

Forensics

by Max Beasley

Submission date: 01-May-2025 10:58PM (UTC+0100)

Submission ID: 257520367

File name: 49929_Max_Beasley_Forensics_662582_495660939.docx (125.95K)

Word count: 4597

Character count: 24906



SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

Computer Forensics

Max Beasley (2304218)
230418@student.uwtsd.ac.uk

Contents

Task 1.....2

 Introduction 2

 Autopsy 2

 Forensic Toolkit (FTK) 3

 OpenText forensic (EnCase) 3

 Wireshark.....4

 Cellebrite.....5

 Comparison table 5

 Conclusion.....6

Task 2.....7

 Pre investigation stage 7

 Investigation phase 7

 Post investigation phase 8

 Sample report 9

References.....13

Task 1

Introduction

In the field of digital forensics there are many ways that one can go about analysing data that has been retrieved from a device, and this is achieved through the use of forensics software, below I will compare research some of the most commonly used forensics software and tools and contrast their abilities and functionality so that I can identify the most suitable software for digital forensics analysis.

Autopsy

The first tool that I will discuss is the software called Autopsy. Autopsy is an open-source digital forensics software package [1], this means that it is developed in an open manner that allows anyone to analyse and modify the source code [2] (given some conditions). Autopsy provides a variety of features that allow for the analysis and recovery of varying data types. Initially developed by Brian Carrier in 2001 it is a graphical interface for the forensics tools known as The Sleuth Kit, the current version of Autopsy (version 4) is maintained by Basis technology under the Apache 2 open-source license [3,4]. Autopsy ships with all of the features that would be needed for a basic forensic analysis of a given data set with tools like Key word search, registry analysis, web artifact search, Email analysis, timeline analysis and tools to recover deleted data and much more [5], unlike other forensics software Autopsy also provides the ability to analyse android based file systems allowing the investigator to work with mobile devices.. However, because of its free and open-source nature the update cycle and update scope for the software is more limited than a comparable commercial software, with the mean time between major updates at the time of writing being every year [6]. Autopsy's open-source nature also allows it to be widely compatible with many operating systems such as Windows, Linux and MacOS [7]. Importantly for a complete forensics package autopsy also includes an inbuilt report generating feature that allows the user to analyse the inputted data and produce an automatic report template with all the selected data that may have been retrieved from the data source so that it can be used as a professional forensics report.

Autopsy is often considered to be a tool more broadly aimed at enthusiasts, although it does attract many non-professional users due to its free nature it is nevertheless widely used by professionals who may not have the resources to purchase a license to a more well-known software package. This is because it provides many of the features of other software's, perhaps not as in depth as others but still Autopsy provides these features for free and in a relatively easy to use graphical environment [8].

Forensic Toolkit (FTK)

An example of a more professional tool is FTK (forensics Toolkit), FTK is a package of different forensics tools developed by Exterro to provide all the functionality that one might need when conducting a digital forensics investigation [9]. The two main aspects of the FTK package are the main FTK software and FTK imager, FTK imager is a free tool used to collect images (one to one copies of data) of data sources such as storage drives so that it can be analysed by forensics software like the main FTK software [10]. When it comes to features FTK provides all of the features of the previously discussed tool Autopsy and more, the main standout feature of FTK being its ability to handle encrypted data sources, FTK allows the user to process data encrypted using a variety of sources such as BitLocker [11]. Furthermore, one of the standout features of FTK is its integration with a shared database that can be used to allow collaboration of multiple technicians to analyse the same piece of data simultaneously. FTK also provides extended support for data retrieved from mobile devices. The main draw of the FTK software is its speed which when compared to other forensics tools like Autopsy and Cellebrite it proven to work at a considerably faster speed especially when it comes to data recovery, this can be seen in a report published in the International Journal of Intelligent Computing Research. In the aforementioned report in which multiple software's are compared the ease of use of FTKs graphical interface is raised as a drawback to the software, however it is noted that this is related to the GUIs (graphical user interface) learning curve instead of its functionality [12]. When it comes to the report functionality FTK like Autopsy provides an integrated report generator which can generate a report in a standardized format that can be used in recognized proceedings, however it as with all automatically generated reports it is vital they only be used as a base template. The final point that I will consider is the price of FTK, whereas Autopsy operates under an open-source license FTK runs under a private license and therefore comes with a cost, as with most protectional software suites this cost is considerable, FTK operates on a subscription model that renews yearly, this comes in at a Regular price of £3,429.00 /year [13].

