Digital Forensics T1 (2023) 1–10

Digital Forensic Analysis - Assignment 1

Olivia Fletcher
ID: 300534281, Email: fletcholiv@myvuw.ac.nz

School of Engineering and Computer Science, Victoria University of Wellington, P.O. Box 600, Wellington 6140, New Zealand.

Abstract

As the world's technology develops, devices become more accessible and more connected with new forms of communications constantly being introduced. This makes the digital investigations sphere more complex and is where the importance of maintaining the integrity of Digital Forensics comes into play. Today, we will review the significance of five different subcategories of Digital Forensics, which play a crucial role in maintaining the integrity of digital investigations as technology becomes more complex and connected. The resource we will be deriving the tools from will be supplied by NDG's Netlab+[4]. We will be reviewing the literature "Digital Forensics"[1] to assist us in this assignment. The following categories are as follows:

1. Chain of Custody

Chain of Custody is a list of processes involved in Digital Forensics which it refers to the procedures followed by ensuring sufficient documenting and maintaining the history that data took before, during and after being seized. Chain of Custody is incredibly important in digital-based investigations as it ensures the integrity and admissibility of evidence provided in a court of law. The various stakeholders involved each play a critical role in maintaining proper Chain of Custody procedures, such as the investigators, the legal team, and the custodians involved in the case. However, it is important to follow recommended guidelines to ensure that the procedures taken place are appropriate, given the delicate nature of data and the risks of occurrences such as data corruption and loss.

2. Forensic Imaging Techniques

Forensic Imaging Techniques refer to the methods and tools implemented in creating a copy image of digital media or storage device contents for forensic analysis. The general process the methods are based on is the procedures involved in making a bit-for-bit copy of original media as a means of a data preservation measures to ensure no alteration takes place. This is important in the Digital Forensics field as it enables the ability to perform a deep analysis on evidence without the potential of altering or damaging the original data. Building from Chain of Custody, the methods using in forensic imaging can help preserve the Chain of Custody principles when conducting an investigation to ensure that the evidence gathered is valid in the court of law. However, documentation at every step is required for the above considerations.

3. Live Acquisition

Live Acquisition in Digital Forensics refers to the procedures involved in collecting live data from a running system or device and ensuring the preservation of digital evidence in its original form. Essentially, live data acquisition is a snapshot of data from a live system.

However, just like the Forensic Imaging Techniques introduction, it is vital to make sure that Live Acquisition follows of the Chain of Custody principle through continually documenting of the data acquisition process and even sometimes requiring multiple snapshots.

A snapshot of a live system can include but is not limited to; currently running processes, network connections and volatile data. Live Acquisition is especially useful in time-constrained investigations where the capturing process for the data collection works quickly and efficiently while also ensuring no disruption to the systems processes. Overall, Live Data Acquisition is an essential tool used in Digital Forensics Investigations which allows for data collection while maintaining proper preservation of data.

4. Data Carving

Data Carving in Digital Forensics refers to the process of extracting deleted or encrypted data from digital media or storage device sources. The procedures involved require specialized software such as Photorec Carver which allows for identifying and recovering data that no longer be accessible through straight-forward means or software. Data Carving practices are vital in a Digital Forensics investigation because

it provides a basis in being able to recover potentially critical evidence that may have had protection measures in place by a suspect. It is particulary valuable in investigations where traditional techniques may not be sufficient which leads to a more effective and accurate output for a case.

5. Keyword Search and Analysis

Keyword Search and Analysis in Digital Forensics refers to the process of specifying and extracting relevant data based on specified keywords or search terms within a media file of storage device. The procedures require specialised software such as Autospsy which allows for the ability to search for specific keys, phrases or patterns within digital evidence such as emails, documents, chat logs or image files. Keyword Search and Analysis is important in Digital Forensics because it allows for an investigator to quickly and efficiently fork through large sets of data to only output relevant information. This is helpful to save time and resources by allowing to reviewer to focus their analysis on more pertinent information.

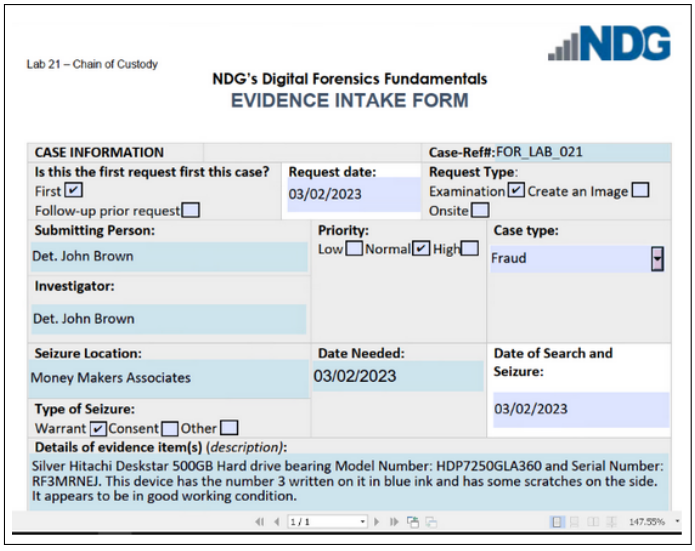
1. Chain of Custody

Digital Forensics has many important steps involved to ensure that a digital-based investigation maintains and adheres to the already well-established forensics standards. One of these procedures is known as 'Chain of Custody' which ensures that an investigation sufficiently follows the correct data collection measures.

