

Assingment 1

by Ethan Robert Matthews

Submission date: 04-May-2023 04:16PM (UTC+0100)

Submission ID: 204742076

File name: 41706_Ethan_Robert_Matthews_Assingment_1_497079_1388621457.docx (12.26K)

Word count: 1677

Character count: 7598

BSc (Hons) Computing Portfolio

Computer Forensics

Synthesise a solution to a potential real life scenario

Assignment 1

ACCD5000

By Ethan Matthews

Due: 27/04/2023

Contents Page

<u>Title</u>	<u>Page Number</u>
Introduction	
Task 1	
Task 2	
Appendix	

Introduction

This is my introduction for my first and only assignment for the 'Computer Forensics' course.

During the course of this document I will be speaking about two separate tasks. The first task that I will be highlighting is researching multiple different Forensic tools and comparing the tools with one another across a variety of different options.

The second task that I will be covering in this document will be a case study that is based on a real world scenario on how I would use the forensics tools to restore files on someone's computer.

Task 1 - Research

So, in this first task for my assignment I am going to be documenting a minimum of three different computer forensics tools. During the course of this I am also going to be describing each and every forensics tool that I document before I then document them in a table and compare them all. I will be categorising them by Open Source, Commercial, Features, Types, Hardware and Software.

As we know, in modern day society, computers are becoming an ever frequent part of our daily lives. With the growing use of computers also comes the growing use of computer forensics and the increase in cyber crime. Due to this, computer forensic tools have been designed, created and implemented into society to ensure that all information that can be recovered from a computer can be done so reliably and successfully.

To do with this, there are a variety of computer forensic tool groups and the tools that they have to offer, these tools are listed below:

Disk and Data Capture Tools -

These types of tools focus on the analysis of a system and use things such as a variety of emails and files to help extract potential things. Some tools that this forensics area has to offer are:

- Autopsy or The Sleuth Kit - Some of the most well known forensics tools out there. These types of tools were designed to analyse disk images and perform an analysis of file systems. As a result of this, this sort of tool can practically cover most of the different types of tools that forensics can offer.

Memory Forensics Tools -

Hence the name, these types of tools focus on extracting information that is stored in the memory and analysing missing files. Tools used by this are:

- Volatility - This is a memory forensics tool and this type of tool specifically focuses on incident response and a variety of malware attacks that can be found. As well as this you can also extract a variety of information from processes, registry hives or programs that are generally already running.
- Windows SCOPE - Just like the tool above, this is also a memory forensics tool, but instead this type of tool focuses on reverse engineering the malware attacks.

Network Forensics Tools -

These types of tools allow you to appropriately analyse traffic over a network.

- Wireshark - This is one of the most commonly known networking tools. This type of tool has an ability to capture live traffic flowing within a network or even capturing files that are trying to escape from out of the network.

As a side note, some information and the sections and tools a I have described above was helped by the use of:

<https://resources.infosecinstitute.com/topic/computer-forensics-tools/>

Obviously there are way more different types of forensics tools that can be used to solve different types of forensics problems but the types that i have listed above are some of the most popular types of forensics tools that people use and know well.

But when it comes to me completing the second task in this report, i will not be using any of the tools that i have listed above, the tool that i will be using in my second task will be mentioned and described in the task below.

Task 2 - Real Life Scenario

This is my second task for this assignment and for this task I will be documenting what I would do in a real life scenario.

For a bit of context during this task, I have been asked to restore some deleted files from an ex-employees computer.

Rob used to work for the GEC Mobile Manufacturing Company over in Swansea, this company designs phone interfaces and GUIs for popular vendors. This company used Autodesk Maya to aid them in designing interfaces to which Rob and the company managed to design something that rivals the Apple iPhone 12.

During this Rob was going to sell the design to the company's main rival Samtech. To which Rob stuck a deal and resigned from GEC. This is where I come in as GEC were shocked to see that the designs were all missing from Rob's computer so they have asked me to help restore their hard work to prevent Samtech or Rob from leaking the designs.

