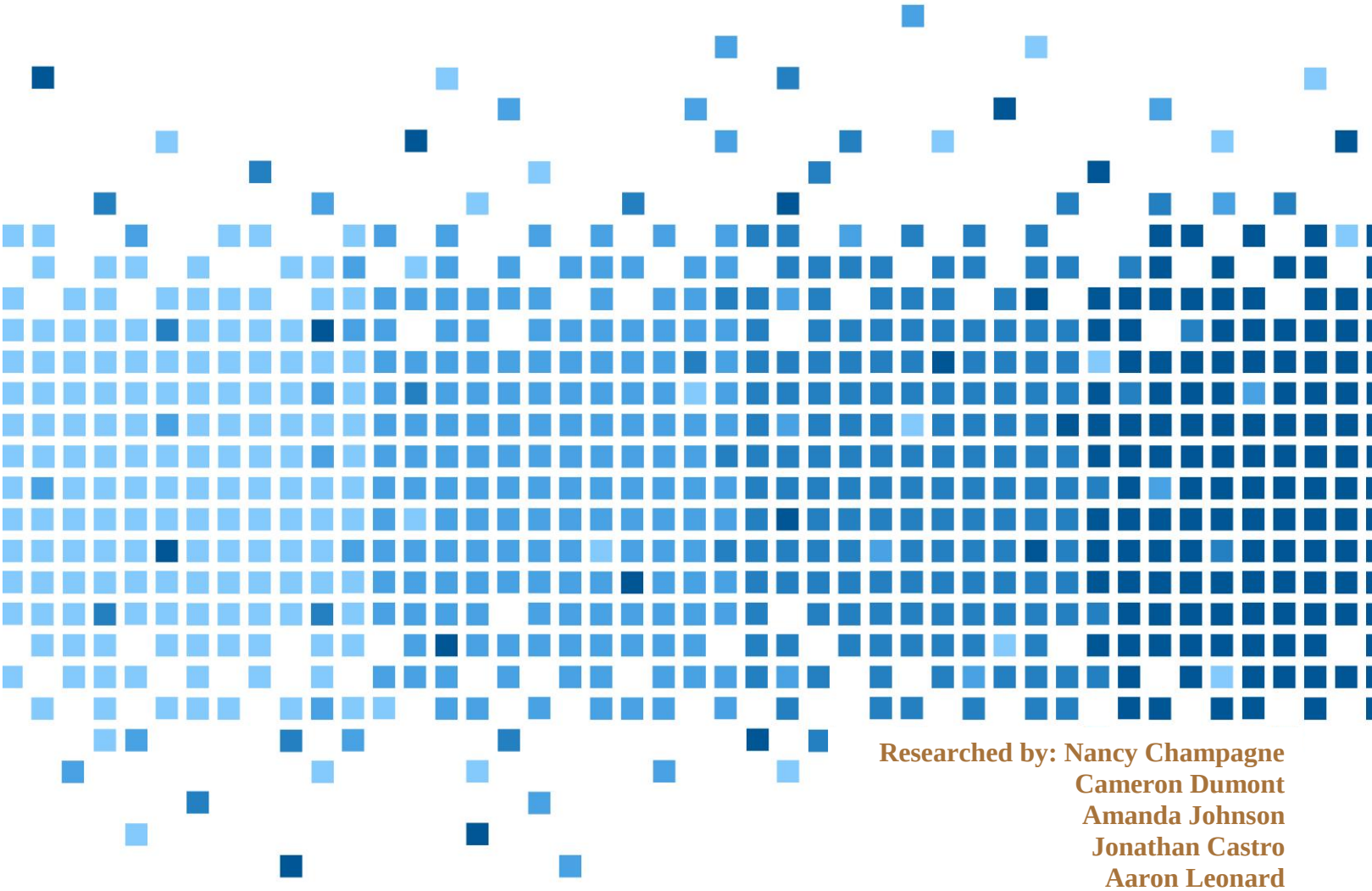
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

Forensic Tool Comparison



Researched by: Nancy Champagne
Cameron Dumont
Amanda Johnson
Jonathan Castro
Aaron Leonard
Jed Palmer
Tim Craig

175 Lakeside Ave, Room 300A
Burlington, VT 05401
Phone: (802)865-5744
Fax: (802)865-6446

5/2/2016
http://lcdi.champlain.edu

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

Recently, Access Data released new updates for their computer forensic program Forensic Toolkit (FTK). Magnet also released its own imaging tool Magnet ACQUIRE. We took the opportunity to record benchmarks and test these programs new features on computers that would be similar to computers used by law enforcement officials and private companies alike.

Background:

Tool comparison research is a staple of LCDI operations. Each time a new version of a forensic tool comes out we investigate the updates to the software and re-compare each tool's performance to discover each tool's strengths and weaknesses of each to aid in forensic investigations.

Purpose and Scope:

Since FTK has released a newer version of their software (version 6.0.1). We have decided to update our findings from the previous projects by comparing Access Data's Forensic Toolkit (FTK) v.6.0.1, Guidance Software's EnCase v7.10, and Magnet's Internet Evidence Finder (IEF) v6.7. We are also going to look at the differences between each tool's corresponding imaging software such as FTK Imager, EnCase's imaging option, and Magnet's new imaging software Magnet ACQUIRE.

Research Questions:

- How long do specific keyword searches on a reasonable set up take to complete in FTK v6.0.1, EnCase v7.10, and Magnet IEF v6.7?
- How many "hits" do the tools receive for each keyword search? If the number of hits differs, what does this tell us about the tools?
- How accurate are the timeline features of FTK v6.0.1, EnCase v7.10, and Magnet IEF v6.7 compared to the known data generation time?
- How do the exporting features of FTK v6.0.1, EnCase v7.10, and Magnet IEF v6.7 compare to each other for exporting both files and folders?

Terminology:

Artifacts – Any data generated by user interaction that can be collected and examined. Any user data retrieved from the browser is considered an artifact, including cookies, caches, geolocation, search history, etc.

Directory – A catalog for filenames and other folders stored on a disk. A directory is a way of organizing and grouping the files and is usually used to group related electronic documents or files pertaining to a particular application program.

dtSearch – developed by dtSearch Corporation, a software company that specializes in text retrieval software, is used by FTK to conduct indexed-based searching capabilities which uses the software development library by dtSearch, dtSearch Text index.

E01 – An E01 is the extension of an image file for EnCase.

EnCase – EnCase is a computer forensics tool designed by Guidance Software. It is an industry accepted tool used in numerous investigations by law enforcement and private companies. EnCase is used to acquire, analyze, and report on evidence.

Forensic Toolkit (FTK) – is a forensic tool made by AccessData. FTK allows users to acquire, process, and verify evidence. FTK supports Raw (DD) .001, SMART .S01, Expert Witness/EnCase .E01 and Advanced Forensic Format .AFF imaging formats.

FTK Imager – is a free extension of FTK. This is a powerful imaging and data preview tool that can be used to create forensic images of a drive and can also be used to quickly assess electronic evidence to determine if further analysis with a forensic tool is warranted. FTK Imager's features also allow it to take forensic images of local hard drives, floppy diskettes, Zip disks, CD's, DVD's, entire folders, or individual filed from various places within the media.

GREP – A search method that uses logical operators to find specific things in the evidence file. Using GREP requires knowledge of the different operators and what each of them does in a GREP search.

Image – often refers to a copy of a hard drive, or disk image, which is compressed into a series of files. Physical images include all information (zeroes and ones) on the hard drive whether the space is being used or not, and ends up being close to the same size as the actual hard drive itself. As opposed to a physical image, a logical image only acquires the parts of the hard drive that have active data and dismisses the rest of the drive. Compared to a physical image, the size can be extremely small or the same size as the drive depending on the amount of data stored.

Index – a table of data that is referenced by a program.

Index Search – uses the data from the index to quickly perform keyword searches.

Imaging time – The time the imaging tool takes to create an image of the device you are trying to image.

Keyword Search – A common technique used in computer forensics and electronic discovery, a keyword search is usually performed to find and identify every instance on a computer or other media of a given word or phrase, even if said word or phrase occurs in unallocated space or in deleted files.

Logical Search – a type of keyword search that looks at ALL logical data of a file regardless of any physical characteristic of how it is stored.

Magnet ACQUIRE – Magnet ACQUIRE is a software solution that enables digital forensic examiners to quickly and easily acquire forensic images of any iOS or Android device, hard drives, and removable media.

Magnet Internet Evidence Finder (IEF) – Magnet IEF is a forensic tool used by forensic professional that automates the discovery of digital forensic evidence to find, analyze and report on the digital evidence from computers, smartphones and tablets.

Processing Time – The time the forensics tool takes to go through the image file and create a user viewable layout of the evidence file

RAW – A file format for forensic images, Magnet ACQUIRE and FTK Imager use this format

Write Blocker – A tool used to disable write permissions on a hard drive to prevent data destruction, alteration, or contamination of data during the acquisition of a hard drive.

Methodology and Methods

Each member on the team started off by researching their respective tools extensively. Each team researched how their tool worked and investigated how do perform each of the functions we planned to examine for the project, including how to image and process our data generation hard drive, how to perform keyword searches, how to export various files and directories, and how to use the timeline feature on each tool.

Upon completing research into the uses and capabilities of each tool, we performed data generation using an 80GB hard disk drive. Data generation took approximately one hour and thirty one minutes to complete, going through our data generation script found in Appendix A. We focused this script on one user session that explored many different actions rather than multiple data generation sessions. Each team was then provided with a workstation computer and given the chance to image the hard drive with their respective imaging tool. After the imaging process was complete, the keyword searching features of each tool were tested along with each tool's ability to recover files and then export the artifacts found onto the workstation directory.

