

Assignment 1

by Alexander Tzafos

Submission date: 27-Apr-2023 09:58PM (UTC+0100)

Submission ID: 203757584

File name: 33391_Alexander_Tzafos_Assignment_1_497079_547472925.docx (132.55K)

Word count: 1907

Character count: 10635

Synthesize a solution to a potential real life scenario

Module: Computer Forensics

Module code: ACCD5000

Lecturer: Dr Carlene Campbell

Table of Contents

Introduction.....	3
Task 1	4
Autopsy	4
Wireshark	4
FTK Imager	5
Comparison	5
Task 2	6
Part 1	6
Part 2	8
Part 3	8
References	10

Introduction

During this assignment I will be researching various tools that are used within the field of computer forensics. These tools are very important due to amount of cyberattacks and breached which are increasing constantly because of the amount of technology around these days. Alongside this I will always be completing a real-life scenario which is based on a company from Swansea and a potential sabotage.

Task 1

Cyber forensics involves collecting and analysing information from a computer or device to provide evidence of cyber-attacks. The primary objective is to detect if any malware is present within the device's software. Professionals achieve this by examining endpoints and identifying malicious files or data which may be entering or leaving the device. Cyber forensics is critical in identifying vulnerabilities, attacks, and even denial of service attacks. Forensic experts follow a structured process, which involves creating a digital copy of data under investigation to ensure that no information is lost during the process. Once verified and authenticated the digital copy guarantees that no data has been altered during copying. The forensic appropriateness of the copied data is also ensured, and a record of its origin and storage location is noted. Finally, any deleted files are recovered, and the changes are then traced back to the cyber-attacker by using keywords to search for data that may lead to the attacker's discovery.

Autopsy

Autopsy is a digital forensics platform and graphical interface that is used by many of the top forensic investigators to understand a series of events that had taken place on a mobile phone or computer. This comprehensive solution includes various modules that can perform timeline analysis, hash filtering, and keyword searches. Furthermore, it can extract web artefacts, recover any deleted files from unallocated spaces, and identify any indication of compromise. All these processes are quick, and Autopsy will also run background jobs in parallel so the users will be able to identify targeted keywords within a matter of minutes even though a full search may take several hours. Alongside this, Autopsy can enable investigators to create a central repository of relevant data points, such as phone numbers and email addresses, when working with multiple devices. This platform was created by the same team that created The Sleuth Kit, an investigative library for disk images. Autopsy is an open-sourced solution, which means its open for public use so anyone can see, modify and distribute the code as they see fit. [1] Autopsy is free, as budgets are decreasing, cost effective digital forensics are essential. Due to this being completely free, open sourced and requiring minimal set up time, it will be at the top of many professionals wish lists.

Wireshark

Wireshark is an application that captures packets of data from a network connection, such as from a computer to the internet or a home office. A packet is a unit of data within an ethernet network. Wireshark is a commonly used application to troubleshoot networks with performance issues, and cybersecurity professionals use it to trace connections, view any suspects network transactions, and identify bursts of network traffic. It is a very valuable tool for IT professionals, but they need to know how to use it. Wireshark is safe and widely used by government agencies, educational institutions, corporations, small business, and non-profit organisations to troubleshoot any network issues they may encounter. It will also be used as a learning tool for those who are new to information security, enabling them to understand network traffic, communication with specific protocols, and how to identify and solve any issue that may arise. [2] Wireshark is very competitive in this area, with its current support of over 750 protocols. Due to the number of protocols that are supported by this application it is clear to understand why so many professionals use this as their go to, and

with it also being easy and safe to use it is again clear to see why it is heavily used in education.

FTK Imager

FTK is a comprehensive computer forensics solution that combines the most common forensic tools all in one place. With FTK, investigators will be able to crack passwords, analyse emails, and search for specific characters within files. Plus, it always has a very user-friendly interface making it straightforward and easy to use. Aside from this what really sets FTK apart from other forensic software is its exceptional performance boost. FTK claims it can cut case investigation times by up to 400%, which is impressive compared to other tools. Another unique feature of FTK is its use of a shared case database for each case instead of having multiple copies of data sets. This makes it much easier for team members to collaborate saving valuable resources. As mentioned FTK provides a range of capabilities. These include email analysis, which allows forensic professionals to quickly parse emails for specific words and conduct header analysis for source IP addresses. FTK's file decryption feature is a central component which is commonly used to crack passwords or decrypt entire files. With over 100 applications supported, FTK can retrieve passwords for various applications. FTK also includes a robust data carving engine that enables investigators to search files based on size, data type, and even pixel size. Finally, FTK empowers forensic experts with various data visualization techniques, such as timeline construction and cluster graphs, to create a much more intuitive case picture. [3] FTK is a complete platform for digital investigations, developed to assist the work of professionals working in the information security, technology, and law enforcement sectors. As stated above FTK is incredibly popular with many different IT and forensic professionals since it's easily accessible and extremely user friendly.