- Arnes, "Chain of Custody refers to the documentation of acquisition, control, analysis, and deposition of physical and electronic evidence."

Chain of Custody closely follows the 'Evidence Integrity' protocol where it is vital to ensure that data is kept at its most original form from the initial time of investigation. The process for physical forensics is very similar to digital forensics however the digital world comes with issues with data conservation as data is subjected to change over time. Due to this, it is important to continually document the data from its most original form using the Chain of Custody principle. In this lab we will be documenting all of our processes of evidence handling for the Chain of Custody standards in order to prove its authenticity and maintain the quality of the court of law data collection. In this lab we will be reviewing physical evidence that has been seized for investigation purposes. We will be taking an important role (Industry standard) where we must properly handle and document evidence of an external Hitachi Hard Drive and Samsung phone. The first step of reviewing the Hard-drive (with proper gear being, gloves etc) will be identifying the unique serial and model numbers and provide an in-depth description of the Hard-drive including the shape, colors and if there are any markings/scuffs/breakage. Below is the image of the Hard-drive with the red outlines showcasing the valuable data (The process is the same for the Samsung phone data recording, as mobile phone are different the means of the serial number collection are different, Googling the device name will provide how to do this, for example my Iphone 14 pro max provides these details under Settings -¿ General - About).

The next step is to record our data in the industry standard appropriate forms, as seen below.


Lab 21 – Chain of Custody

NDG's Digital Forensics Fundamentals

EVIDENCE INTAKE FORM

CASE INFORMATION — Case-Ref#:FOR_LAB_021

Is this the first request first this case? First ☑ Follow-up prior request ☐ | Request date: 03/02/2023 | Request Type: Examination ☑ Create an Image ☐ Onsite ☐

Submitting Person: Det. John Brown | Priority: Low ☐ Normal ☑ High ☐ | Case type: Fraud

Investigator: Det. John Brown

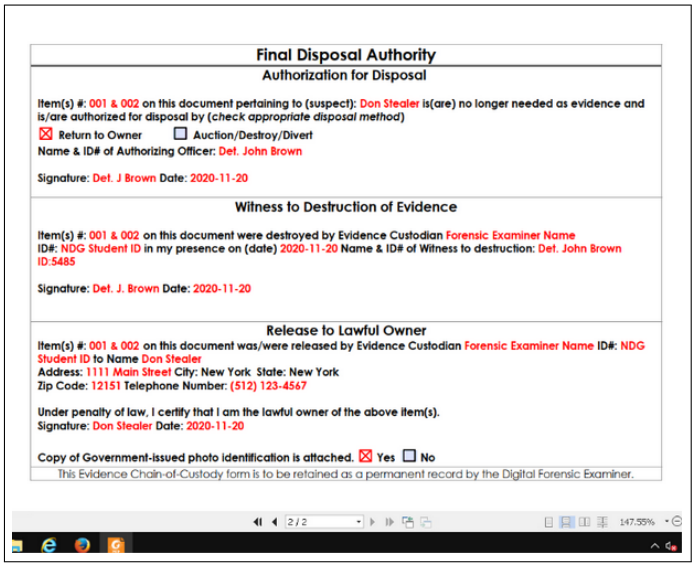
Seizure Location: Money Makers Associates | Date Needed: 03/02/2023 | Date of Search and Seizure: 03/02/2023

Type of Seizure: Warrant ☑ Consent ☐ Other ☐

Details of evidence item(s) (*description*):

Silver Hitachi Deskstar 500GB Hard drive bearing Model Number: HDP7250GLA360 and Serial Number: RF3MRNEJ. This device has the number 3 written on it in blue ink and has some scratches on the side. It appears to be in good working condition.

Figure 1: Evidence Intake Form


Final Disposal Authority

Authorization for Disposal

Item(s) #: 001 & 002 on this document pertaining to (suspect): Don Stealer is(are) no longer needed as evidence and is/are authorized for disposal by (*check appropriate disposal method*)

☒ Return to Owner ☐ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: Det. John Brown

Signature: Det. J Brown Date: 2020-11-20

Witness to Destruction of Evidence

Item(s) #: 001 & 002 on this document were destroyed by Evidence Custodian Forensic Examiner Name ID#: NDG Student ID in my presence on (date) 2020-11-20 Name & ID# of Witness to destruction: Det. John Brown ID:5485

Signature: Det. J. Brown Date: 2020-11-20

Release to Lawful Owner

Item(s) #: 001 & 002 on this document was/were released by Evidence Custodian Forensic Examiner Name ID#: NDG Student ID to Name Don Stealer

Address: 1111 Main Street City: New York State: New York

Zip Code: 12151 Telephone Number: (512) 123-4567

Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: Don Stealer Date: 2020-11-20

Copy of Government-issued photo identification is attached. ☒ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Digital Forensic Examiner.

Figure 2: Final Disposal Authority Form

Data of this means are to be submitted with breakdowns of every single details from the evidence provided. It is important to do these steps for documenting physical evidence so they maintain the standards set by the court of law.