Equipment Used

Four computers were built and used for this project and all were built to resemble a law enforcement digital investigations laboratory. The specifications of each computer are listed below in Table 1: Equipment Specifications and
Table 2: Software Specifications.

Table 1: Equipment Specifications

Device	OS Version	Hardware
Data Generation Computer	Windows 7 Enterprise	Intel Core i7-3770K 16GB RAM 1TB HDD NVIDIA GeForce GTX 650 Ti
Encase Evaluation Computer	Windows 7 Enterprise	Intel Core i7-3770K 16GB RAM 1TB HDD NVIDIA GeForce GTX 650 Ti
Magnet Forensics Evaluation Computer	Windows 7 Enterprise	Intel Core i7-3770K 16GB RAM 1TB HDD NVIDIA GeForce GTX 650 Ti
FTK Evaluation Computer	Windows 7 Enterprise	Intel Core i7-3770K 16GB RAM 1TB HDD NVIDIA GeForce GTX 650 Ti
Write blocker	Firmware 3.01.0004.000	WiebeTECH Forensic UltraDock v5

Table 2: Software Specifications

Software	Version	Comments
Microsoft Windows	Windows 7 Enterprise	Installed on computers prior to data generation and tool evaluation
Magnet ACQUIRE	v.2.0	Only on Magnet Forensics Evaluation Computer
Magnet Internet Evidence Finder (IEF)	v6.7	Only on Magnet Forensics Evaluation Computer
AccessData Forensic Toolkit (FTK)	v.6.0.1.30	Only on FTK Evaluation Computer
AccessData Forensic Toolkit Imager	v.3.4.2.2	Only on FTK Evaluation Computer

Guidance Software Encase	v7.10	Only on Encase Evaluation Computer

Data Generation

In order to make the project more fun and engaging, we structured our data generation around the well-known Casey Anthony trial. We spent a few weeks researching the case and coming up with scenarios we believed would have been on the suspect's, Casey Anthony, computer. By doing this we created specific data sets that actual digital forensic investigators may have been looking for at the time of the investigation and trial.

When we initially began writing our data generation list we encountered an issue with browsing data affecting search results. When using a specific search engine, such as google, it usually monitors your previous searches (i.e. through browser cookies) and learns from that to assist the user in getting search results he/she might be looking for. Because we were researching on our Research systems (each member on their own Research system), all members of the project were receiving different search results based on what their search history or browser cookies looked like. We wanted identical data from multiple web browsers to simulate normal computer usage. Since we would be doing this on a fresh image (no previous activity recorded on the drive) we knew the results would differ when conducting data generation. Because of this, we made our searches less specific and generic. This allowed each search engine on each web browser to produce three identical search results which we used for data generation.

Once our data generation sheet was complete, we began creating data generation. The actual data generation took one hour and thirty one minutes to complete. Data generation occurred on its own computer identical to the computers we performed examination tool evaluations on. See Appendix 1 for our completed data generation list and results.

Analysis

For this project, we wanted to compare the newest versions of Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase Forensic, and Magnet's Internet Evidence Finder (IEF). Upon the completion of data generation, each team imaged the hard drive using their perspective imagers. When imaging the hard drive, each team used a write blocker to disable write permissions on the hard drive to prevent destruction, alteration, or contamination of data during the acquisition of a hard drive.
Once each tool successfully created an image of the hard drive, we proceeded in processing the image on our respective forensic examination tool to examine the data and begin specific feature trials.

One of the main components of our project was to compare the newest version of each tool's corresponding imager; Forensic Toolkit (FTK) Imager, EnCase Forensics' built-in imager, and Magnet's new imager ACQUIRE, as well as each examination tool's performance in specific features. We compared the time it took for each imaging tool to create the image of our hard

drive from data generation. When analyzing these times we also took note of the file size and type of each image. After analyzing each tools imager performance, we compared each tools performance in processing their images into their examination tools (FTK, EnCase Forensic, and IEF).

After analyzing each imaging tool's performance in imaging and each examination tool's performance in processing the created image, we proceeded to comparing several different features for each of these tools, including time and results from various keyword searches, time and results from exporting different file extensions and directories, the number of popular file extensions each tool could find, and lastly, each tool's ability to create an accurate timeline of events. The keyword searches we performed included:

- "chloroform
- "bury"
- "ducttape"
- "c"
- "duct tape"
- "zxcvbnm,./"

We chose these keywords based on data we knew would be on the image from our data generation. We included "c" and "zxcvbnm,./" as baseline searches. "c" should create a large amount of hits in a search and "zxcvbnm,./" should return almost no hits.

For the exportation of file extensions and directories part of the project, we compared each tool's ability to export a .pdf, .jpg, .mp3, and the Windows Downloads folder. We chose these file extensions and the Downloads folder for two reasons. First, .pdf, .jpg, and .mp3 are all popular extensions and every popular operating system has a Downloads folder where it stores items downloaded from the internet in that specific directory. Second, we knew there would be files with these extensions based on the files we created during data generation. When performing exportation of file extensions, we also noted how long it took each tool to export specific files which can be seen in Table 11: Exporting results.

When determining the number of popular files each tool could find, we found that each tool had a different process for identifying the number of popular file types. This will be elaborated in our Results Section.

Lastly, we examined each tools timeline analysis feature and then compared the number of artifacts each timeline found in its report and determined whether or not the timeline was accurate according to our data generation.

Results

Imaging Time Results

Below, in Table 3, are the results of our imaging process. We compared how long it took for each tool to image our data generation hard drive with their respective imager. Below is also information specific to each tools performance during the imaging process.

Table 3: Imaging Time Results

Program	Imaging Time	Size of image	Format of Image
EnCase	0H 55M 00S	74.4GB	E01
Forensic Toolkit Imager	0H 39M 38S	76.3GB	E01
Magnet ACQUIRE	0H 44M 00S	74.5GB	RAW

Processing Time Results

Once each tool imaged the data generation hard drive, each team then proceeded to processing their image into their respective forensic examination tool. Each team then recorded the amount of time it took to process the image into their tool. You can see these results below in Table 4: Processing Time Results. The detailed results of this process can be found in each tool's section below Table 4.

Table 4: Processing Time Results

Program	Processing Time
EnCase	0H 0M 14S
Forensic Toolkit	0H 22M 22S
Internet Evidence Finder	0H 43M 00S

EnCase Forensic Imager

Unlike the other tools showcased in this report, EnCase Forensic has an imager built into the tool. Since the imager and the examination tool are in the same program, EnCase allows investigators to do a live preview of the evidence while it creates the image and processes it. We used a write blocker to ensure the data on our data generation hard drive did not get corrupted. As you can see from Table 3 and Table 4, EnCase took the longest to image the drive, but had the shortest processing time. This is most likely since the software is imaging while you are previewing the evidence. This would slow the software down while imaging, but it would take virtually no time to process the data. EnCase had the smallest file size, however, all of the file sizes were relatively close.

Forensic Toolkit Imager (FTK Imager)

FTK Imager's user friendly GUI (Graphical User Interface) allowed us to begin imaging of the hard drive in the matter of minutes and allowed us to actually preview files before and during imaging of the hard drive. Although AccessData does state that FTK Imager can create perfect forensic copies of computer data without making any changes to the original evidence, we decided to still use a write blocker to ensure that nothing within the hard drive was destroyed, altered, or contaminated during the acquisition of the hard drive. As you can see on Table 3: Imaging Time Results, FTK Imager was the fastest imaging tool with 39 minutes and 38 seconds for an EnCase (.E01) Image. Although FTK allows for the creation of multiple image formats, we decided to create an .E01 due to it being the most common image format used by Digital Forensic Investigators.

Magnet ACQUIRE

We initially ran into a problem when testing out the imaging capabilities of Magnet ACQUIRE. We received the error message half way through the imagine process which would make the program crash and terminate the rest of the imaging process, yielding no results. After emailing Magnet Support, we discovered that error was from Magnet ACQUIRE attempting to validate the available free space from the location that would be populated in the "Folder Destination" field. We had to edit the user.config xml file to repair this problem by inserting new lines of code into the file so that ACQUIRE would be able to save the image. After getting the fix, saving the .xml file and relaunching Magnet ACQUIRE, we were able to successfully complete the imaging process and produce results without a problem.