Comparison

When comparing the three forensics tools side by side I would personally opt for Wireshark as based on my research and existing knowledge it's the most used application and has an impressive user-friendly interface ensuring it's easy to navigate. Overall, I'd rank Wireshark as number 1, secondly, I would choose Autopsy and lastly FTK Imager 3. However, taking all three applications into consideration all the tools are straightforward and easy to download and very cost effective as all three of them are free of charge. Resulting in a difficult decision for forensic professionals as all three of them are attractive in their own way.

Task 2

Part 1

Digital forensics involves identifying, acquiring, and analysing electronic evidence, which is crucial in today's world, where most criminal activity has a digital component. Digital forensic experts are crucial in assisting police investigators, and their findings are often used in court proceedings. A significant aspect of digital forensics is analysing suspected cyberattacks to identify, mitigate, and eliminate cyber threats, making it a vital part of the incident response process. It is also valuable for providing the information auditors, legal teams, or law enforcement need after an attack has taken place. Electronic evidence can be collected from various sources, including computers, mobile devices, remote storage devices, Internet of Things devices, and any other computerised system.

In addition this type of investigation can reveal crucial information and clues that may help discover cybercrime, data theft, crypto crimes, security breaches, hacking and much more. Furthermore, digital forensics is essential in solving complex data-related problems. Digital forensics investigators use specialised tools and software to conduct investigations that can help to:

- Determine the source and cause of a cyberattack.
- Identify if a hack occurred and how long the hacker had system access.
- Create a timeline of criminal events, such as unauthorised data access or alteration.
- Secure digital evidence.

A digital forensic investigation can help identify and prove different types of wrongdoing, including data theft or disclosure, internet abuse, network or system breaches, espionage, and financial fraud.

There are roughly 5 crucial stages to a digital forensic investigation, and they are:

Stage 1:

The first step is identifying the devices and resources containing the data relevant to the investigation. This data may be located on organisational devices like computers or laptops or personal devices like mobile phones and tablets. Once identified, these devices are seized and isolated to prevent any further tampering. If the data is stored on a server, network, or cloud, it is crucial to ensure that only the investigating team can access it.

Stage 2:

Once the devices involved in an investigation have been taken and secured, a digital forensics investigator or analyst will use forensic techniques to extract any data that may be relevant to the investigation. This data is stored securely, and a forensic image may be created for further analysis and evaluation. The original data and devices are kept in a secure location, like a safe or similar as this would prevent tampering with any evidence, even if the investigating becomes compromised.

Stage 3:

Digital forensic investigators first identify and isolate the devices involved and can duplicate the data, storing it securely, they then extract and examine relevant data using various techniques to search for evidence of wrongdoing. These techniques include reverse steganography, which involves examining the underlying hash or string of characters representing an image or other data item to extract confidential data. Investigators also use file or data carving to identify and recover deleted files by searching for the fragments that these files may leave. Additionally, they use keyword searches to analyse information related to the investigation, including deleted data.

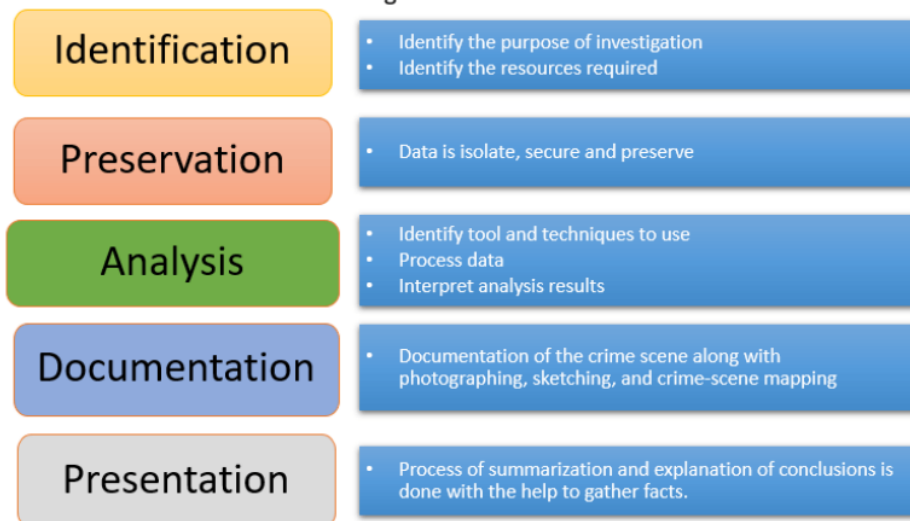
Stage 4:

After conducting an analysis, the investigation's results are thoroughly documented clearly and visually. This documentation allows for a clear timeline of any misconduct, such as embezzlement, data leaks, or network breaches, to be established.

Stage 5:

After finishing the investigation, the results are presented to either a court or committee responsible for resolving a lawsuit or internal complaint. Digital forensics investigators can serve as expert witnesses, presenting and summarising the evidence they found and disclosing their findings.

