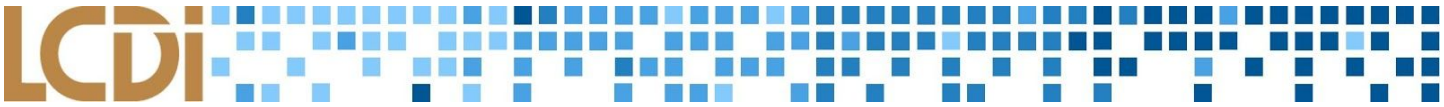


CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

Tool Evaluation

	175 Lakeside Ave, Room 300A
	Phone: (802)865-5744
	Fax: (802)865-6446
11/12/2017	http://www.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

In the world of Digital Forensics, the researcher is only as good as their tool. It is essential for the accuracy and the validity of an investigation that one has the best tools at their disposal to extract, locate, and document digital evidence. At the Leahy Center for Digital Investigations (LCDI), the Tool Evaluation team will be working to determine the ease of use, similarities, differences, utility, and effectiveness of EnCase, Forensic Toolkit (FTK), Magnet Internet Evidence Finder (Magnet IEF), and SANS Investigative Forensic Toolkit (SIFT)..

Background:

At the Leahy Center for Digital Investigation, an evaluation of digital forensic tools occurs bi-annually (each semester) and this comparison usually involves FTK and EnCase. Due to an increased demand for internships at the LCDI, this toolset has been expanded to many other forensic software tools such as Magnet IEF and SIFT. The tools that will be examined this semester are EnCase, FTK, Magnet IEF, and SIFT.

Purpose and Scope:

A valid comparison between tools cannot be constructed without hands on experience with the tools in question. The main purpose of this project is to compare and contrast the different forensic tools using quantifiable data. This data can be used to draw conclusions about which tool is best based on ease of use and efficiency. It is important for the LCDI to do this report as each new version of a tool comes out to keep data up to date. Additionally, as interns, this project helps introduce us to the basic principles of the digital forensics field.

Research Questions:

1. The tool's features
    a. *How does it process, index, search, etc.?*
2. The tool's ability to obtain artifacts
    a. *How many artifacts?*
    b. *How many relevant artifacts?*
    c. *How quickly were artifacts obtained?*
3. The tools searching speed
    a. *What differences are present between the tool's searches?*
4. The tool's ability to recover deleted files

5. The tool's level of difficulty
    a. *Is it easy for beginners?*

Terminology:

Acquisition - The process of copying data from a piece of evidence to another location in a forensically sound manner so that the data may be analyzed at a later time.

Artifact - Any digital data, created by user interaction, than can be used during a digital investigation.

Cache - A fast access portion of memory that is stored in a separate location from normal memory.

Clone - Copies the drive exactly to another drive.

Compression - The process of altering data or changing the data storage in order to store it using less space.

EnCase - A specific branch of tools developed by Guidance Software for various forms of digital investigation. Different versions include EnCase Forensic, Cybersecurity, eDiscovery, and Portable.

Encryption - A way of translating plain text into unreadable ciphertext, which needs to be decrypted in order to be read.

Forensic Toolkit (FTK) - A computer forensics software made by Access Data. It scans a hard drive looking for artifacts. For example, it can locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.

Hashing - A process that converts text or a file into a string or value representation which can be used to verify the data's validity.

Image - A file that contains a copy of a hard disk drive.

Linux - An open-source operating system modelled on UNIX.

Magnet Internet Evidence Finder (Magnet IEF) - Magnet IEF is an acquisition software developed by Magnet Forensics. It emphasizes the ability to find hundreds of types of evidence while remaining intuitive.

Partition - The process of separating one physical drive into several separate, independent data locations.

SANS Investigative Forensic Toolkit (SIFT) - A collection of various tools that aid in several forensic analysis tasks.

Verification - A process that utilizes the hash values of a source media as well as the image in order to verify the accuracy of the imaging process.

Virtual Machine (VM) - Software that mimics a computer. It has an operating system and is capable of running applications.

Write Blocker – Allows acquisition of a drive by blocking "write commands" which might alter data.

Methodology and Methods

For our Data Generation, we used a virtual machine using vSphere that was running Windows 10. The use of the virtual machine allowed every team member to log in to a tool specific VM from any workstation in the LCDI Research room. The virtual machine was imaged using FTK Imager 3.4.2.6 and was placed on virtual machines running FTK, EnCase, Magnet IEF, and SIFT. The use of virtual machines for running these forensic tools allowed team members to pick up where others left off. Searches could be run on a server machine where individual workstations were powered down.

Equipment Used

Table 1: Hardware used

Device	Specifications
Virtual Machine (Tool)	16GB RAM, 4 x 10369MHZ CPU cores, Windows 10 Enterprise, 185GB Storage
Virtual Machine (Data Generation)	16GB RAM, 4 x 10369MHz CPU cores, Windows 10 Enterprise, 50GB Storage

Table 2: Software

Device	Version	OS
Forensic Toolkit (FTK) 6.1	V6.1.0.130	Windows 10 Enterprise
Forensic Toolkit (FTK) Imager	V4.1.1.1	Windows 10 Enterprise
SANS Investigative Forensic Toolkit (SIFT) Workstation	v2017.36.0	Linux Ubuntu 16.04
EnCase Forensic v8	V8.01.01.03	Windows 10 Enterprise
Magnet Internet Evidence Finder (Magnet IEF)	V6.9.3.7144	Windows 10 Enterprise
VMware vSphere	V6.0.0	Windows 10 Enterprise

Tool Evaluation:

Data Collection:

In order to replicate a real digital forensic investigation, our team needed to create a case by accessing a virtual machine as if we were the criminal. Our first order of business was to construct and agree upon a schedule of events \which we would execute on the VM. All of our work acting as the criminal in our search history, downloaded files, and installed applications was contained within the virtual machine that acted as the criminal's computer. After this point, the VM was imaged and evaluated for artifacts and keyword searches using our tools. Each tool was run on a separate VM to save physical real estate and ensure the analysis was not interrupted between shifts.