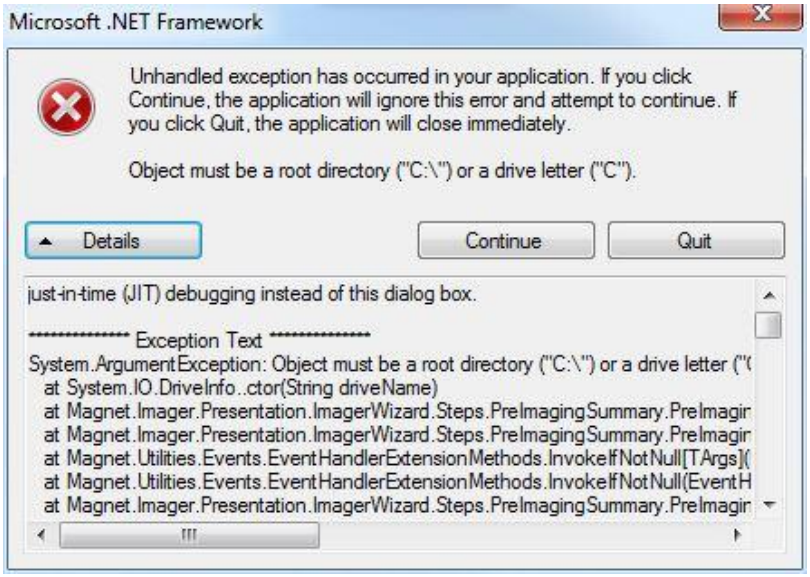


Figure 1: Magnet ACQUIRE error recovery halfway through imaging process

Keyword Search Results

After processing each tool was complete, we proceeded to conduct keyword searches in each tool. A keyword search is a common technique used in computer forensics and electronic discovery which is usually performed to find and identify specific instances on a computer or other media using a given word or phrase even if the event occurs in unallocated space or in deleted files. Keyword searches can be very beneficial for a forensics investigator to use because it allows them to search through files and/or folders for specific terms or phrases without having to physically parse through all the data individually. For this project, we compared how long it took for each tool to perform each keyword search as well as the results of each keyword search. Below on Page, in Table 5 through Table 10, are our results for the keyword searches we conducted as well as information specific to each tools performance in keyword searching.

Table 5: Keyword search for "chloroform"

Keyword Search "chloroform"	EnCase	FTK	Magnet IEF
Number of hits	Logical: 2,617 Indexed: 4,374	2,434	771
Time Elapsed	Logical: 0H 14M 14S Indexed: 0H 0M 0.1S	0H 0M 0.3S	0H 0M 48S

Table 6: Keyword search for "ducttape"

Keyword Search "ducttape"	EnCase	FTK	Magnet IEF
Number of hits	Logical: 421 Indexed: 70	59	26
Time Elapsed	Logical: 0H 13M 015S Indexed: 0H 0M 0.1S	0H 00M 01S	0H 00M 45S

Table 7: Keyword search for "duct tape"

Keyword Search "duct tape"	EnCase	FTK	Magnet IEF
Number of hits	Logical: 543 Indexed: N/A	2,076	84
Time Elapsed	Logical: 0H 13M 14S Indexed: N/A	0H 00M 02S	0H 00M 45S

Table 8: Keyword search for "bury"

Keyword Search "bury"	EnCase	FTK	**Magnet IEF**
Number of hits	Logical: 217 Indexed: 9	8	11
Time Elapsed	Logical: 0H 13M 00S Indexed: 0H 0M 0.1S	0H 00M 02S	0H 00M 45S

Table 9: Keyword search for "c"

Keyword Search "c"	EnCase	FTK	Magnet IEF
Number of hits	Logical: 125,985,968 Indexed: 3,463,989	1,947,069	38,564
Time Elapsed	Logical: 1H 00M 20S Indexed: 0H 0M 0.1S	0H 01M 06S	0H 3M 37S

Table 10: Keyword search for "zxcvbnm,./"

Keyword Search "zxcvbnm,./"	EnCase	FTK	Magnet IEF
Number of hits	Logical: 9 Indexed: N/A	28	1
Time Elapsed	Logical: 0H 13M 10S Indexed: N/A	0H 00M 01S	0H 1M 10S

EnCase Forensic

Our initial research indicated EnCase has the ability to perform two different types of keyword searches: logical and index. Logical searches look at all logical data of a file regardless of any physical characteristic of how it is stored. This means that when you conduct a logical search every hit is counted. In EnCase, a logical search is called a "raw search." For example, a "raw search" for the expression "bury" would produce 65 *items*, or the number of files which contain any number of *hits* for the expression "bury", but it finds 217 *hits*, or the number instances the expression "bury" is found in the 65 *items.* You can see in

Table 8 above that EnCase found 217 hits in the *logical* search (Widup). The screenshot in Figure 2: Raw Search Results in EnCase v.7 on the next page is from EnCase and shows this instance:

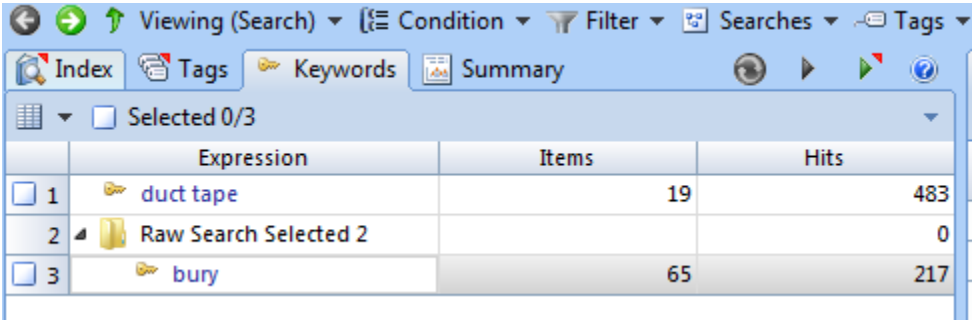


Figure 2: Raw Search Results in EnCase v.7

However, an index search looks at the index table created when the hard drive was imaged and processed. It looks for exact matches of the search expression. Therefore, it produces significantly less results than a "raw search" and is much faster, since the information is already organized. The screenshot below shows an example of the results from the index search for "bury." The index table has multiple instances of expressions that meet the search criteria. The user can than determine which result they would like to examine further. For our project, we used the first result since it was an exact match to our search expression. The screenshot in Figure 3 shows our index search results:

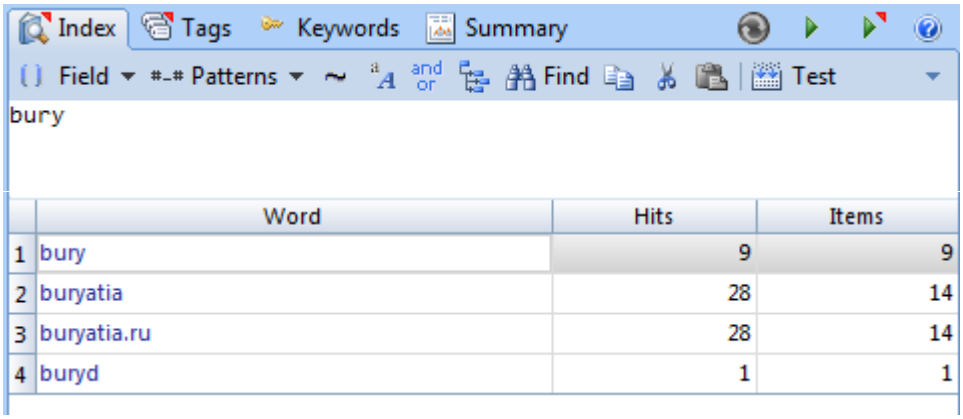


Figure 3: Index Search Results in EnCase v.7

For this project, we initially did logical searches. Our research on how to perform keyword searches in EnCase indicated this was the best type of keyword search to perform. However, EnCase produced significantly more results than the other tools and took a much longer amount of time to complete. After some more research, we found that the other two tools performed index searches. In order to get results more in-line with the other tools, we started to run index searches on EnCase.

Due to issues with GREP and string search methods on EnCase, we could not get accurate results with the "duct tape" keyword search and the "zxcvbnm,./" keyword search. We tried various methods to get results including using various GREP characteristics such as; putting the phrase in quotations, parentheses, adding a period, putting an "and" in between the words, and lastly putting in the phrase "within two" of tape (duct w/2 tape). Each time the results varied and were

nowhere near the results from other tools. Our conclusion as to why the index searches behaved this way for "duct tape" and "zxcvbnm,./" was that it was due to the way EnCase mounts the files during the initial imaging of the drive. Due to these issues, we did not include index results for the searches in Table 7: Keyword search for "duct tape" and Table 10: Keyword search for "zxcvbnm,./" since we could not get conclusive results. We believe this problem can be solved in future updates of the software.

Forensic Toolkit (FTK)

FTK creates an index of all the data during processing which means that it creates a table of data that it can reference back to when necessary. This made it the second fastest in processing with 22 minutes and 22 seconds. Although FTK does allow for the option to perform a live search, similar to EnCase's logical search, we decided to perform an index search due to the fact that it would bring faster results by allowing FTK to refer to a data table during searches instead of running over the data which would have created more but unnecessary hits. This is due to the fact that if it parsed through all the data, it would have definitely referred to the same file more than once and taken a bit longer to complete. FTK conducts indexed-based searching by incorporating indexed search capabilities provided by dtSearch's dtSearch Text Index. dtSearch is a third party software vendor that specializes on text retrieval software. FTK yielded the fastest search speeds during all of the keyword searches and yielded similar results to EnCase. All of the files that were created during data generation process were found counting files that were deleted

