Computer Forensics: Dark Net Forensic Framework and Tools Used for Digital Evidence Detection

May A. Alotaibi[1], Mohammed A. AlZain[1], Ben Soh[2], Mehedi Masud[1] and Jehad Al-Amri[1]

[1]College of Computers and Information Technology, Taif University, Saudi Arabia
[2]La Trobe University, Bundoora 3086, Australia

***Abstract*:** As the development of technology increases and its use becomes increasingly more widespread, hence computer crimes grow. Computer forensics research is becoming more crucial in developing good forensic frameworks and digital evidence detection tools to deter more cyber-attacks. In this paper, we explore the science of computer forensics, a dark web forensic framework, and digital evidence detection tools.

Keywords: Digital forensics, digital evidences, computer forensics.

1. Introduction

The world now is easy to get any information by a click on the button. High speed access to any valued information, high performance computers and networks are available almost everywhere.

This development serves the community but also has threats such as eavesdropping and illegal use of information [1-10]. A new term that protects the user has appeared which forensic science is. Forensic science has many branches and one of them is digital forensics. Digital forensics involves investigation and retrieval of items found in digital devices; oftentimes digital forensics is a relation to computer crime also called cyber forensics. Computer forensic includes stratifying techniques of computer investigation and analysis to fix criminality and supply evidence to support status. It is identifying, analyzing, presenting and preserving the digital evidence process. Cyber forensic tools are very easily used and play an important role to gather the evidence[11, 12, 38].

Cyber-crimes are in general classified into three categories, based on its impact on those affected. Cyber-crimes are hostile to persons, property, and the government. All categories of cyber-crimes impact us in many ways. Each category can use a different process and the process could be used differently from one criminal to another one. In cyber-crimes against persons: This form of cyber-crime can be in the form of cyberstalking deal or trade in something illegal, such as sharing pornography, trafficking, and grooming. Recently, law enforcement agencies deal with this category of cyber-crime very industriously and join forces around the world to reach the perpetrators and arrest them. In cyber-crimes against property: Just as in the actual world where a felon can rob and steal, a felon in the cyber domain resorts to theft and robbing. Currently, cyber felons can steal a person's information like bank details and the wrong use the credit card to make several purchases online. Although crimes against a government are not as common as the previous two categories, crimes against a government are still considered a crime. Crimes in this category occur when criminal hacks government sites. If the sites were hacked successfully, this would cause panic to the citizens[13]. Figure 1 shows the types of cybercrimes with some examples of each category.

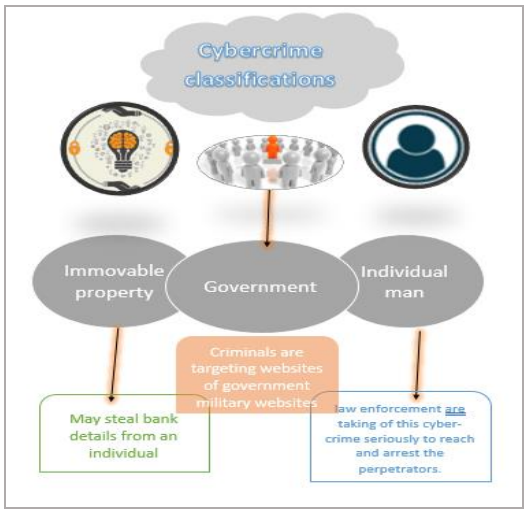

Figure 1. Cybercrime classifications [13]

This paper is organized as follows. Section 2 discusses basics terminology used in computer forensics and its classification.. Science 4 explains deep web forensics. Section 4contains implementation of example digital forensics tools. Section 7 concludes the paper.

2. Computer Forensics and the Procedure Used

We can recreate past events in forensic science using tools for court cases. Digital forensics (DF) is defined as using scientifically derived and actually proven methods to identify, transport, collect, analyze, store, present, distribute, revert back, destroy and/or interpret digital evidence from digital sources, in addition to preservation of evidence [14]. DF is generally divided into several classes. These include network forensics, computer forensics, and mobile forensics. Each of the above digital forensic classes helps figure out the authors of cyber-attacks, phishers, and fraudsters [15]. Details of the three classes of the forensics science are given below:

1- Computer forensics: It is the evaluation of the digital nedia via a scientific process for reconstructing real information for judicial review. That is collecting and analyzing data from different computer resources including computer networks, lines of communication,

computer systems and suitable test storage media [16-18].

2- Network forensics: A network of telecommunication enables computer data sharing. Most digital devices such as PCs, notepads, and terminators are connected through wired or wireless contact in the network. It aims to catch with evidence cybercriminals for their illegal actions, thus limiting online crime [19, 20].

3- Mobile forensics: Mobile Forensics (MF) is a type of digital forensics related to the restoration from a mobile device of evidence. It is also called mobile device testing involving interacting components like authority, people, resources, investigators team, procedures, and policy [20, 21] [22].

