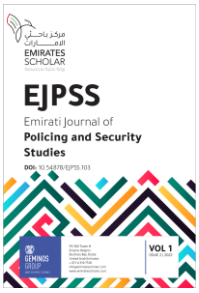


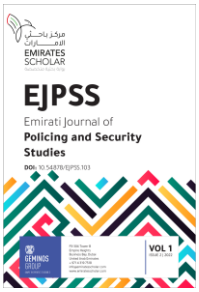
Emirati Journal of Policing and Security Studies
Vol 1 Issue 1 (2022) 4 - 11
DOI: 10.54878
Emirates Scholar
Available at www.emiratesscholar.com

Windows Forensics Analysis

Mariam Al Jouhi, Sara Al Hosani
Zayed University, Abu Dhabi, UAE
Mariamaljouhi94@gmail.com (ESID-8577-2744-2022), skm_92_4@hotmail.com

Abstract
Computer forensics investigates crimes on digital devices hard disk and any other digital storage devices to determine the evidence of any unauthorized access. Essentially, forensic investigators conduct forensic analysis with the help of different approaches (Static and Dynamic) and also tools like ProDiscover, Encase, Accessdata FTK and Autopsy to guarantee the security of a system in an organization. The process requires knowledge of different registry, laws, and regulations related to computer crimes, the operating system (Windows, Linux, etc.) and the network in an organization (e.g., Win NT). In this paper we will use different forensic tools to extract forensic evidence from a windows environment.

Keywords:
Digital Forensics, Windows Registry, Digital Evidence, Computer Investigation, Forensic Tools.



Emirati Journal of Policing and Security Studies
Vol 1 Issue 1 (2022) 4 - 11
DOI: 10.54878
Emirates Scholar
Available at www.emiratesscholar.com

I. Introduction

Computer technology has become an essential part of human life. Several operations require the use of a computer. As technology grows rapidly, so is the cybercrimes such as unauthorized access, financial fraud and identical and intellectual theft (Carvey, 2011). Computer forensics involves extracting and analyzing digital data that can be used to present in the court and prevent the identity of such crime. Since it may not be possible to block all the cybercriminals from internet and computer breach entirely, forensics is seen as a vital tool that can be employed in the curbing and recovering process. Nevertheless, there are several tools that can be used to conduct digital forensics. Therefore, it is important to address the dynamics which are involved in the digital forensics, the significance of Windows Registry during the forensic processes and evaluates tools used to analyze the windows registry so as to provide the digital protection. In this project, we will analyze the crime scene using different forensic tool such as Accessdata FTK imager and Autopsy to retrieve the deleted files and images, as well as other files from the windows registry files, to solve the crime and identify the real offender.

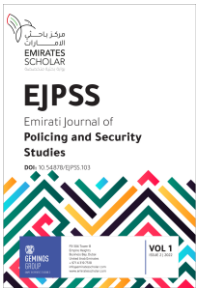
II. Literature Review

A. Digital Forensics

In daily operation, system maintainers and agency need to understand the dimensions of the digital forensics. Carvey (2011) defined digital forensics as the processes involved in the acquisition, authentication as well as the analysis of the documented evidence extracted from online or a system utilized to commit digital crimes. The system in the case ranges from computers, phones, networks, storage devices, and other digital media that the investigators analyses to provide evidence of a crime. When it comes to online, e-commerce domains as well as other websites can be examined. Significantly, past studies noted that file or data carving methodologies are widely adopted technologies for extracting digital evidence and other valuable information from the suspected source (Carvey, 2011; Casey, 2011). Also, it has been observed that these pieces of evidence can be used in a number of ways an in accordance with the law. The laws define guidelines under which the evidence is collected and authenticated. Many studies have defined digital forensics as:

- Digital forensics, also known as computer forensics, is the application of scientific methods in order to get a digital evidence from a device or media storage (Gogolin, 2014).
- The science of Digital Forensics was identified as “the collection, preservation, analysis, and presentation of computer-relate evidence” (Vacca, 2010).
- Also, (Solomon et al. , 2005) identified Digital Forensics as “Computer investigation and analysis techniques that involve in the identification, preservation extraction, documentation, and interpretation of computer data to determine potential legal evidence”.

