Evaluating Tools and Technologies used in Digital Forensics

Raymond Bernard Milián
Master of Engineering in Computer Engineering
Dr. Alfredo Cruz Triana
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— The use of the Internet and digital gadgets in our daily lives has increased significantly in recent years. This explosive growth has impacted society in both a positive and negative manner. With the advancements of technology, cybercrimes, hackings, and exploiting have also increased rapidly. Therefore, the proper use of digital forensics tools is very important to investigate cybercrimes and recover data. The scope of digital forensics is not limited to personal computers and networks; smartphones, gaming consoles and smart gadgets are also vulnerable and included in the scope of digital forensics. This paper focuses on the latest forensic investigation trends and the use of five popular forensic tools. At the end a comparison is made based on the results of the experiments done.*

Key Terms *— Computer Forensics Tools, Cybercrime, Exploiting, Hacking.*

INTRODUCTION

The Internet is considered as one of the greatest developments in the world today. It has been able to enhance productivity in nearly all areas of humanity, increasing the efficiency and effectiveness of our daily work. One of the most amazing foundations of the Internet mainly rests on its decentralized nature. Though this can be considered one of the reasons behind its success, this accessibility also brings about threats due to the Internet's openness and availability. This leads to cybercrimes [1]. Cyber-crime is defined as the act of stealing or trading intellectual property or trade secrets via the Internet.

Both online and offline companies are built on trade secrets and intellectual property. This means that once this information is accessed by the wrong individual, it will negatively affect the company; eventually leading to a disadvantage that produces losses [1]. Apart from the theft of trade secrets, cyber criminals find it attractive to get involved in financial fraud such as stealing credit card information. Another type of cyber-crime is trading obscene sexual content over the Internet [1]. This is what is referred to as cyber obscenity. In most cases these criminals tend to hide the illegal pornographic materials on external drives. These are some of the main types of cyber threats available in the world today.

The only way that criminals are able to perform these crimes is by taking advantage of loop holes or vulnerabilities of the devices that have access to the Internet [2]. Once they obtain this access, they are able to view, edit or copy this information to an external drive or another computer. The most challenging part about cybercrimes is the fact that hackers or intruders can try to access data or information from almost any part of the world. This means that once the crime is done, it might be hard to find and prosecute any suspects.

Computer Forensic Specialists (CFS) are responsible in the investigation of cyber-crimes. They analyze and document all digital sources involved and provide a detailed report [2].

According to Nelson, B. Phillips, Digital Forensics (DF) is the science of obtaining, examining, digging up and interpreting any evidences from digital sources [3]. The digital sources may include: PC's, smartphones, smart devices and gaming consoles, among others. Digital forensics is not only limited to criminal or corporate cases of cybercrime, but also used for penetration testing, data recovery and several other aspects where data is compromised or vulnerable [3].

In this paper an initial discussion is made on cyber security and the importance of digital forensics. Then the paper discusses the digital forensic procedure, steps, and digital forensics tools.

Some selected forensic tools are evaluated (Wireshark, EnCase Forensic, Digital Forensic Framework, Metasploit and FTK). All these tools have a different functionality (e.g. packet analyzing, data recovery etc.). The different functionalities of these tools is evaluated. The paper discusses the findings of the work done and at the end a conclusion is drawn for future studies.

CYBER SECURITY AND THE IMPORTANCE OF DIGITAL FORENSICS

Cyber security has become one of the most important aspects of high profile companies, especially in the area of IT and the management of financial transactions. Digital forensics deals with the recovery and examination of data and information found in different devices. Its major use lies in the investigation of cybercrimes. It has become a necessity for organizations to monitor their networks and digital/intellectual assets to fight any malicious attack on their systems. To make sure that security remains top notch, digital forensics takes a noticeable share in the organizational budgets [1].

There is a difference between digital forensics and what is known as incident response. Incident response is a way to deal with security breaches or assaults and the efforts made to contain the effect of the attack [2]. The main objective is to handle it in a way that harm is reduced to the minimum. For example, when a system is targeted with a virus or a dangerous malware, the incident response team decides how far the damage has spread and contains the issue by disengaging every influenced framework and device to forestall further harm [3]. The major difference between them is based on the following points:

In an incident response case, the cause of the harmful attack is usually found. It is usually provoked when a file or e-mail already infected is open, or even a Web page or downloaded application. There's no need of further examination of the event, and the problem can be dealt with the help of capable security professionals to avoid future vulnerabilities [3].

