



INDIVIDUAL ASSIGNMENT

TECHNOLOGY PARK MALAYSIA

CT113-3-M-ADF

ADVANCED DIGITAL FORENSICS

HAND OUT DATE: 21 November 2024

HAND IN DATE: 7 February 2025

INSTRUCTIONS TO CANDIDATES:

1. This is an individual assignment consisting of 1 Section
2. Answer **ALL** questions
3. You will be given time as specified above to complete the assignment and submit it online through Moodle
4. Please contact the module lecturer before the start of the assessment should you need any clarification



INDIVIDUAL ASSIGNMENT

NAME (TP NUMBER)	:	Koo Wai Kit (TP081761)
INTAKE CODE	:	APUMF2406CYS
MODULE TITLE	:	Advanced Digital Forensics (102024-MSB)
MODULE LECTURER	:	Dr. Mohamed Shabbir
PROJECT TITLE	:	ADF Individual Assignment (Digital Forensics Procedure and Practical Investigation)
DATE ASSIGNED	:	21 November 2024
DATE COMPLETED	:	7 February 2025

Contents

1. Executive Summary	4
2. Introduction.....	5
3. Digital Forensics Procedure.....	5
3.1 Authorization and Preparation	5
3.1.1 General Procedures	6
3.1.2 Application to the Case Study.....	7
3.2 Evidence Handling.....	7
3.2.1 General Procedures	7
3.2.2 Application to the Case Study.....	8
4. Practical Investigation.....	9
4.1 Analysis and Examination	9
4.1.1 General Procedures	10
4.1.2 Performing Analysis and Examination Using Autopsy.....	10
4.2 Reconstruction and Reporting.....	13
4.2.1 General Procedures	13
4.2.2 Using Autopsy for Better Reconstruction and Reporting.....	14
4.2.3 Event Reconstruction	14
5. Conclusion	15
6. References.....	17
Appendix A.....	18

List of Figures

Figure 1: Types of files present on the disk	11
--	----

1. Executive Summary

The allegations of unauthorised activities carried out by an employee on the company's network were the cause of this forensic investigation. The main goal of the investigation was to find out whether the employee had committed malicious activities, including unauthorised access, data interception, and the use of hacking tools. The investigation, which analysed digital evidence recovered from the employee's workstation, was used to look for conclusive evidence of wrongdoing and to provide a solid case for legal or disciplinary action.

In order to achieve these objectives, standard forensic procedures were followed, and the integrity of the evidence was maintained. The methodology was structured with stages including authorization and preparation, evidence handling, analysis and examination, and reconstruction and reporting. Autopsy, an open source digital forensic platform which can index the file systems, recover deleted files and analyse the user activity, was the primary forensic tool. To track the suspect's activities, various forensic techniques were used, such as keyword searches, examination of the registry as well as the examination of event logs.

The investigation finds an apparent association with suspicious user account 'Mr. Evil' to repeated login, unauthorized network activity and use of hacking tools.. Further research revealed that the registered owner of the system, Greg Schardt, was also linked to the "Mr. Evil" account, which was an attempt to hide his identity. Intercepted network traffic, shell bags pointing to directories like "ENUMERATION" and "EXPLOITATION," along with the presence of hacking tools like Ethereal, Cain & Abel and John The Ripper showed that the employee was actively trying to conduct malicious activities. The discovery of a zip bomb and software related to botnets also indicated the possibility of conducting other cyberattacks.

This investigation provides conclusive evidence that the employee was engaged in unauthorised and potentially malicious activities. The compiled forensic report not only confirms the allegations of the company, but it is also a legally admissible document for further actions. Continued monitoring, strict access controls, and diligence in security awareness are critical to mitigate insider threats, as these findings demonstrate. The outcome of this investigation highlights the critical role of digital forensics in identifying and addressing security breaches within an organisation.

2. Introduction

Digital forensics is a very important field of investigation, in which digital evidence is identified, collected, preserved, analysed, documented and presented in a manner that is legally acceptable (Slonopas, 2024). With technology advancing, so do the methodologies and tools used by cyber criminals, thus, organizations have to resort to implement effective forensic procedures to secure its network and data from being exploited. This report details the steps and techniques used in the investigation of an employee accused of committing malicious and illegal activities over a company network.

The goal of this report is to provide the results of the digital forensic investigation on the employee's computer system, with a particular focus on memory imaging, hard disk acquisition and data analysis. The goal for a forensic analyst is to prove or disprove the charges levied against the employee. All investigation will be conducted in accordance with established digital forensics procedures and results will be valid and admissible in a court of law.

The structure of this report is based on the guidelines of digital forensic investigation, and it covers the following key areas: the digital forensics procedure, the practical investigation process, and the supporting evidence obtained during the investigation. It aims to offer a full view of the investigation so that the evidence is handled properly and the findings reported accurately, in order to achieve a fair conclusion to the case.

3. Digital Forensics Procedure

Digital forensics procedure is a systematic approach to handle the integrity and reliability of evidence in an investigation. This section outlines the authorization, preparation and evidence handling steps of the procedure.

3.1 Authorization and Preparation

Authorization and preparation deal with the initial steps needed before a digital forensic investigation can be carried out. This phase is to ensure all actions taken during the investigation are legally and ethically sound. It covers the acquisition of legal authorization, setting up of forensic tools and environment, proper documentation of the evidence, and ensuring a secure chain-of-custody.

3.1.1 General Procedures

3.1.1.1 Legal Authorization

Before any evidence is gathered, investigators are required to have proper legal authorization. It can be search warrants, written consent from the organisation or other forms of legal orders that comply with national and international legislation. Such legal permission not only legitimises the investigation but also supports the chain-of-custody that is necessary in court proceedings (Interpol, 2021).