Data Generation:

Our data generation was conducted on a clean virtual machine instead of a physical computer. This was to free up physical real estate in the lab and ensure our data came out as intended. There was three days' worth of data that had been generated. This data included file management and manipulation using OpenOffice version 4.1.4, web surfing on a variety of browsers including Mozilla Firefox, Google Chrome, and Microsoft Edge, and image manipulation. We put in deliberate breaks in the activity to simulate a user logging on and off to run errands, go to class, or some other interruption. Our scenario involved Professor Plum killing his colleague, Professor White, with sodium cyanide. The following data generation involves his research, planning, and day-to-day activities including correcting homework, researching jazz and golf, and looking for new recipes to prepare at home. The data generation schedule can be viewed in its entirety in the appendix.

Search Results:

Table 3: Keyword search for "e"

Program	Number of Hits	Number of Files	Time Elapsed (MM:SS)
EnCase (raw)	600,083,899	206,359	59:05
EnCase (index)	12	6	00:01
FTK	28,537,152	363,459	6:18:00 (estimation)
SIFT	34,115,445	N/A	14:43

Tool Evaluation:

Magnet IEF	199,876	64,480	4:27

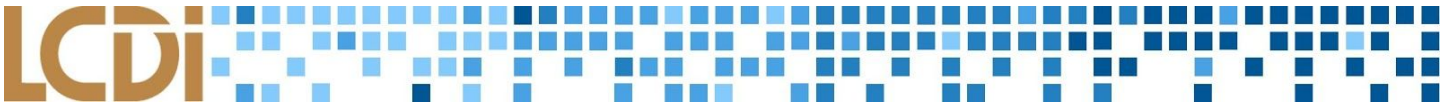
Table 4: Keyword Search for “asdfghjkl”

Program	Number of Hits	Number of Files	Time Elapsed (MM:SS)
EnCase (raw)	1,590	1,542	24:21
EnCase (index)	0	0	00:01
FTK	78	43	34:43
SIFT	0	0	1:00
Magnet IEF	2	2	1:58

Table 5: Keyword search for "sodium cyanide"

Program	Number of Hits	Number of Files	Number of Relevant Files	Time Elapsed (MM:SS)
EnCase (raw)	20	2	1	26:41
EnCase (index)	0	0	0	00:01
FTK	95	14	3	47:55
SIFT	0	0	0	1:00
Magnet IEF	0	0	0	2:00

Tool Evaluation:



Analysis

What processing capabilities are available for each tool?

EnCase

The EnCase processor is able to recover folders, perform file signature analysis, perform protected file analysis, create thumbnails, perform hash analysis, expand compound files, find emails, find internet artifacts, index data, prioritize data by type and date of file, and do keyword searches. EnCase also offers a processor manager where tasks can be queued and run on local and remote processors. This processor manager also allows the user to see the times it took for each process to run, and offers discrete pathways in Version 8, such as Full Investigation that easily allows an investigator to complete all necessary steps for completing a case.

Forensic Toolkit

The processing capabilities of FTK begin with adding a disk as evidence. This process is divided into three different tasks: processing, post-processing and indexing. First, the disk is processed. After this, post-processing, which is FTK verifying the new digital image, begins. Lastly, it indexes, which takes the longest out of the three. This part usually includes the rearranging and the organizing of data on the digital image, allowing for faster index searches when needed. Once the processing is completed, the user is given the times for all the various parts along with the number of items found, processed, and indexed.

SIFT

SIFT comes with a variety of tools that can be used to process and index data. Autopsy 2.24 allows for indexing and searching of ASCII and Unicode on forensic images. It also has tools like mactime and log2timeline that can be used to generate a timeline of events that occurred on the system by taking the artifacts extracted from another tool. There are also various tools and methods you can use to recover deleted files and fragmented files. SIFT can analyze a variety of forensic image formats, including Expert Witness Format, Advanced Forensics Format, and Raw Formats. SIFT can also process images of volatile memory using Volatility.

Magnet IEF

Magnet IEF has one processing function to scan hard drives, image files (including EnCase files, FTK images, raw images, virtual machine images, and DMG images), archive images, and volume shadow copies. It also allows you to select individual partitions on drives, as well as specific files and folders. There is provided support for mobile forensics on Android, iOS, Windows phones, and Kindle devices. An image will be taken and scanned for social media, web activity, applications, chat logs, text documents, PDFs, and other user files. While the processing lacks the granularity of other tools, it is very easy to use and accepts a multitude of image types and other media. With Magnet IEF, the analyst is able to control what the tool scans for in the image, this allows shorter processing times while finding exactly what is needed.

How quickly does each tool process data?

EnCase

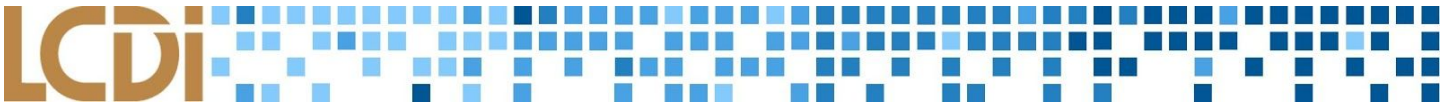
EnCase took 10:56 to process the image with the standard processing preset that excluded indexing. For indexing alone, it took EnCase 7:40. A standard search with indexing took 11:12. These fast processing times were largely due to the fact that EnCase allowed us to search specifically for what we wanted and gave total control over the parameters of the search to the user.

Forensic Toolkit

Forensic Toolkit required 01:15:16 to process the image, and 01:57:08 to index the image. A standard search in FTK took at least 30 minutes. When searching for a common phrase, FTK could go on for hours depending on how large the drive is. When we were browsing for the keyword "e", FTK crashed multiple times due to a potential overload of hits. FTK is probably the slowest tool of the bunch here, but the results are usually very accurate.

SIFT

The speed of processing in SIFT depends on the tool. The searches listed in the tables were completed using Autopsy's keyword search function. Searches using this method were fast because they only extracted the ASCII and Unicode strings and then searched them. We later ran a search using Bulk_Extractor which ran for about 30 minutes before being unable to read the image for an unknown reason. We then looked through the results manually to find artifacts.



Magnet IEF

When Magnet IEF was tested it took 2 hours, 58 minutes, and 37 seconds to process the data generation image, but it did not have indexing options. Magnet IEF seems to be in the middle of the pack regarding time. This is because it was searching for specific artifacts while not going too in depth into the image.

What are some key features of each tool?