But in the case where the cause of the attack is unknown or the extent of damage is unknown, further investigation is required. At this stage a digital forensics team is needed to deal with the problem. The members of a digital forensic team must not only understand the technical part of the procedure but also the legal aspect of the issue. They should have the knowledge to work inside the legal framework to guarantee that the information they obtain is lawfully acquired and can be used in a court of law.

DIGITAL FORENSICS PROCEDURES

According to the National Institute of Standards and Technology (NIST) the following four steps must be followed in a digital forensics investigation [4]:

- Data collection
- Examination
- Analysis
- Reporting

Data Collection: The data collection stage is an important part in digital forensics. This stage basically encompasses 3 steps [5]:

- Planning
- Data acquisition
- Authentication of data

The digital forensic procedure must start with the appropriate planning. In the planning stage the strategies to be followed are documented. Then the digital forensics team accumulates electronic evidence and related materials as the basis of a system investigation. This evidence could reside in numerous parts of a network infrastructure. Data collection is required for small incidents (a solitary desktop), or larger incidents in an organizational network.

Only well trained digital forensics professionals have what it takes to obtain huge volumes of information in a short period of time. In the last stage the acquired data is verified and/or authenticated using DF tools to make it available for legal purposes

[5]. The data which is directly linked to the incident is retrieved in this stage.

Examination: Manual extraction is almost impossible at this stage due to the large amount of data to be examined. It would be cumbersome and costs both time and money. DF tools provide the following methods for the efficient extraction of data:

- Keyword search for text and patterns
- Data filtration of different data types

Keywords and relevant patterns are searched throughout the digital evidence. The searched data is then filtered.

Analysis: In the analysis stage conclusions are drawn from the data extractions. Cross drive analysis is also done, which is basically the acquirement of data from different sources or devices and finding their mutual relation.

Reporting: Analysis leads to the final stage of the DF process, which is combining all the findings in the form of a well-structured report for the respective authorities; documenting the incident in detail with the conclusions and/or possible solutions [5].

DIGITAL FORENSIC TOOLS

The Internet has made it possible to reach any person in the world in a matter of seconds. However, it also can be used for unethical purposes. For example, cyber bullying, cyber-crime, hacking and data theft.

This motivated the authors to compare the use of digital forensic tools. In this paper the emphasis is given to the process of investigating digital media. DF tools help to analyze the data which is transferred over nodes and networks. In some cases, it analyzes the information transfer from one node to another which is very important when investigating unauthorized data transfer.

For example, in cyber-crimes, it is very important for the government agencies or security agents to trace the point which was used for initiating the activity. This process can be cumbersome as thousands of nodes could be involved when transferring data from source to destination. To achieve this purpose, various types of forensic tools are available which have features for tracing the information being transferred.

The first step in the methodology of forensic investigation involves the protection of the specific computer/system from any kind of alteration or corruption of data. This is achieved by completely isolating the computer system from the computer user which is typically the first suspect. The success of the investigation mainly depends on the ability to analyze and access the content of the files.

The core task of a Computer Forensic Specialist (CFS) in an investigation involves the discovery of files or procedures that might link the suspect to the crime. Digital forensic tools provide the combination of various technologies; which can be helpful when investigating the interaction of digital media which generally occurs in the form of data transfer over the Internet.

The other advancement in forensic tools includes mobile device forensics which helps to analyze mobile devices such as smartphones running on IOS, Android, among other operating systems.

Wireshark

Wireshark has been in the industry for more than a decade and has proven itself to be one of the best packet capturing and network monitoring tools as compared to other industry leading DF tools. It can be used for various types of attacks like de-authentication attack, Trojan attack, data theft cases, and many more. In the de-authentication attack, all the attached nodes are automatically disconnected from the network. With Wireshark we can also detect a Trojan in any of our computer systems available on the network. We can also get the delivery IP address using Wireshark [6].

Dumpcap is one of the executables provided in the command line utility. It is single threaded and captures packets and dumps them to the disk without processing. On the initiation of the capture session in Wireshark GUI, it launches the Dumpcap instance in the console for capturing the packets. Dumpcap also

informs the Wireshark GUI about the file to which it is writing packets.

When we are capturing packets with Wireshark, it turns the computer's network adapter to promiscuous mode, which can be enabled in the Wireshark "Capture" options. An experiment on Wireshark packet capture was initiated to check the packet capturing capability of Wireshark. Two host machines were used: Host A (Kali Linux OS) and Host B (Windows XP). Please see Figure 1.