Investigators in computer forensics must follow proper procedure to obtain legal evidence. Accuracy is the main priority in computer forensics. Forensic practitioners must strictly follow policies and procedures and maintain high working ethics rules to ensure accuracy. Investigations in computer forensics follow rigid set of methods to make sure that computer evidence is obtained correctly. The following steps are listed [13]:

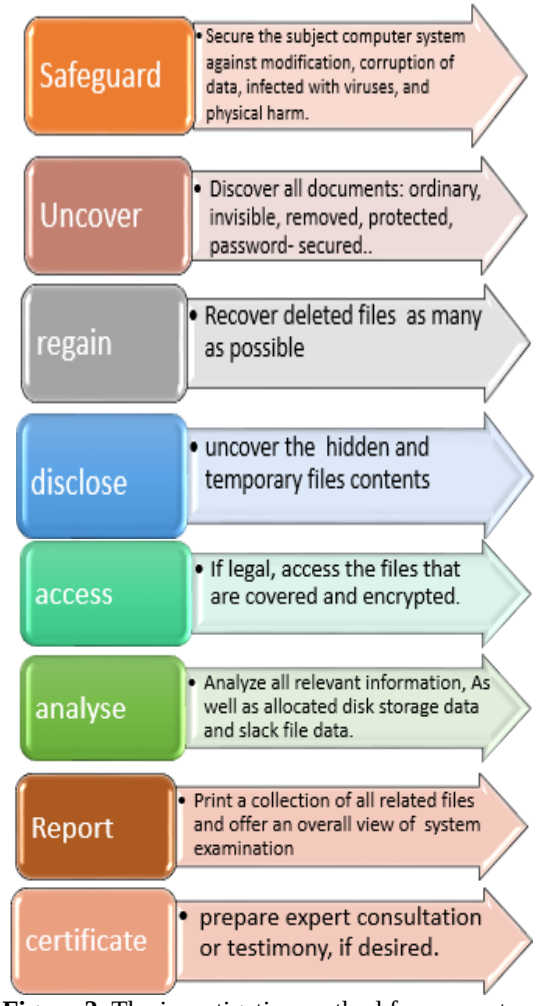

Figure 2. The investigative method for computer forensics[13]

3. Deep Web Forensics

In this section, we explore the types and characteristics of webs.

The Internet has two different webs: surface web and deep web shown in figure 3. The surface web is a regular web that is used by the public. It is containing web content and web pages that will be indexed by the famous search engine also called a clear web or visible web, such as Google. We can open it without additional, separate software [24].

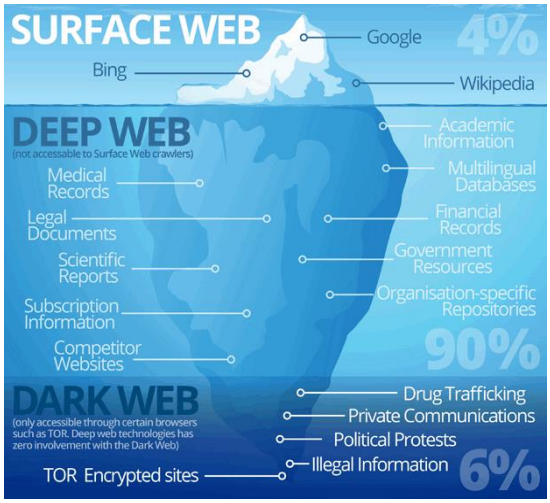

Figure 3. Types of webs[23]

On the other hand, there is another special web called deep web where it hides the address of the user. Deep web holds Darknet and so Darknet represents as a small part of the deep web. Darknet has been purposely hidden within the deep web. The crucial point is that deep web cannot be accessed using standard web browsers because the content of the deep web is not indexed by famous web browsers. People use these webs to do many illegal operations, such as selling and buying drugs, selling body parts, and downloading unauthorized software or files in their country. The Onion Router (TOR) browser is a virtual tunnel which is encrypted. It allows individuals to hide their identity and action, that is allowing them to use the Internet anonymously[25, 26]. In effect, users of these webs intentionally hide their identity, operations and locations[27].

The actual problem is that when malicious people use the deep web that hides their information, authorities can't know anything about their identities, locations, and transactions. Rathod has mentioned how people can use the deep web and the forensic science to detect them[24].

3.1 Mechanizations of Deep Web and Darknet

Some of mechanizations of deep web [24] are given below:

1- Virtual Private Network VPN with TOR: It prevents users' access to IP and increases privacy. Many users use VPN while using TOR to have more privacy[24, 28] [29].

2-Free Anonymous Internet (FAI): It is used in blockchain because it is a decentralized deep wed like a system using blockchain.

3- Free Net: Freenet is a network of peers to peers and designed to securely and privately spread information on the Internet. Like FAI it allows users to export files anonymously. It uses Darknet mode to pass an encrypted network packet including the IP header to a router node [30, 31].

4-ZeroNet: It is a new instituted torrent with Bitcoin encryption. This system until now is in the process of development and showing promise for the future[32].