3.1.1.2 Team and Tool Preparation

The next step after legal authorization is granted is to prepare the required tools and the forensic environment. Being the forensic analyst, I have to make sure that the right tools are picked, and the forensic team is prepared to take on the task. Even though my team could consist of a first responder and other specialists, my job as the forensic analyst is to collate and analyze the evidence using validated forensic tools. To maintain the integrity of the data, it is necessary to use court-accepted tools like EnCase, FTK or Autopsy, which allow for the creation of bit-for-bit copies and the generation of hash values like SHA-256 (Neel, 2024).

3.1.1.3 Documentation and Chain-of-Custody

Integrity and authenticity of the evidence are ensured by initial documentation. It includes recording information like the device details, the physical condition of the device, and active network connections. In addition, photographs of the scene are taken to illustrate the context of the evidence and to reinforce its authenticity. These steps are also important to set up a solid record of the evidence that was found (Office of Justice Programs, 2008). Another important aspect in maintaining the validity of the evidence is the chain-of-custody. There must be a thorough log that goes into the details of each individual who touched the evidence, the timestamps, and the reasons why in different transfers and handling. The importance of meticulous tracking at every step of the investigation is demonstrated by the fact that any gaps or inconsistencies in this log could render the evidence inadmissible in court (Karush, 2024).

3.1.1.4 Ethical and Legal Review

Before extracting and analysing data, all methods should be compliant with applicable legal frameworks, such as the Personal Data Protection Act (PDPA) (MyGovernment, n.d.). It involves going through the legal boundaries to accessing and extracting data, for instance, the cloud data or encrypted files. It is also important to anticipate potential problems such as encrypted drives or anti-forensic techniques. Legal counsel's involvement in the review process

diminishes risks and ensures that the forensic procedures are done legally, so that the evidence is not overreached and will be admissible in court (Kasper & Laurits, 2016).

3.1.2 Application to the Case Study

For the case study, the digital forensics team can acquire the memory image from the employee's computer, supported by documented authorization from the IT company, and any required judicial orders. It ensures that when the investigation is conducted, all actions that are taken are legal and that the data remains intact. Using Autopsy, a validated forensic analysis tool, I will examine the disk image that was provided for me to analyse. The in-depth examination of the disk image in autopsy can reveal any suspicious activity, hidden files and anomalies (Libby, 2023).

Furthermore, in the analysis, I will create hash values to verify that the image was not tampered with, so this image is credible and admissible in court. The chain-of-custody form was not shared by the first responder, but the disk image was provided by them. The form may have been created and maintained by the first responder, however I will be documenting my own chain-of-custody to keep track of the evidence throughout the investigation. It was also established that the employee's workstation data was corporate owned, ruling out any privacy concerns under PDPA. In addition, the pre-investigation review did not find any encrypted data. I remained proactive and made sure that each step taken in the investigation followed legal and ethical standards.

3.2 Evidence Handling

The focus of evidence handling is on the procedures for handling digital evidence after it has been collected. This phase is to protect the integrity of the evidence, store and handle the evidence securely throughout the investigation. This includes keeping a detailed chain-of-custody log, keeping the evidence in a controlled environment, creating forensic duplicates to retain the original data, and handling volatile evidence such as RAM contents.

3.2.1 General Procedures

3.2.1.1 Chain-of-Custody and Documentation

The chain-of-custody logs have to be detailed for every piece of digital evidence, including who collected the evidence, when and where, where it was stored, and what actions were performed on it. The evidence has to be shown not tampered with or contaminated throughout the investigation and this is important documentation. Interpol Guidelines for Digital Forensics

First Responders highlight the significance of the complete and unbroken chain-of-custody to provide evidentiary value of digital artefacts (Interpol, 2021).

3.2.1.2 Secure Storage and Access Control

Evidence that has been collected needs to be stored in a secure environment, such as an evidence locker or a dedicated secure server, available only to people with appropriate access. This controlled storage also provides the added benefit of ensuring that the evidence is not tampered with by unauthorised personnel. There may be secure handling measures such as using tamper-evident seals and environmental controls to protect both the physical medium and the data on it.

3.2.1.3 Forensic Duplication and Verification

Investigators acquiring digital evidence, particularly volatile data such as those found on memory images or hard disk contents, should use forensically sound methods like write blockers when creating bit-for-bit copies. This duplicated evidence is then hashed using methods such as MD5 or SHA-1, to create a digital fingerprint that can be used later to check that the copy is identical to the original. This step is critical so that any subsequent analysis is performed on an exact replica of the source data, not on any altered version of it.

3.2.1.4 Handling Volatile Evidence

If the digital device is still active, extra precautions must be taken to record volatile evidence such as RAM contents, before the system is shut down. To minimise any impact on data integrity, live acquisition tools must be used carefully. In order to justify the chosen method and support the reliability of the evidence in court, detailed documentation of the live acquisition process is necessary.

3.2.2 Application to the Case Study

In the context of the case study, the evidence handling phase is of utmost importance as the company is investigating allegations that a key employee is engaged in malicious activity on the network. A memory image has already been acquired from the employee's computer hard disk by a first responder. Upon acquisition, this image was documented, labelled, and sealed in accordance with forensic best practises immediately. Validated imaging tools such as Autopsy were used, along with write-blocking devices so that the memory image is an exact, bit-for-bit duplicate of the original system state. This method preserved all volatile and non-volatile data without any alteration and thus the integrity of the evidence was maintained.

A detailed chain-of-custody log was kept throughout the process of the seizure of the computer at the scene, the imaging process, and the secure transfer of the memory image to the forensic lab. A digital evidence log establishes the authenticity of the digital evidence containing timestamps, identity of each handler and storage conditions. The reason is that if the evidence is ever challenged in court, such rigorous documentation is crucial.