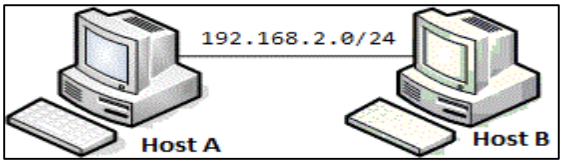

Figure 1
Capturing Packets using Wireshark on Host A

In this experiment the IP address and physical address of Host A are *192.168.2.129* and 00:0c:29:a4:0e:33, respectively. Also the Host B's IP address and physical addresses are *192.168.2.132* and *00:0C:29:3A: BD: 37.* Both machines are on the 192.168.2.0/24 network.

Host A has Wireshark and all operations are done on it, including the ICMP (Internet Control Message Protocol) request from one host to another. The screenshot in Figure 2 was taken when an ICMP request was made to the Wireshark host machine.

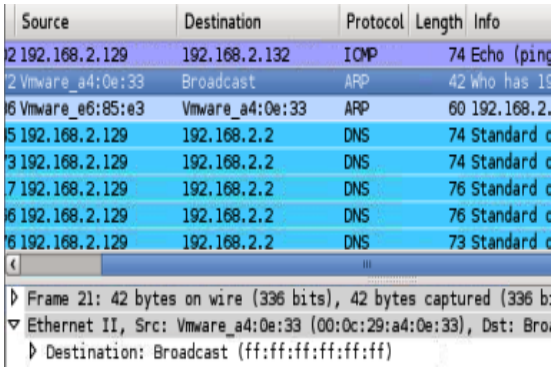

Figure 2
Captured Packet using Wireshark

We can also filter the data, such as the ARP (Address Resolution Protocol) packets: Select the "Filters Dialog" or "Filter Textbox" in the Menu Bar. ARP is a network layer protocol which is used for converting an IP address to a physical address. To capture ARP packets, it is required to clear the arp cache executing the command "arp –d". Packets can be captured by clicking the 'Start Capturing' button in the toolbar. Executing the command "ping *192.168.2.129"*. Figure 2 shows the ARP request packet. The Packet contains the IP address and physical address of the sender which is host A and the IP address of the receiver which is host B. As the physical address of host B is not known to host A, the request is broadcasted over the LAN and all hosts present on the LAN will receive the request. The second line is the ARP reply; every host on the LAN receives and processes the request packets of ARP, but only host B sends the ARP reply back.

The reply packet has the physical address and IP address of host B. This packet is directly unicasted to host A using the physical address which is received by the request packet. The hardware size of 6 indicates that the physical address length to account for is 6 bytes.

The mac address of the target is *00:00:00:00:00:00* which has '0' in all fields as the physical address of the target is unknown. The IP address of the target is *192.168.2.132*. The format, transmission process, content, and format of the ARP can be analyzed with the captured data, which is more effective when compared to the traditional teaching of the working principle of ARP [7]. An IP graph was also generated from the statistics menu of Wireshark. When the screenshot in Figure 3 was taken the ICMP was still transferring packets between the 2 hosts.

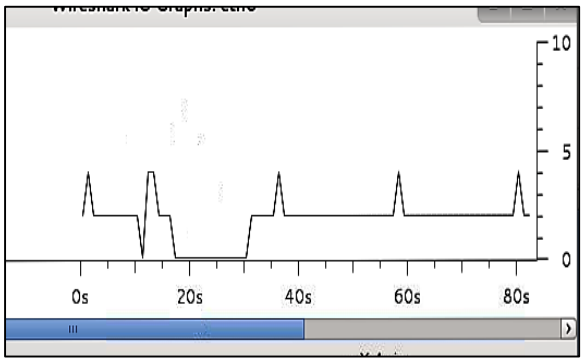

Figure 3
IO Graph Function

The graph plots the two end points of traffic. The figure shows the transfer of packets over the course of 60s time. The vertical axis shows the number of packets transferred. We can also see the number of packets transferred at any given instance of time. Forensic investigations can find the Transition Communication Protocol (TCP) flow between any compromised server and client server.

If the investigator finds a Trojan, that computer is instantly removed from the network. After that the same packet capturing technique is used to trace the IP address.