3.2 Darknet Forensic Framework

The forensic methods recommended for Darknet forensics are divided into two categories: Bitcoin forensics and TOR forensics.

3.2.1 TOR forensic

Table 1. TOR forensics in the application of Darknet techniques [24].

Techniques	kits	Goal
RAM forensic evidence	1- Belkasoft RAM capturer is used to capture the RAM dump. 2- Hex dump is used to view hexadecimal view of RAM dump.	The purpose of RAM forensics is to obtain the description of the types of documents, visited websites as well as other downloaded content.
Registry forensics	Registry changes	Would be performed by Regshot to obtain evidence of TOR installation and last access date information.
Network forensics	Wireshark and miner network[33]	Would be performed by Wireshark and Miner network to gather evidence of web traffic information[34]
Database forensics	The TOR browser database is housed in \TorBrowser\Browser\TorBrowser\Data\Browser\Profile.default	Can be used to access the database content.

3.2.2 Bitcoin forensics

Table 2. Bicoin forensics in the application of Darknet techniques [24].

Techniques	kit	Goal
Bitcoin wallet	Internet Evidence Finder (IEF)	Would be performed by extracting forensic artifacts from the Bitcoin wallet application downloaded on the client device. Internet Evidence Finder allows Bitcoin artifacts to be recovered.

4. Implementation of Digital Forensics Tools

Data gathering and analysis from different resources of computer that include computer networks, computer systems, appropriate storage media for trial and communication lines is called computer forensics[16].

Some computer-related crimes are not recognized as evidence. The reason is that many computer-related crimes cannot be proven in real terms. The extent of study of computer forensics in different aspects depends on the level of complexity in the crime related to the computer field [35, 36, 37].

Digital evidence (DE) is categorized based on various types of documents. The tools used in computer forensics to detect digital evidence vary on several aspects, as follows.

4.1 Winhex software

Winhex is software that displays original signatures files. Suppose somebody take a IPEG files and modified it to JPG. The investigator can use Winhex to obtain original file and use it as evidence.

Let's show the steps on how to use Winhex. Consider we have a picture in JPEG signatures as shown in fig (4).

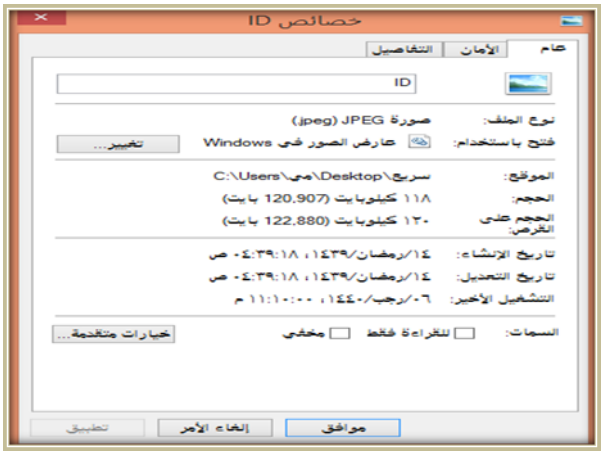

Figure 4. Properties of pic ID

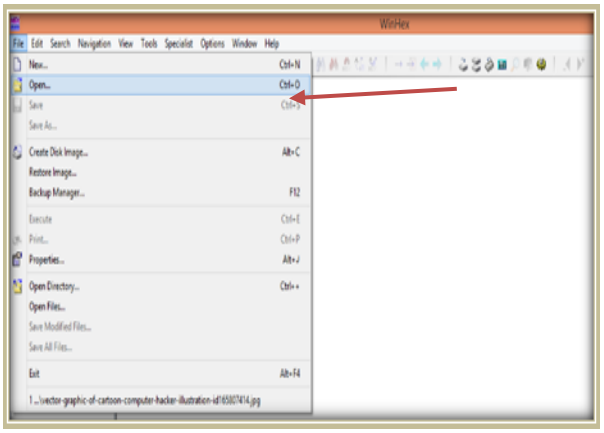

Figure 5. Open file in Winhex

After you open Winhex select file>open>select file. Then select pic ID and open it.

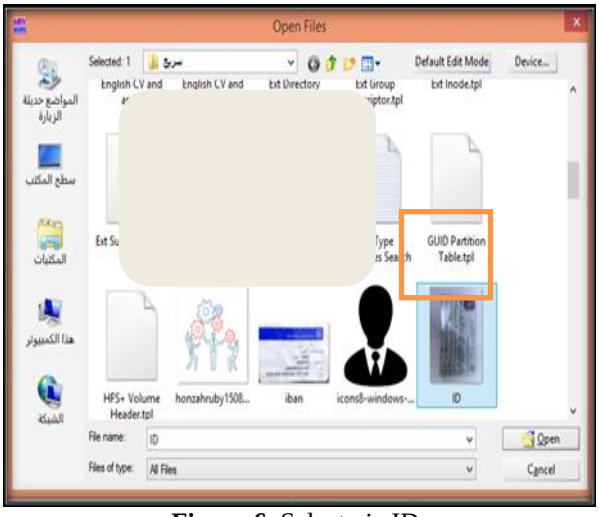

Figure 6. Select pic ID

The first line contains the type of file in hexadecimal as can be seen in fig (7) where hexadecimal is for JFIF.