EnCase

The key features of EnCase include multiple write blockers, pathways, backwards compatibility, different evidence file types, and mobile support. The write blockers prevent any damage to files when they are being acquired or indexed. Pathways are templates for parts of a case or even a whole investigation. These are especially useful for people new to forensic software that need a little guidance. Version 8 of EnCase is also backwards compatible with version 7, which means that evidence files made in 7 can be used in 8. In addition, there are a variety of evidence file types: EnCase file, logical evidence file, and encrypted evidence file.

Forensic Toolkit

FTK has a wide variety of features that increase the tool's ease of use. The tool indexes the image during the initial processing to decrease the amount of time spent searching. FTK has a condensed yet easily navigated user interface, including a search filter allowing the user to view files fitting a certain description or file type and a simple navigation system that would be familiar to any computer user. It allows users to "bookmark" for later viewing and analysis.

SIFT

SIFT is a free collection of digital forensics tools, scripts, libraries and utilities. This creates a wide variety of options when processing data. Autopsy can be used to search for artifacts on a forensic image through a graphical interface. Tools like Scalpel can automatically find and recover many deleted files. Volatility can be used to examine a system's volatile memory.

SIFT comes with these and various other tools to help process various types of data. While some of these tools offer a graphical user interface, most run solely on the command line interface. More tools, scripts, libraries, and utilities can also be added to a SIFT image to increase its functionality. The base version SIFT can be installed and run on any Ubuntu 16.04 or can be downloaded as a premade VM Appliance.

Magnet IEF

The main goal of Magnet IEF is its ease of use while not sacrificing evidence. Magnet IEF is very easy to use, the interface is user-friendly, and it has everything needed for a comprehensive case analysis. From the minute Magnet IEF boots up, the interface is streamlined, clearly describing what each option on the screen means and what it does. After processing, everything is organized by the type of data that was collected such as social media, email, web activity, files, chat, and media.

Inside those categories, it is refined even further based on the type of file or content. The logos next to the categories allow for easy recognition of desired content and make finding specific files a breeze. The timeline feature also allows for easy searching of files. The timeline organizes the processing results based on the timestamp of the activity, giving a detailed chain of events that can be viewed and analyzed. Magnet IEF also has a bookmarking feature where if a file in question is found, it can be marked for further processing.

To what extent is each tool able to correctly obtain artifacts?

EnCase

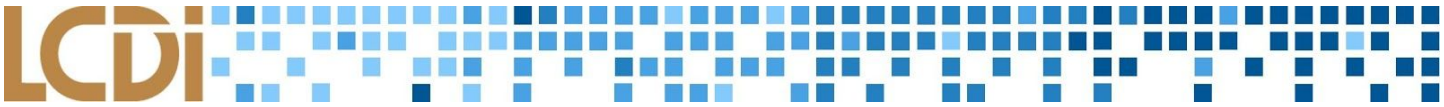
EnCase did a decent job at extracting artifacts from the image, but could not locate the .odt file with the keyword “sodium cyanide.” EnCase was able, however, to locate the same keyword in websites that were visited in Google Chrome. In our case, index searches did not return relevant results, but keyword searches did. This can be due to the fact that raw keyword searches will return data that is stored in a non contiguous manner. Index searches in EnCase will only return data that is stored continuously and will not find data if keywords from a file are stored across various physical locations.

Forensic Toolkit

FTK did a very good job at locating and extracting artifacts of many kinds from the image. The tool was able to find all of the files that were created during data gen, regardless of whether or not they were deleted, and organize them in an easy to understand manner.

SIFT

We were unable to extract relevant artifacts from the image with the default tools that came in SIFT. This may be due to SIFT being incapable of extracting the data from the image, or a lack of knowledge on our part. We had to install the Bulk_Extractor tool on the image to find artifacts relevant to the scenario. Even



though it was not able to examine the entire image, it still was able to extract artifacts that we missed with other tools available in SIFT, such as the Internet search history, email, and references to "sodium cyanide", which was missed in the keyword search we performed with Autopsy.

Magnet IEF

Magnet IEF did not sufficiently find all the artifacts from the image. Although searches can done within a couple of minutes, they were not as accurate as other tools. For example, when searching “sodium cyanide” our tool resulted in zero artifacts even though there were certainly artifacts containing the words sodium cyanide in them. It should be noted that there are slightly different results when searching the same keywords multiple times.

How fast were the Forensic tools able to do their search for terms?

EnCase

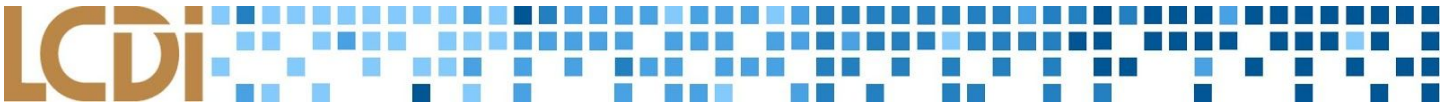
It took anywhere from 24 minutes to nearly an hour to complete raw keyword searches. The time varied based on what was being searched for and the options selected for the search. This was due to the fact that EnCase index searches will not find non contiguous data, but will find this data in a raw keyword search. This means that if a piece of data such as a word in a document is stored across different sectors on a hard drive, an index search will not find this data, whereas a raw keyword search will.

Forensic Toolkit

Depending on the type of search, and the search term, FTK’s search time varied. In the searches for “sodium cyanide” and “asdfghjkl”, FTK required thirty to forty minutes during a live search, and around one second for an index search. During the search for “e” the index search required around forty minutes, and the live search was unable to be completed due to the VM crashing before the search was finished. Due to this, the length of the search had to be estimated and the amount of hits and files found used. FTK was extremely consistent with its searches returning the same amount of hits and files each time a search for a term was ran.

SIFT

Times did not vary much between index and live searches in Autopsy. The search for “e” took 14 minutes 43 seconds and produced a large number of results. The searches for “asdfghjkl” and “sodium cyanide” each took about a minute and did not produce any results. These searches are fast, but may indicate that the tool is not finding certain files. After further research into SIFT and its other tools, we were able to use



Bulk_Extractor to extract information to a .txt file. This file contained URL searches from data-gen and we counted over 20 hits for “sodium cyanide”. This led us to believe Autopsy was not able to properly search through the image.