The memory image was stored in a controlled forensic environment with restricted access once it was acquired. This secure storage prevents unauthorised access and prevents alteration of the evidence during subsequent analysis phase. The integrity of the evidence is upheld as only authorised forensic analysts are allowed to access and work with the evidence.

To start any further analysis, the forensic team ensured the memory image was valid and verifiable by generating cryptographic hash values against them. The hash values are used as reference points for comparison in the future and attest the digital evidence has not been tampered with since it was first acquired.

4. Practical Investigation

In the section of the investigation, as a forensic analyst, I will analyse two disk images, 4Dell Latitude CPi.E01 and 4Dell Latitude CPi.E02, to prove or disprove the allegations the company made against the employee. In a thorough analysis of both disk images, any signs of malicious activity or unauthorised activity will be uncovered. To perform this analysis, I will use Autopsy, a very powerful digital forensics tool, to thoroughly examine the data and extract the information that will help further the investigation's findings. The process will involve recovering data, identifying artefacts, analysing the system's contents and attempting to find any evidence of misconduct. All screenshots taken will be included in Appendix A for reference.

4.1 Analysis and Examination

Analysis and examination are crucial steps in the digital forensic process. During this phase, the forensic analyst examines the acquired digital evidence to extract, interpret and correlate data which can support or refute the case hypothesis. As such, this stage is performed on a forensic copy of the data to preserve the evidence's integrity and to ensure that all subsequent findings can be used in court.

4.1.1 General Procedures

Forensic examiners check the integrity of the acquired image before diving into the data by verifying the hash values of the image are in accordance with the hash values recorded during the acquisition phase. This guarantees that the data is not corrupted and in its original form.

Furthermore, investigators carry out systematic searches for any important files, log entries, and metadata. Techniques like file carving, keyword searches and timeline analysis are used to recover deleted files and reconstruct user activity. For instance, analysis may include examining file headers, file slack, unallocated space to locate unseen or erased data (Infosec, 2019). All steps are documented meticulously throughout the analysis. Logs and reports of the methodologies used, the tools applied, and the evidence gathered are detailed. This documentation is crucial for the reporting phase.

4.1.2 Performing Analysis and Examination Using Autopsy

4.1.2.1 Autopsy Case Setup

To analyze the files in Autopsy, first, I open Autopsy and create a new case. Once the case is set up, I click on “Add Data Source” to add the disk images as data sources for investigation. I select “Disk Image or VM File” from the options and then browse to locate the E01 file on my system. After selecting the file, I choose the appropriate options, such as including or excluding specific partitions, depending on what I need to investigate. Additionally, since Autopsy automatically recognises the E02 file when the E01 file is added, I will only need to include the E01 file in the case and the E02 file will be automatically included by the software.

4.1.2.2 Autopsy Interface and Capabilities

Autopsy’s ingest modules can index the file system, recover deleted files, and parse data from installed applications. For example, the timeline analysis module summarizes MAC times (Modified, Accessed, and Created) in order to recreate the user’s activity in a visual representation, and the keyword search module focuses on highlighting data based on the terms defined. With the Autopsy’s browser-like interface, I can browse through the hierarchical file system, check file attributes, and review detailed reports. In addition, Autopsy can also be integrated with additional modules, such as registry analysis and web artifact extraction, to gain even more in-depth knowledge about how the system is used and potentially unusual cases. All enabled modules are shown in Screenshot 4 under Appendix A. The findings can also be exported in HTML or PDF formats.

4.1.2.3 Relevant Artefacts That Can Be Analyzed

A possible analysis may be to look at specific artefacts of the user's activity and login patterns by reviewing user accounts, login timestamps, and system event logs in search for evidence of abnormal behaviour. Furthermore, the installed applications and their metadata could be examined to identify any unauthorised software that may be involved in malicious activity. Files in the file system and network logs may also be scrutinised for indicators of data exfiltration, like, for instance, unusual file transfers or network connections.

Additionally, Autopsy can recover files that were intentionally deleted to cover evidence, and these files can be thoroughly examined. In order to come to a better understanding of the employee's activities, system artifacts like browser history, email logs and temporary files may also be investigated. With this, it will be known if the employee's actions were in line with suspected malicious behaviour or if they were part of normal operational tasks.

4.1.2.4 Artifacts Analyzed and Results

After adding the disk image as a data source and Autopsy done analyzing it, a lot of information is obtained. A summary of the files is shown under Figure 1.

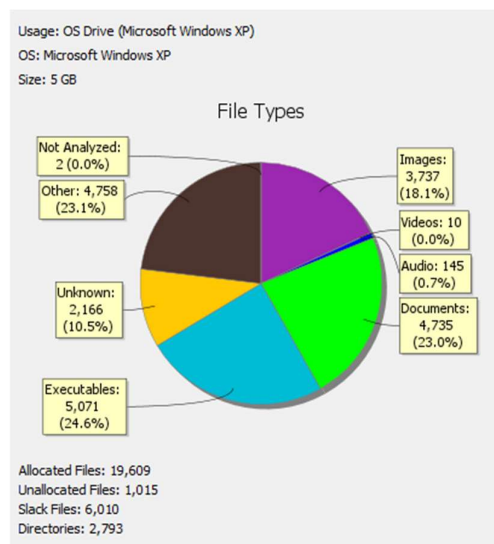


Figure 1: Types of files present on the disk

Due to the extensive nature of a digital forensic investigation, only information that can contribute to the investigation outcomes will be discussed here.

There are a total of 8 OS accounts on the device. I found a suspicious account with the login name "Mr. Evil," and the home directory of the account is located at /Documents and Settings/Mr. Evil. After further checking, it can be determined that Mr. Evil is the one who used the computer the most, with a total login count of fifteen times.