2. Creating a Forensics Image

Building onto the previous lab of Chain of Custody where we documented physical evidence of a harddrive and cell phone we will now undertake the digital side of evidence collection using the same principles. Forensic Imaging is another vital part of a forensic investigation and is evidently more delicate and important to ensure that the procedures used are forensically sound due to the ever-changing nature of data in its lifetime. In this lab we will be utilizing industry standard forensic imaging software so that digital copied evidence can be admissible in court. Due to this, it is important that the investigation's data is preserved in its most original form. Following the correct procedures to create a forensics image of given data will ensure that we maintain the 'Evidence Integrity' principle. Evidence integrity [def 1.1.8, Arnes] goes hand-in-hand with this lab as the principle makes certain that the individuals conducting the investigation continually document file/system changes due to the nature of data inevitably changing over time on a live computer. For this lab we utilized the FTK Imaging software provided. The process for imaging comes quite simple just by inputting the drive with some straight forward settings such as destination of copied image, type of image and how the image will be outputted. The following image types the FTK offers are;

- Raw (dd), an image type which uses no compression as a full image dump but does not store the image information.
- SMART, image format specific for the SMART tool in Linux systems. Does allow for compression and segmentation of imaged data however this feature is not utilized as much anymore.
- Advanced Forensic Format (AFF), creates a raw image format which creates a separate file that contains the image metadata. Also has segmentation and compression abilities.
- Expert Witness Format (E01), the created image also stores the metadata within the produced container which is helpful when verifying.

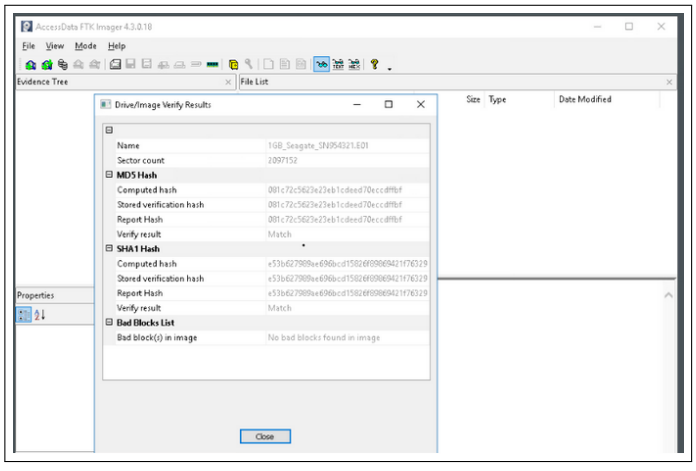


Figure 3: FTK Image Types

The most common imaging type used for forensic investigations and is considered up to industry standard is the E01 imaging format as it not only supports compression/ segmentation but also stores the metadata within the output image which directly assists us in manually verifying the contents. During this lab on NDG we created a logical forensic image of a physical drive containing evidence for later analysis and then compared the resulting hash to the original to ensure evidence integrity. To do this, we used software known as FTK Imager which does this process automatically for us. As seen in the below screenshot from the lab we can verify the output by checking that the MD5/SHA1 hashes are matching & that there are no bad blocks detected in the list.

Another important way we can verify images (as per the E05 image format) is manually via the text output file, as seen below;

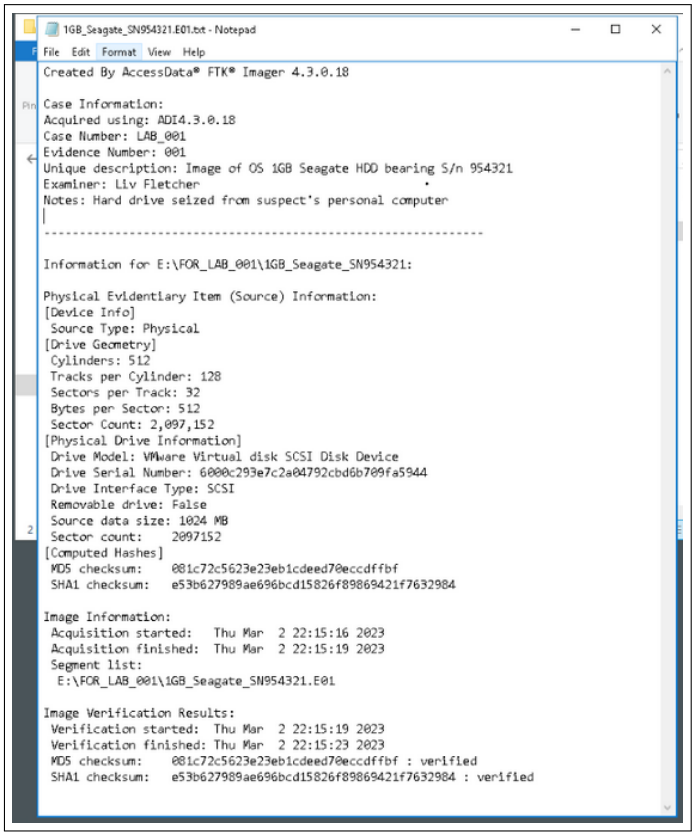


Figure 4: Manual Checking

In conclusion, in this lab we learnt the tools and techniques used in a practice investigation where we needed to directly image a drive without changing its data properties. We then analyzed the imaged data and used the FTK imaging software to ensure the outputted hash matches the original.