During this I will be using my knowledge from the first task and documenting forensics methodology in how I restored the files on Rob's computer. I will also be providing a report on the Actions I took as to which an invoice at the end of the report will be made documenting the costs of the entire process.

When it comes to speaking about this task, the favoured option to completing this would be using a forensics data recovery tool.

Now, what is forensics data recovery?

This is a process of recovery, performed by highly trained computer specialists who have studied a variety of different topics in order to fully understand how it works. Typically data recovery is used and more

involved in recovering data for criminal or civil investigations but it can also be used in a more appealing manner to help recover files that were meant to be lost or deleted. Forensics data also involves the use of a physical hard drive to attempt to try and recover the lost and deleted files.

Now onto the steps that would need to be taken in order to recover the deleted files.

Following on to the start of the steps required I will be taking some advice off of the website 'Hackers Arise'. As we all know recovering files is one of the most basic skills to have when it comes to being a forensics expert and over time once you start to develop those skills you will come to find out that the files that are deleted off of a system will come to be found to be on the 'Storage Medium' until the files are eventually overwritten and replaced.

After knowing the above statement we know that there is a chance that the files that Rob deleted off of his computer system at work may still be in there as it was only a short period of time after he had left the company.

The tool that I will be using is one that I have previously mentioned in the first task. This tool is known as 'The Sleuth Kit' which is one of the Disk and Data Capture tools that I had spoken about before.

Originally this kite was designed to be used on Linux machines but has since been ported over to the Windows machine for further use. Following on from this, in 'The Sleuth Kit' there is a GUI interface known as 'Autopsy' which is what I will be using in an attempt to recover the files that Rob had deleted.

First of all, you will need to download Autopsy on the system of your choice, in this instance it would be on Rob's system that he was given when he was still with the company. After the installation is completed you will be met with a screen asking you to either 'Create a New Case' or either 'Open an Existing Case', in this instance we would need to 'Create a New Case'.

After completing this step we would then need to name the case and determine what directory we would want to place the cases in, in my instance the case will be named 'Deleted Designs Case 1' and i would assume that the desktop only has one drive which would be the 'C' Drive so this would be where i will store the cases. After this we can skip the optional step and then click on finish to take us right up to the next step.

After this, the next step would then be to 'Adding a Data Source' to narrow down the search for deleted files. In this instance I will be using a previous design image that the company should have stored on their system. After adding in the image the next step would be to click on finish and then wait for the autopsy to begin analysing the system files.

Next after that we would then be greeted with a screen depicting our data source as the image that was given us by the company. Then we should be able to expand the data source views page to come across the section 'Deleted Files'. In this section we should find the files that Rob deleted, and as this was a short period of time the files were in that location.

After discovering that the files were still there we can then export them by clicking on the files and clicking the 'Export' button which would then export the files into where we first created the file to save the cases into, which would be the 'C' drive. After that we just repeat the steps until we find all the files that Rob had deleted off of the system so that the company has them back into their possession.

As a side note to this task I had taken some inspiration from the 'Hackers Arise' site

<https://www.hackers-arise.com/post/2016/10/10/digital-forensics-part-3-recovering-deleted-files>

But all the words in the task came from my own,

Assingment 1

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

30/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

GRADING FORM: L5 CF (ACCD5000)

ETHAN ROBERT MATTHEWS

30

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

5

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 to demonstrate your knowledge and understanding.
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

3

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)



Introduction needs a lot of improvement
Introduction 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.. No conclusion done. Your conclusion should summarized your key areas of the report.

The case study discussion needs a lot of improvement. You could list the methodology steps. The first two steps that you could include in the methodology steps are 1. Barry would visit Rob's desk and seized all the hardware devices such as hard disks, CDROM, iPods, and DVD disks etc.

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

You have not done the invoice for services provided.

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 generated a sample 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 writing style need improvement. First person writing is not use in academic report.. Formatting require and you have not used IEEE report writing for at least task 1.

4