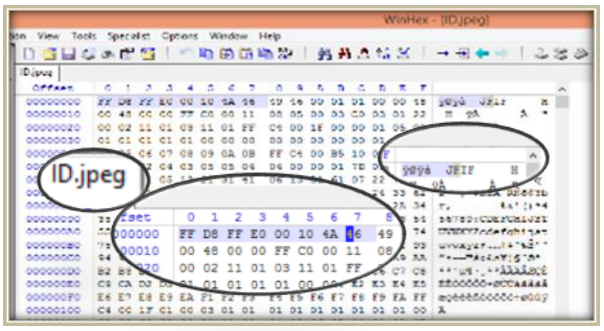

Figure 7. Hexadecimal is for JFIF elect pic ID

Now in fig (8) we change PIC ipeg to JPG to examine it in Winhex.

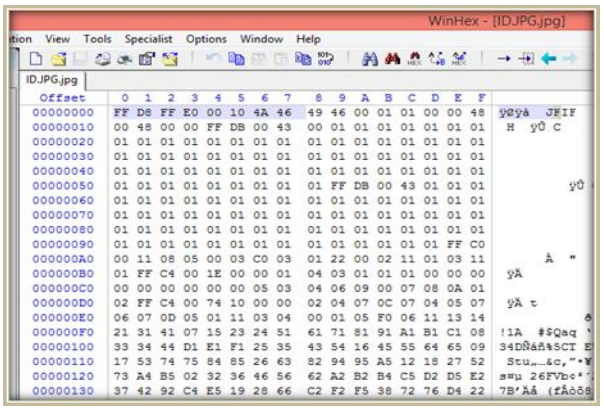

Figure 8. Hexadecimal after changing format

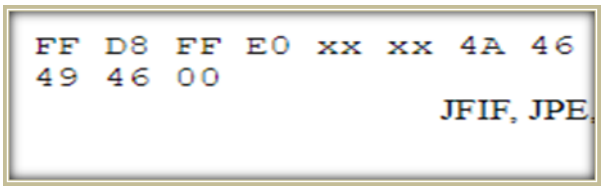

Figure 9. Value of JFIF in database

4.2 Last Activity View

Last Activity View is free software for Windows operating system. It collected information about activities carried out by system users from different resources on the operating system. It includes erroneous processes that occur in any program or operating system. It also exports data on various formats such as CSV, XML, and HTML. This tool is useful if we want to prove that a user has performed a particular operation on the operating system. It can also be used in the case of multiple users on the operating system through which the user who has performed the operation can be determined. The steps of using LastActivityView are as follows.

i. Open program

This is the first interface that appears in Last Activity View.

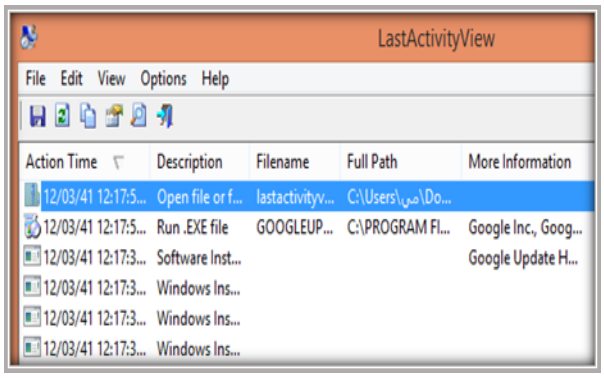

Figure 10. Last Activity View interface

ii. Elements of each activity

As can be seen in fig (11) each activity has time, description, file name, path, file extension, data source and other information.

Figure 11. Elements of Last Activity View.

iii. Save evidence

Evidence can be saved in different format. First select file that needs to be saved.
After that, Edit->copy selected items.

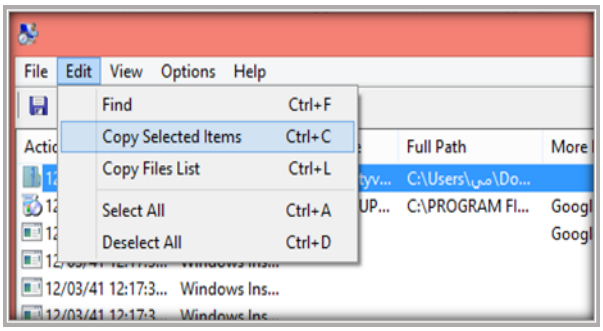

Figure 12. Step 1 to save evidence

Then, file->save selected items.