3. Live Data Acquisiton

Live Data Acquisition is a form of data collection involving a live computer where a timeframe of data is captured for later analysis. This includes memory captures, Windows registry hives, file systems and open processes. Live Data Acquisition is becoming a more common form of data collection because it can help assist in investigations where a drive containing evidence has been encrypted. However this process has proved to be quite complex in nature and delicate proceedings are vital, if implemented correctly can provide plenty of valuable data but, if not implemented correctly can prove your findings to be admissible in the court of law and be dropped. In this lab we will be implementing two different types of data acquisition techniques such as the use of Mandiant's Redline Data Analysis and revisiting AccessData's FTK Image viewer. These techniques of data acquisition are important to digital forensics due to providing better accountability for the 'Chain of Custody' process and maintaining the 'Evidence integrity' principle. The first half of this lab involves bypassing an encrypted drive by implementing the "Magnet RAM Capture tool" to take a live snapshot of a provided system and then uploading the data to the FTK Imager for analysis. However, in this lab we used the already acquired dataset and we started by assessing the hashed data for any JPG images by searching for its header "FF D8 FF E0" and selecting the full hash with the ending "FF D9". We then save this hash into a JPG format for viewing. We can then open the image using the IrFanView software provided (as seen below).

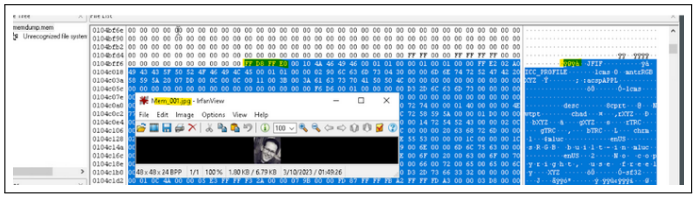


Figure 5: PNG Live Data Carving

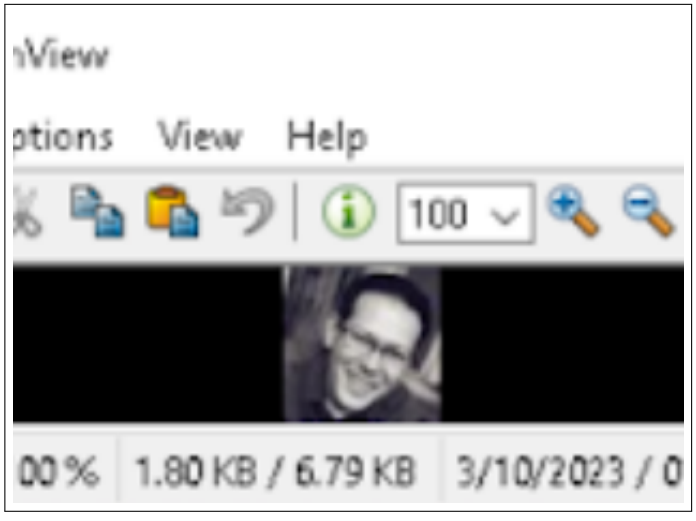


Figure 6: PNG Output

The second half of the lab was a quite different form of live data analysis using the Mandiant Redline software. Redline shows a more detailed breakdown of what processes have been running during the image capture time and also creates a timeline of events in chronological order, this is useful in a real-world scenario as it provides valuable data of what processes were running before/during/after the scene of a crime. In this lab we will be checking the data during the time of the FTK Imager snapshot and check any potentially suspicious processes that ran along-side/after the FTK imaging was taking place.

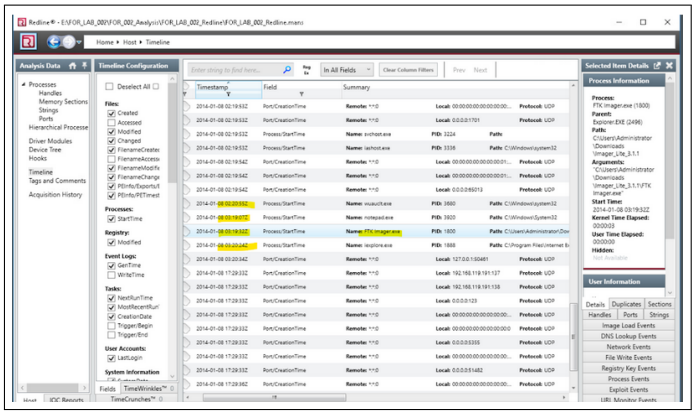


Figure 7: System Resource Check

Our findings from utilizing the Redline software show that during the start time of FTK Imager we can see a list of data in chronological order which shows what processes were running during our imaging time as seen above in figure 7.

Overall we have learned some very useful techniques by executing Live Data Acquisition via the FTK Image Viewer & Mandiant Redline software's which are industry standard tools used by real-world Digital Forensics investigators. Being able to manually fork through large data sets and be able to sufficiently locate where blocks of data and what type of data are within these large data sets is a necessary skill to have.

4. Data Carving

Data Carving is an advanced form of recovery where we perform searches through large data sets for information that may be useful in a case, however this data is usually located in unallocated spaces or has been either encrypted/deleted/broken. Data Carving is a form of advanced data recovery that aids digital forensics investigation in industry spaces. There are many ways Data Carving can be utilized but the main two ways which we will be addressing in this lab are either performed manually or automatically. Automatic data carving is using software where it automatically carves through hashed data for blocks of data that can be converted back into its file type. It is important for digital forensics to know the ins and outs of how to perform manual data carving and be able to identify specific file signatures and blocks of hash from a given data set. In this lab we will be going in-depth into the manual forms of data carving and by the end will be able to identify different file type headers, recognize full blocks without false positives and finally convert these blocks of hash back into its file type for later analysis. To manually carve the data, we will be using a hex editor where we will be searching for different file types, these files we will search for are as seen below with its hex signature data.