Next, I want to find out who is the owner of the computer. I found out that the registered owner is named "Greg Schardt" by looking into the Windows NT folder under directory C:\Windows\system32\config\Software\Microsoft\Windows NT. Upon further checking, I can determine that the last user logged on to the computer was Mr. Evil by checking the Winlogon subdirectory. By using the Keyword Search feature, I searched for "Greg Schardt" to find information related to this owner. From the results returned, in the file named "irunin.ini", there is indication that Greg Schardt is Mr. Evil, since %REGOWNER%=Greg Schardt and %LANUSER%=Mr. Evil entries were found in the file. The %REGOWNER%=Greg Schardt entry indicates that "Greg Schardt" is the registered owner of the system, and the presence of %LANUSER%=Mr. Evil suggests that the user account "Mr. Evil" may have been created or configured by the registered owner.

Furthermore, by inspecting the installed programs, several programs that could be used for malicious activities were identified. 123 Write All Stored Passwords, Ethereal, Cain & Abel v2.5 beta45, Look@LAN 2.50 Build 29, Network Stumbler 0.4.0, and WinPcap 3.01 alpha are tools that can pose significant security risks. Ethereal, which was the original name for Wireshark, can be used to intercept wired and wireless packets (Digi, 2024). Under the Mr. Evil subdirectory, there is a folder named "Ethereal". This is most probably the directory for the Ethereal software. By checking the directory, I found a file named "recent" which shows information about a recent packet capture file saved in C:\Documents and Settings\Mr. Evil\interception. Examining the 'interception' file provides a lot of insights into the device and user involved in the interception. The target's device is identified as a wireless computer running Windows CE (Pocket PC) - Version 4.20.

Additionally, there are several shell bags created by Mr. Evil with paths to directories like EXPLOITATION and ENUMERATION. By looking into these directories, it was discovered that there are many hacking tools like John The Ripper and Brutus installed. This may indicate that Mr. Evil is actively searching for ways to exploit the system.

Moreover, the Recent Documents tab in Autopsy shows files from mIRC, an IRC client often associated with botnets, suggesting potential use for command-and-control communication.

The Anonymizer folder with keys.txt indicates the use of anonymity tools, possibly for concealing illicit activity. The GhostWare folder, especially with files like Receipt.rtf, suggests stealthy malware tools designed to evade detection. Additionally, the presence of a network path (\\4.12.220.254) points to possible remote access or data exfiltration.

In the Autopsy analysis, a potential zip bomb was found in the Interesting Files section under the name 'unix_hack.tgz'. This file appears to be a compressed archive, and zip bombs are known for their ability to decompress into an extremely large size, potentially overwhelming system resources. This could be an attempt to disrupt system performance or evade detection.

4.2 Reconstruction and Reporting

This phase is where the evidence is organised in order to understand what happened and whether the employee was involved in the alleged activities. Finally, the results are documented in a clear and detailed report.

4.2.1 General Procedures

Reconstructing is about combining the evidence to make a coherent story by creating a chronology of events. The forensic analyst uses file timestamps, system logs, and user activity records together to determine a series of actions. It involves connecting events across different data sources, such as file created, modified, or accessed times, to guarantee the timeline's accuracy and reproducibility. Cross-referencing the metadata and the log data events provides an opportunity to correlate these events and identify the relationships between artifacts and create a more robust narrative. The advantage of this is that it serves as validation of the initial hypothesis, filling out any holes or resolving any inconsistencies. Once the timeline is reconstructed, the analyst can determine if the employee was involved in the alleged activities and whether the evidence is legally sound.

In addition, reporting involves translating the technical findings into a clear and concise document which is suitable for legal proceedings. Forensic investigation report must document in detail how the report has been conducted, including the methodologies, the tools used, the results obtained. The findings should be explained in clear and objective language so that it is easy for non-technical stakeholders to understand what the significance of evidence is. Using visuals such as timelines and annotated screenshots, adds that supporting narrative and helps complicated data to make sense. The report should also be reproducible, that is, another expert should be able to follow the same procedures and come to the same conclusions. This is a

means of ensuring the legitimacy of the investigation and serving a useful purpose of a solid grounding for expert testimony in court.

4.2.2 Using Autopsy for Better Reconstruction and Reporting

In the reconstruction and reporting stage of the investigation, I used Autopsy to simplify the process and to guarantee a thorough analysis. The Timeline Analysis module of Autopsy automatically aggregated key file metadata, such as creation, modification and access times, as well as system logs, for the reconstruction. This helped me quickly see and understand the critical events, periods of high activity, and any anomalous events. With the help of the events filtering, I could filter events by user account, file type or keywords, and focus on the most relevant moments in the timeline. Autopsy's artifact correlation capability also enabled me to correlate and link various digital artifacts, including registry entries, browser histories, and email records, in order to reconstruct what the employee did.

For the reporting phase, Autopsy provided an automated report generation, where all analysis results such as timelines, keyword search results, file metadata are compiled into a comprehensive report. The reports were available in HTML or PDF format, so they could easily be shared and presented. Also, I also used Autopsy's capability to add customizable documentation within the tool, through annotations and narrative explanations. This allowed me to modify the content to fit to the requirements of the audience – to maintain some level of technical details, as well as to make the outcome more accessible to the people who are not technical. The final report enabled a reproducible record of the forensic analysis, reporting all methodologies and document findings in a manner suitable for legal proceedings.