Magnet IEF

Magnet IEF took 4 minutes and 27 seconds to search the processing results for “e” which had 199,876 hits with 64,480 files. Searching “asdfghjkl” took 1 minute and 58 seconds to get 2 files and 2 hits. Finally, the search for “sodium cyanide” took 2 minutes with no results. While the searches are fast compared to other tools, they go less in-depth.

How easily was each tool able to find and recover deleted files?

EnCase

Deleted files could be recovered through a fairly simple process. While setting up a keyword search, there was an option to “Undelete Entries Before Searching”. When used, however, EnCase could not find “sodium cyanide” in our deleted .odt document.

Forensic Toolkit

Deleted files in FTK were relatively simple to recover. When on the explore tab, the deleted file can be found in the recycle bin file located in the root folder. From there,navigate through the folders to find the desired file.Simply right click on the file, and select the export option.

SIFT

SIFT includes Scalpel in its toolkit, which is a tool that recovers files based on known headers and footers for various file types. When searching for a file not found by Scalpel normally, the user can add it to its configuration file which allows it to be searched for. In practice, however, this did not seem to work, as even after adding headers and footers for .odt files, Scalpel did not find any of the files created in data generation.

Magnet IEF

Magnet IEF did recover some deleted files, but they were not presented in an easily readable form, making it impractical for real-world application. Although we do believe this is because of the file type since .odt is not commonly used, we cannot give solid evidence that it is not a side effect of recovering deleted files.

How easy would each tool be in the hands of an individual with limited digital forensic experience?

EnCase

EnCase seems daunting at first for someone with little to no experience. The user interface is confusing to navigate and the tools are not explained in the software itself. However, there are plenty of ways to get familiar with it. There are many free guides online that explain the basics of indexing, imaging, and acquisition. To make things even simpler, pathways can be used as a guide in Version 8 for individual local jobs or a full investigation. If all else fails, there are online forensics courses that focus on EnCase, though they have to be paid for. Overall, it takes a lot of getting used to, but can be a very useful tool once the user understands the vast array of options with EnCase.

Forensic Toolkit

FTK is an extremely intuitive tool to use. Every task and operation that the user might run is clearly marked with clear and easily understood labels. All symbols used in FTK are equally simple and easily understood. For example, deleted files are marked with a red "X" over the file thumbnail. Locating a specific file in the system is simple, as files are displayed in a tree hierarchy format which would be familiar to anyone but those with the most minimal computer usage experience. For first time users though, this overlay may seem daunting and easily overwhelming. Although everything is written clearly, it is still difficult to fully understand the steps needed in order to achieve a goal. It will take, as with any other tool, a little bit of manual reading to get a general grasp and use it for intended purposes.

SIFT

SIFT Workstation is very hard to use with limited Digital Forensics experience. There is little to no documentation on the tools included in SIFT. When you do find documentation, it generally assumes you have some experience already and does not explain why or how things work. Because all the tools run on command-line, the user has to know what they are doing, the commands needed for input are, and what their output means. After extensive research, one can start to have a simple understanding of SIFT. However, prior experience or training is vital for gaining a more in-depth, usable understanding of how to use SIFT and the various tools included in it.

Magnet IEF

The great thing about Magnet IEF is that it is very easy for anyone to use, including those with limited Digital Forensics experience. The program makes things very straightforward for the user and performs a lot of basic steps.. From the moment it is opened, there is a very simple display with clear words pointing in the right direction. If things are still confusing, Magnet has a website that explains all the features provided in the program. They also have a YouTube channel that provides many tutorials for beginners as well as more advanced users. Magnet IEF is also able to export the search results to HTML files to have an interactive interface while not having it in the tool. Its ability to export search results and important evidence to an easily readable file makes it easier for people without a license for the tool to view evidence extracted from it. Overall, Magnet IEF is a user-friendly application that is approachable for any user.

Results

Processing Capabilities and Speed

After our teams compared results for all of our tools, we came to the conclusion that EnCase has the fastest processing speed. This was concluded by comparing how many files the tool was able to scan per second of time searching contrary to other tools. In this section, we were not looking for its capability to find all of the deleted files, simply how fast it could go through the files.

SIFT was determined to be the slowest when compared to other tools. This is because multiple tools need to run in order to fully process an image. This means that files need to be scanned multiple times by different tools, drastically reducing the speed of processing in SIFT.

Magnet IEF seems to have quick speeds while still having decent results. While it is not as in depth as EnCase, it does have a faster processing time. This makes it ideal for more time sensitive evidence or the user with no time to spare.

FTK is very slow at searching for keywords but has very accurate results. If time is not an issue than FTK will be one of the best tools to get accurate results. Indexing is very fast in FTK. Taking less than one second with many word searches.

Ability to Correctly Obtain Relevant Artifacts

To determine which tool could find relevant artifacts best, we used its ability to recover the predetermined deleted files which we had marked before analysis. These items consisted of downloaded images

and Microsoft office documents. FTK was able to find all of the deleted files and the process in which this was done was very simple and self-explanatory. We did have to sort through many junk files to find the one we were looking for but it was found.

EnCase could not find the deleted OpenOffice document, but it did find evidence of web history that included the keyword "sodium cyanide." This was more difficult to find, as text needed to be analyzed in a specific view within EnCase to be readable. Magnet IEF very well could have recovered some deleted files but if it did then they were buried under other results and not made clearly available. SIFT was able to see the deleted files in the results from Bulk_Extractor but was not able to recover them through the use of other tools like Scalpel. This could have been due to the extremely large number of files extracted by Scalpel.

Search Capabilities

The tools all had relatively similar searching capabilities. Some did have more advanced features that made them more useful for certain jobs. For example, EnCase contained options for index and raw keyword searches, allowing for a greater amount of control in searches across the image. Raw keyword searches in EnCase tended to find more hits due to the ability to search through both contiguous and noncontiguous data.

FTK was able to search live and index search. We would receive information on how many hits we got within a search but the specifics of where those hits came from were not exactly present. Magnet IEF had an easy search but it came up with limited results and sometimes had different results for the same search. SIFT had limited search functionality and was more based on using the Ubuntu grep command on the results from other tools.

Scope of Use

In terms of the tools scope of use, we wanted to determine the possibilities that one could use the tool and compare it with the other tools. Magnet IEF was determined a better application for general use by an inexperienced or surface-level investigator. The program guides the user through the investigation process using clear instructions and easily identifiable interface icons. There is also very little technical knowledge needed, as many of the operations are done automatically once the user selects them.