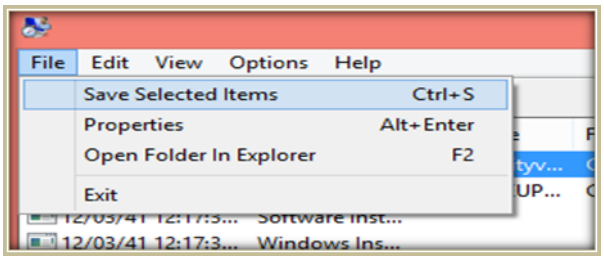

Figure 13. Step 2 to save evidence

Save file named with evidence in text file format.

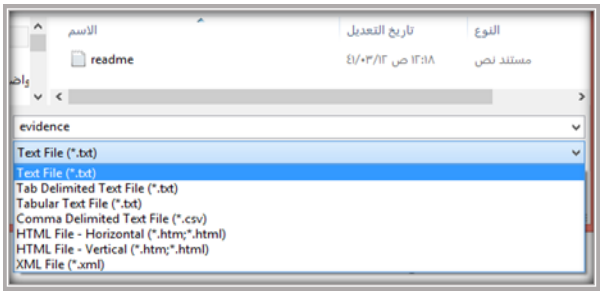

Figure 14. Save file in chosen format

Then, click the save button. Finally, open file.

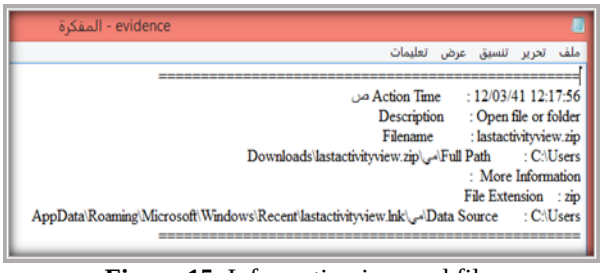

Figure 15. Information in saved file

4.3 History Viewer

History viewer is used to display the pages of images, videos, and/or files visited in different search engines.
Fig (16) shows the interface when history viewer is opened.

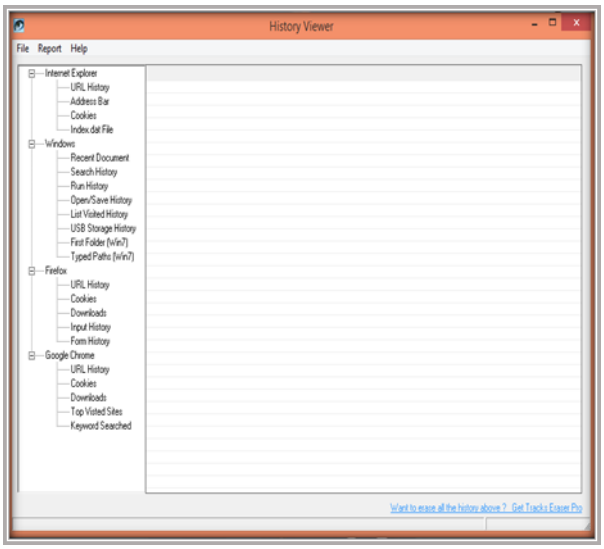

Figure 16. First interface in history viewer

Fig (17) displays different browsers, such as Internet Explorer, Firefox, and Google Chrome, and Windows.

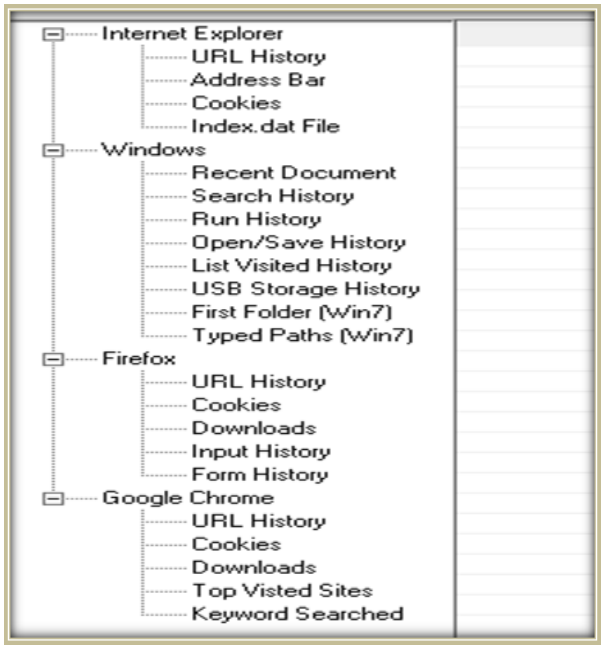

Figure 17. Element of history viewer

Fig (18) shows the response of clicking on URL history in the Internet.

Figure 18. URL history

Address bar is shown in fig (19).

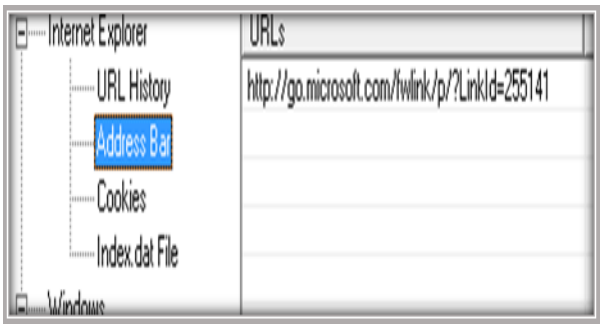

Figure 19. Address bar

Results of cookies are displayed in fig (20).