4.2.3 Event Reconstruction

Several critical findings on the device were uncovered by the event reconstruction process. Fifteen attempts were logged in through the "Mr. Evil" account, which is a highly suspicious account, implying active use. Also, "Greg Schardt" was registered as the owner, and there are some links between him and Mr. Evil, so they could be the same person. There was malicious software, including Ethereal, Cain & Abel and Network Stumbler, that could indicate network sniffing and password cracking. Notably, under the Mr. Evil subdirectory, there was a folder called 'Ethereal' that contained a file that led to the recent packet capture activity, which showed the interception of network traffic. Moreover, multiple shell bags were found leading to directories like "EXPLOITATION" and "ENUMERATION" with their directory listing

containing hacking tools like John The Ripper and Brutus, which can indicate system exploitation.

In recent documents analysis, there are files like mIRC that are often associated with botnet activity, as well as an Anonymizer folder which could suggest efforts to conceal illicit activities. There was a network path (\4.12.220.254) which can imply remote access, and the presence of a zip bomb “unix_hack.tgz” could indicate an attempt to disrupt system resources or evade detection. Combining these findings and matching them with the system logs can help reconstruct timeline of malicious activities on the device.

5. Conclusion

The evidence gathered through a thorough and methodical digital forensic investigation of the employee’s computer, primarily through analysis of the acquired memory image, is very compelling in support of the company’s allegations of malicious network activities. Despite the employee denying any knowledge of the offence, the thorough examination based on established forensic procedures has produced several critical findings:

- i. **Evidence of Suspicious User Activity:** The investigation revealed a specific user with a user account named “Mr. Evil,” that had been involved with a significant amount of network activity. Timeline analysis and log examination showed that this account was in active use on the affected machine with indications of events that were not normal operational behaviors.
- ii. **Discovery of Hacking Tools and Artifacts:** The forensic analysis determined installation of various applications that when executed, could potentially be used to accomplish unauthorized activities, such as network sniffing and password cracking. Additional artefacts related to these tools, including directories containing Ethereal script, and folders labelled “EXPLOITATION” and “ENUMERATION” can indicate that the system was in use for nefarious means.
- iii. **System Anomalies:** The discrepancies revealed in correlation of file metadata, registry information and system logs indicate attempts to obfuscate the true nature of the system’s use. An example of this is cross-referencing the entries of the operating system’s configuration files to establish a connection between the registered owner (“Greg Schardt”) to the suspicious user account (“Mr. Evil”), and it can be assumed that the latter was most likely an alias used to hide malicious intent.

The findings from all of these were reconstructed employing validated forensic methodologies, and documented in rigorously chain-of-custody procedures. Together with its excellent timeline analysis and keyword search capabilities, Autopsy's use made sure that every important artifact was found, and contextualised in a coherent story. With this approach, the resulting report contains precise, reproducible logs showing the history of the investigation, screenshots, and cross-verified hash values.

In conclusion, the digital forensic evidence confirms the company's claims against the employee. The findings indicate that the employee's actions were not in accordance with the legitimate business operations and were instead in line with a pattern of deliberate, malicious network activity. This evidence is credible and admissible in court, which adds up to a strong case for any following legal proceedings.

6. References

- Digi. (2024, January 1) How to install and use wireshark (ethereal) for ethernet packet sniffing. <https://www.digi.com/support/knowledge-base/how-to-install-and-use-wireshark-ethereal-for-ethe>
- Infosec. (2019, July 6). *Computer forensics: forensic analysis and examination planning*. <https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-forensic-analysis-examination-planning/>
- Interpol. (2021, March). *Guidelines for digital forensics first responders*. https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf
- Karush, S. (2024, October 27). *Legal considerations and challenges in cyber forensics*. Cyber Secure. <https://cybersecure.monster/legal-considerations-and-challenges-in-cyber-forensics/>
- Kasper, A., & Laurits, E. (2016). Challenges in collecting digital evidence: a legal perspective. *The future of law and eTechnologies*, 195-233.
- Libby, K. (2023, October 3). *Autopsy: the digital forensics toolkit*. eForensics. <https://eforensicsmag.com/autopsy-the-digital-forensics-toolkit/#:~:text=Drone%20Analysis,external%20hard%20drive%20or%20USB.>
- MyGovernment. (n.d.). *Personal data protection act*. <https://www.malaysia.gov.my/portal/content/654>
- Neel, A. (2024, October 29). *Digital evidence: collection, preservation and forensic analysis*. Legal Bites. <https://www.legalbites.in/forensic-law/digital-evidence-collection-preservation-and-forensic-analysis-1074008>
- Office of Justice Programs. *Electronic crime scene investigation: a guide for first*

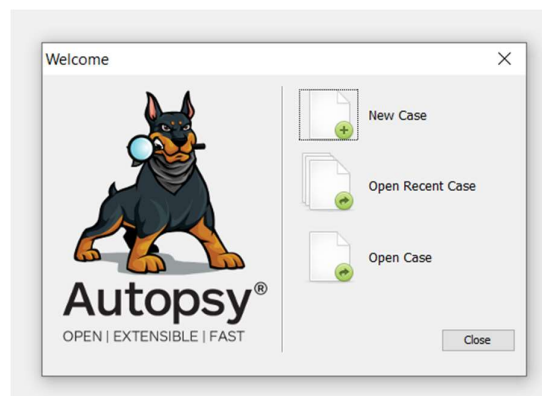
responders, second edition. U.S. Department of Justice.