Forensic Toolkit

Forensic Toolkit (FTK) provides a range of tools for analysis, where the most important feature is FTK imager. The FTK Imager is an imaging tool which allows users to preview data as well as access the evidence on a machine. This tool allows to make a forensic image of data, duplicating anything present on the machine so that nothing can be modified from the original data. It can be used separately or along with the other FTK's. It can help recover deleted information by creating the image of a partition and then analyzing it for evidence.

The test performed for FTK proves how we can recover deleted data in an image file. We can obtain data available on RAM and the files protected by the operating system. RAM contains volatile data, such as memory contents, and has important evidence that must be analyzed [8]. Though the collection in the memory, one can extract information such as running processes, documents in use, websites accessed, username and password, and more. We can also detect the files with EFS (Encrypting File System) encryption. The contents of the image can be previewed and duplicated data can be reviewed for determining if any additional analysis is required, which can be done using the FTK [9].

Figure 4 is a screenshot that shows the Hex value of wshext.dll.mui file of this experiment. The arrow shows the hex value field. These hex values are actually the data within the file showed in hex form. On the right side we can see the values which refer to the file header. The file header contains the information about file type, its size, the starting & ending addresses for the data part. In cases when the file type is unrecognized and the header doesn't contain the information about file size and the data part, we can navigate to the particular hex values to regenerate the file from these values.

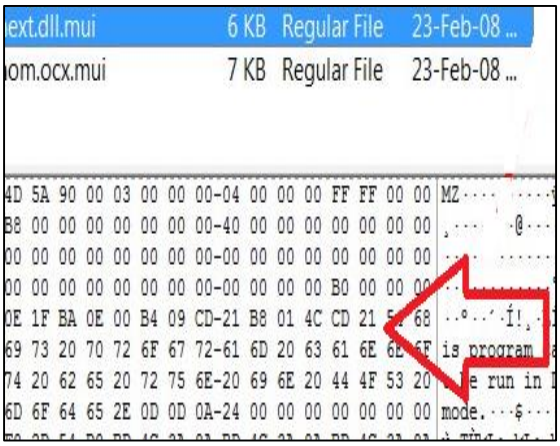

Figure 4
Finding the HEX Values of the Evidence Files

To analyze the evidence from the FTK imager menu (in "Add Evidence") a sample evidence image file was added [10]. One dll (wshext.dll.mui) file was analyzed from the example VMDK file.

Creating a forensic image using FTK imager can be performed in a step-by-step process. It can also be used for viewing the image file created using other tools. It can write or read image files in dd Raw, SMART, FTK or EnCase image formats. This implies that if the forensic image is created by another person of another organization, then the image file can still be viewed and also used for determining if it contains any evidence [10].
This can be very useful in scenarios where an internal investigation is being done. A forensic image from a suspect computer is created and police can view the acquired evidence [10].

In addition to the various formats of an image file which can be used for analyzing the disks, many types of file formats can be created and read for DVD or CD forensics. The software can also create these images: CloneCd, ISOBuster CUE, PlexTools, Virtual Cd, Alcohol and many others. FTK imager provides the user a friendly interface. The evidence file directory structure can be viewed from the upper

left-hand pane. Viewing the files stored in a folder is easy by selecting it from the upper-right pane [11].

The file list is used to select the designated file and then it can be analyzed in the viewer pane. The creation date can be seen using the 80 offset marker, which points to the creation time of a file. Similarly, alteration time can also be checked [12]. We can also use the 80 offset marker to locate information. The file can also be recovered from the value by checking if the information we are looking at was deleted or not.

In Figure 5, we can see in hex format the data section '$DATA' of file starts from code value, 0 x 80 00 00 00 which can be used to recover the file as it tells us where it starts in the address of the file.

To recover the file, we need to see the size, and this can be analyzed from the header of that particular file, which can reveal the information in hex and it is then converted to decimal to find the exact size. This exact size can then be used to set the selection length for recovery.

Please see Figure 5 below:

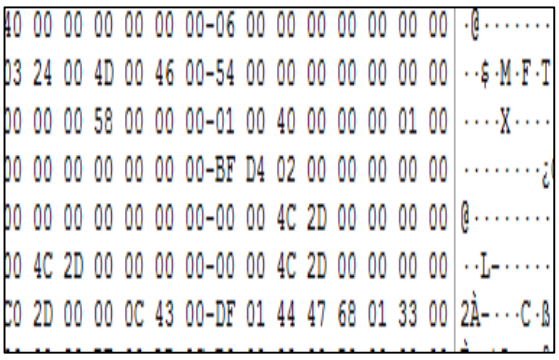

Figure 5
Working with HEX in FTK Imager

From the figure above we can see that there are hex values shown for files, therefore we can set the selection length after setting the exact size in bytes, which refers to the data part of the file. The selected length can then be saved in data form to get the actual file by using the 'Save Selection' option and appending the file format to the end of the name. The starting and ending address can be navigated through the search option in imager IDE, while we also have to calculate the actual file size before going to the save option that requires it.