OpenText forensic (EnCase)

OpenText or as it was formally known EnCase is a digital forensics tool that was initially released in 1998 by Guidance Software and later purchased by OpenText and renamed to OpenText Forensic in 2017. Like the other software's mentioned OpenText aims to be an expansive suite of tools to allow a forensics investigator to retrieve information from a data source that can be used in an investigation. It includes all the features of the two aforementioned software's with tools enabling the recovery of previously deleted data and data that may have been obfuscated [13]. OpenText places a large amount of emphasis on the programs ability to be implemented into a workflow by providing a streamlined workspace environment, this is done by the program using a customizable GUI (graphical user interface) so that forensics technicians can optimize their workflows, this notably

includes the ability to detach windows from the program to make optimal use of desktop setups with multiple monitors or displays [15]. As with FTK OpenText can also handle data sources that are encrypted, like FTK OpenText can also handle BitLocker encrypted devices however unlike FTK OpenText has the ability to devices encrypted with the apple security chips [14], this includes all of the modern MAC and MacBook devices [16]. Unlike the previously mentioned software's OpenText has pioneered the implementation of AI (artificial intelligence) into their software, this is to further the goal of efficiency and speed that is so prominent in OpenText's marketing. AI is primarily used in OpenText to categorize and flag images that may be of interest to the investigator thus saving them time when analysing the recovered data [14]. AI is also used to help detect information text that may be hidden in file formats such as PDFs. In the ever-interconnected world cloud integration is key to optimizing workflows, it is for this reason that like FTK OpenText also includes many tools that can pull information from cloud platforms like Google, iCloud etc [17]. The report writing capabilities of OpenText are also extensive with many differing templates available when generating a report with the data retrieved, furthermore OpenText includes formats that are legally recognized. When it comes to price OpenText also follows the trend of other professional forensics software packages by only offering its software through a yearly subscription, in OpenText's case this comes in at £2725.63 for a 12-month license.

Wireshark

Wireshark unlike the previously discussed programs is a tool for analysing network traffic originating from or being received by a networked device. Released in 1998 it is open-source software that was released under the GNU General Public License version 2 [18] meaning that anyone can download the software source code which is publicly [19] available and make changes to the software to modify it to fit their specific uses. When it comes to the field of computer forensics Wireshark is used to determine what communications are being conducted with the device in question, this is useful as this information can be used to determine if the device has been compromised or is communicating with a compromised device. Wireshark does this by analysing the hundreds of different network protocols for any traffic and then capturing that information and then displaying that data through a GUI (graphical user interface) [20]. Wireshark with its deep integration with network protocols has the ability to decrypt a variety of network protocols such as IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2. The software also provides robust filtering options so an investigator can filter out routine or unwanted network traffic so that only the relevant programs or protocols are being monitored therefore increasing the workflow of the person using the software. However, as Wireshark is a specific standalone program which is not integrated with a forensics suite it does not provide any forensics report functionality, therefore it is required to use Wireshark alongside other forensics suites to help produce a complete report. Unlike forensics toolkits which will analyse an image of a device's storage

Wireshark needs to be run on a live instance of the device therefore a running copy of the device needs to be made or for the last resort the device itself.