<https://www.ojp.gov/pdffiles1/nij/219941.pdf>

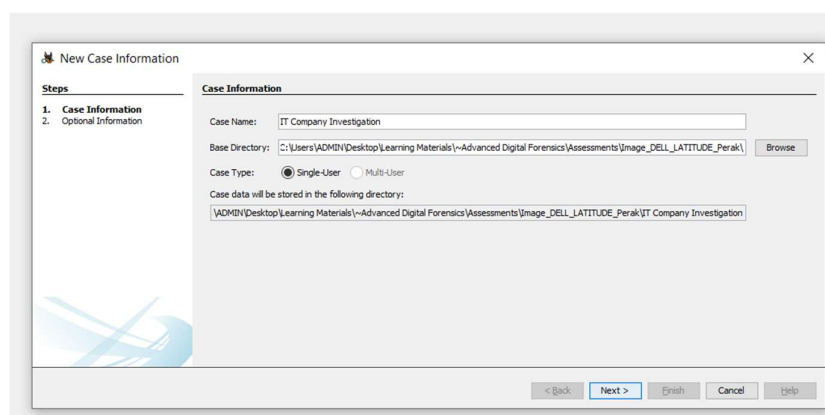
Slonopas, A. (2024, March 22). *What is digital forensics? a closer examination of the field*.

American Public University. <https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-digital-forensics/>

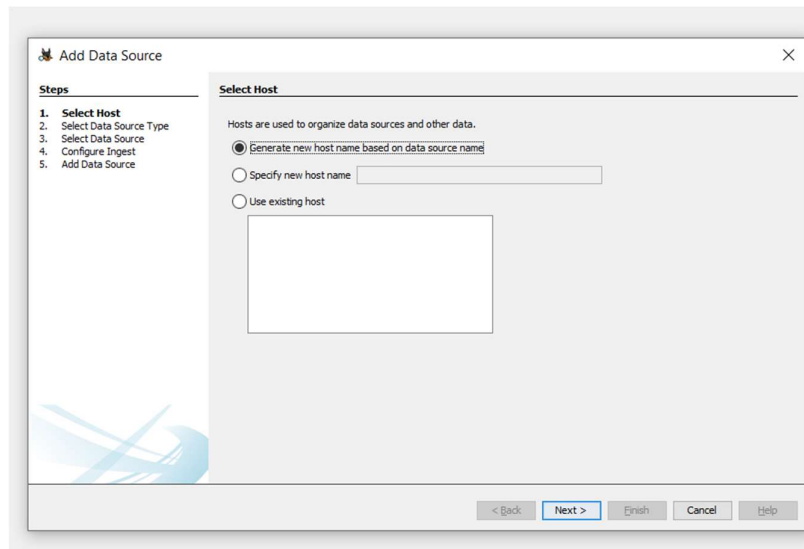
Appendix A



Screenshot 1: Creating new case in Autopsy



Screenshot 2: Entering case information

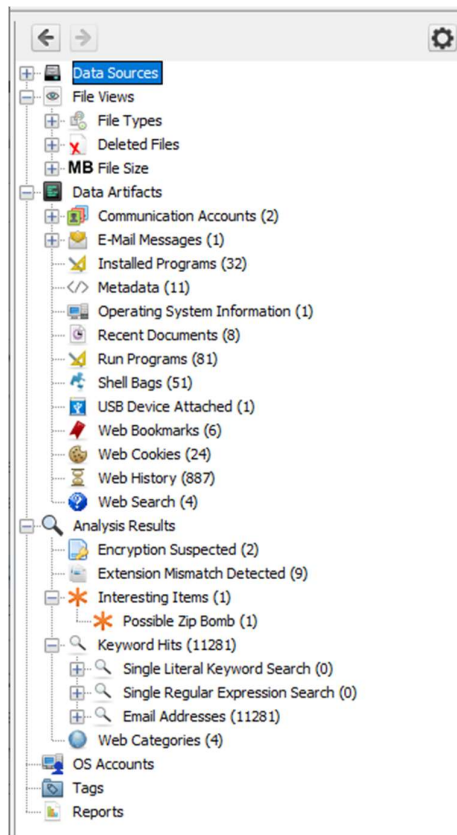


Screenshot 3: Adding data sources

Enabled Modules:

- Recent Activity
- Hash Lookup
- File Type Identification
- Extension Mismatch Detector
- Embedded File Extractor
- Picture Analyzer
- Keyword Search
- Email Parser
- Encryption Detection
- Interesting Files Identifier
- Central Repository
- PhotoRec Carver
- Virtual Machine Extractor
- Data Source Integrity
- Android Analyzer (aLEAPP)
- DJI Drone Analyzer
- YARA Analyzer
- iOS Analyzer (iLEAPP)
- GPX Parser
- Android Analyzer

Screenshot 4: Modules enabled in Autopsy analysis



Screenshot 5: Information obtained from the disk image

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-2000478354-688789844-1708537768-1003			3	Mr. Evil	4Dell Latitude CPi.E01_1 Host	Local		2004-08-20 07:03:54 SGT

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
-----	------	-------------	---------------	------------	----------------	------------------	---------	-------------	-------------------

Basic Properties	
Login:	Mr. Evil
Full Name:	
Address:	S-1-5-21-2000478354-688789844-1708537768-1003
Type:	
Creation Date:	2004-08-20 07:03:54 SGT
Object ID:	7

4Dell Latitude CPi.E01_1 Host Details	
Last Login:	2004-08-27 23:08:23 SGT
Login Count:	15
Administrator:	True
Password Settings:	Password does not expire
Flag:	Normal user account
Home Directory:	/Documents and Settings/Mr. Evil

Screenshot 6: Suspicious OS account found

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
						Metadata			
						Name: CurrentVersion			
						Number of subkeys: 57			
						Number of values: 17			
						Modification Time: 2004-08-27 15:08:22 GMT+00:00			
						Values			
						Name	Type	Value	
						CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)	
						InstallDate	REG_DWORD	0x41252e3b (1092955707)	
						ProductName	REG_SZ	Microsoft Windows XP	
						RegDone	REG_SZ	(value not set)	
						RegisteredOrganization	REG_SZ	N/A	
						RegisteredOwner	REG_SZ	Greg Schardt	
						SoftwareType	REG_SZ	SYSTEM	
						CurrentVersion	REG_SZ	5.1	
						CurrentBuildNumber	REG_SZ	2600	
						BuildLab	REG_SZ	2600.xpclient.010817-1148	
						CurrentType	REG_SZ	Uniprocessor Free	
						SystemRoot	REG_SZ	C:\WINDOWS	
						SourcePath	REG_SZ	D:\	
						PathName	REG_SZ	C:\WINDOWS	
						ProductId	REG_SZ	55274-640-0147306-23684	
						DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 35 35 32 37 34 2D 36 34...	
						LicenseInfo	REG_BIN	34 54 AE DC C7 2E 3D E5 88 15 06 1A 8C 74 A6 55...	

