CIS8708: Digital Forensics

Written Assessment

Created by: Deep Shah

Student id: U1137064

Date: 22 April 2022

Question 1: Discuss the tools

Solution:

There are many tools that used in investigation for crime related to virtual world which is known as cybercrime. Preservation, extraction, identification, data analysis, and report generation are all common tasks in digital forensics.

There are tools such as

1. EnCase
2. Digital Forensic Framework (DFF)
3. Pro-Discover
4. X-ways Forensic
5. Forensic Toolkit (FTK)
6. Quest changeauditor
7. The Sleuth Kit
8. Computer Online Forensic Evidence Extractor (COFEE):
9. Bulk_Extractor
10. WindowsScope
11. SANS Investigative Forensic Toolkit (SIFT)

Each of the tools mentioned above have their own set of functions, but are all utilized for digital forensics. DFF is an open-source program that is mostly utilized by law enforcement agencies, educational institutions, and private organizations, similar to how Encase is the most widely used forensic tool in the world. As a result, different tools has various features in various sectors.

Here we are discussing four different tools from above list

The tools are as following:

- Pro-discover
- Forensic toolkit (FTK)
- Bulk_Extractor
- WindowsScope

Lets discuss them first one by one and then we will compare all of them on the basis of their special feature (Vakharia , Ghazinour, Kannaji, & Satyakumar, 2017).

1) Pro-discover: Pro-Discover Forensic was founded by the ARC Group of New York. It comes in three versions: $50 for Pro-Discover Basic, $1,679 for Pro-Discover Forensic Edition, and $2,799 for Pro-Discover Incident Response Edition. The Pro-Discover Basic collects snapshots of actions that are necessary for safeguarding user data. When necessary, a report may be used to collect time zone, online surfing behaviors, and device information. Pro-Discover Forensic Edition, on the other hand, allows users to view files without changing metadata such as the last time they were visited, and Pro-Discover Incident Response Edition is a reactive, interactive, and proactive forensic investigation tool. It enables the investigators to do real-time analysis. It also employs Connect Collect Protect, a patent-pending technology and technique that enables the user to connect to a device, acquire data, and assess the situation in the event of a security breach.

   Features:

   - It provides for Hardware Protected Area
   - Inspection, picture capture, and search. It searches for regular expressions and keywords
   - Using the Boolean search capabilities. It is adaptable and quick
   - Within minutes of receiving an alert, Pro-Discover Incident Response Edition can assist in stopping the danger. When the SMART AGENT is necessary, it may be installed and then removed.
   - It also has malware detection hash sets
   - Perl Scripts are used to carry out research activities
   - It generates reports automatically that contain the facts that must be submitted as evidence.

2) Forensic toolkit (FTK): FTK was created by Access Data Group. They are the leading source of forensics tool certification and training. FTK is used by over 130,000 governing bodies and legal firms worldwide. In the entire globe, it can analyze laptops, personal computers, and other mobile devices. Computers, network connections, and mobile phones are all

examples of technology. Its filtering capability is faster than any other tool on the market.

Features:

- It could collect and store data via a network.
- It can collect data from 3,500 mobile devices. It can detect missing data, malicious conduct, and data leakage.
- Whether data is stored somewhere other than where it was originally, FTK can figure out how it got there, who altered the location, and even if any changes were made to the original.

3) Bulk_Extractor: The Bulk Extractor is a utility that runs on Windows, Linux, and Mac. The bulk extractor's key benefit is that it ignores all file systems, allowing any form of file to execute on it.

- It can perform disk imaging.
- Can Recover the data.
- Data carving is possible.
- Password can be recovered.
- It can make an analysis on E-mail.
- Live analysis on any system can be performed.
- And can decrypt the file if it is encrypted.

4) Windowsscope: Out of all the tools, is the only one that can perform reverse engineering. It has consumers in 16 different nations. It has graphical user interface.
Features:
   - Can perform live analysis.
   - It does incident response.
   - Can perform disk imaging.
   - Memory Dump analysis.
   - Data Recovery can be done.
   - Will alert the user if any attack has occurred on the device.