Other tools, such as EnCase and SIFT, are better-placed in the hands of experienced investigators with more extensive knowledge of digital forensic tools. EnCase has an easy-to-use graphical user interface, but has extensive options that can easily be confusing to somebody without prior knowledge of the tool. FTK was a tool

that a user with no experience could use but also has the option of going extremely in depth for forensic research. Since its interface is easy to use, it makes its ability to be used for multi-purpose projects easier. SIFT has the ability to go extremely in depth but requires extensive knowledge of the Linux command line interface and digital forensics concepts to do so. With all of that said, we concluded that Magnet IEF was the best all-around tool when paired against the other tools.

Ease of Use

We began analyzing how user friendly each tool was by listing and drawing comparisons between all of the tools. Then we conducted a poll to finalize our results. The teams came to a conclusion that SIFT was by far the most difficult tool to use, especially for beginners in the forensic field. The team also identified Magnet IEF as the simplest of the tools and the most user friendly. We came to these conclusions for SIFT because it was almost like tackling a new language. It used almost solely the command line for running tools which made it very difficult to use. Additionally, the fact that each tool that could be run then had to be learned increased the difficulty. Since we examined this as beginners, we did not have the benefit of any prior experience and had to learn specific digital forensics concepts before even being able to use the tools in SIFT. In contrast, Magnet IEF has a very simple interface allowing almost anyone to use it with ease. It was purposely designed for law enforcement so an officer with minimal technical experience would still be able to get artifacts from a hard drive. The program uses basic language and images to help guide you.

In the middle of these two tools, EnCase had an easy-to-use graphical user interface, but lacked documentation on the vast array of options that are available for the user. EnCase was an overwhelming tool for a beginner to use without prior knowledge, but pathways introduced in Version 8 greatly assisted in completing the investigation process. FTK was a relatively easy tool to use for all tabs and windows are written clearly and concisely,although the steps in order to achieve a task aren't as clear and will need some research and manual reading.

Average Ease of Use

Tool	Keyword Search	User Interface	Timeline	Indexing/Processing
EnCase	5	1	3	6.5
Magnet	9	8	9	7
FTK	9	8	4.5	7.5

SIFT	1	1	1	1

Scale: 1-10, with 1 being the most difficult and 10 being the least difficult

Conclusion

According to the data, it is apparent that EnCase is the most feature-rich tool on average for keyword searches and processing. For the searches for “e” and “asdfghjkl”, the number of results far exceeded the other tools, though the length of times were longer than most. However, EnCase fell behind FTK in the search for deleted files. While most other tools’ processing speeds take hours, the EnCase processing with and without indexing is only a matter of minutes. IEF is perfect for the inexperienced investigator. Its streamlined interface and clearly labelled buttons make operating the tool effortless. SIFT is the most inexpensive to operate since it is based on open source tools. However, SIFT also requires the most training to use effectively.

Appendix

Data Gen Sheet

Time	User Action	Machine Actions	Comments
05 / 10 / 17			
8:04 AM	Powers on PC	PC Powers on, begins boot	
8:07 AM	Logs on		
8:07 AM	Opens Microsoft Edge	Launches Microsoft Edge	
8:07 AM	Opens new tab		
8:08 AM	In one tab search google chrome	Searches and displays results	
8:08 AM	In the other tab search Open office	Searches and displays results	
8:08 AM	Clicks on first link under google chrome, Download, Accept & install		
8:09 AM	Accepts all pop ups	Accepts all pop ups	
8:09 AM	Google Chrome opens		

Tool Evaluation:

8:10 AM	Clicks “set as default app” after open Chrome		
8:11 AM	Clicks the first link under Open office search		
8:11 AM	Clicks on “I want to download Apache Open office”		
8:11 AM	Clicks download Full Installation	Machine downloads apache_OpenOffice installer	
8:12 AM	Clicks run at bottom of the screen	Installs OpenOffice	
8:13 AM	Searches “Firefox”	Searches and displays results	
8:13 AM	Clicks “Free download”	Downloads Firefox installer	
8:13 AM	Clicks downloadable file and follows prompts		
8:14 AM	Closes all web browsers		
8:14 AM	Logs off PC		
8:18 AM	Powers down PC	PC Powers off	

Tool Evaluation:

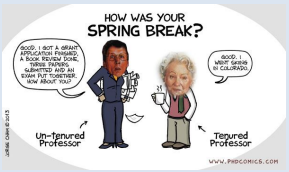
1:06 PM	Powers on PC	PC powers on, begins to boot	PC is updating
1:30 PM	Logs in		
1:32 PM	Opens Google Chrome		
1:33 PM	Searches “difference between Google Chrome and Mozilla Firefox”	Searches and displays results	
1:33 PM	Clicks on “Firefox vs Google Chrome - difference and comparison”		http://www.diffen.com/difference/Firefox_vs_Google_Chrome
1:33 PM	Searches “Which is the safest browser”	Searches and displays results	
1:34 PM	Clicks on “What is the safest web browser? Chrome, Firefox, IE, Opera, and Safari comparison chart”		https://tiptopsecurity.com/safest-web-browser-chrome-firefox-ie-opera-safari-comparison-chart/
1:34 PM	Searches “what are cookies on a website”	Searches and displays results	
1:34 PM	Searches “Are cookies bad on a website”	Searches and displays results	
1:34 PM	Opens incognito tab		

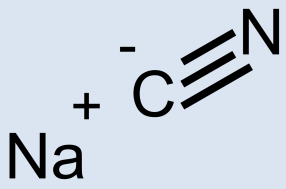
Tool Evaluation:

1:35 PM	Searches “world’s best golf courses”	Searches and displays result	
1:35 PM	Clicks on “Ranking: World’s 100 Greatest Golf Courses - Golf Digest”		https://www.golfdigest.com/story/worlds-100-greatest-golf-courses-2016-ranking
1:35 PM	Searches “Air fare to Scotland”	Searches and displays results	
1:35 PM	Clicks on “Flights to Scotland - Boston to Scotland - icelandair.us”		http://www.icelandair.us/destinations/?gclid=EAIaIQobChMIrqeYmo7V1gIVG57ACh0D_Q7AEAAYBCAAEgInIvD_BwE
1:37 PM	Closes incognito tab		
1:37 PM	Searches “2016 chemistry Nobel prize”	Searches and displays results	
1:37 PM	Clicks on “The Nobel Prize in Chemistry 2016”		https://www.nobelprize.org/nobel_prizes/chemistry/laureates/2016/
1:38 PM	Opens “The Nobel Prize in Chemistry 2016” PDF		https://www.nobelprize.org/nobel_prizes/chemistry/laureates/2016/press.pdf
1:40 PM	Saves PDF to Desktop		
1:40 PM	Searches “who is the best classical composer”	Searches and displays results	