Cellebrite

The final tool that I will consider in this report is Cellebrite. The Cellebrite software is a full digital forensics suite that also provides a wide range of tools to analyse data collected from a device for evidence that may be relevant in a forensics investigation. Unlike the other tools mentioned in this research Cellebrite offers a solution for extracting data from devices as well as tools to manage and analyse this data, this is done through their UFED software [21]. However, Cellebrite as a software is foremost a tool designed for mobile devices therefore the tools are tailored to use with mobile device data therefore it has been noted that the performance with desktop data was worse than similar software whereas its Performance with large volumes of data like call logs was exceptional in comparison [12]. Because of its focus on mobile devices Cellebrite provides multiple tools that are based on retrieving data that is usually specific to mobile devices like call logs contacts and app data with ways to visualize this data in various ways so that it can be more efficiently understood and analysed, therefore there is less emphasis on the desktop tools. Cellebrite also offers hardware in companion with its software to allow for a truly integrated workflow, the software like OpenText provides extensive AI features in the newest versions to help increase productivity and allow the investigator to more easily recognize data that may be of Importance. Because all of the aforementioned factors Cellebrite has become the go to solution for forensics analysts when it comes to working with mobile devices. As with the other full forensics packages Cellebrite also includes many ways to generate a variety of reports so that the collected data can be organized in a way that can be presented in a recognized and professional way. Finally when it comes to cost I was unable to find any figure for the average cost of the Cellebrite software, however it believe that it is safe to assume that Cellebrite's pricing structure will follow a similar one to that of other enterprise forensic software's, so the price is likely to be in the range of the thousands of pounds for the software and possibly even more for the companion hardware that Cellebrite offers.

Comparison table

Name	Type	License	Cost	Decryption	AI integration

Autopsy	All round	Open source	Free	No	No
FTK	All round	Private	£3,500 + /year	Yes	No
OpenText (EnCase	All round	Private	£2726 / year	Yes	Yes
Wireshark	Network	Open source	Free	Yes	No
Cellebrite	All round (mobile focus)	Private	?	Yes	Yes

Conclusion

There are many choices available when deciding what forensics tool to use, there are far more tools available than what was mentioned above. From this research I have discovered that although there are many tools that may at first seem similar, they all have benefits and shortcomings (as shown above) and all have more suited use cases.

Task 2

Pre investigation stage

The first step that the forensics investigator (Troy Simpson) will take is to complete the pre-investigation checklist. This is the first stage of any forensics investigation and ensures that the investigator has a robust starting point for the investigation. The first aspect of this will be for the investigator to construct his forensics lab, this will involve the set up and modification of his forensics workstation with any upgrades that might be needed to work on the case that he has been given (increased storage etc.). After the appropriate hardware is functioning the investigator will then move onto determining the various tools and software that he will need to conduct this investigation. This will consist of reviewing the types of evidence that will be handled during the investigation and then reviewing which forensics package or packages will be needed to most effectively carry out the investigation. In this case as the suspects device is a desktop computer the investigator would find a tool focused on desktop forensics and avoid mobile tools like Cellebrite. Once the tools are chosen and installed onto the investigators lab the final stage of the pre-determined stage will take place, this is the verification of the tools and hardware being used. This is to hopefully detect any problems with the hardware or tools before the investigation takes place, so the integrity of the investigation is not compromised in the future. This will be done by stress testing the software with sample evidence to ensure the workflow is consistent and stable. Finally, changes in the configurations will be made after the tests have been completed so that the lab can be suitable for the anticipated upcoming workflow.

Investigation phase

The first step in the investigation stage will in most cases not be carried out by the investigator, this is because the first step in an investigation is the first response and during this stage the most important task is to preserve as much evidence as possible, this takes the shape of documenting the evidence scene by taking pictures of the area and making notes, this should all be done without tampering with any potential evidence, an example might be not turning on or off devices and preventing anyone else from doing so. The next step is when the forensics investigator comes into play, they will gain permission from the owner of the device (in this case CMMC) to seize the device so that they can conduct the investigation. It is at this stage in the investigation that the any further information will be gathered from any people of interest in the investigation for key facts that might be pertinent to the case. It is important to note that if the investigation is taking place in a law enforcement capacity permission to seize devices may not be required as warrants may be issued for the confiscation of data and devices. It is at this stage that a chain of evidence / custody will be created, this is a record of who has handles and had possession of the

device. After the evidence has been preserved and seized the main body of the investigation can begin, this being the data acquisition and analysis.