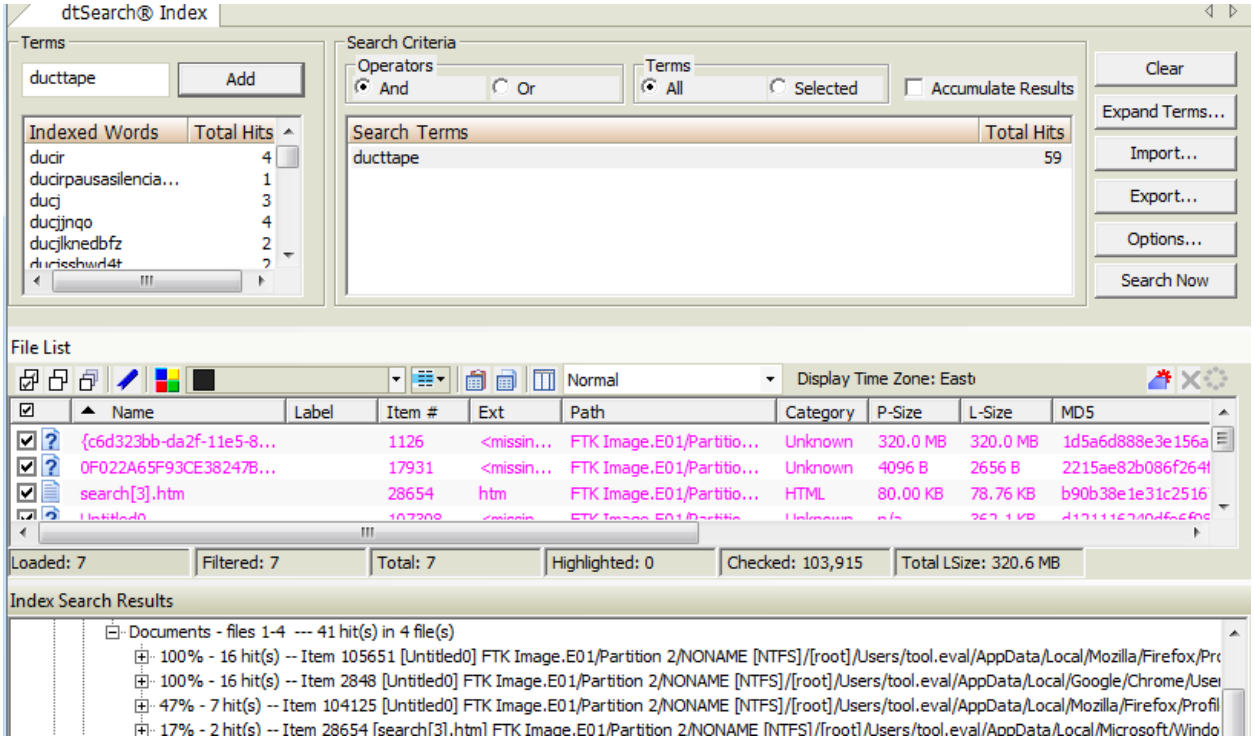


Figure 4: Index Search on FTK for the term "ducttape"

Magnet Internet Evidence Finder (IEF)

Internet Evidence Finder yielded the lowest number of results in five out of six of the keyword searches. This is because IEF performs a common, generalized search instead of focusing on every detail. When doing searches in IEF, you aren't searching the image, you are searching the results that IEF has found from the image. It's only looking for internet related artifacts. EnCase and FTK on the other hand allow you to look at the entire image and will perform multiple searches (EnCase can conduct a logical or physical keyword search and FTK can perform live, indexed, single term and multi terms searches) causing them to get more detailed results. These factors explain why FTK and Encase yielded results similar to each other and IEF did not. This is most likely why IEF had lower keyword search results yet found a higher number of total hits.

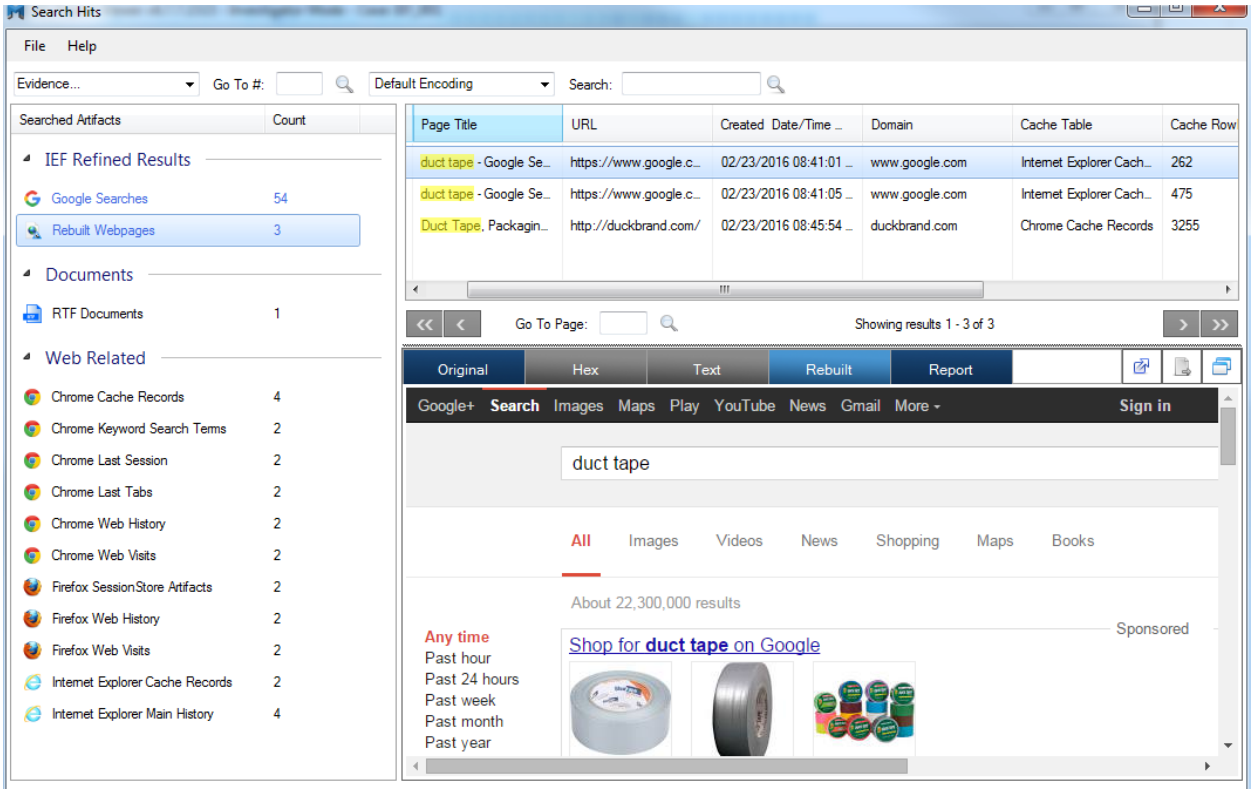


Figure 5: Search results for "duct tape" in IEF

Exporting Results

Once keyword searches were complete, we then proceeded to examine each tool's exportation feature. Exporting refers to the process of converting a file into a different desired format that can be opened and used on a different application. During a forensics investigation, an investigator might need to export a file or folder to evaluate on a different tool or to use for evidence presentation of a case. For this project, we compared each tools speed on exporting specific documents and directories onto our systems desktop. Below, in Table 11: Exporting results, are our results for the time it took to export specific files and the Downloads folder as well as information specific to each tools performance in exportation of files and folders.

Table 11: Exporting results

Time to Export Files	EnCase	FTK	Magnet IEF
Galaxy.pdf	0H 0M 1S	0H 0M 03S	0H 0M 02S
Ducttape1.jpg	0H 0M 1.46S	0H 0M 06S	0H 0M 01S
MP3_file1.mp3	0H 0M 1.46S	0H 0M 04S	N/A (Doesn't look for MP3 files)
Downloads folder	0H 0M 5.91S	0H 0M 5.30S	N/A (Can't see file structure)

EnCase Forensic

EnCase provided the fastest exporting times. One of the features of EnCase is the ability to export virtually any file for further examination by either copying the files out of the program or mounting the file to the computer. Since EnCase can export any file it makes this tool very useful on cases that have a lot of different files and types because it can all be done on one tool and be in a central location.

Forensic Toolkit (FTK)

FTK includes by default a number of exporting features such as KFF Data Group exporting, Email to PST exporting, Word list exporting, Recycle Bin Index content exporting, and many more. FTK exporting features allow the examiner to export files or folders to specific locations and allows the examiner the option to mount folders to the computer. Similar to EnCase, FTK can export any file but differs in that FTK can also identify specific files by comparing known contraband or malicious file's hash values against the data in the case and can export those files into a specific folder for further examination and can also export files as specific formats such as CSV or TSV if desired which can become useful for an examiner if he/she wants to conduct further analysis on another tool or software. FTK was able to export all files into their native format.

Magnet Internet Evidence Finder (IEF)

Since IEF doesn't allow the user to see the file structure of an image, and it doesn't look for .mp3 files, we were unable to export those two items. Other than that, IEF was just as quick as and sometimes faster than the other tools. We also ran into an issue with the latest version of IEF Report Viewer, 6.7.5: there was a bug in it that didn't allow us to export identifiers. Magnet support advised us to download and install IEF 6.7.4 in another location and use Report Viewer from the older version. This workaround was successful in fixing this issue.

File Extension Results

After exportation features for each tool were examined and compared, we proceeded to test each tool's ability to find specific file extensions. A file extension is the suffix at the end of a filename that indicates what type of file it is. File extension searches can be beneficial for an investigator to conduct in situations where a specific file extension might hold evidence important for the case. For this project, we compared each tools ability to find the following file extensions: .pdf, .rtf, .txt, .jpg, .gif, .png, .dat, .mpg, .wav, .mp3, and .mp4. Below, in Table 12, are our results along with information specific to each tools performance in file extension searching.