© guru99.com



<https://www.guru99.com/digital-forensics.html>

Based on the research above, I recommend that CEC Mobile Manufacturing utilize the autopsy application to retrieve the deleted design files from Rob's computer. This software offers various features such as keyword searching, hash matching, registry analysis, and web analytics, which will significantly aid the company in recovering lost designs. Due to Autopsy

being a windows-based desktop tool it's easy to download and the fact its free will make it even better for the company to go with when looking into ways of recovering said data. Furthermore, its an open-source platform which means it can be tailored for their own specific needs which in turn makes it an even better fit. Aside from this Autopsy runs in the background and is incredibly quick at searching, so a keyword search would be done in a matter of minutes, whereas with another application it could take several hours. The speed and easy to use application should defiantly be at the top of CEC's lists when looking at suitable applications.

Part 2

Part 3

Your Logo

Your details

FROM

Developer

ABC Seller
Developer Location
Street, City
United Kingdom
code@developer-email.com

Client's details

TO

ABC Company

XYZ Seller
Client Location
Street, City
client@client-email.com

Invoice No : 012345

Due Date : Dec 31st, 2021

Invoice Date : Dec 14th, 2021

Item	HRS/QTY	Rate	Subtotal
API Development Custom API creation integration from payment gateway to schedule calendar	1	250.00	USD 250.00
Desktop Software Development Activity and email monitoring, file transfer tracking, keystroke logging & screen recording	65	110.00	USD 7,150.00
IOS Chatbot Front-End Scope : 7-8 states, 9-11 pages, a/c to the adobe design from UI/UX designer	28	85.00	USD 2,380.00
Magento Development Streamline seller registrations, E2E order replacement, payment functionality on backend & UI	1	650.00	USD 650.00

Invoice Summary	
Subtotal	USD 10,430.00
Total	USD 10,430.00

The image above is of a sample invoice which is used by forensic investigators.

References

- [1] Brian Carrier, 'Autopsy', 2023 2003, [Online]. Available:
<https://www.sleuthkit.org/autopsy/>
- [2] Jay Beale, *Wireshark and ethereal network protocol analyser toolkit*. [Online]. Available:
https://books.google.co.uk/books?hl=en&lr=&id=-AdTE9S3kigC&oi=fnd&pg=PP1&dq=wireshark&ots=Y9CXy2MLrM&sig=IMEkBFLqAD4sojEzxGmpciwVsAU&redir_esc=y#v=onepage&q=wireshark&f=false
- [3] Fernando Carbone, *Computer Forensics with FTK*. [Online]. Available:
<https://www.uplooder.net/ofiles/1622331468ea76ed7280e98491588cc8/Computer-Forensics-with-FTK.pdf>

Assignment 1

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

48/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

GRADING FORM: L5 CF (ACCD5000)

ALEXANDER TZAFOS

48

ENGAGEMENT WITH LITERATURE SKI

Your work must include articles published by peer reviewed journals, conference proceedings, books, and related website (e.g. IEEE, ACM, Science direct). Information from website such as how, wiki, forums, etc. will not be accepted. (20 marks)



Engagement with the literature is lacking. Try to use/engage peer reviewed articles and journals in your research /literature areas, especially for general background research. Try utilising the university online resources and journals.
No referencing provided

9

KNOWLEDGE AND UNDERSTANDING SK

On chosen topic, your work must demonstrate understanding of concepts and underlying principles. You should explain and analyse the tools you have chosen from the research in a meaningful way. The IEEE report format must be used for the research aspect (task 1) but not mandatory for the case study (task 2). (10 marks)



See comment above to improve this section.
An example of a good article: Cyber Forensic Tools: A Review, B. V. Prasanthi, Assistant Professor & Department of Computer Science & Engineering, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India, International Journal of Engineering Trends and Technology (IJETT) – Volume-41 Number-5 - November 2016

5

COGNITIVE AND INTELLECTUAL SKI

Your work must demonstrate critical analysis and evaluation of the investigation and reporting documentation. Your work must also justify Computer Forensics Investigation procedures. The labs you do in class should help you to complete the processes or forensic methods Barry would have used. (45 marks)

30



Tools explained were not categorised.

Your introduction needs improvement, it should give a background to the work along with some general research information of the subject areas, followed by what the rest of the report will include.

You have not done a conclusion for your report.

You have discussed the case study, The key was to have discussed the steps taken during the investigation process example: step 1: He would visited Rob's desk and seized all the hardware devices such as hard disks, CDROM, iPods, and DVD disks etc.

Step 2: He placed all the seized devices carefully in anti-static bags and transported them to a forensics laboratory. Etc.

You have done an invoice

PRACTICAL SKILLS

Marks will be awarded based on the sample professional forensics report generated by a forensics tool. AccessData FTK tool is recommended as this tool is on the computers in room IQ 205 or any other of your choice will be accepted. Use sample evidence file(s) from the shared folder. Less than 40% will be awarded for Internet downloaded report. (15 marks)



You have not provided a generated report or any other form of report.

0

TRANSFERABLE SKILLS FOR LIFE A

The report should be presented in an academic way (IEEE/ACM format) and therefore must include an abstract, an introduction, a conclusion and a list of references. The report must be submitted via Turnitin as well. (10 marks)



Your work required formatting. Avoid 1st person writing in academic report. Avoid long paragraphs. This report require improvement in all aspects.

4