To be able to conduct the analysis the investigator will need to create a copy of the data to work with, this is done for a multitude of reasons, the foremost being the need to maintain the integrity of the evidence and the investigation as a whole. The process of doing this will differ if the device was recovered running or not, but the goal is to create a bit for bit copy of the device so that it can be analysed as if the technician was analysing the device itself, to ensure that this data remains unaltered hash values can be employed, these are values that are calculated from the data and will remain the same if the data has not been changed in any way, the investigator can use these values to ensure that the working data does not deviate from the source. Once a working copy has been made the analysis proper can begin, this will involve uploading the data to the forensics program of choice, the program will automatically scan the data for various types of data present on the device and data that may have been deleted. In the case of CMMC the investigator will be looking to recover the lost product data that was maliciously deleted by the perpetrator, this will be possible if the items have only been de indexed from the file system but if they have been professionally deleted the chance of recovering the data may be small. However, when it comes to finding evidence of the perpetrator's sabotage there are many areas that may provide evidence. Arguably the most promising area will be in the recovery of emails sent to and from the third party when arranging the theft, if the emails were sent from the recovered device there may be remnants of these emails saved on the device that can be recovered and used as evidence. The investigator may also be able to recover system logs that show when he modified and deleted the files in question, this information and that recovered from the emails can be used to create a timeline of events that can be used as evidence of guilt. Throughout the analysis process it is vital that the chain of custody be maintained with rigorous record keeping and ensuring all data is stored securely to avoid any unauthorized persons from tampering with the data with the aim to discredit the investigation. Once all of the analysis has been completed and a satisfactory amount of evidence has been found and collected the investigator will then need to present their findings through a report.

Post investigation phase

When it comes to compiling a report there are many areas that should be covered, and most reports will have a somewhat standardized format. This format will usually start with the

purpose of the report, this will tell the reader what is going to be covered and why, then comes an overview of the incident that has caused the investigation to take place this is crucial to establish the context of the evidence, then the evidence itself is presented to the reader in an unmodified state so that the reader can if necessary draw their own conclusions from the presented evidence, then comes the conclusion and further details section, this is where the report writer will give their interpretation of the evidence and summarize their findings. The report must document all of the steps taken during the analysis and show that the most rigorous standards were followed when ensuring the data's integrity has been maintained, this is done by showing that the rules of evidence have been maintained, these rules are. Admissible, the data must be allowed by a court of law and must follow the rules of evidence collection. Authentic, the evidence must not have been altered in anyway by the analyst throughout the course of the investigation. Complete, if you find evidence that contradicts your point of view you must still include it to have a fair report. Reliable, the evidence must have been collected and handled by reliable software and qualified persons so that its reliability cannot be questioned. And finally, the evidence must be believable, there should not be any massive jumps and conclusions drawn that are not supported by evidence.

Finally, if the investigation is as part of a criminal investigation or becomes one there is a chance that the investigator (if qualified) may be asked to act as an expert witness in a court proceeding. In this situation the expert will be asked to summarize a case and the technical details that are involved in the report and will need to educate the members of the court on the facts and what they mean, however the expert should not try to persuade the parties towards one conclusion as they are only there to state the facts and let the parties draw conclusions from this information.

Sample report

Below is an example of a forensics report that might be created following the investigation conducted by Troy Simpson. The report is a template created by Nebraska Elmrabit

from Glasgow Caledonian University [23]. The report has been edited to show the type of information that might be included in the context of the CMMC investigation.

Investigation Report

Case Against: Rich Daley

Case No: 12345678

Report compiled by Troy Simpson

Date of investigation 12/3/25 - 20/4/25

Date report compiled 25/4/25

Endorsement

The contents of this report are the result of an investigation undertaken by myself, and I hereby confirm that:

1. The investigation was conducted in accordance with the UK ACPO principles.
2. The software and hardware used to support this investigation were prepared and used in a manner designed to assure the forensic integrity of both the process and its outcomes.
3. The **opinions** presented at the end of this report are mine and mine alone and are based solely on the evidence found.

Signed by Troy Simpson [**Signature**]

Date [**25/4/25**]

Executive Summary

This report aims to establish present the evidence and facts that show that the employee of CMMC Rich Daley has been complicate in the wilful destruction of company property and has engaged in actions aimed at distributing propriety company property for financial gain. All of the evidence presented in this report has been gathered from the accused's work devices and has been analysed and stored using the most rigorous industry practices.