From the previous mentioned definitions, we understand the main goal of digital forensics is to identify the digital evidence found on computers or digital media storage devices in a way that is that is acceptable in the court. Previous studies have examined the significance of such digital forensics and provide cutting-edge opportunities. For instance, Carvey suggested that it assists in the recovery of the hidden or deleted files from the storage system (Carvey, 2011). In another study, Petroni et al. pointed out that it assists the forensic experts to determine the existence of the malicious activities in the organization system and determine the identity of the criminal in the process (Petroni et al., 2006). If there is any tampering, the process will be able to tell in different ways. The sophistication of the approach is evident in the way


Emirati Journal of Policing and Security Studies
Vol 1 Issue 1 (2022) 4 - 11
DOI: 10.54878
Emirates Scholar
Available at www.emiratesscholar.com

it can recover information from deleted or corrupted files. In most cases, criminals format the files as a way of concealing the evidence of a crime. Also, different techniques are available in the market, but the commonly used include live analysis, steganography, volatile and also defensive approach among others.

B. Digital Forensics in Windows

Microsoft Windows is the most advanced and commonly used operating system because of its compatibility with a number of other software. From previous studies on forensics, evidence suggests that windows account for a greater proportion of traffic globally and may contain valuable information regarding cybercriminals (Casey, 2011). Because for a computer to work it needs an operating system as its core components, cybercriminals can interfere with the OS so as to tamper with the evidence. On the other hand, examiners will look into the windows as the first digital element that can provide information regarding breach of data. But, it is important to note that windows forensics can be considered in terms of Windows registry forensics. Thus, forensics is conducted in form of the registry file system itself.

C. Windows Registry and its importance in digital forensics

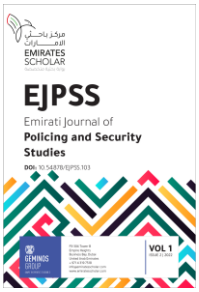
The Windows registry in several "Hives" is among the valuable forensic artifacts considered by most examiners and analysts. According to Carvey (2011), the registry can be considered as a log file. The reason is that it has data which can be extracted by the forensic investigator. In Carvey's examination of windows as artifacts for forensics, it was evident that windows registry act as databases order utilized by different Microsoft like Windows 98, Windows CE, and Windows 2000 to include Windows NT among others. It is utilized in hardware devices configuration and user application storage processes.

Carvey outlined a number of benefits of windows registry in digital forensics. The registry carries windows configuration as is an alternative for INI files (Carvey, 2011). Being a binary and hierarchical database, different computer applications, and configuration settings rely on windows registry. This suggests that windows registry is a great source for extracting OS records as well as the application settings. In addition, any manipulation on the user-specific data so as to interrupt user's experience can be extracted from the windows registry.

A research by Khawla and Andy (2010) included exploring the "locations that are most likely to contain digital evidence" in Windows 7. These locations include five logical root keys in the Windows Registry of Windows 7 which are HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG.
In our experiment, we are going to focus on the HKEY_LOCAL_MACHINE to get possible evidence in from the local machine. This includes HKEY_LOCAL_MACHINE\SYSTEM\, HKEY_LOCAL_MACHINE\SOFTWARE, HKEY_LOCAL_MACHINE\SAM and the NTUSER.DAT hive file.

D. Digital Forensics Tools

Forensics tools play an important role in digital forensics. Numerous tools have been proposed to be of a big importance in the forensic process in the investigation of digital crime in modern time. Casey (2011) classified these tools into imaging, analytical and forensic toolkits (Pollitt, 2007). Encase is among the tools used in forensics in the entire process like the acquisition of evidence, investigation, and analysis. Features like inbuilt sub tools in Encase V7 offers sophistication. It has


Emirati Journal of Policing and Security Studies
Vol 1 Issue 1 (2022) 4 - 11
DOI: 10.54878
Emirates Scholar
Available at www.emiratesscholar.com

advantages like binary duplicates generation and simple architecture. In addition, FTK (Forensics Tool Kit) is another tool that offers sophisticated service than Encase and AccessData (Pollitt, 2007). According to Pollitt (2007), digital evidence from devices such as memory cards and hard disks can be scanned with FTK. In addition, it is possible to scan evidence from remote sources such as emails and password via FTK.

Other tools include Helix, ProDiscover and autopsy among others. Helix is UNIX OS based digital forensics tool constructed on Ubuntu architecture. It is primarily useful in the acquisition, investigation, analysis and ultimate generation of digital forensics reports. It works in the same way as FTK with little modifications. Finally, autopsy is a forensic tool largely used by the military, law enforcement agencies and corporations to analyze the breach of the computer. It has simple interface compared with other forensic tools.