- XLSX spreadsheet file with a hexadecimal header value; 50 4B 03 04 14 00 06 00 Hexadecimal footer value; 50 4B 05 06 PK followed by an additional 18 bytes Note: this header signature is the same as DOCX word document & PPTX slideshow document and when converting the doc can try the different forms for testing and analysis. It is useful to check as the file can contain different data on different forms of output. As seen below; (put image)
- PDF file with a hexadecimal header value; 25 50 44 46 Hexadecimal footer value; 0D 25 25 45 4F 46 0D, however there may be multiple footers so make sure you have selected the last one of the block. Another way to ensure you have reached the end of the block is that the next block begins with empty hex values.
- JPG image file with a hexadecimal header value; FF D8 FF E0 & footer value; FF D9, we utilized this same technique in Lab 3, Live Data acquisition for JPG format.

Recognising file signatures is an important skill because it allows us to identify the types of files within a data set. To convert the data blocks back into its file type is very simple, assuming you have the full block correctly selected you just save the block from the viewing software and add the file extension once you're in the desired directory. The top left, Figure 8 is a screenshot showing where we have successfully saved the full block and opened as a spreadsheet file

The top left image, figure 9 is a screenshot that showcases the "ending block" of an XLSX file, however, this is a false positive due to the following block not containing empty hexes with the below image showing the legitimate ending block; [Note: this is the case for every file type, not just XLSX]

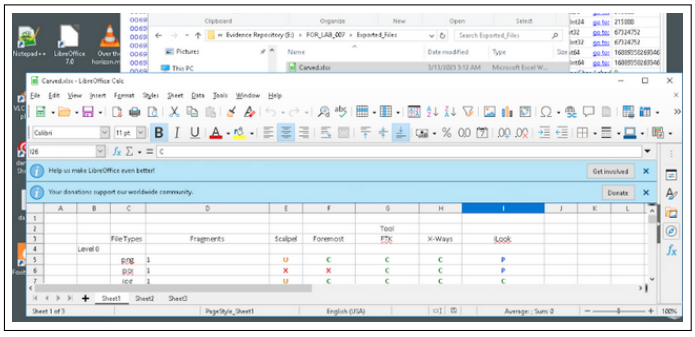


Figure 8: Successful Data Carve

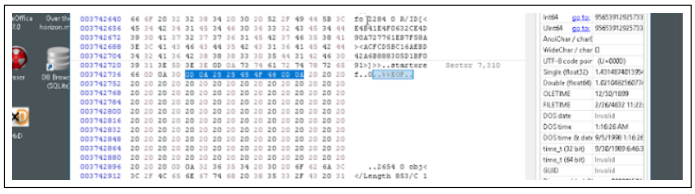


Figure 9: XLSX False Positive End Block

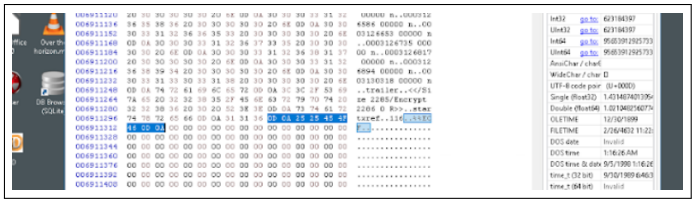


Figure 10: XLSX Legitimate End Block

Our next objective is to do this same product using automated software where the outcome is far less time consuming than manual collection. We will be using Autopsy Forensics with the Photorec Carver for the automation and provided GUI which allows us to open and view each file found. In this lab we are able to find 13 files. The way Photorec works within Autopsy is by scanning through the metadata and looking for valid clusters and with a block containing enough metadata it will rename and output the file.

It is quite common to deal with broken/lost/encrypted or deleted data in a digital criminal investigation. However there are means of which we can utilize to access even the most destroyed files to analyze. Data Carving is incredibly important in the digital forensics world as it allows investigators to analyze broken or deleted data. It is important for us and forensic investigators to know the ins and outs of data carving measures and be able to do this process manually with a provided hash data set. Manual data carving and be an tedious but rewarding task. In this lab we will be reviewing the manual data carving process and implementing industry standard data carving software to garner the same results.

5. Keyword Search and Analysis

Keyword search and analysis are crucial components of digital forensics due to the challenge of handling large volumes of data that are difficult to manually search through within a limited time frame. In this lab, we will continue the implementation of our data carving lab using Autopsy software, which is an industry-standard software that provides different ways to sift through large data sets and provide breakdown lists with specifications for further analysis by the examiner. To begin, we will create a case in Autopsy, which allows us to load evidence, save and create tags, create bookmarks, and generate reports. The setup and use of Autopsy ensure that there is no cross-contamination of evidence, as each case file's output is separated to preserve the data in a forensically sound manner.

Autopsy is able to extract many different types of data from differing sources using a plugin called Ingest Modules. We will be searching for the following keywords:

- Lootatlan
- 0010a4933e09
- yahoo
- hackersteam
- hack
- hack*

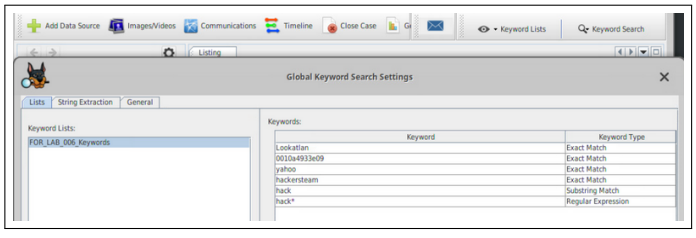


Figure 11: Autopsy Case Keyword Specification

After we have set our desired keywords we then can start our scan through the selected drives data.