Contents

<u>1. Credentials of the Investigator.</u>	<u>4</u>
<u>2. Purpose of the Investigation.</u>	<u>4</u>
<u>3. Target Systems and Devices.</u>	<u>4</u>
<u>4. Software to be Used in Support of the Investigation.</u>	<u>4</u>
<u>5. Investigation Methodology.</u>	<u>5</u>
<u>6. A Graphical Timeline of the incident.</u>	<u>5</u>
<u>7. Evidence Acquisition.</u>	<u>6</u>
<u>8. Analysis of the Evidence.</u>	<u>6</u>
<u>9. Summary and Finding in Relation to the Case.</u>	<u>6</u>
<u>References.</u>	<u>6</u>
<u>Appendix 1.</u>	<u>6</u>

1. Credentials of the Investigator

In this section of the report the investigator would state their qualifications and the experience they have in the field of digital forensics and possibly include some examples of other cases they have worked on. All of this is in an effort to help persuade the reader to have confidence in the validity of the findings that are presented and have confidence that the processes carried out to come to these conclusions were done to the highest standards.

2. Purpose of the Investigation

This investigation is being conducted on the request of CMMC after they raised suspicion that one of their employees had been involved in malicious practices against the company. The purpose of this report is to establish the facts of the case against the accused and determine if there is evidence of his complicity in these actions.

3. Target Systems and Devices

Item # 1

A desktop computer that is owned by CMMC that was used by the accused. This device has been analysed with the permission of CMMC.

Photos of the device can be included here.

4. Software to be Used in Support of the Investigation.

The investigation of the aforementioned systems and devices was conducted using the **X** forensics software. All software used during the duration of this investigation is fully licensed and follows industry and legal standards.

5. Investigation Methodology

- Identification
- Preservation
- Collection
- Examination and Analysis
- Documentation
- Reporting
- Presentation of Findings

6. A Graphical Timeline of the incident

A timeline of events that can be included to give the reader an overview of how the incident occurred so that the reader will have context when examining the evidence that will be presented later on in the report. For the case of CMMC this could be a timeline of when the accused first contacted the third party and the dates of key communications and finally when he actually deleted the data and stole the information.

7. Evidence Acquisition

All of the evidence used in this report was gathered by the analysis of a bit for bit copy of the suspect's work on the computer HDD. This was analysed for evidence of the accused's actions through the reviewing of system logs and emails.

8. Analysis of the Evidence

In this section of the report an in-depth analysis of all of the evidence that you have found and how it relates to the case. In this case emails could be examined and for evidence of suspicious communication with a third party which can be used to show the likelihood of guilt.

9. Summary and Finding in Relation to the Case.

In this section the evidence will be summarized with the key findings from the analysis presented in a way so that a judgment can be drawn from the evidence as a whole and how those points towards the possible guilt of the accused.

References

References to any tools or resources used to find the evidence or compile the report.

Appendix

Any additional material that may be relevant to the report or the investigation can be included here.

References

[1] Sleuthkit.

"Autopsy." <https://www.sleuthkit.org/>. <https://www.sleuthkit.org/autopsy/> (accessed Aug 29).

[2] Open source Initiative. "OSI Approved Licenses." Open source Initiative. <https://opensource.org/licenses> (accessed Aug 29).