Many Tools have been developed to perform Windows Forensics some of them are:

1) Access Data - Forensic Toolkit

AccessData a well-known digital investigations tool provider, which serves law enforcement, government agencies and corporations around the world. "It is accepted all over the world as an industry leader, AccessData delivers state-of-the-art computer forensic, network forensic, eDiscovery, password cracking and decryption solutions. Its Forensic Toolkit® and network-enabled enterprise solutions allows establishments to preview, search for, forensically preserve, process, examine and produce electronic evidence" (Carrier & Spafford, 2003).

Access Data – Forensic Toolkit provides rich features for the users like:

- It allows creating forensic images from different storage media such as, local hard drives, floppy diskettes, Zip disks, CDs, and DVDs.
- Decrypting files need to use brute-force attack and trying every possible key or password until finding the correct password and this process may take many days, while using AccessData FTK provides all possible keys that already calculated and it takes seconds- to-minutes to find the password. FTK provide password recovery solutions by cracking password to access password protected files, recover system passwords, and lost personal passwords using AccessData Password Recovery Toolkit (PRTK) and Distributed Network Attack (DNA).
- FTK is providing the fastest and most accurate processes data, so the investigator will not waste time waiting the results unlike other products on the market.
- Support different file system, file type and email types.
- Generate most detailed and accurate FTK reports with different native format such as, HTML, PDF, XML, and RTF with a links back to the original evidence. Also, create a CSV of processed files that can be imported into Excel or database application and export MSGs for different email types.

2) ProDiscover Basic

ProDiscover is another powerful commercial forensic tool that can be used to extract forensic data. It can automatically generate data and analyse a broad range of devices. Basically, ProDiscover enables imaging, analysis, and generation of a report on the extracted evidence

Emirati Journal of Policing and Security Studies
Vol 1 Issue 1 (2022) 4 - 11
DOI: 10.54878
Emirates Scholar
Available at www.emiratesscholar.com

from digital drives. ProDiscover Basic is very useful tool for generating reports. It is also capable of showing unallocated (deleted) deleted files in the suspect device.

3) Autopsy

Autopsy is an Open Source tool, which allows users to collect and analyze evidence data on both computer systems and mobile phones. Law enforcement, military, and corporate examiners can use Autopsy to investigate cybercrimes. It also recovers photos from the device camera. Autopsy is the graphical user interface (GUI) used in The Sleuth Kit, and other digital forensics tools.

E. Digital Forensic Model

In this section, we will discuss different existing process models for digital forensic investigation.

1) Computer Forensic Investigative Process (1984)

In 2000, Pollitt & Presley discussed the Computer Forensic Investigative Process of 1984, which comprises of 4 distinct phases include Acquisition, Identification, Evaluation and Admission. First, the evidence is being acquired in the Acquisition phase after getting a proper approval from authority. This is followed by identifying digital components from the seized evidence in the Identification phase. Then, the Evaluation phase determines if the identified items are relevant and can be used as legitimate evidence. Finally, the acquired evidence is presented in the court in the Admission phase.

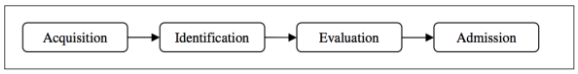


Figure 1: Computer Forensic Investigative Process

2) DFRWS Investigative Model (2001)

A report by (Palmer, 2001) mentioned the 1st Digital Forensics Research Workshop's proposed digital forensics investigation process (DFRWS), which consists of 6 phases which are Identification, Preservation, Collection, Examination, Analysis and Presentation. In the Identification phase, profile detection, system monitoring, audit analysis is performed. This is followed by preservation phase, which includes setting up case management and an appropriate chain of custody in order to make sure that the collected data hasn't been contaminated. Then comes the collection phase where the authorized people collect relevant data based on the approved methods and recovery techniques. The next two phases are the examination phase and analysis phase, where investigators start to trace and validate evidence, recover hidden/encrypted data and draw potential timelines. The last phase is the presentation where all tasks are carefully documented to be ready for presenting in the court.

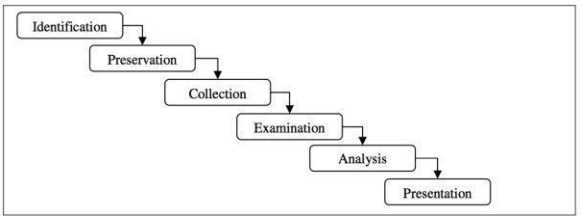


Figure 2: DFRWS Investigative Model

3) Digital Forensic Model based on Malaysian Investigation Process (DFMMIP) (2009)

A Research by (Perumal, 2009) proposed the DFMMIP, a digital forensic investigation model based on the Malaysian investigation processes. It consists of 7 phases which are Planning, Identification, Reconnaissance, Transport & Storage, Analysis, Proof & Defense and Archive Storage.