Features	**Name of Tools**			
	Pro-Discover	Forensic Toolkit (FTK)	Bulk_Extractor	WindowsScope
Platform	All	USB	All	All
License	Three forms	Free source	Free source	Multiple forms

Disk imaging	No	No	yes	yes
Data carving	No	yes	yes	yes
Password recovery	No	yes	yes	No
Static and live analysis	Yes	No	yes	yes
Slack space	No	yes	No	No
Email analysis	No	yes	yes	No
Real-time alert	No	No	No	yes

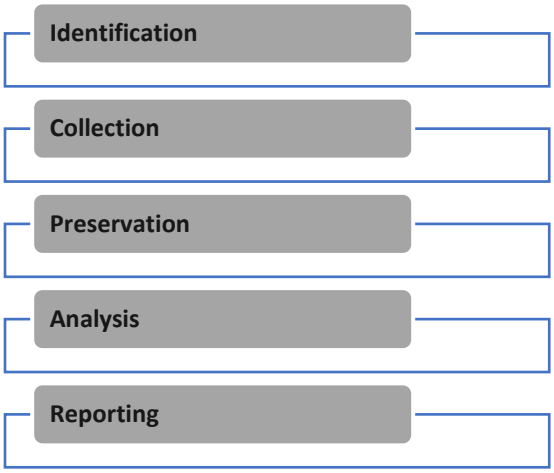
Question 2: Report

Put your self in the shoes of digital forensics detective for local police and Detail in the report, the steps that you are taken to gather evidence from IT support of Woolworth, Woolworth systems, and customers.

Solution:

Let's start with a step-by-step breakdown of how digital forensics is employed in any investigation:

There are five steps that include full investigation:



The first step is to identify the evidence, in this case all the information saved or sent in digital form from the Woolworths servers. As digital evidence is considered as physical evidence, it is sometimes necessary to print out all the digital evidence to submit it in court. The most fundamental things to accomplish when working with digital evidence are to identify digital information or artefacts that might be used as evidence, gather it, preserve it, and record it. It's a good idea to repeat or reconstruct the evidence once you've analyzed and organized it to make sure the results are accurate. Now, to improve the credibility of this evidence, I must first grasp the rules to comply with the states or federal rules of evidence. For example, in this situation, it is necessary to first understand the Australian standards for gathering

evidence. Because I need to make sure that the data, I'll retrieve from the Woolworths servers from forensic investigation, is complies with Australia's evidence laws. As Digital evidence differs from physical evidence in that it may be altered more quickly. Only by comparing the original data to a duplicate can these modifications be detected. As a result, the computer records displayed must be genuine and trustworthy to be acknowledged in court. They are frequently thought to be genuine if the application that generated the result is working properly.

There are three types of data I need to collect

- Volatile data collection: It collects all running data, such as user-logged in information, date, time, and other RAM data. During the enquiry, the system should stay powered on.
- Live system imaging: During the examination, it contains the imaging activity done on the data. The system should stay turned on throughout the study.
- Forensic imaging: To undertake imaging operations, a duplicate copy of the original device is made. To execute alterations, an exact replica of the original device is generated. To ensure the privacy factor, hashing methods are used. During the investigation, the system should be turned off.

To take care of the pc that is now running Conduct a live acquisition if possible. To keep log data while shutting down Windows XP or later, or Linux/Unix, do a regular shutdown. Existing app data should be preserved as securely as possible. Keep track of all the windows and shell sessions that are open. Take a screenshot of the screen. Keep note of everything you do while transferring data from a live suspicious machine. Open files should be saved to a network share or an external hard drive, or under a different name if that isn't possible. Turn off the computer and close all programs.