- [3] sleuthkit.org. "www.sleuthkit.org: About." sleuthkit.org. <https://www.sleuthkit.org/about.php> (accessed Aug 29).
- [4] sleuthkit.org. "Autopsy: License." sleuthkit.org. <https://www.sleuthkit.org/autopsy/licenses.php> (accessed Aug 29).
- [5] sleuthkit.org. "Autopsy: Features." sleuthkit.org. <https://www.sleuthkit.org/autopsy/features.php> (accessed Aug 29).
- [6] bcarrier. "Autopsy 4.22.1." github. <https://github.com/sleuthkit/autopsy/releases> (accessed Aug 29 ,25).
- [7] gdicristofaro. "autopsy /README.txt." github. <https://github.com/sleuthkit/autopsy/blob/release-4.22.1/README.txt> (accessed Aug 29)
- [8] K. Libby. "Autopsy: The Digital Forensics Toolkit - eForensics." <https://eforensicsmag.com/>. <https://eforensicsmag.com/autopsy-the-digital-forensics-toolkit/> (accessed Aug 29).
- [9] <https://www.exterro.com/>. "FTK Forensic Toolkit." <https://www.exterro.com/>. <https://www.exterro.com/digital-forensics-software/forensic-toolkit> (accessed Aug 29).
- [10] <https://www.exterro.com/>. "Create Forensic Images with Exterro FTK Imager." <https://www.exterro.com/>. <https://www.exterro.com/digital-forensics-software/ftk-imager> (accessed Aug 29 , 25).
- [11] C. Dodt. "Computer forensics: FTK forensic toolkit overview [updated 2019]." Infosec. <https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-ftk-forensic-toolkit-overview/> (accessed Aug 29).
- [12] V. Agbooda, J. Osamor and F. Olajide, "Evaluating the Efficiency of FTK, Autopsy, and Mobile Forensic Tools: A Comparative Study in Criminal Investigations," *International Journal of Intelligent Computing Research (IJICR)*, vol. 15, no. 1, 2024. Accessed: Aug 29, 2025, [Online]. Available: <https://infonomics-society.org/wp-content/uploads/Evaluating-the-Efficiency-of-FTK-Autopsy-and-Mobile-Forensic-Tools.pdf>
- [13] exterro.com. "FTK 8.1 Physical License." exterro.com. <https://store.exterro.com/products/ftk-8-0> (accessed Aug 29).
- [14] OpenText Forensic. "Forensic data acquisition, triage, and analysis for law enforcement, agencies, and corporations." <https://www.opentext.com/media/product-overview/opentext-forensic-po-en.pdf> (accessed Aug 29).

- [15] J. Williams. "One-Click Forensic Analysis: A SANS Review of EnCase Forensic." SANS Institute. <https://www.sans.org/media/analyst-program/Product-Review-One-Click-Forensic-Analysis.pdf> (accessed Aug 29).
- [16] apple.com. "Mac computers with the Apple T2 Security Chip." apple.com. <https://support.apple.com/en-us/103265> (accessed Aug 29).
- [17] <https://www.opentext.com/>. "Digital Forensics Software | OpenText Forensic." <https://www.opentext.com/>. <https://www.opentext.com/en-gb/products/forensic> (accessed Aug 29).
- [18] .wireshark.org. "Wireshark Frequently Asked Questions." .wireshark.org. <https://www.wireshark.org/faq.html#sec1> (accessed Aug 29).
- [19] Wireshark. "Wireshark." gitlab.com. <https://gitlab.com/wireshark/wireshark> (accessed Aug 29, 25).
- [20] wireshark.org. "About Wireshark." wireshark.org. <https://www.wireshark.org/about.html> (accessed Aug 29).
- [21] cellebrite.com. "Cellebrite UFED." cellebrite.com. <https://cellebrite.com/en/ufed/> (accessed Aug 29).
- [22] dataexpert.eu. "Cellebrite Pathfinder." dataexpert.eu. <https://www.dataexpert.eu/products/mobile-forensics-cellebrite/cellebrite-pathfinder/> (accessed Aug 29).
- [23] N. Elmrabit, "Digital Forensic Expert Opinion Report Template," Glasgow Caledonian University, Accessed: Aug 29, 2025.
[Online]. https://www.researchgate.net/publication/375911176_Digital_Forensic_Expert_Opinion_Report_Template
- [24] microsoft.com. "Simple black & purple commercial invoice." microsoft.com. <https://create.microsoft.com/en-us/template/simple-black-%26-purple-commercial-invoice-0eed7676-b2f0-4b4b-9a44-093f37ae2b9b> (accessed Aug 29).



FINAL GRADE

GENERAL COMMENTS

65/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

GRADING FORM: L5 CF (ACCD5000)

MAX BEASLEY

65

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)



Source variety with clear referencing. However, it is lacking peer reviewed articles. Some minor inconsistencies in citation formatting

13

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)



Clear understanding of tools, though some explanations could be more concise or better structured.

6

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)

40



Logical progression in both tasks with comparisons and conclusions. More critical depth could be added in Task 2.

You could outline/list/document the forensics methodology steps/stages Barry would take.

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 not done the invoice for services provided or generated a sample forensics report using a forensics tool such as FTK. However a sample one has been adapted.

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)

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)



Structure is logical and format is mostly followed. Try to avoid long paragraphs in some areas and using first person tense such as "I". Could benefit from better text justification.

6