After completing the Planning and Identification phases, Reconnaissance phase starts by running the investigation while the devices are operating. Then, data is being securely transported properly stored in the investigation site during the Transport & Storage phase. After that, data is

Emirati Journal of Policing and Security Studies
Vol 1 Issue 1 (2022) 4 - 11
DOI: 10.54878
Emirates Scholar
Available at www.emiratesscholar.com

analyzed using the appropriate tools and techniques during the Analysis phase. Then, investigators support their presented case in the Proof & Defense phase. The final phase is Archive Storage, where all relevant evidence is securely stored to be used in the future.

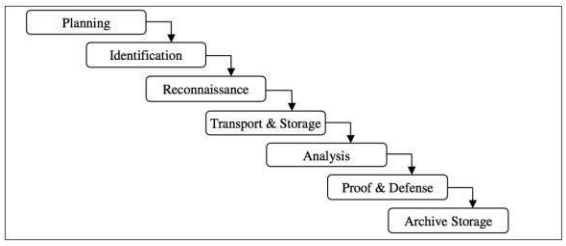


Figure 3: DFMMIP model

III. Research Problem

On October 20, 2018 at 3:00 pm the forensic investigation team started to investigate a real crime scene related to a criminal activity of transfer the trade secrets that targeted Dell company. The investigators collected all the suspected devices and other evidences securely. Then, they moved the collected evidences from the crime scene to the forensic lab start examine the crime. The investigators documented all findings related to the seized potential evidence such as USB drive and a computer hard drive from the crime scene. After that, the investigators start the chain of custody form and evidence custody form at the Zayed University forensics lab for digital forensics investigation. The investigators were trying to solve the crime by using different forensic tools such as forensic toolkit (FTK) and autopsy 4.9.0. The objective of this project was to find out if the suspect ex-employee Granny Smith is a real offender. The investigators trying to prove whether Granny Smith was guilty or blameless.

In the below table are the investigators names with their assigned roles:

Investigator ID	Investigator Name	Investigator Role
#		
001	Mariam Talal	Crime Investigator
002	Sara Al Hosani	Investigation Photographer
003	Noora Talal	Investigation Documenter

I. Proposed Methodology

A. *Digital forensic method*

In our investigation, we chose the DFRWS Investigative Model (2001) because it is a general investigation process and we think that it is appropriate for this particular case. As mentioned previously in this paper, this model consists of 6 phases which are identification, preservation, collection, examination, analysis, and presentation.

The below diagram shows the DFRWS Investigative Model (2001) phases with the description of each phase.

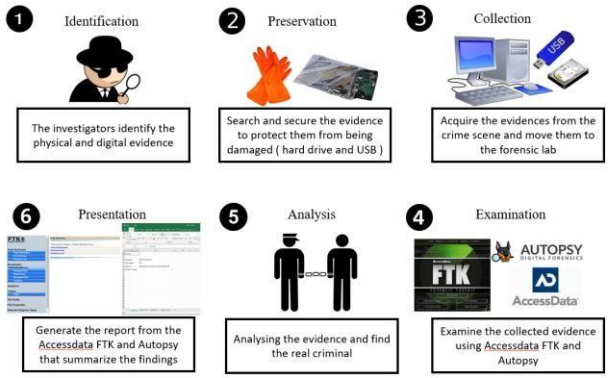


Figure 4: The selected digital forensic process

B. *Case Scenario: Data Leakage - Trade Secret*

1) Problem statement

On the 1st August 2018, an employee dubbed Mr. Granny Smith has left Dell, the computer technology company, where he worked in for the past 15 years. Mr Smith's leaving was sudden and somewhat suspicious. He resigned from Dell to join one of its competitors in the market, Samsung. The management of Dell was afraid that Mr. Smith leaked confidential information to Samsung. All employees in Dell has signed a non-disclosure agreement to protect all confidential information.

Emirati Journal of Policing and Security Studies
Vol 1 Issue 1 (2022) 4 - 11
DOI: 10.54878
Emirates Scholar
Available at www.emiratesscholar.com

Mr Granny denied the allegations of him leaking confidential information to the Samsung.

2) Why Dell Company suspect Mr. Smith?

Dell has suspected that Mr. Granny Smith leaked confidential documents detailing its new product ideas to Samsung because after 2 months of his resignation, on 04/10/2018, Samsung has announced the same idea that was developed by Dell since the past 5 years. Dell's idea was to produce a water-resistant laptop. This product was supposed to increase the profit rate of Dell since it is a new product in the region.