Figure 20. Cookies

Fig (21) shows a recently selected and displayed document.

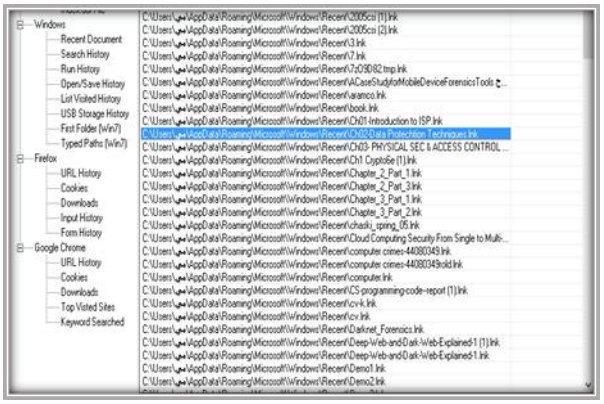

Figure 21. Recent document

Fig (22) displays the selected file.

Figure 22. Selected file from recent document

Fig (23) displays open/save file.

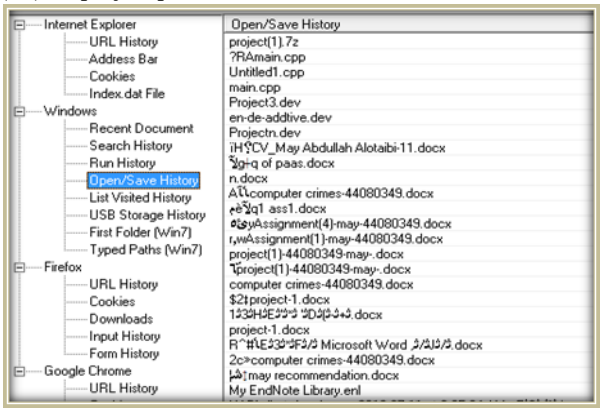

Figure 23. Open/save file

Fig (24) displays the Windows with the last visited history, which shows exe files.

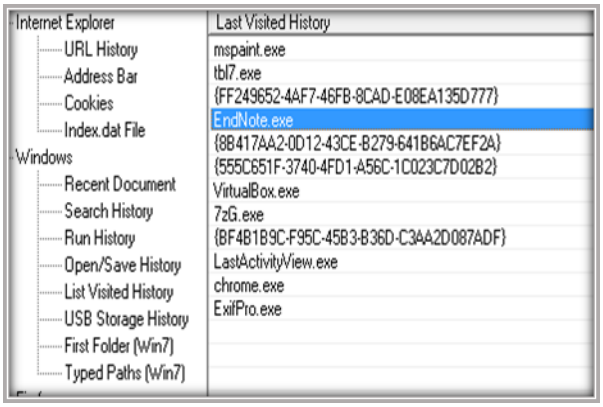

Figure 24. Windows of last visited history

Firefox was not used and so nothing was displayed in fig (25).

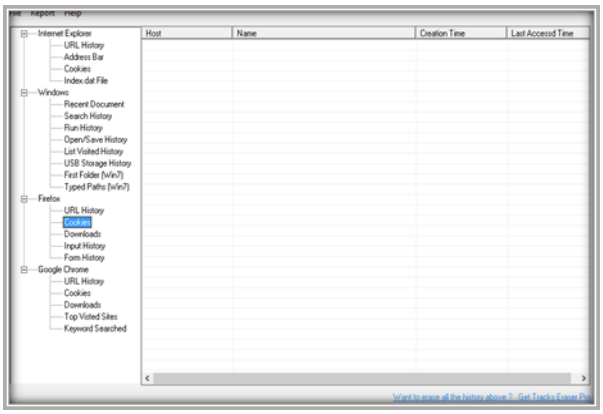

Figure 25. Firefox

URL in Google Chrome is displayed in Figure 26.

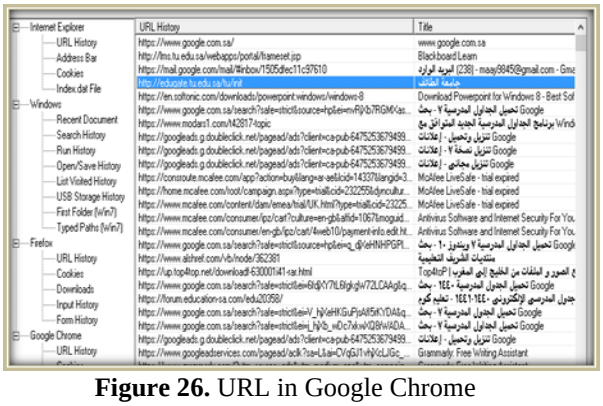

Figure 26. URL in Google Chrome

Cookies in google chrome displayed in fig (27).