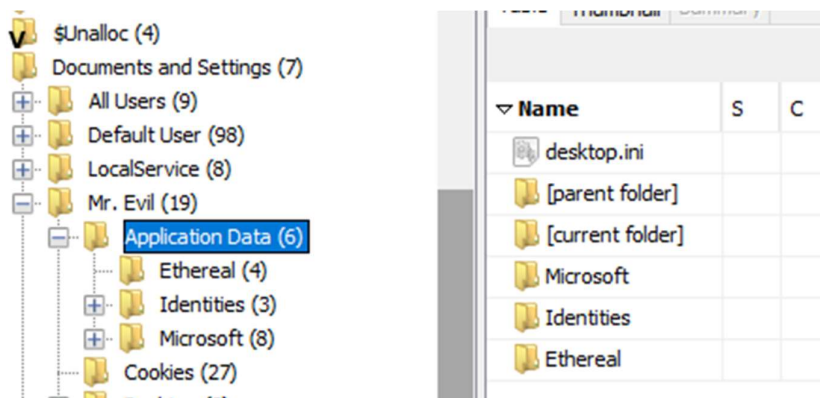
Screenshot 7: Registered owner of the computer

```
%LANDMAIN%=N-1A90UIN6ZXK4LQ
%LANUSER%=Mr. Evi
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
%ISWIN98%=FALSE
%ISWINNT3%=FALSE
%ISWINNT4%=FALSE
%ISWIN2000%=FALSE
%ISWINME%=FALSE
%ISWINXP%=TRUE
%ISUSERNTADMIN%=TRUE
%TEMPLAUNCHDIR%=C:\DOCUME~1\MRD51E~1\EVI\LOCALS~1\Temp
%WINDIR%=C:\WINDOWS
%SYSDRV%=C:
%SYSDIR%=C:\WINDOWS\System32
%TEMPDIR%=C:\DOCUME~1\MRD51E~1\EVI\LOCALS~1\Temp
%SCREENWIDTH%=800
%SCREENHEIGHT%=600
%REGOWNER%=Greg Schardt
```

Screenshot 8: irunin.ini file

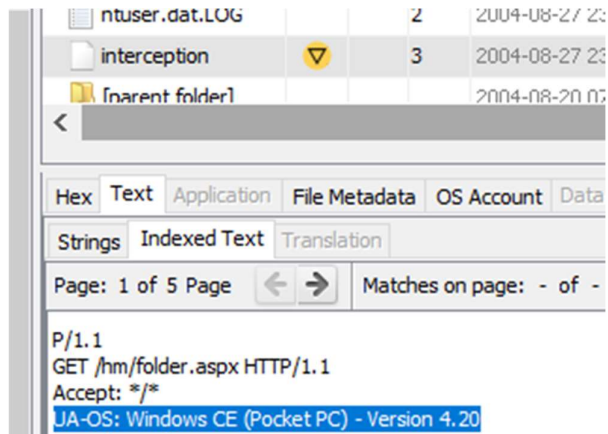
Source Name	S	C	O	Program Name	Date/Time	Data Source
software			2	mIRC	2004-08-20 15:10:04 SGT	4Dell Latitude CPl.E01
software			2	WinPcap 3.01 alpha	2004-08-27 15:15:19 SGT	4Dell Latitude CPl.E01
software			2	WebFldrs XP v.9.50.5318	2004-08-19 23:04:50 SGT	4Dell Latitude CPl.E01
software			2	SchedulingAgent	2004-08-19 22:31:32 SGT	4Dell Latitude CPl.E01
software			2	PowerToys For Windows XP v.1.00.0000	2004-08-20 15:12:43 SGT	4Dell Latitude CPl.E01
software			2	PCHealth	2004-08-19 22:32:06 SGT	4Dell Latitude CPl.E01
software			2	OutlookExpress	2004-08-19 22:31:51 SGT	4Dell Latitude CPl.E01
software			2	Network Stumbler 0.4.0 (remove only)	2004-08-27 15:12:15 SGT	4Dell Latitude CPl.E01
software			2	NetMeeting	2004-08-19 22:31:52 SGT	4Dell Latitude CPl.E01
software			2	MobileOptionPack	2004-08-19 22:31:32 SGT	4Dell Latitude CPl.E01
software			2	Microsoft NetShow Player 2.0	2004-08-19 23:04:36 SGT	4Dell Latitude CPl.E01
software			2	MPlayer2	2004-08-19 23:04:36 SGT	4Dell Latitude CPl.E01
software			2	Look@LAN 2.50 Build 29	2004-08-25 15:56:11 SGT	4Dell Latitude CPl.E01
software			2	IEData	2004-08-19 22:31:32 SGT	4Dell Latitude CPl.E01
software			2	IESBAKEX	2004-08-19 22:31:32 SGT	4Dell Latitude CPl.E01
software			2	IE4Data	2004-08-19 22:31:32 SGT	4Dell Latitude CPl.E01
software			2	IE40	2004-08-19 22:31:32 SGT	4Dell Latitude CPl.E01
software			2	ICW	2004-08-19 22:31:51 SGT	4Dell Latitude CPl.E01
software			2	Forté Agent	2004-08-20 15:08:19 SGT	4Dell Latitude CPl.E01
software			2	Fontcore	2004-08-19 22:31:32 SGT	4Dell Latitude CPl.E01
software			2	Faber Toys v.2.4 Build 216	2004-08-20 15:07:25 SGT	4Dell Latitude CPl.E01
software			2	Ethereal 0.10.6 v.0.10.6	2004-08-27 15:29:19 SGT	4Dell Latitude CPl.E01
software			2	DirectDrawEx	2004-08-19 22:31:32 SGT	4Dell Latitude CPl.E01
software			2	DirectAnimation	2004-08-19 22:31:52 SGT	4Dell Latitude CPl.E01
software			2	CuteHTML	2004-08-20 15:09:03 SGT	4Dell Latitude CPl.E01
software			2	CuteFTP	2004-08-20 15:09:02 SGT	4Dell Latitude CPl.E01
software			2	Connection Manager	2004-08-19 22:21:41 SGT	4Dell Latitude CPl.E01
software			2	Cain & Abel v2.5 beta45	2004-08-20 15:05:58 SGT	4Dell Latitude CPl.E01
software			2	Branding	2004-08-19 22:37:31 SGT	4Dell Latitude CPl.E01
software			2	Anonymizer Bar 2.0 (remove only)	2004-08-20 15:05:09 SGT	4Dell Latitude CPl.E01
software			2	AddressBook	2004-08-19 22:31:51 SGT	4Dell Latitude CPl.E01
software			2	123 Write All Stored Passwords	2004-08-20 15:13:08 SGT	4Dell Latitude CPl.E01