Digital Forensic Framework

Digital Forensic Framework (DFF) GUIs are rapidly being developed by a large developer community. Applications such as 'pyFLAG' don't have many features included, but it has a simple GUI and it is very easy to build on as well as to install on Windows, Linux and/or OS X. It is very extensive, as it uses plugins and scripts, so that a skilled examiner can easily discover flaws. This distinct feature can be used to enhance the experience in DF. In case when files are not identifiable, another feature uses the files header to analyze the file information. This was the reason for selecting it for DF studies.

DFF's like PyFLAG software create a Virtual File System (VFS) where deleted files are also included. DFF application's core is used to handle VFS's node creation in memory. DFF refers to the nodes as unique items. Nodes are the small data structures that hold information about unique items that DFF identifies. The GUI layer helps analyze the data visually. The population of nodes with the data is taken care in modules. The VFS in DFF GUI has a tree like structure having nodes as children under the root (/) or as other nodes' children [13].

To test an investigative scenario an evidence file was added in the DFF from the 'Add Evidence' menu. Figure 5 shows the hex value of a test file: file.docx which was obtained while exploring the evidence file. After the experiment it was observed that the DFF is capable of identifying the Hex values. Also the DFF tool is capable of finding the EXIF (Exposure, Shutter speed, ISO and Focal length) data for image files. Moreover, it segments the evidence in different modules from the module's option [14].

A module does the discrete tasks and population of nodes with the task's output. Various tasks can be performed by the current version of DFF (0.8 when developing the paper) which includes processing the dumps of cell phone memory, comparison of hash, viewing images, movies, and the generation of statistics about nodes and set of nodes, which refers to a tree/hierarchy of related files.

All the analysis tasks are performed by modules in DFF and the exposed API (Application Programming Interface) provides various functionalities. Additional modules can be written using Python or C++. Also, the scripts can be generated on the fly by the built-in scripting engine of Python.

DFF also provides access to remote and local devices like remote file system, removable devices, and disk drives. It can read the standard digital forensic file formats i.e. Encase EWF, AFF 3 or raw file formats [14]. It can also analyze Skype, web browser history, connected USB devices and recent documents, executed binaries and event logs.

Event logs are very important when analyzing a computer system. If a computer system is hacked with some physical attack like OS password cracking, then the DF Specialist can find out how the attack was perpetrated by observing the logs.

DFF provides the preservation of digital chain of custody which is the calculation of a cryptographic hash and a blocker, that doesn't allow unauthorized people to access it. But with the help of DFF we can also bypass this security measure to gather evidence for multimedia analysis, Windows OS analysis and memory analysis [14]. A perfect registry analysis can be done using DFF.

In Figure 6 below we simply access the hex values of a file to identify its type and size, even if it was corrupt, and its file type becomes unrecognizable. It is a good option for recovering the files which were hidden by changing their file type, or corrupted to hide the evidence.

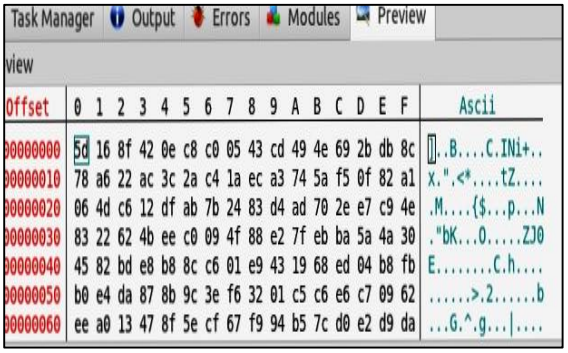

Figure 6
DFF Investigation

DFF also supports the reconstruction of Virtual Machine Disk (VMDK) and is compatible with VMware [8]. It provides the Linux and Windows OS forensic like registry, NTFS, Mailboxes, FAT 12/16/32 and EXTFS 2/3/4 file system formats. It also provides a quick search for Meta data like dictionaries, time-lines, tags, content search and regular expressions. It also helps in recovering the hidden or deleted artifacts including files, folders, carvings and unallocated spaces. It provides volatile memory forensics for local files, network connections, binary extraction and processes [15].