1:40 PM	Clicks on “Top 15 Greatest Composers of All Time”		http://listverse.com/2009/12/17/top-15-greatest-composers-of-all-time/
1:45 PM	Opens new tab		
1:45 PM	Searches “The Best of Johann Sebastian Bach video”	Searches and displays results	
1:45 PM	Clicks on “The Best of Bach - YouTube”		https://www.youtube.com/watch?v=vwp9JkaESdg
1:52 PM	Searches “The Best of Wolfgang Amadeus Mozart video”	Searches and displays results	
1:52 PM	Clicks on “The Best of Mozart”		https://www.youtube.com/watch?v=Rb0UmrCXxVA
1:57 PM	Searches “The Best of Ludwig Van Beethoven video”	Searches and displays results	
1:57 PM	Clicks on “Ludwig Van Beethoven -The Best of”		https://www.youtube.com/watch?v=ZjjXGdQwRac
2:02 PM	Closes Google Chrome		
2:02 PM	Logs off PC		
2:03 PM	Powers down PC	PC Powers off	

06 / 10 / 17			
8:04 AM	Powers on PC		
8:06 AM	Logs on to PC		
8:06 AM	Opens Google Chrome		
8:07 AM	Searches “Walter White”	Searches and displays results	
8:08 AM	Clicks on eighth image		https://www.google.com/search?q=walter+white&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi5pJ2rqbfWAhUk34MKHe2RCSwQ_AUICigB&biw=987&bih=954#imgrc=kq5ppwbZLgjS2M: 
8:08 AM	Saves image to desktop	Saves image to desktop	
8:09 AM	Sets image as desktop background		
8:21 AM	Searches “mail.google.com”		

8:25 AM	Logs into email and reads email from Prof. White		"Dear Professor Plum, You'll never guess what just happened to me today. I got tenure!!!!! I never thought I would get tenure before you. Guess that makes me the better teacher.  Your friend, White"
8:25 AM	Reads emails from students and clicks "Saver to Drive" on documents		Two emails containing mock homework
8:26 AM	Opens new tab		
8:26 AM	Searches "youtube.com"		
8:26 AM	Searches "sodium cyanide" on YouTube	Searches and displays results	
8:27 AM	Clicks on "Synthesis of Sodium Cyanide"		https://www.youtube.com/watch?v=xz7i11XC9wk
8:29 AM	Comments "Thanks for the info!"		
8:29 AM	Opens new tab		
8:29 AM	Searches "drive.google.com"		

8:30 AM	Views homework on Google Drive		
8:30 AM	Open new tab		
8:31 AM	Searches “sodium cyanide”	Searches and displays results	
8:31 AM	Clicks on “SODIUM CYANIDE - Centers for Disease Control and Prevention”		https://www.cdc.gov/niosh/ershdb/emergencyresponsecard_29750036.html
8:39 AM	Returns to search results		
8:40 AM	Clicks on an image		https://upload.wikimedia.org/wikipedia/commons/thumb/8/83/Sodium_cyanide.svg/1200px-Sodium_cyanide.svg.png 
8:40 AM	Saves image	Saves image to hard drive	
8:41 AM	Searches “sodium cyanide ingredients”	Searches and displays results	
8:42 AM	Clicks on “toxicological profile for cyanide”		https://www.atsdr.cdc.gov/toxprofiles/tp8-c4.pdf
8:42 AM	Opens OpenOffice	Launches OpenOffice	

8:53 AM	Writes a recipe for sodium cyanide in a new file	Saves file on hard drive	File named “instructions.odt”
8:53 AM	Closes OpenOffice		
8:53 AM	Closes Google Chrome		
8:54 AM	Logs off PC		
8:54 AM	Powers off PC	PC Powers off	
9:55 AM	Powers on PC	PC Powers on	
9:56 AM	Logs on PC		
9:56 AM	Opens Mozilla Firefox		
9:57 AM	Searches “mail.google.com”		
9:59 AM	Logs in to email		
10:02 AM	Replies to Professor White’s email		To Professor White: “Congratulations on getting tenure. I still remember your first day here you were so lost. I’m so happy for you we should celebrate! Would you like to come to my house for a celebratory dinner at 6pm?”
10:02 AM	Opens new tab		

10:02 AM	Searches “Golf Course”	Searches and displays results	
10:03 AM	Clicks on an image		https://www.poipubaygolf.com/wp-content/uploads/2017/02/Kauai-Oceanfront-Golf-Course.jpg 
10:04 AM	Saves image		
10:04 AM	Searches “golf balls”	Searches and displays results	
10:05 AM	Clicks on ‘Golf Balls for Sale | Dick’s Sporting Goods”		https://www.dickssportinggoods.com/products/golf-balls.jsp
10:05 AM	Clicks on first result		https://www.dickssportinggoods.com/p/top-flite-xl-7000-super-straight-golf-balls-16tflmtf2016xl700gbl/16tflmtf2016xl700gbl
10:06 AM	Closes tab		
10:07 AM	Searches “nat king cole”		
10:07 AM	Clicks on videos		https://www.google.com/search?q=nat+king+cole&source=lnms&tbm=vid&sa=X&ved=0ahUKEwjqy6mLpfjWAhVq4YMKHYO-DuMQ_AUICigB&biw=958&bih=969

10:08 AM	Clicks on “Nat King Cole, Unforgettable”		https://www.youtube.com/watch?v=Fy_JRGjc1To
10:09 AM	Opens new tab		
10:09 AM	Searches “drive.google.com”		
10:09 AM	Corrects saved homework		
10:19 AM	Clicks on email tab		
10:19 AM	Reads email from Professor White		From Prof. White: “I would love to come over for dinner. It’s not everyday someone gets tenure. You should know.”
10:19 AM	Clicks on homework tab		
10:20 AM	Continues correcting homework on email		
10:24 AM	Closes Mozilla Firefox		
10:25 AM	Logs off PC		
10:25 AM	Powers off PC		
12 / 10 /17			
8:04 AM	Powers on PC	PC powers on	
8:04 AM	Logs on to PC		