Screenshot 9: Installed programs



Name	S	C
desktop.ini		
[parent folder]		
[current folder]		
Microsoft		
Identities		
Ethereal		

Screenshot 10: Application data of Mr. Evil



Screenshot 11: Packet capture file by Ethereal


Source Name	S	C	O	Path	Key
NTUSER.DAT				Tools	Software\Microsoft\Windows\Shell\Bags\1\Desktop
NTUSER.DAT				Tools	Software\Microsoft\Windows\Shell\NoRoam\Bags\10\Shell
NTUSER.DAT				Recycle Bin	Software\Microsoft\Windows\Shell\Bags\1\Desktop
NTUSER.DAT				Recycle Bin	Software\Microsoft\Windows\Shell\NoRoam\Bags\10\Shell
NTUSER.DAT				NOVELL	Software\Microsoft\Windows\Shell\NoRoam\Bags\12\Shell
NTUSER.DAT				My Network Places	Software\Microsoft\Windows\Shell\Bags\1\Desktop
NTUSER.DAT				My Network Places	Software\Microsoft\Windows\Shell\NoRoam\Bags\10\Shell
NTUSER.DAT				My Documents	Software\Microsoft\Windows\Shell\Bags\1\Desktop
NTUSER.DAT				My Documents	Software\Microsoft\Windows\Shell\NoRoam\Bags\10\Shell
NTUSER.DAT				My Computer	Software\Microsoft\Windows\Shell\Bags\1\Desktop
NTUSER.DAT				My Computer	Software\Microsoft\Windows\Shell\NoRoam\Bags\10\Shell

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Basic Properties Login: Mr. Evil Full Name: Address: S-1-5-21-2000478354-688789844-1708537768-1003 Type: Creation Date: 2004-08-20 07:03:54 SGT Object ID: 7									

Screenshot 12: Shell bags created

Source Name	S	C	O	Path
Anonymizer.Ink				D:\Drivers\Anonymizer
channels (2).Ink				C:\Program Files\mIRC\channels
channels.Ink				C:\Program Files\mIRC\channels\channels.txt
GhostWare.Ink				D:\Drivers\GhostWare
keys.Ink				D:\Drivers\Anonymizer\keys.txt
Receipt.Ink				D:\Drivers\GhostWare\Receipt.rtf
Temp on m1200 (4.12.220.254).Ink				No preferred path found
yng13.Ink				\\4.12.220.254\TEMP\yng13.bmp

Screenshot 13: Recent documents

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Ju
 unix_hack.tgz				File	Likely Notable		Possible Zip Bomb	

Screenshot 14: Potential zip bomb found

Report Navigation

- Case Summary
- Accounts: Email (2)
- Data Source Usage (1)
- E-Mail Messages (1)
- Encryption Suspected (2)
- Extension Mismatch Detected (9)
- Installed Programs (32)
- Interesting Items (1)
- Keyword Hits (11280)
- Metadata (11)
- Operating System Information (1)
- Recent Documents (8)
- Run Programs (81)
- Shell Bags (51)
- Tagged Files (0)
- Tagged Images (0)

Employee Investigation

Autopsy Forensic Report

HTML Report Generated on 2025/02/07 18:01:23

Case:

IT Company Investigation

Case Number:

1

Number of data sources in case:

1

Examiner:

Koo Wai Kit

Image Information:

4Dell Latitude CPl.E01

Timezone:

Asia/Singapore

Path:

C:\Users\ADMIN\Desktop\Learning Materials\~Advanced Digital Forensics\Assessments\Image_DELL_LATITUDE_Perak\Image_DELL_LATITUDE_Perak\4Dell Latitude CPl.E01

Path:

C:\Users\ADMIN\Desktop\Learning Materials\~Advanced Digital Forensics\Assessments\Image_DELL_LATITUDE_Perak\Image_DELL_LATITUDE_Perak\4Dell Latitude CPl.E02

Screenshot 15: Autopsy forensic report

Word count: 4553