Metasploit

Metasploit is generally categorized as an anti-forensic tools but it also provides the information related to vulnerabilities which might potentially harm the system or which can result in the theft of data. It provides help when analyzing the threats which might be used to access system information.

As an open-source project under the framework of Metasploit, this multi-platform tool is developed by Rapid7 and can be used for accomplishing different tasks [16]. As an anti-forensic and evasion tool it is mainly used for the purpose of penetration testing and finding the exploits in a system. It works similar to performing the analysis using the other forensic tools. It also provides robust testing features which are unique when compared to other tools.

Metasploit tests a system against possible vulnerabilities which can cause system failure. It contains many testing techniques which help to keep the system protected against new vulnerabilities. It can also be used in simulating real-world attacks for testing, finding the loopholes, and weak spots in the system. It also helps in prioritizing the task and vulnerabilities, helping to focus initially on the most significant incidents. It also helps in penetration testing using various scenarios, multiple hosts, platforms, and various versions of OS [17]. It is also used to identify the weakness in OS and software applications.

The aim is to demonstrate how penetration testing works. The screenshot below in Figure 7 was taken from a host machine with Kali Linux OS. It

had the IP address *192.168.2.129*. To do the arp_sweep and basic discovery first from the Kali Linux Machine (Host A), Metasploit console is accessed using the "msfconsole" command.

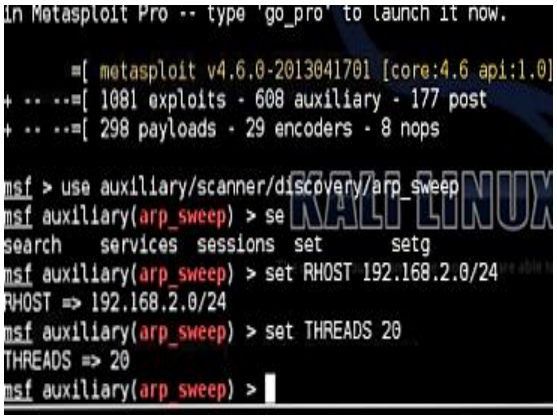

Figure 7
Metasploit ARP-Sweep

A "use auxiliary/scanner/discovery/arp_sweep" command is then used and the RHOST is set to *192.168.2.0/24*. Also the threads are set to 20. When the ARP Sweep is performed all the hosts from the network will respond to the request [18]. The Metasploit tool will receive the MAC addresses of the hosts. The following commands were used in Figure 7):

- use auxiliary*/scanner/discovery/arp_sweep*
- *Set RHOSTS 192.168.2.0/24*.
- *set THREADS 20*

EnCase

Encase is written in C++. It offers an integrated set of forensic utilities. Encase comes with several products designed for forensic, cyber security, security analytics and e-discovery. One can do file signature analysis, hash analysis and file finder with which one can search files in unallocated space. Its wide use has made it a de-facto standard in forensics. Previously, more than 15 tools were required to provide the same functionality. Using EnCase, investigators can start the inspection by placing the suspected hard drive in their forensic computer. This drive can have a Windows, Linux, DOS or Macintosh OS. EnCase makes a bit-stream mirror image of the drive and is mounted as read-only evidence. This prevents investigators from any kind of alteration of the data that could invalidate it as evidence [19].

To verify that the data in the mirror-image is the same as the original, EnCase calculates the checksum of cyclical redundancy as well as MD5 hashes. The evidence Image's MD5 hashes, and hex values were obtained from this experiment [19]. The evidence hex value was obtained after adding the evidence from the sample file. The file structure of the drive is reconstructed by EnCase using the logical data in the mirror image. The examination of the drive is then done by using Windows GUI by the investigators. Please see Figure 8.

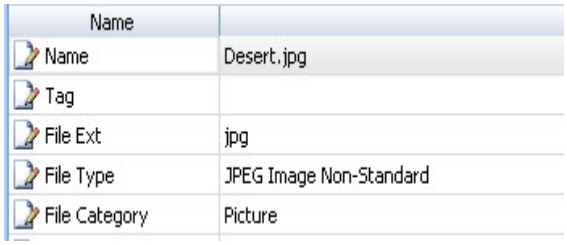

Figure 8
Investigating Evidence using EnCase

The figure above shows the lower portion of the Encase Forensic v7 interface. This dialog shows the related information about the selected file in the upper right panel. The file attribute information about name, file size, file type, file ext., category and other variables can be seen here.