Table 12: File Extension Results

File type and total number of hits	EnCase	FTK	Magnet IEF
Documents	.pdf – 3 .rtf – 247 .txt - 513 Total = 763	.pdf – 3 .rtf – 247 .txt – 513 Total = 763	.pdf – 8 .rtf – 395 .txt – 513 Total = 916
Pictures	.jpg – 516 .gif – 134 .png – 2,332 Total = 2,982	.jpg – 516 .gif – 134 .png – 2332 Total = 2,982	Total = 19,344
Video	.dat – 199 .mpg – 4 Total = 203	.dat – 200 .mpg – 6 Total = 206	Total = 276
Audio	.wav – 605 .mp3 – 8 .mp4 – 7 Total = 620	.wav – 606 .mp3 – 9 .mp4 – 7 Total = 622	N/A (Doesn't look for audio)

EnCase Forensic

EnCase allows you to filter data based on certain parameters. We created filters by file extension and chose the extensions we looking for. We then counted the number of hits each filter produced and added them up. You can see the totals of each in Table 12: File Extension Results above. EnCase and FTK had similar results, however IEF showed very different hits. Below, in Figure 6, you can see screenshot that captures the option to "Find Items based on Extension."

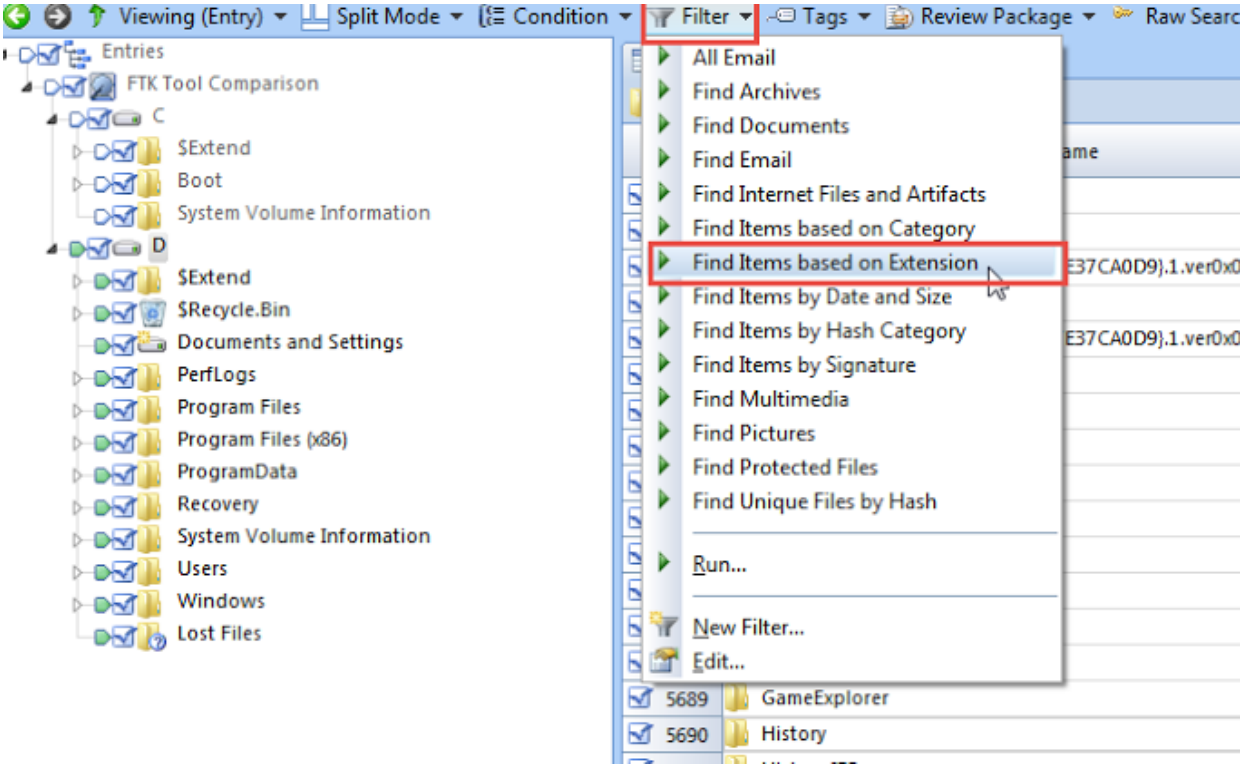


Figure 6: Screenshot of how to "Find Items based on Extension" in EnCase v.7

Forensic Toolkit (FTK)

FTK allows the user to create filters to locate specific files. In this stage, we created filters to look for certain file extensions. To do this, we first had to bookmark all of the data in the case. Then inside the bookmark tab, we created a filter for the specific file extension we were looking for. We created filters for all of the file extensions we were looking for which is a lot easier and not as time consuming as it sounds. After each filter was created, the user has the option to save the filters to use them later if desired. As shown in the table above, EnCase and FTK displayed similar results for most of the file extension searches.

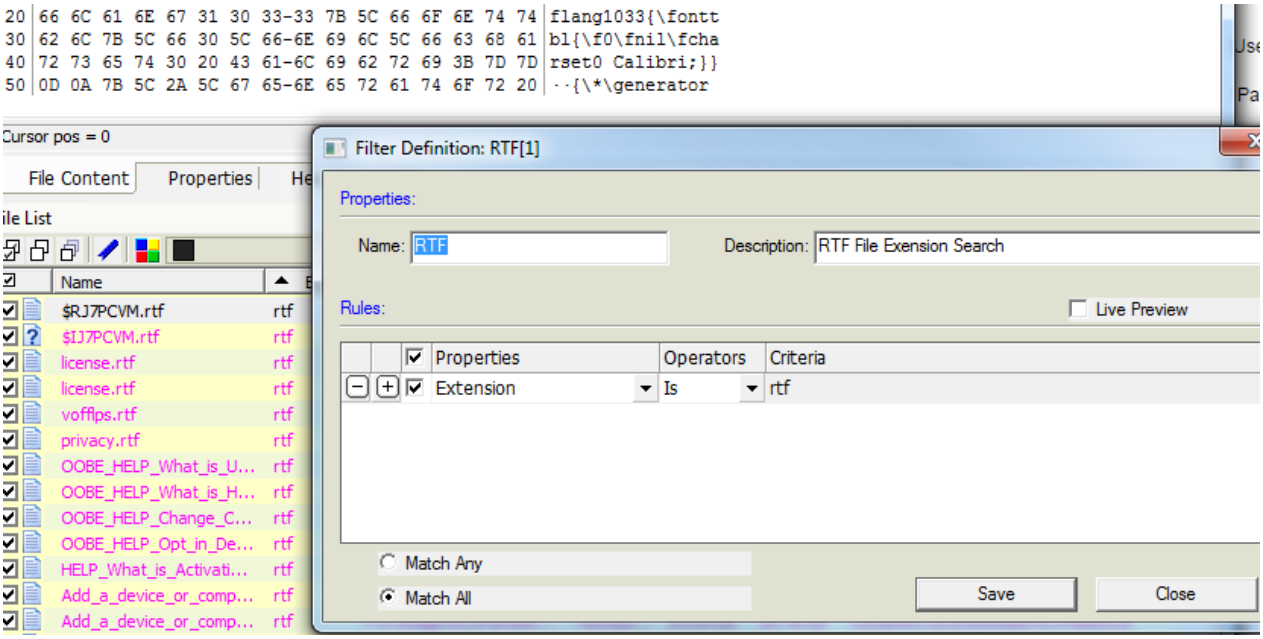


Figure 7: Filter for .RTF File Extension in FTK

Magnet Internet Evidence Finder (IEF)

IEF found more picture files than the other tools. This is because the other tools were only looking at file extensions and were only looking for known file extensions for pictures. IEF also looked for images inside .dll files. EnCase and FTK would not recognize .dll files as images unless they were manually checked for images. These files are system libraries and Windows will sometimes store icons in them, which composes of a majority of the .dll hits in the pictures section. On Page 19, in Figure 8 , you can see a screenshot of the .dll image results in IEF. Someone could potentially hide images in these libraries, however IEF checks for any images hidden that way. This was also true for the other categories that IEF had more hits in, the other tools were being checked for known file types of those categories - .docx for documents, .mpg for videos, etc. - but IEF also checks lesser known formats that would be categorized as a document.