Figure 27. Cookies in google chrome

Keywords in Google Chrome are displayed in fig (28).

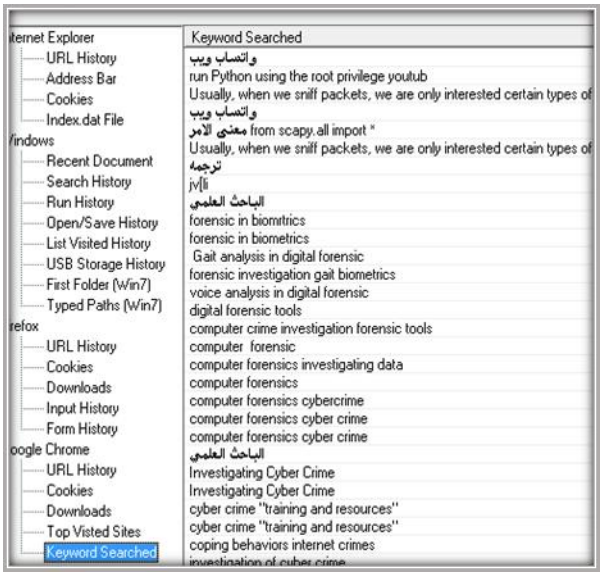

Figure 28. Keyword in Google Chrome

5. Conclusion

This paper explored many concepts in forensics as shown in Table 3. It also led to discuss the procedures that must be followed by each researcher in this area of research. The techniques differ from case to case depending on the evidence and methods used. In the paper we have mentioned some examples of the digital evidence and how to detect it. Moreover, this paper explains some of the methods used by the criminal to hide and increase their efforts to prevent authorities from obtaining proofs of their identity. Finally, we have demonstrated some of the tools used in the detection of digital evidence. All in all, the objectives of this paper are to explore the idea of the digital evidence detection methods that can be a starting point for navigating a crime scene as this can reduce the amount of work of investigating the crime once the directories are located through the use of digital evidence.

References

[1] M. A. Alzain and E. Pardede, "Using multi shares for ensuring privacy in database-as-a-service," in 2011 44th Hawaii International Conference on System Sciences, 2011, pp. 1-9: IEEE.

[2] M. A. AlZain, B. Soh, and E. Pardede, "Mcdb: using multi-clouds to ensure security in cloud computing," in 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, 2011, pp. 784-791: IEEE.

[3] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud computing security: from single to multi-

clouds," in 2012 45th Hawaii International Conference on System Sciences, 2012, pp. 5490-5499: IEEE.

[4] M. A. AlZain, B. Soh, and E. Pardede, "A new model to ensure security in cloud computing services," Journal of Service Science Research, vol. 4, no. 1, pp. 49-70, 2012.

[5] M. A. AlZain, B. Soh, and E. Pardede, "A new approach using redundancy technique to improve security in cloud computing," in Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012, pp. 230-235: IEEE.

[6] M. A. AlZain, B. Soh, and E. Pardede, "A byzantine fault tolerance model for a multi-cloud computing," in 2013 IEEE 16Th International Conference On Computational Science And Engineering, 2013, pp. 130-137: IEEE.

[7] M. A. AlZain, B. Soh, and E. Pardede, "A survey on data security issues in cloud computing: From single to multi-clouds," Journal of Software, vol. 8, no. 5, pp. 1068-1078, 2013.

[8] M. Alzain, B. Soh, and E. Pardede, "TMR-MCDB: Enhancing security in a multi-cloud model through improvement of service dependability," International Journal of Cloud Computing and Services Science, vol. 3, no. 3, p. 133, 2014.

[9] M. A. AlZain, A. S. Li, B. Soh, and E. Pardede, "Multi-cloud data management using Shamir's secret sharing and quantum byzantine agreement schemes," International Journal of Cloud Applications and Computing (IJCAC), vol. 5, no. 3, pp. 35-52, 2014.

[10] M. A. AlZain, A. S. Li, B. Soh, and M. Masud, "Byzantine Fault-Tolerant Architecture in Cloud Data Management," International Journal of Knowledge Society Research (IJKSR), vol. 7, no. 3, pp. 86-98, 2016.

[11] M. Pollitt, "A history of digital forensics," in IFIP International Conference on Digital Forensics, 2010, pp. 3-15: Springer.

[12] N. Jain and D. R. Kalbande, "A comparative study based digital forensic tool: complete automated tool," Int. J. Forensic Comput. Sci, 2014.

[13] C. C. Chigozie-Okwum, D. O. Michael, and S. G. Ugboaja, "Computer forensics investigation; implications for improved cyber security in Nigeria," AFRREV STECH: An International Journal of Science and Technology, vol. 6, no. 1, pp. 59-73, 2017.

[14] A. Valjarevic and H. S. Venter, "A comprehensive and harmonized digital forensic investigation process model," Journal of forensic sciences, vol. 60, no. 6, pp. 1467-1483, 2015.