EnCase goes beneath the OS while examining the drive, viewing all kinds of data which includes file size on disk, windows swap files, and unallocated space, in which all potential evidences or deleted files can be stored.

EnCase can also sort the files displayed based on some criteria like a time stamp or extension. In addition, EnCase can also compare the file signature with the file extension which can help in determining if the user has tried to hide evidence from detection by changing the extension of the file.

Guidance also offers EnScript macro language, which allows advanced users to build on the EnCase tool, providing customized functionality.

COMPARISONS AND RECOMMENDATIONS OF THE STUDY

Some of the most important findings when comparing the functions of these tools is given below:

- Capturing packets –The Wireshark tool was the only tool able to capture packets. It managed to identify the packet source IP address. Moreover, it was also able to identify the type of request.
- Finding of files- DFF, EnCase and FTK were able to discover all the files in the evidence image. This includes the deleted files that are still present as well as all the encrypted files. This allows the data forensic analyst to fully assess the computer.
- Recovery- No tools were used to recover deleted files. But DFF, EnCase and FTK are capable of recovering deleted files for more complex evidence. Metasploit is also able to recover files but in this experiment recovery of files was not tried.
- Hidden and temporary files- All hidden and temporary files were able to be read by DFF, EnCase and FTK.
- Access of hidden files- All the hidden and protected files are accessed and acquired by DFF, EnCase and FTK.
- Reporting- Other than Wireshark all the 4 tools were able to generate reports.

Table 1 is based on the above observations.

Table 1
Comparison of the DF Tools with their Functions

	Wireshark	EnCase Forensic v7	DFF	Metasploit	Forensic Toolkit
Image reader	X	X			X
Image creation		X			X
Browsing history analysis		X	X		
File Recovery	X	X	X	X	X
Email Support	X	X	X	X	
Boolean searches	X	X			X
Hex searches	X		X		X
MD5 hash support	X	X	X	X	X
RAM analysis		X	X		X
Automated report generation		X	X	X	X
Evidence creation	X	X	X	X	X
Penetration testing				X	
Total number of features offered by each tool	**7**	**10**	**8**	**6**	**9**

One of the most successful areas of the tools was imaging. The tools that supported image functionality were functioning flawlessly [19].

The quality of imaging was always tested by using some hashing functions that were supported within the tools properties.

To compare these tools, we considered the number of features, as compared in Table 1.

Figure 9 shows the number of features each tool provides in a bar chart.

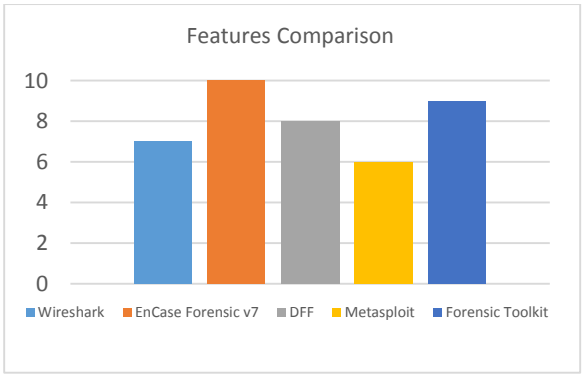

Figure 9
Features Comparison of the DF Tools

CONCLUSION

To explore each tool a lab scenario was created and the end result was analyzed. The testing helped to understand the capability of each tool although it is difficult to compare forensic tools with a few experiments. Real life forensic investigations are highly dependent on tools and procedures that are used depending on the devices comprised, and the threats or incidences that have occurred.

After experimenting with these tools it is observed that Wireshark is suitable for packet sniffing and analyzing the captured packet, or monitoring the network for suspicious activities. It is

best for this scenario because the toolset it offers is outstanding for analyzing the traffic over networks.

On the other hand, Encase can be used to create and read images. It has the capability to generate reports. Also the timeline menu helps to keep things organized. Like Encase, DFF is also a good evidence analysis tool. But it has some limitations and lacks many functions other programs have. Metasploit is different than the other tools. In the experiment ARP_Sweep exploitation was done and found that Metasploit is capable of penetration testing. It is the only tool with this capability in this study. FTK is highly suitable for complex analysis, which can slow the file-based system (i.e. in systems where there is no indexing), while it stands out in performance when working with complex systems. From the experiment it is observed that it can create evidence images and can also read evidence.