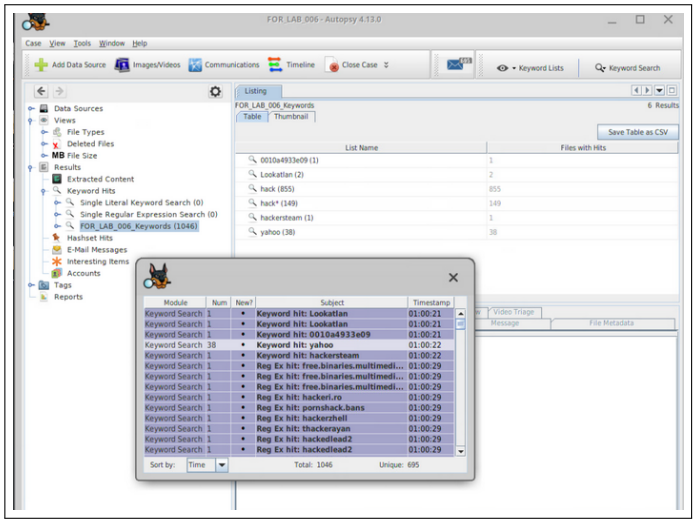


Figure 12: Autopsy Case Scanning Output

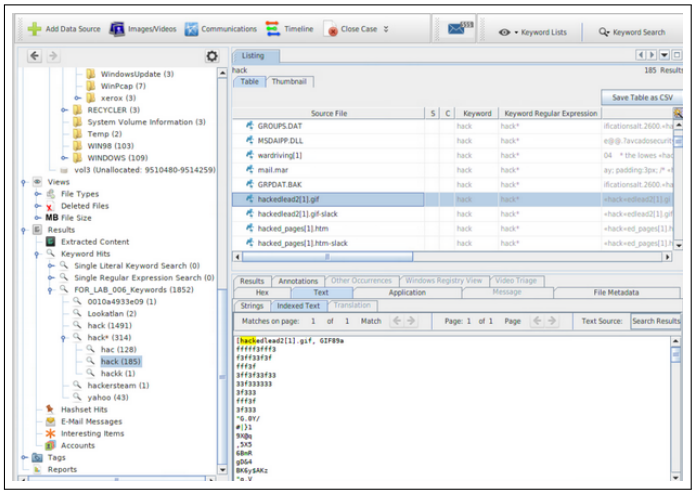


Figure 13: Autopsy Case Scanning Output 2

In the below screenshot we can see that the Autopsy GUI screen has picked up files containing the keywords we specified and provide the location of which it was discovered from. Upon opening the keyword location such as the channels.txt as seen in Figure 12 it provides the full text file within the GUI below where we can further investigate the findings. Within the channels.txt we can see the keyword 'hack*' was picked up on with the output being 'hackerstone.org' which could indicate some malicious activity and should be investigated further. The autopsy GUI also provides the other found keywords and their locations which has overall provided pretty extensive information.

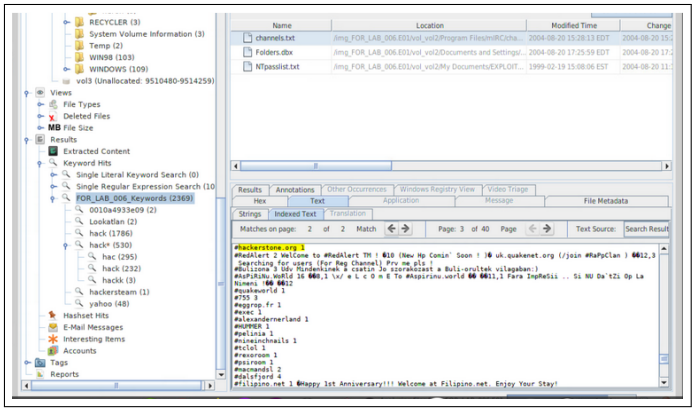


Figure 14: Autopsy Case Scanning Output 3

In conclusion, in this lab session we gained hands-on practical experience in working with Autopsy Ingest Modules to search for keywords within a drive containing many different file types. The techniques we utilized are used in real-world scenarios and will prove to be a useful starting point for developing our understanding in the world of Digital Forensics.

Questions - Digital Forensics

Question 1

As part of a drug cartel case, you have been asked to seize all digital devices from one of the potential drug dealers' homes and perform a forensically sound collection of potential evidence. The "dealer" was caught sitting in the living room and brought to custody. The devices pictured below were found in the living room. Assume all devices are switched on and running except for the Galaxy S22 phones and PS5. The WD elements drive connected to the laptop, and the USB stick were found down the back of the living room couch. Consider the identification and collection phases described in lectures and the textbook (chapter 2).

Task A

How might these devices be relevant to the drug cartel case?

With the assumption that devices Samsung S22 phones & PS5 devices being switched off that leaves the following currently active; Panasonic 32" HD LED Android Smart TV, Apple iPhone 13 128GB Midnight Black, Google Nest Cam (Indoor, wired), Google Home - Smart Speaker, WD Elements Portable HDD 5TB, Wifi Router, Alienware x17 Gaming Business Laptop & Sandisk 64GB Cruzer Glide USB3.0 Flash Drive. Every single one of these devices will be incredibly relevant in a drug cartel case and must be seized immediately. However, to maintain evidence integrity & the chain of custody principles we would need to process each device individually. Due to the crime being quite high-stakes it would be best to conduct the device examinations simultaneously as the timestamps of activity together can form the final evidence and be presented in court.