[15] G. M. Jones and S. G. Winster, "Forensics analysis on smart phones using mobile forensics tools," International Journal of Computational Intelligence Research, vol. 13, no. 8, pp. 1859-1869, 2017.

[16] S. Ramadhani, Y. M. Saragih, R. Rahim, and A. P. U. Siahaan, "Post-Genesis Digital Forensics Investigation," Int. J. Sci. Res. Sci. Technol, vol. 3, no. 6, pp. 164-166, 2017.

[17] G. K. Sodhi et al., "Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code," Indonesian Journal of Electrical Engineering and Computer Science, vol. 12, no. 3, pp. 1297-1304, 2018.

[18] M. A. AlZain and J. F. Al-Amri, "Application of Data Steganographic Method in Video Sequences Using Histogram Shifting in the Discrete Wavelet Transform," International Journal of Applied Engineering Research, vol. 13, no. 8, pp. 6380-6387, 2018.

[19] G. S. Chhabra and P. Singh, "Distributed Network Forensics Framework: A Systematic Review," International Journal of Computer Applications, vol. 119, no. 19, 2015.

[20] B. Hazarika and S. Medhi, "Survey on Real Time Security Mechanisms in Network Forensics," International Journal of Computer Applications, vol. 151, no. 2, 2016.

[21] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Towards adapting metamodeling approach for the mobile forensics investigation domain," in International Conference on Innovation in Science and Technology (lICIST), 2015, p. 5.

[22] S. G. Punja and R. P. Mislan, "Mobile device analysis," Small scale digital device forensics journal, vol. 2, no. 1, pp. 1-16, 2008.

[23] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," arXiv preprint arXiv:1904.05735, 2019.

[24] D. Rathod, "Darknet forensics," future, vol. 11, p. 12, 2017.

[25] H.-Y. Huang and M. Bashir, "The onion router: Understanding a privacy enhancing technology community," in Proceedings of the 79th ASIS&T Annual Meeting: Creating Knowledge, Enhancing Lives through Information & Technology, 2016, p. 34: American Society for Information Science.

[26] R. B. Yetter, "Darknets, cybercrime & the onion router: Anonymity &security in cyberspace," Utica College, 2015.

[27] Y. Yannikos, J. Heeger, and M. Brockmeyer, "An Analysis Framework for Product Prices and Supplies in Darknet Marketplaces," in Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019, p. 50: ACM.

[28] T. A. Hengeveld, "Multi-tunnel virtual private network," ed: Google Patents, 2016.

[29] H. S. Yoon et al., "System for managing virtual private network and method thereof," ed: Google Patents, 2015.

[30] J. E. Berkes, "Decentralized peer-to-peer network architecture: Gnutella and freenet," University of Manitoba Winnipeg, Manitoba, Canada, 2003.

[31] M. Zaman, B. N. Bristy, and T. M. Mukur, "Internal Security Monitoring of an Organization by Scapy & Kali Linux," 2018.

[32] M. F. B. Rafiuddin, H. Minhas, and P. S. Dhubb, "A dark web story in-depth research and study conducted on the dark web based on forensic computing and security in Malaysia," in 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017, pp. 3049-3055: IEEE.

[33] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, "Network forensics analysis using Wireshark," International Journal of Security and Networks, vol. 10, no. 2, pp. 91-106, 2015.

[34] C. Fachkha and M. Debbabi, "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1197-1227, 2015.

[35] S. Perumal, "Digital forensic model based on Malaysian investigation process," International Journal of Computer Science and Network Security, vol. 9, no. 8, pp. 38-44, 2009.

[36] M. Chourasiya and A. Wadhe, "Implementation of Video Forensics Frame Work for Video Source Identification," in International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, 2016.

[37] R. Rowlingson, "A ten step process for forensic readiness," International Journal of Digital Evidence, vol. 2, no. 3, pp. 1-28, 2004.

[38] W.Alosaimi, M. Zak, K. Al-Begain, R. Alroobaea, M. Masud, "Economic Denial of Sustainability Attacks Mitigation in the Cloud," International Journal of Communication Networks and Information Security (IJCNIS), Vol 9, Issue 3, 2017

[39] O. ACHBAROU, "A New Distributed Intrusion Detection System Based on Multi-Agent System for Cloud Environment," International Journal of Communication Networks and Information Security (IJCNIS), Vol 10, Issue 3, 2018

Table 3. Related work in forensics.

	Forensics									
year	Registry	Network	Database	RAM	Deep web	Wireshark and miner network	Investigation Models	VPN	TOR	Zero net & FAI
2015							√ In general,			
2015		√								
2015									√	
2015								√		
2015						√ Network forensics in deep net				
2015		√								
2016		√								
2016									√	
2016								√		
2017							√ Mobile forensics			
2017							√ Computer Forensics			
2017	√ Darknet	√ Darknet	√ Darknet	√ Darknet	√			√	√	
2017										√ Darknet