Tool Evaluation:

8:04 AM	Opens Google Chrome		
8:04 AM	Searches “homedepot.com”		http://www.homedepot.com
8:05 AM	Searches “Charcoal” on Home Depot		
8:05 AM	Searches “Lye” on Home Depot		
8:06 AM	Searches “Chlorine Stabilizer” on Home Depot		
8:07 AM	Opens new tab		
8:07 AM	Searches “the three degrees of murder”	Searches and displays results	
8:07 AM	Clicks on “Three Degrees of Murder / Useful Notes - TV Tropes”		http://tvtropes.org/pmwiki/pmwiki.php/UsefulNotes/ThreeDegreesOfMurder?from=Main.ThreeDegreesOfMurder
8:10 AM	Opens new tab		
8:10 AM	Searches “sentencing for first degree murder in VT”	Searches and displays results	
8:10 AM	Clicks on vermont.gov link		

Tool Evaluation:

8:12 AM	Opens new tab		
8:12 AM	Searches “YouTube”		
8:12 AM	Clicks on “YouTube”		https://www.youtube.com
8:12 AM	Searches “Easy Mac and Cheese Recipe” on YouTube		
8:13 AM	Clicks on “SUPER EASY MAC N’CHEESE!!! 4Minute Recipe!!”		https://www.youtube.com/watch?v=PvfS1wiR4QM
8:14 AM	Creates new OpenOffice file		
8:17 AM	Writes new file with recipe for mac and cheese	Saves file to the desktop	Mac and Cheese Recipe.odt
8:18 AM	Closes OpenOffice		
8:18 AM	Closes Chrome		
8:18 AM	Logs off PC		
8:19 AM	Powers off PC	PC Powers off	
10:01 AM	Powers on PC	PC Powers on	

Tool Evaluation:

10:01 AM	Logs on to PC		
10:02 AM	Opens Google Chrome		
10:02 AM	Searches “food allergies”	Searches and displays results	
10:03 AM	Opens “Food Allergies | Causes, symptoms & Treatment | ACAAI Public Website” in new tab		http://acaai.org/allergies/types/food-allergy
10:04 AM	Clicks on “Milk” on ACAAI		http://acaai.org/allergies/types-allergies/food-allergy/types-food-allergy/milk-dairy-allergy
10:07 AM	Closes tab		
10:07 AM	Opens new tab		
10:08 AM	Searches “Jazz documentary”	Searches and displays results	
10:08 AM	Clicks on videos		https://www.google.com/search?q=jazz+documentary&source=lnms&tbm=vid&sa=X&ved=0ahUKEwiJr7y1sPjWAhUW24MKHSK4AP4Q_AUICigB&biw=958&bih=969
10:08 AM	Clicks on “1959 The Year that Changed Jazz - YouTube”		https://www.youtube.com/watch?v=dou3aSZmEg0

Tool Evaluation:

10:09 AM	Bookmarks page		
10:09 AM	Searches “how to play beethoven 5th symphony on piano”	Searches and displays results	
10:10 AM	Clicks on “Beethoven Symphony 5 - Piano Tutorial EASY SLOW - 5th Symphony - No. 5 How To Play (Synthesia)		https://www.youtube.com/watch?v=OTHHimZrCF4
10:13 AM	Refreshes page		To replay video
10:17 AM	Closes Google Chrome		
10:17 AM	Logs off PC		
10:18 AM	Powers off PC	PC Powers off	
1:02 PM	Powers on PC	PC Powers on	
1:03 PM	Logs on to PC		
1:04 PM	Opens Chrome		
1:04 PM	Searches “How long does it take to master	Searches and displays results	

	Beethoven 5th Symphony”		
1:04 PM	Closes tab		
1:05 PM	Opens Google Chrome		
1:05 PM	Searches “When did Beethoven die”	Searches and displays results	
1:05 PM	Searches “Was Beethoven deaf”	Searches and displays results	
1:06 PM	Clicks on “Beethoven’s deafness - Ludwig Van Beethoven Website”		http://www.lvbeethoven.com/Bio/Biography Deafness.html
1:14 PM	Returns to results		
1:14 PM	Searches “Who was better Beethoven or Mozart”	Searches and displays results	
1:14 PM	Searches “How old was Mozart when he died”	Searches and displays results	
1:15 PM	Clicks on “Cause of Mozart’s death revealed - 128 years late - Houston Chronicle”		http://www.chron.com/news/bizarre/article/Cause-of-Mozart-s-death-revealed-218-years-1735278.php
1:18 PM	Returns to results		

1:18 PM	Searches “Why did mozart die so young”	Searches and displays results	
1:18 PM	Closes tab		
1:18 PM	Closes Google Chrome		
1:18 PM	Logs Off PC		
1:19 PM	Powers off PC	PC Powers off	
1:28 PM	Powers on PC	PC Powers on	
1:28 PM	Logs on to PC		
1:28 PM	Opens Google Chrome		
1:29 PM	Searches “CNN”	Searches and displays results	
1:29 PM	Clicks on “CNN”		
1:29 PM	Reads daily news headlines		
1:30 PM	Opens new tab		
1:30 PM	Clicks on bookmarked “1959 The Year that Changed Jazz - YouTube”		

2:00 PM	Closes Google Chrome		
2:00 PM	Moves instructions.odt to recycling bin	Changes file location	
2:00 PM	Moves Mac and Cheese Recipe.odt to recycling bin	Changes file location	
2:01 PM	Empties recycling bin	Deletes files from recycling bin	
2:01 PM	Opens Google Chrome		
2:01 PM	Searches “Molview.com”	Searches and displays results	
2:01 PM	Searches “ptable.com”	Searches and displays results	
2:06 PM	Searches “Chemistry Professor Website”	Searches and displays results	
2:06 PM	Clicks on “Chemistry Professor”		www.chemistryprofessor.com
2:12 PM	Searches "Chemistry practice websites"	Searches and displays results	
2:12 PM	Clicks on the first link		http://www.sciencegeek.net/Chemistry/taters/directory.shtml
2:14 PM	Opens Openoffice	Launches open office	

Tool Evaluation:

2:14 PM	Writes file containing links followed by a brief description of each link	Saves file on hard drive	to be saved as student Link.odt
2:17 PM	Closes Open Office		
2:18 PM	Searches "Interesting things in chemistry"	Searches and displays results	
2:19 PM	Clicks on the first link and reads through article		https://www.thoughtco.com/fun-and-interesting-chemistry-facts-604321
2:19 PM	Searches "Chemistry breakthroughs"	Searches and displays results	
2:20 PM	Clicks link		https://phys.org/chemistry-news/
2:24 PM	Clicks first link under "Chemistry News"		https://phys.org/news/2017-09-hybrid-indiumlithium-anodes-fast-interfacial.html
2:24 PM	Returns to previous page		
2:24 PM	Clicks second link under "Chemistry News"		https://phys.org/news/2017-09-precisely-polymer-chains-reality.html
2:26 PM	Returns to previous page		
2:27 PM	Clicks third link under "Chemistry News"		https://phys.org/news/2017-09-self-healing-catalysts-easier-solar-energy.html
2:29 PM	Searches "How to handle stress"	Searches and displays results	
2:29 PM	Clicks on the first link		https://www.helpguide.org/articles/stress/stress-management.htm
2:31 PM	Searches "How to handle regret"	Searches and displays results	

Tool Evaluation:

2:31 PM	Clicks on the first link		http://www.huffingtonpost.com/christine-hassler/dealing-with-regret_b_2265065.html
2:25 PM	Searches "Periodic Table Song Video"	Searches and displays results	
2:35 PM	Click first link		https://www.youtube.com/watch?v=VgVQKCcfwnU
2:38 PM	Deletes picture of chemical structure		
2:38 PM	Closes Chrome		
2:41 PM	Logs off PC		
2:41 PM	Powers off PC	PC powers down	
2:41 PM	Time Passes		
2:41 PM	Powers on PC	PC turns on, begins boot	
3:31 PM	Logs on PC		
3:31 PM	Opens chrome		
3:31 PM	Searches "police reports Burlington Vermont"		
3:32 PM	Searches "woman found dead burlington in last 24 hrs"		
3:32 PM	Closes tab		
3:32 PM	Opens new tab		

Tool Evaluation:

3:32 PM	Searches "How long do autopsies take police"		
3:32 PM	Closes tab		
3:32 PM	Closes chrome		
3:32 PM	Opens Google chrome		
3:33 PM	Searches "Gmail"		
3:33 PM	Clicks on first link		
3:33 PM	Opens email from "(someone)"		
3:34 PM	Opens new tab		
3:34 PM	Closes (other) tab		
3:34 PM	Searches "Things you should have on your bucket list"		
3:34 PM	Clicks on first link		https://daringtolivefully.com/bucket-list-ideas
3:34 PM	Clicks back button		
3:38 PM	Searches "trip to Machu Picchu cost"		
3:39 PM	Clicks on link		https://www.whereverwriter.com/trip-machu-picchu-part-2-breakdown-costs-schedule/
3:39 PM	Clicks back button		

Tool Evaluation:

3:40 PM	Searches "How much do people travel"		
3:40 PM	Clicks on link		https://www.techopedia.com/definition/4805/virtual-machine-vm
3:41 PM	Searches "What to do if this was your last day"		
3:41 PM	Clicks on link		https://www.quora.com/If-today-were-the-last-day-of-your-life-would-you-want-to-do-what-you-are-about-to-do-today
3:42 PM	Clicks on back button		
3:44 PM	Search "How many murders go unsolved"		
3:44 PM	Clicks on first result		http://www.npr.org/2015/03/30/395069137/open-cases-why-one-third-of-murders-in-america-go-unresolved
3:44 PM	Search "burlington vermont news"		
3:51 PM	Closes Chrome		
3:51 PM	Logs off PC		
3:52 PM	Shutdown PC	PC powers down	
	Time Passes		
4:51 PM	Powers on PC	PC turns on, begins boot	
4:52 PM	Logs on PC		

Tool Evaluation:

4:52 PM	Opens Google Chrome		
4:52 PM	Goes to gmail.com	Brings directly to site	Plum goes through his emails for a while
4:53 PM	Opens new tab		
4:54 PM	Goes to pandora.com	Plays classical station	
4:55 PM	Goes back to gmail tab		
4:55 PM	Goes to Martha Stewart's website		http://www.marthastewart.com/
4:55 PM	Clicks WHAT'S FOR DINNER TONIGHT		
4:59 PM	Clicks on link below the first item		
5:00 PM	Opens Openoffice		
5:10 PM	Copies the recipe into Open Office		saves on desktop as dinner.odt
5:10 PM	Closes Open Office		
5:10 PM	Clicks on Google Chrome		
5:11 PM	Searches "Why did Martha Stewart go to jail?"		
5:11 PM	Clicks on second link		http://biography.yourdictionary.com/articles/why-did-martha-stewart-go-to-jail.html
5:16 PM	Clicks the back button		
5:16 PM	Clicks on the next link	the wiki page	https://en.wikipedia.org/wiki/Martha_Stewart

Tool Evaluation:

5:17 PM	Clears history on Google Chrome		
5:17 PM	Closes Google Chrome		
5:17 PM	Moves studentLink.odt to recycling bin		
5:17 PM	Clear the recycling bin		
5:18 PM	Logs off PC		
5:18 PM	Shutdown PC	PC powers down	

Tool Evaluation:

References

Refs need to be APA 7 in alphabetical order by author's last name. On a page by itself.

Encase Forensic Version 8.01.01 Release Notes [PDF]. (2016, July 7). Guidance Software

Hirwani, M., Pan, Y., Stackpole, B., & Johnson, D. (2012). *Forensic Acquisition and Analysis of VMware Virtual Hard Disks* [PDF]. Rochester, NY: Rochester Institute of Technology

Miller, P. (2010, January 7). *How and Why to Partition Your Hard Drive.* Retrieved November 09, 2017, from https://www.pcworld.com/article/185941/how_and_why_to_partition_your_hard_drive.html

Most Trusted Endpoint Detection & Response Solution. (2017). Retrieved November 02, 2017, from https://www.guidancesoftware.com/

What's New in EnCase Forensic Version 7.06 [PDF]. (2013). Guidance Software

Write Blockers. (n.d.). Retrieved November 09, 2017, from http://www.forensicswiki.org/wiki/Write_Blockers