Task B

What would you advise first responders to do to protect the data's integrity? Use law examples from the book to illustrate real world examples.

def. 2.2.3 'At The Scene of the Incident' Arnes et al.

The first steps I would advise the first responders to take would be to follow the principles of chain of custody and evidence integrity and proceed with care. The first simple step would be to photograph the scene and the location of each device untouched with descriptions of each device's features, location, and timestamps.

The next step is to verify if each device is either currently running (live system) or turned off (dead system) as each has different handling processes involved. Assuming that we have now identified the live systems, we next need to consider the use of containers (RF shield, e.g., Faraday Bag) to shield the live devices to avoid either intentional tampering through network/remote connections or unintentional physical changes.

According to preparation and deployment of tools and resources (2.2.1), when it comes to handling devices in a crime scene, it is important that preparations are already in place for the next investigation to take place. With this assumption, the digital forensics team will already be sufficiently prepared and will arrive with the necessary equipment/software. The team will have prepared for any scenario such as encryption, tampering protection, and data deletion. With everything being sufficiently documented as per the chain of custody principle when handling devices with valuable data.

Task C

When time is limited, how would you choose which devices to collect data from first?

Collecting data from live systems first is often prioritized in digital forensics investigations because they may contain volatile data that could be lost if the system is turned off or disconnected from the network. I would also request that while conducting the examination to do so simultaneously with multiple investigators so it can assist in helping save time, as they can work on different devices simultaneously. Additionally, it may be beneficial to prioritize devices that are believed to be most relevant to the investigation based on information gathered during the initial stages of the investigation.

Task D

What barriers exist to collecting data from the devices?

- Login access, the suspects will have password protection in place on their devices especially and assuming extra security on devices containing evidence or volatile data. This can make it difficult to collect data from these devices and will require specialised tools and techniques to be able to bypass the security measure in place. However, the investigators also need to follow the legal and ethical standards set by the New Zealand Government.
- Data encryption, another barrier could be that some devices contain encrypted data to make it difficult or sometimes impossible to decrypt. As we have already performed in our above sections, there are specialised tools available of which that can be used to uncover encrypted data however, some data loss can occur.
- Remote destruction of data, if the suspects have added extra security measures they could have the tools in place to remotely wipe data (from live machines) that could contain evidence for a case.
- Device destruction, there could be devices containing important evidence that have been destroyed especially if any of the suspects on the premise are expecting police to show up.

- Legal implications. There may be legal barriers in place of which the investigator/s do not have the proper authorization to probe the devices. There may be limitations on what types of data can be collected or devices accessed.
- The above are only a few of many different types of barriers that an investigation could be faced with and as each investigation is unique there will be differing barriers in place. There are some specialised tools that are able to perform data recovery however some or all data loss could occur.

Task E

What is recommended in terms of documentation for the Chain of Custody?

Chain of Custody ensures that everything done to evidence has been documented. Documentation is a critical component of the Chain of Custody process. It helps to ensure the integrity and admissibility of the evidence in court. The following are recommended in terms of documentation for the Chain of Custody:

- The first recommendation is to always start with a plan or written protocol that contains the procedures that should be followed.
- The next step would then be recording the identify of the devices by labeling and categorizing evidence and including in-depth descriptions of each item with timestamps of collection/handlings. This would also include the reviewers/investigators identification that is performing this task.
- Document all transfers that the evidence takes including who, what, where and why this data was used/accessed for. Include the identities of all individuals that have directly accessed or travelled with the evidence.
- When it comes to examination of evidence, include thorough documentation including date, time, examiner identities and reasoning of accessing data.
- Once seized data has been properly examined, securely store the data in a location with limited access and record the date/time and individuals with access to this space.
- As per Chain of Custody, ensure any extra movements the data takes has been sufficiently documented with the above requirements.

Task F

What devices could be used to ensure you do not affect the integrity of the copied data?

- Offline, fresh install virtual machines to feed the data through, this can be helpful due to the ever changing nature of data when being accessed through a live device.
- Tools we implemented in the above sections covered during the lab such as the use of forensic imaging software as its designed to be copying/creating forensically sound images of storage devices/material.
- Implementing the use of hashing tools which creates hash values for the original data and the copied data. These hashes can then be compared against one-another and if they match this will verify the integrity of the copied data and and ensures an exact replica has been made.

Task G

What technical measures can be used to protect data against tampering?

- Encryption, encrypt data with only authorized individuals having key access.
- Hashing, keeping a hash of the original file and then using this hash to compare the files authenticity at a later date. If tampering has taken place the file will hash a different hash.
- Digital Signatures, signatures can be used to verify that the data has not been altered since signing date/time.
- Passwords, setting up access controls for only authorized individuals to be able to access the data. Another addition could be to add extra security measures such as 2FA.
- Logging, have an automatic logging system in place such as audit logging which tracks every movement data takes and who has accessed it.

Question 2

Task A

When is an investigation coercive according to European law? According to the literature Digital Forensics [1] Definition 3.2 Coercive investigation method states

- ”An investigation method is coercive when it lawfully can be applied against an individual without her consent or cooperation, despite that her right to personal liberty, property, or private life is interfered with.”

Legal Provision 3.2: The Right to Respect for Private life

1) “Everyone has the right to respect for his private and family life, his home and his correspondence.
2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of . . . the prevention or disorder of . . . crime . . . , or for the protection of the rights and freedoms of others.”