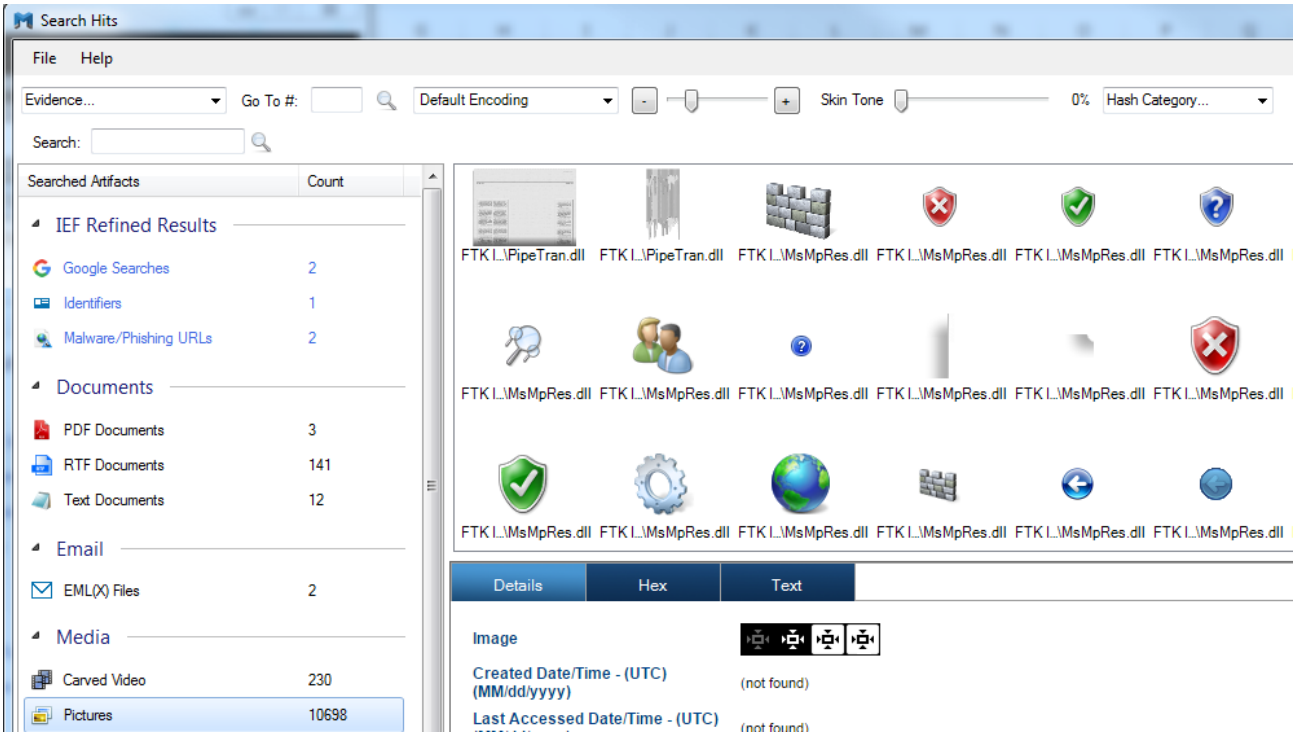


Figure 8: .dll Image results in IEF

Timeline Feature Results

The last feature we examined was timelines. Timeline features are beneficial for an investigation as they can serve as a useful analysis tool when trying to see when a system was used and/or what events occurred before and after a given event. Each tool has significantly different ways to capture a timeline of events. Since each tool has such varied ways of capturing the timeline of events and the way it presents those events, the number of artifacts differs dramatically. For this project, we were more concerned if the timeline produced an accurate timeline of events. Below in Table 13 are the results for each tools ability to display a timeline of events that occurred on the system being investigated as well as each tools ability to accurately display these events.

Table 13: Timeline February 22-24

Timeline feature	EnCase	FTK	Magnet IEF
Are the Results Accurate? Yes/No?	Yes	Yes	Yes

Number of artifacts	20,332	4,523	71

EnCase Forensic

In EnCase, when you enter the timeline feature, you are provided with three panes. One looks like the screenshot below in Figure 9: EnCase v.7 Timeline Feature Results. Next to this pane is the file structure of the image. The bottom pane provides a description of the entry you are viewing. In order to find a specific entry you have to parse through the chart below until you find the entry you are looking for. You have the option to broaden or narrow the timeline to see the data further out in time or closer to a specific time and date. Once you have the entry you are looking for, it will be highlighted in the file structure on the side pane described earlier. You can then choose to examine the entry in the description pane, or switch back to "Table Mode" which is how you usually parse through the image in EnCase. This process is tedious, but can be useful. As you can see in Table 13: Timeline above, EnCase produces a significant amount of artifacts because it is *everything* in the image, just like in "Table Mode", graphically organized into a timeline. Essentially, EnCase's timeline feature reorganizes the data from "Table Mode" to a graphical representation of the artifacts at a given time range.

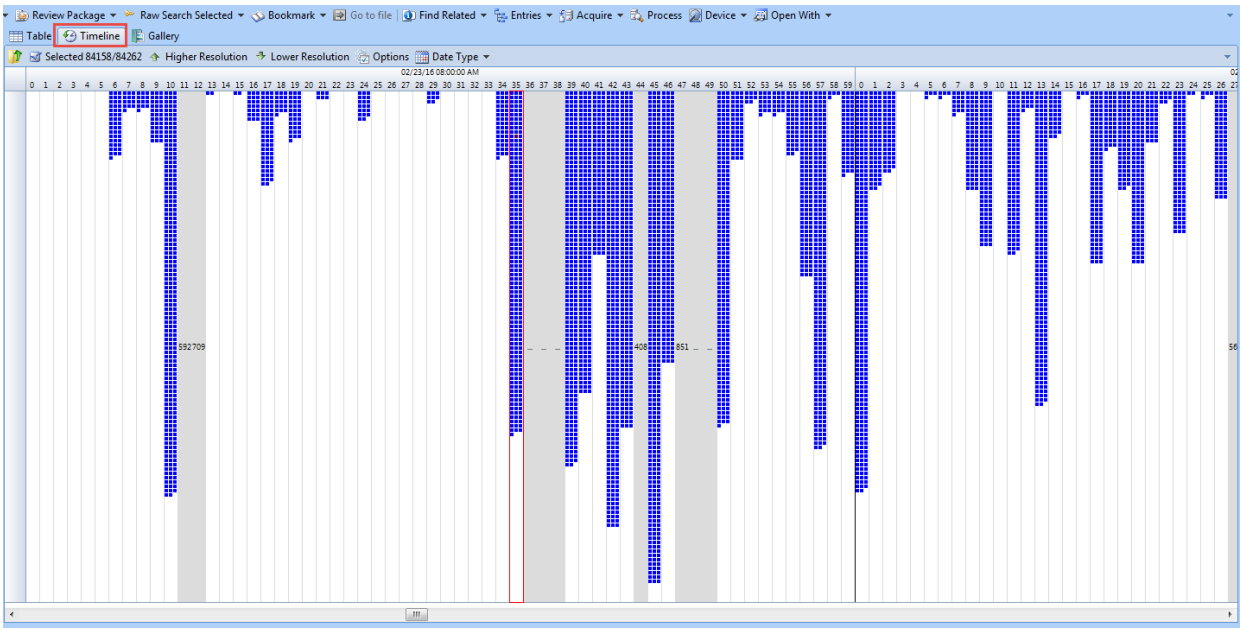


Figure 9: EnCase v.7 Timeline Feature Results

Forensic Toolkit (FTK)

Similar to EnCase, FTK's timeline feature was a bit tedious to use at first. We first attempted to enable CSV and HTML file listings to export a timeline but the timeline that was created was missing specific files. We confirmed that these files were not listed in this timeline by conducting searches for MD5 hashes of specific documents and pictures in the timeline. Our second attempt to create a timeline included bookmarking all of the data in the case and then creating a filter for files accessed, created, and modified between February 22 and February 24,

2016. Here we created a timeline that contained events that occurred during the associated time and produced more results then IEF but less then EnCase.

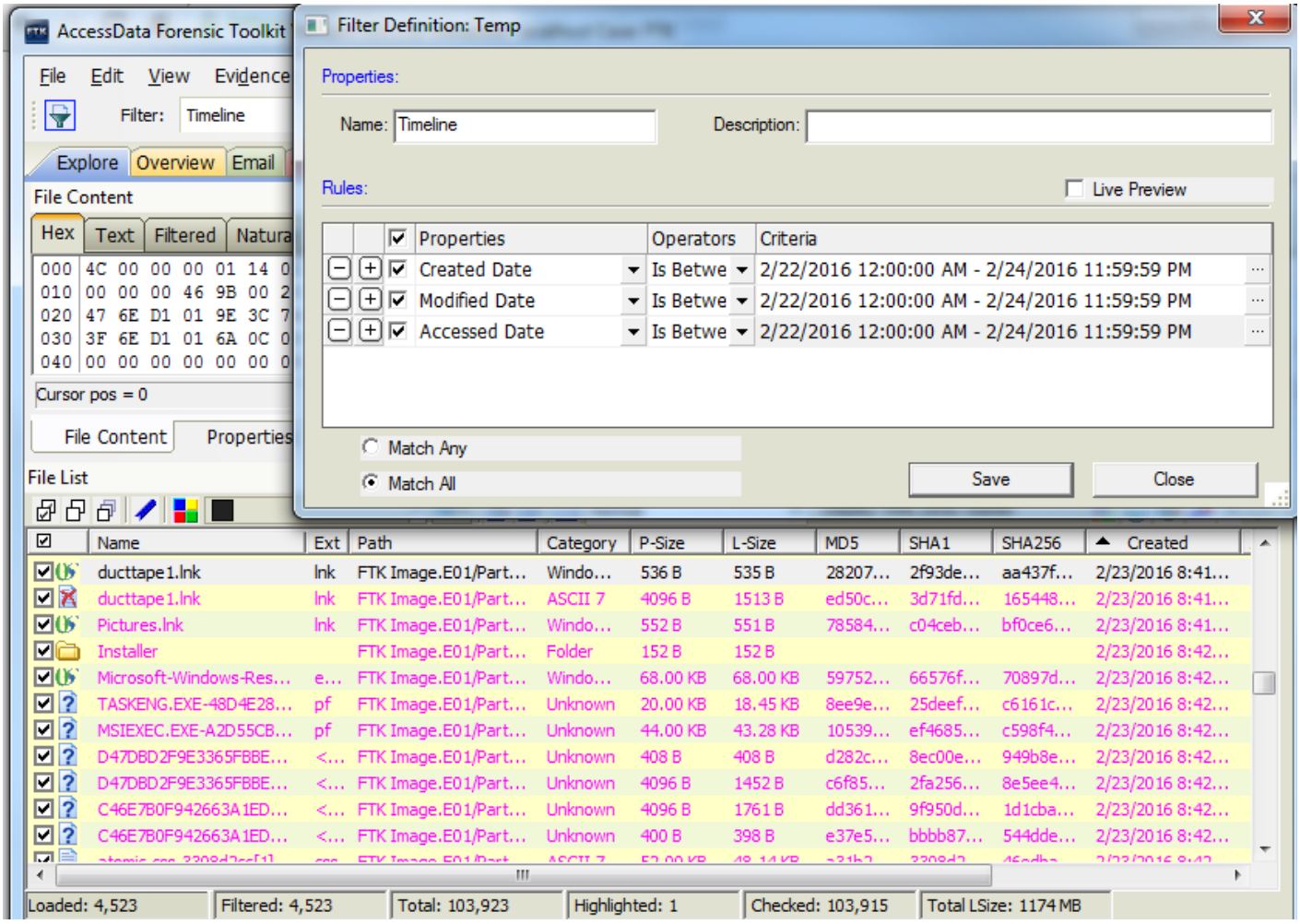


Figure 10: Timeline Filter and Results on FTK

FTK produced more results then IEF because IEF primarily looks for Internet-related events while FTK is looking at all events that occurred during the specified time. With this timeline, we were able to follow with extreme accuracy the events that occurred on the day we conducted data generation on our test computer.