Digital Forensics tools are an important part of the digital evidence gathering process. The most complete forensic tool proved to be EnCase Forensic v7, offering a larger set of features [5].

Future studies will be centered in analyzing the functions of each tool on more complex scenarios with encrypted files and complex networks, comparing the efficiency of every feature in each tool.

REFERENCES

[1] K. Arthur and H. Venter, "An Investigation into Computer Forensic Tools. Information and Computer Security Architectures (ICSA) Research Group", 2004.

[2] J. Reinke and H. Saiedian, "The availability of source code in relation to timely response to security vulnerabilities", *Computers & Security*, vol. 22, no. 8, pp. 707-724, 2003.

[3] B. Nelson, A. Phillips and C. Steuart, *Guide to computer forensics and investigations*. Boston, MA: Course Technology Cengage Learning, 2010.

[4] K. Kent, S. Chevalier, T. Grance and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response", *NIST Special Publication 800-86*, 2006.

[5] M. Zareen, A. Waqar and B. Aslam, "Digital forensics: Latest challenges and response", *2013 2nd National Conference on Information Assurance (NCIA)*, 2013.

[6] A. Dabir and A. Matrawy, "Bottleneck Analysis of Traffic Monitoring using Wireshark", *2007 Innovations in Information Technologies (IIT)*, 2007.

[7] S. Wang, D. Xu and S. Yan, "Analysis and application of Wireshark in TCP/IP protocol teaching", *2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*, 2010.

[8] "AD eDiscovery | Industry Leading Legal Software", *AccessData*, 2016. [Online]. Available: http://accessdata.com/solutions/digitalforensics/forensic-toolkit-ftk. [Accessed: 1- Feb- 2016].

[9] "Forensic ToolKit product review | SC Magazine", *Scmagazine.com*, 2016. [Online]. Available: http://www.scmagazine.com/forensic-toolkit/review/574/. [Accessed: 3 - Jan- 2016].

[10] H. Duc, "How to investigate files with FTK imager", *eForensics*, 2016. [Online]. Available: https://eforensicsmag.com/how-to-investigate-files-with-ftk-imager/. [Accessed: 12 - Dic- 2015].

[11] "Bsmuir.kinja.com", *Bsmuir.kinja.com*, 2016. [Online]. Available: http://bsmuir.kinja.com/encase-imager-vs-ftk-imager-1677906594. [Accessed: 12 - Dic- 2015].

[12] "acid-burninfo(in update status): Advantages and Disadvantages of FTK and EnCase", *Acid-burninfo.blogspot.com*, 2011. [Online]. Available: http://acid-burninfo.blogspot.com/2011/04/sadvantages-and-disadvantages-of-ftk.html. [Accessed: 14 - Dic- 2015].

[13] "Information Security Short Takes: Digital Forensics Framework - A Perspective Forensics Tool", *Shortinfosec.net*, 2016. [Online]. Available: http://www.shortinfosec.net/2009/11/digital-forensics-framework-perspective.html. [Accessed: 02- Feb- 2016].

[14] "ToolWar | Information Security (InfoSec) Tools | Network Security, Web Security, Mobile Security", *Toolwar.com*, 2016. [Online]. Available: http://www.toolwar.com/2014/06/dff-digital-forensics-framework.html. [Accessed: 02- Feb- 2016].

[15] S. Brueckner, D. Guaspari, F. Adelstein and J. Weeks, "Automated computer forensics training in a virtualized environment", *Digital Investigation*, vol. 5, pp. S105-S111, 2008.

[16] "Penetration Testing Software, Top Rated | Rapid7", *Rapid7*, 2016. [Online]. Available: https://www.rapid7.com/products/metasploit/. [Accessed: 04- Jan- 2016].

[17] "Metasploit for Penetration Testing: Beginner Class", *Slideshare.net*, 2016. [Online]. Available: http://www.slideshare.net//georgiaweidman/metasploit-for-penetration-testing-beginner-class. [Accessed: 09-Jan-2016].

[18] "Attack Analysis - Metasploit Unleashed", *Offensive-security.com*, 2016. [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/karmetasploit-attack-analysis/. [Accessed: 09- Jan- 2016].

[19] "Analyze-forensic-evidence", *www2.guidancesoftware.com*, 2016. [Online]. Available: https://www2.guidancesoftware.com/products/Pages/EnCase-Forensic/Analyze.aspx. [Accessed: 09- Jan- 2016].