As the investigation progresses, the next step is to safeguard any evidence so that it is not damaged or tampered with while being transported to the forensic lab. If the organization has a private computer system, the best course of action is to hard shut it down, disconnect it, and place it in an antistatic bag, remove the battery from a laptop and transport it to the lab for further study. Secure any CCTV footage discovered and turn it off temporarily while the investigation is underway. For this process we need a warrant for removing the computer and for the CCTV footage and if removing computer will harm the business they should not be taken off.

Now that the evidence has been gathered, it is time to conduct an interview with Woolworth's employees, including IT department and visitors such as managers and cleaning staff. As the organization has also stated that their customers are experiencing strange pop-ups during online shopping and order processing, and that they are frequently redirected to a payment page that does not appear to be legitimate, it would be beneficial to investigate this issue by going through the same process and asking questions of customers who have previously experienced this. In addition, I should keep a log of papers and actions, film the area around the computers, and sketch the incident or crime scene.

Now for the prevention of the evidence and further process of the investigation it is important to isolate the evidence and investigate the copies that were created during the forensic imaging. The original evidence is safeguarded while it is evaluated to find the source of the problem. Using extra assistance, such as seeking for a professional, is beneficial for this phase. Finding the correct individual might sometimes be difficult. Evidence damage can be avoided by trained specialists in investigative tactics.

And the final step is to prepare the report providing all information and events related to the crime in a logical order. These reports are then produced as evidence in a court of law to solve the crime (Mailxaminer, 2020) (Hassan, 2019).

Question 3: Digital Forensics in cloud.

Solution:

When compared to traditional computer forensics, the procedure for investigating a cloud platform is quite different in many respects. Let's begin by identifying the evidence, which is the first stage in any enquiry. In traditional forensics, investigators have complete control over the system, making it simple to find evidence, however in the cloud, data management varies depending on the service model. Such as IaaS, PaaS, and SaaS.

To identify the evidence investigators must first determine which service the user uses, after which they may approach the cloud service provider (CSP) and proceed with the enquiry.

Given that the investigators are completely reliant on CSP for information, it is only logical to raise concerns about the evidence's integrity. The simplest approach is to create a system in which every cloud system provider is required to report their system logs to the nearest police station via the system, rather than manually, utilizing the Merkle tree concept. As a result, modifications to the log files will not go unnoticed.

As in the cloud, numerous virtual machines might share the same physical address, and data stored in them will be destroyed if the virtual machine is turned off or restarted. As a result, while collecting evidence from virtual machines, it is critical to keep volatile data in persistent storage so that investigators can access it even if a malicious user terminates the virtual machine. Even if the malicious user claims that his/her system has been compromised, investigators can prove that this is not the case.

Maintaining a proper chain of custody is challenging in clouds. In a cloud, we do not know where a VM is physically located. Also, investigators can acquire a VM image from any workstation connected with the internet. The Investigator's location and a VM's physical location can be in different time zones.

To address this problem, we may gather, analyze, and report all evidence in same time format. We can utilize GMT time, which is the same in all regions of the world owing to its geographic position. As a result, capturing both local and GMT time for evidence processing can be beneficial.

References

Hassan, n. a. (2019). Initial Response and First Responder Tasks. In n. a. Hassan, *Digital Forensics Basics* (pp. 93-110). new york: Apress, Berkeley, CA. doi:https://doi.org/10.1007/978-1-4842-3838-7_4

Mailxaminer. (2020, 11 21). *whats is digital forensics and how it is used in investigation*. Retrieved from Mailxaminer: https://www.mailxaminer.com/blog/what-is-digital-forensics-and-how-is-it-used-in-investigations/#:~:text=%20There%20are%20sequential%20steps%20for%20the%20digital,Analysis%3A%20Analysis%20involves%20in-depth%20examination%20of...%20More%20?msclkid=8b77c99

Vakharia , D., Ghazinour, K., Kannaji, K., & Satyakumar, R. (2017). *A Study on Digital Forensic Tools.* Kent: IEEE International Conference on Power.