Magnet Internet Evidence Finder (IEF)

IEF's timeline allows you to see any activity related to the artifacts it finds. It has a relatively simple interface, allowing you to see a timeline of activity arranged in categories. It does not chart as many things as the other tools as the timeline only reflects specific artifacts.

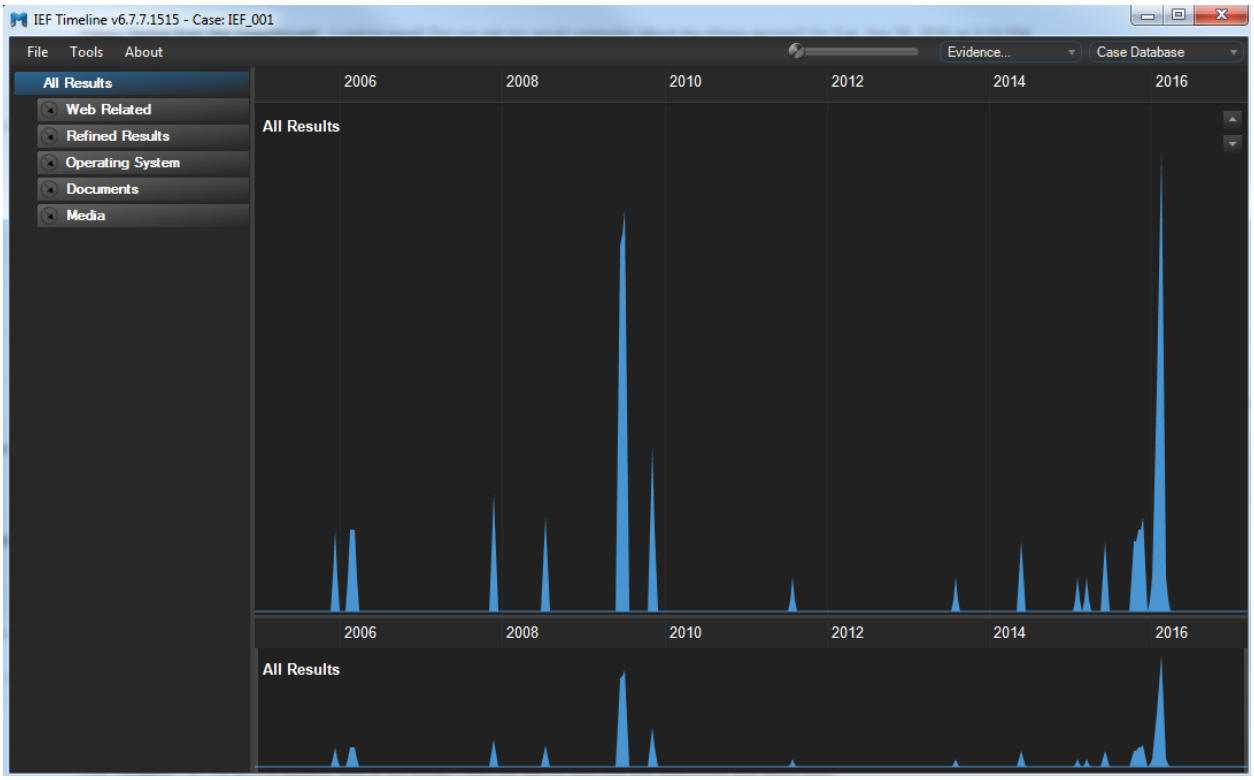


Figure 11: IEF Timeline showing all of the activity on the image

Conclusion

Upon completion of this project, it is evident that each tool has its strengths and weaknesses, compiled in the results of our analysis. The main features of the tools we were testing included each tool's ability to conduct various keyword searches, the accuracy each tool's timeline feature, and the time it takes to export different files and directories.

One feature that is unique to IEF is the ability to rebuild some webpages in the Report Viewer. Provided that the entire webpage is still stored in the cache of the web browser that viewed it, a user can see what the page looked like at the time it was viewed without needing to use a separate tool to rebuild the HTML text.

The time it took to conduct specific keyword searches on a reasonable set up was dependent on the type of search. In this project, we focused on index-based searches which meant that the tool itself would refer to a table it created in order to find the search criteria. IEF and FTK both created indexes by default during processing of data while EnCase required us to activate index search capabilities. Our index searches averaged between 0.1 and 0.3 seconds. This was because each tool referred to its index to find the specified term instead of parsing all the data. We were

able to test this type of search in EnCase and when conducted, EnCase took on average 10 to 14 minutes to complete this type of search and produced significantly more results due to the way files are mounted.

Although we were not able to use FTK's timeline report feature, we were able to create a bookmark timeline which allowed us to view events that occurred from February 22 to February 24. All the artifacts found in each tool's timeline was accurate to the data generation sheet we produced before the project.

The results of the exporting features of each tool were close in time, ranging from one and six seconds. We ran into a problem with Magnet IEF because that tool does not provide the file structure of the image it took of the hard drive, so we were unable to export the Downloads folder. IEF does not allow for file extension searches so we were unable to find and export mp3_file1.mp3. EnCase was on average the fastest in exporting files while IEF was close behind. FTK on average took a bit longer (about 2 seconds longer) than both IEF and EnCase but was able to export all 3 files as well as the Download folder.

Further Work

As each of these tools are being constantly updated, tool comparison will continue to be common LCDI project.. In fact, as we were compiling our results, EnCase released another software update. For future work, we could examine Linux-based forensic tools as well as other open source forensic tools such as Autopsy or The Sleuth Kit. We could also build upon this specific project and examine each tool's ability to perform these tests in a very limited environment, with less allocated memory and processing power. We could also test each tool's ability to perform live memory forensic analysis. Additionally there are modules for mobile forensics in the tools we tested that could be compared. When any of these forensic tools are updated, typically new features are added and in the future these features and tools can be compared.

References

Shah, Megh and Paradise, David. *Tool Comparison.* Leahy Center for Digital Investigation, 2013. Web

Widup, Suzanne. *Computer Forensics and Digital Investigation with EnCase v7*. McGraw-Hill Education, 2014. Print.

Appendix

Appendix 1: Data Generation List

Color Codes

Site	Color	Comments
Google	Green	Includes Google searches and Gmail usage.
Yahoo	Yellow	
Bing	Blue	
Facebook	Orange	
Non-search Engine actions	White	I.e. Microsoft word, Paint, actions not done on a search engine.
Other websites	Grey	I.e. YouTube, ask.com, etc.
File movement	Violet	Copying, deleting, moving files
Opening or Closing	Black	Web browser, major website, or application opened or closed

Below are the list of actions that will be performed during our data generation. The instructions were followed accurately so we could compare what we did to what the forensics tool we are using says we did.

Time (24HR Time)	User Action	Machine Action	Comments
2/23/16			
08:15	Turn on computer	Computer powered on	
08:35	Log into computer	tool.eval account logged on	tool.eval is password protected
08:36	Open Internet Explorer		
08:36	Go to Google.com		
08:37	Search “Google Chrome”		
08:37	Download Google Chrome	Chrome Downloaded	

Time (24HR Time)	User Action	Machine Action	Comments
08:37	Install Google Chrome	Chrome Installed	
08:38	Search “Firefox”		
08:38	Download Mozilla Firefox	Firefox Downloaded	
08:39	Install Mozilla Firefox	Firefox Installed	
08:39	Go to Google on Internet Explorer	Internet Explorer Opened	Went to google.com
08:39	Search for “Chloroform”		**The sites that you must visit will be listed below. The caption of the site will be listed in the comment section of the row.**
08:40	Open en.wikipedia.org from search results		“Chloroform - Wikipedia, the free encyclopedia”
	Go back to search results		
08:40	Open dictonary.reference.com from search results		“Chloroform | Define Chloroform at Dictionary.com”
08:40	Go back to Google		
08:41	Search “duct tape” on image search		Download **first** image result, result shown below. Save to pictures as “ducttape1” 
08:43	Go to Yahoo.com		
08:43	Search for “Chloroform”		**The sites that you must visit will be listed below. The caption of the site will be listed in the comment section of the row.**
08:44	Open en.wikipedia.org from search results		“Chloroform - Wikipedia, the free encyclopedia”
	Go back to search results		
08:44	Open dictonary.reference.com from search results		“Chloroform | Define Chloroform at Dictionary.com”
08:44	Go to Bing.com		