3) Case Identification and Preservation

The investigators have secured the area and wore the gloves to search for any possible evidence. Then, the investigators removed all connection cables and took the suspect hard drive using the forensic toolkit bag. All seized evidence, including the suspect USB flash drive and the suspect computer hard drive, were kept it in antistatic bags to protect them from being damaged. The investigators have documented all evidence in single and multiple evidence forms and started the chain of custody form.

The below table summarizes crime scene investigation findings along with the actions that have to be done:

Evidence #	Evidence Name	Evidence Size	Location	Action	Note
01	USB Drive	2 GB	Connected to the Computer	Will be investigated in the forensic investigation lab	TwinMOS
02	Hard Drive	500 GB	In the Computer Case	Will be investigated in the forensic investigation lab	Seagate, Barracuda 7200.12 Serial Number: Z2A6YBCC

Data Collection

After acquiring the suspect USB flash drive and computer hard drive, which were found in the crime scene, investigators have securely transfer the collected evidence to the digital forensics lab. The collected evidences were placed in a secure container and only authorized people can access it. Digital forensics investigators started analyzing the evidence using different forensic tools such as Toolkit® (FTK®) that includes AccessData FTK, PRTK, FTK imager and registry viewer. The have also used Autopsy digital forensic tool in the investigation.

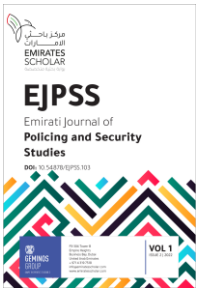
II. Conclusion

In conclusion, forensic investigators used several forensic tools to find out the real criminal. There are some digital evidences that have been found in different storage devices such as a USB and a computer hard drive. Digital files that were deleted from the storage media by the suspect were successfully retrieved too. The team has found that the forensic tool kit (FTK) is a more advanced than other forensic tools, such as Autopsy. The AccessData FTK Toolkit is more robust versions and highly recommended for digital forensic because it is more user-friendly tool than other forensic tools. Also, it is used for password recovery, encryption protection, and analysis for different operating systems with creating different image types. Dissimilar the Autopsy, which is open source, free version and much more limited for finding deleted and hidden files or partitions.

The available open and commercial forensic tools helped the forensic investigators to search for the target evidences, analyze them and generate the report to summarize all the findings, which prove the crime and to claim the suspect actions in the court.

References

[1] Alghafli, K. A., Jones, A., & Martin, T. A. (2010). Forensic analysis of the windows 7 registry. The Journal of Digital Forensics, Security and Law : JDFSL, 5(4), 5.



Emirati Journal of Policing and Security Studies
Vol 1 Issue 1 (2022) 4 - 11
DOI: 10.54878
Emirates Scholar
Available at www.emiratesscholar.com

[2] Alwis, Chirath De. (2018, March 2). Evidence Acquisition Using Accessdata FTK Imager. Retrieved from https://articles.forensicfocus.com/2018/03/02/evidence-acquisition-using-accessdata-ftk-imager/

[3] Autopsy. (n.d.). Sleuthkit. Retrieved from https://www.sleuthkit.org/proj.php

[4] Autopsy. (n.d.). Sleuthkit. Retrieved from https://www.sleuthkit.org/autopsy/download.php

[5] B. Carrier & E. H. Spafford, (2003) "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, Vol. 2, No. 2

[6] Carvey, H. (2005). The windows registry as a forensic resource. Digital Investigation, 2(3), 201-205. doi:10.1016/j.diin.2005.07.003

[7] Carvey, H. (2011). Windows registry forensics: Advanced digital forensic analysis of the windows registry. Elsevier.

[8] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.

[9] Forensic Evidence", Forensic Science Communications, Vol. 2, No. 4.

[10] Christin. (2018, June 10). Why is Mailbird the best alternative to Outlook? Retrieved from https://www.getmailbird.com/mailbird-best-alternative-to-outlook/

[11] Gogolin, G. (2014). Investigations: What is digital forensics and what should you know about it?

[12] G. Palmer, (2001) "DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research", Digital Forensics Workshop (DFRWS), Utica, New York.

[13] M. G. Noblett, M. M. Pollitt & L. A. Presley, (2000) "Recovering and Examining Computer

[14] Michael Solomon, D. B. (2005). Computer Forensics, jump start. SYBEX.

[15] Perumal, S., (2009) "Digital Forensic Model based on Malaysian Investigation Process", International Journal of Computer Science and Network Security, Vol. 9, No. 8.

[16] Vacca, J. R. (2010). Computer Forensic, computer crime scene investigation. Charles River Media.