Time (24HR Time)	User Action	Machine Action	Comments
08:44	Search for "Chloroform"		**The sites that you must visit will be listed below. The caption of the site will be listed in the comment section of the row.**
08:44	Open en.wikipedia.org from search results		"Chloroform - Wikipedia, the free encyclopedia"
08:45	Open dictonary.reference.com from search results		"Chloroform | Define Chloroform at Dictionary.com"
08:45	Close Internet Explorer		
08:45	Open Google Chrome		
08:45	Go to Google.com		
08:45	Search for "Chloroform"		**The sites that you must visit will be listed below. The caption of the site will be listed in the comment section of the row.**
08:45	Open en.wikipedia.org from search results		"Chloroform - Wikipedia, the free encyclopedia"
08:45	Open dictonary.reference.com from search results		"Chloroform | Define Chloroform at Dictionary.com"
08:45	Go back to Google		
08:46	Search "duct tape" in image search		Download **second** image result shown below. Save to pictures as "ducttape2" 
08:46	Go onto Yahoo.com		
08:46	Search for "Chloroform"		**The sites that you must visit will be listed below. The caption of the site will be listed in the comment section of the row.**
08:47	Open en.wikipedia.org from search results		"Chloroform - Wikipedia, the free encyclopedia"
08:47	Open dictonary.reference.com from search results		"Chloroform | Define Chloroform at Dictionary.com"
08:47	Go to Bing.com		

Time (24HR Time)	User Action	Machine Action	Comments
08:47	Search for “Chloroform”		**The sites that you must visit will be listed below. The caption of the site will be listed in the comment section of the row.**
08:47	Open en.wikipedia.org from search results		“Chloroform - Wikipedia, the free encyclopedia”
08:47	Open dictonary.reference.com from search results		“Chloroform | Define Chloroform at Dictionary.com”
08:47	Close Chrome		
08:47	Go onto Mozilla Firefox		
08:48	Go to Google.com		
08:48	Search for “Chloroform”		**The sites that you must visit will be listed below. The caption of the site will be listed in the comment section of the row.**
08:48	Open en.wikipedia.org from search results		“Chloroform - Wikipedia, the free encyclopedia”
08:48	Open dictonary.reference.com from search results		“Chloroform | Define Chloroform at Dictionary.com”
08:48	Go back to Google.com		
08:48	Search “duct tape” on image search		Download **third** image shown below. Save to pictures as “ducttape3” 
08:48	Go to Yahoo.com		
08:49	Search for “Chloroform”		**The sites that you must visit will be listed below. The caption of the site will be listed in the comment section of the row.**
08:49	Open en.wikipedia.org from search results		“Chloroform - Wikipedia, the free encyclopedia”
08:49	Open dictonary.reference.com from search results		“Chloroform | Define Chloroform at Dictionary.com”
08:49	Go to Bing.com		

Time (24HR Time)	User Action	Machine Action	Comments
08:49	Search for “Chloroform”		**The sites that you must visit will be listed below. The caption of the site will be listed in the comment section of the row.**
08:49	Open en.wikipedia.org from search results		“Chloroform - Wikipedia, the free encyclopedia”
08:49	Open dictonary.reference.com from search results		“Chloroform | Define Chloroform at Dictionary.com”
08:49	Close Firefox		
08:50	Open Google Chrome		
8:50	Go to Facebook.com		
08:51	Log on to Facebook.com using the email aguirre3946@gmail.com		Log in using credentials on Secret Server
08:51	Go to Settings on Facebook		Click on down arrow drop down menu in top right and click on Settings.
08:52	Click on “Download a copy of your Facebook data.”		
08:52	Click on “Download Archive” and then click on “Start My Archive”		
08:52	Like a post in the newsfeed		**Posted By:** The Senator Leahy Center for Digital Investigation (LCDI) **Content:** “Bluetooth Security”
08:53	Post to your timeline “Gonna be a great day, just gotta find my duct tape!”		
08:54	Message Joseph Mitchell: “It was murder” along with image “ducttape3”		
08:56	Check in at Bibens Ace Hardware Burlington VT		
08:56	Search for “puppies” like the result page marked as an interest with a white dog as the profile picture		
08:56	Logout of Facebook		

Time (24HR Time)	User Action	Machine Action	Comments
08:57	Go to Gmail.com		
08:58	Log in to Gmail using aquirre9999@gmail.com		Log in using credentials on Secret Server
08:59	Send email to champtoolcompare@mailinator.com		Subject: "shovel" Message: "I got the shovel, just need the duct tape. Let me know if you have the bag. Can't wait!"
08:59	Log out of Gmail		
08:59	Log back in to Gmail		
09:00	Open Facebook archive email, download Facebook data		
09:00	Logout of Gmail, close tab		
09:01	Go to YouTube.com		
09:01	Search & Watch "How To Make Chloroform" by Magneto!"		
09:08	Copy video URL		
09:08	Search "Mtn Dew Kickstart: Puppymonkeybaby | Super Bowl Spot"		
09:09	Search "Concrete Does Not Dry Out" by minutephysics		
09:12	Exit YouTube		
09:12	Open a new tab in Chrome Go to Google.com Search for "youtube downloader" Click on savefrom.net search result		
09:12	Enter in video URL, right click on download link, save as "making chloroform" to videos directory		
09:12	Go to YouTube on another tab, keep SaveFrom.net open.		
	YouTube		
09:12	Search "Phoenix - Chloroform (Official Video)"		
09:15	Copy Video URL		

Time (24HR Time)	User Action	Machine Action	Comments
09:15	Go back to SaveFrom.net tab		
09:15	Enter in video URL, right click on download link, save as “phoenix chloroform” to videos directory		Savefrom.net did not work for the subsequent videos so we did a different site.
09:17	Watch a video in the related videos side column		We picked “chloroform haloform reaction video”
09:20	Click on back button and click on another video in the related videos side column		We picked “Phoenix – Entertainment”
09:21	Copy video URL		
09:23	Go to Google.com		
09:23	Search for “youtube downloader” Click on videograbby.com		
09:25	Enter in video URL, save to downloads		
09:26	Rename video “phoenix chloroform”, cut and paste to videos		
09:27	Go to Devices and Printers, add the LCDI printer		The printer should show up in the add printer wizard
09:28	Go to maps.google.com		
09:28	Search “Orlando, Florida”, click on directions, and enter starting point as “Warren, Ohio”		
09:28	Click on the first route, then on print Icon.		
09:29	Only print text and print Pages “1-2”		
09:29	Go to Google.com		
09:30	Search “DP Shredder”		
	Click on the www.pendriveapps.com search result		
09:30	Scroll down and download DP Shredder.		

Time (24HR Time)	User Action	Machine Action	Comments
09:31	Extract DP_Shredder.exe to desktop		
09:31	Go to Google.com		
09:32	Search “iphone 6 manual		
9:32	Click on first link at manuals.info.apple.com		
9:32	Save to downloads as “iphone”		
09:32	Search “galaxy s6 manual		
9:32	Click on the downloadcenter.samsung.com search result		
9:32	Save to downloads as “galaxy”		
9:32	Go to Bensound.com		
09:33	Download three MP3 files, rename them “MP3_file1”, “MP3_file2”, and “MP3_file3”		**The MP3 Files we used are below with their file name and the title of the MP3 we used.**
	MP3_file1		“Dubstep”
	MP3_file2		“Cute”
	MP3_file3		“Buddy”
09:33	Go to Windows start menu Click on “Computer” Click on “Downloads”		
09:34	Delete “iphone” from Downloads		
09:36	Open WordPad		
09:36	Create new document Type “shovel”, “chloroform”, “duct tape”, and “murder” on separate lines. Save to Documents as “document1”		
09:36	Create a new document Type “bury”, dispose, “hide” on separate lines. Save to Documents as “document2”		
09:36	Close WordPad		

Time (24HR Time)	User Action	Machine Action	Comments
09:38	Open Notepad		
09:38	Type “shovel”, “chloroform”, “duct tape”, and “murder” on separate lines. Save to Documents as “text1”		
09:39	Create a new document Type “bury”, “dispose”, “hide” on separate lines. Save to Desktop as “text2”		
09:39	Close Notepad		
09:39	Start Menu → Computer		
09:39	Copy “ducttape1” to desktop		
09:39	Copy “ducttape2” to desktop		
09:40	Open DP Shredder		
09:40	Delete “ducttape1” from desktop using DP Shredder and use one round and US DoD 5220.22-M (E) 3x		
09:40	Delete “text1” from Documents using DP Shredder and use one round and US DoD 5220.22-M (E) 3x		
09:41	Delete Facebook data using DP Shredder and use one round and US DoD 5220.22-M (E) 3x		
09:41	Delete “MP3_file2” using using DP Shredder and use one round and US DoD 5220.22-M (E) 3x		
09:41	Close DP Shredder		
09:41	Delete “ducttape2” from desktop		
09:42	Delete “document2” from Documents		
09:42	Delete “MP3_file1” from downloads		

Time (24HR Time)	User Action	Machine Action	Comments
09:44	Plug in a flash drive, make note of the size, model and manufacturer in comments.		3.76GB Blue Champlain ITS “Generic UDISK USB Device”
09:44	Copy “ducttape1” from pictures to USB drive		
09:44	Copy “DP_Shredder.exe” from desktop onto USB drive		
09:45	Delete DP_Shredder.exe from desktop		
09:45	Eject USB drive then remove		
09:45	Shut down computer (Installed updates)		