The ECHR article 8 (excerpt)

Task B

Discuss why secret surveillance of a drug smuggling cartel could be used, whereas secret surveillance of an opposition political party meetings might not.

Secret surveillance of a drug cartel could be justified due to the nature of the crime causing potentially irreparable damage to society. The act of surveying the cartel may be seen as a legitimate law enforcement tool to improve the safety and livability of a community. Due to the nature of the crimes taking place the cartel would probably have tools/plans in place if they have been notified/suspect they are under surveillance. To be able to sufficiently gather valuable information about the workings of the cartel it would be best to do so prior to their awareness.

However, when it comes to secret surveillance of an opposition political party would require sufficient justification due to not only no mentioned crime taking place but also the members involved in the meeting can exercise their personal right to privacy.

Task C

Consider the New Zealand context; what rights do we have concerning coercive search and what legislation defines the application of coercive investigation?

In New Zealand, the rights of individuals concerning coercive search and investigation are primarily protected by the New Zealand Bill of Rights Act 1990 (NZBORA)[5] and the Search and Surveillance Act 2012 (SSA)[6].

The NZBORA states that individuals in New Zealand have a range of fundamental rights and freedoms. These rights also include the right to deny unreasonable search and seizures of personal belongings without a valid reason to do so. It states that law enforcement must follow the jurisdiction and provide sufficient documents/warrants to be able to conduct a search of an individuals belongings.

The SSA provides the surveillance framework of which law enforcement in New Zealand must abide to such as procedures and requirements for obtaining search warrants and deploying monitoring devices.

Question 3

Is it lawfully obtained, if digital evidence has been secretly secured from a user account on a cloud service? What would make it unlawfully obtained, and in that case, who would be the aggrieved party? Is the consequence that the evidence must be excluded from being cited as evidence at trial? Which rule (principle) is relevant in this respect, and who decides? Discuss in three contexts - The EU, USA and New Zealand as covered in Arnes et Al.

EU

According to the the General Data Protection Regulation (GDPR)[2] the lawfullness of obtained evidence via a user account on a cloud service would depend of whether or not the obtained data was consented to by the owner. If data has been collected without the knowledge or consent of the owner it will be in direct violation of the GDPR.

USA

An individuals digital and personal privacy in the United States are governed by a combination of state and federal laws. As per the Fourth Amendment section within the U.S Constitution the methods of obtaining data of a user through a cloud service would require sufficient documents and warrants that are in accordance with the individuals amendments rights.

NZ

If evidence has been obtained secretly from a users cloud service account this may go directly against an individuals rights as per The New Zealand Privacy Act 2020 and would be considered unlawful evidence. In accordance with the Act, law enforcement must obtain sufficient documents/warrants in order to perform a search on the users cloud account.

Question 4

Consider each of the following cases and identify whether New Zealand enforcement officials could conduct a forensic investigation as described. In your answer, cite the relevant section of the Search and Surveillance Act 2012. In the case of ambiguity, please state any additional questions that need to be answered.

Task A

New Zealand police want to install a tracking device on the car of 'Person X'. This person is suspected of mass importation of pistol carbine conversion kits. Assume that the tracking device can only be installed by coming onto private property without the owner's consent. There is no urgency in this case.

Task A.1

Explain why a surveillance warrant would be required in the following case

A surveillance warrant is required in this case because the police will be accessing private property, as seen in Section 46 of the Search and Surveillance Act 2012. The procedure of attaching a tracking device on a suspect's car is considered a form of electronic surveillance, and therefore requires a surveillance warrant to be obtained prior to installation.

Task A.2

What is the maximum period of time the data could be retained, assuming no criminal proceedings occur?

The Search and Surveillance Act 2012 section 101 underlines the rules for retention of seized items and digital based evidence however it does not specify a maximum period for data retention but states that the retention period for digital evidence may vary depending on the specific circumstances of the case and the applicable laws and regulations.

Task B

How does your answer change when 'Person X' is suspected to be traveling to a location to carry out a murder, and the NZ police do not have time to apply for a warrant? Justify your answer concerning the Act and discuss any restrictions that might be placed upon using a gun. Note that murder in New Zealand carried a mandatory ten-year sentence.

In a situation where the police do not have sufficient time for obtaining proper documents/warrants needed for surveillance there are cases which allow for emergency exceptions to the warrant requirement as accordance with the Search and Surveillance Act.

This exception is recognised via section 48 of the Search and Surveillance Act 2012 and is only applicable in circumstances of which involve immediate risk to an individuals life or safety.

Question 5

On 2nd of October 2014, Police searched Mr. Hager's home in Wellington and seized or cloned many items, including USB storage devices, documents, CDs, phones and computers. The search lasted for over 10 hours. While Mr. Hager was not himself a suspect, Police were seeking evidence regarding the identity of a hacker known as 'Rawshark' who had confidentially provided Mr. Hager with information for his book.

Task A

What were the reasonable grounds specified in the search warrant?

The Search and Surveillance Act 2012 requires that a search warrant be issued by a judicial officer based on reasonable grounds to believe that there is evidence at the location to be searched. The warrant must specify the particular items or categories of items that can be seized and must be executed within a certain time frame.

In terms of seizing Mr Hagers items despite not being a direct suspect may potentially fall under reasonable grounds due to being in possession of evidence related to the commission of a crime and due to the obstruction of justice by withholding information related to the Rawshark hacker identity. However, because of the circumstances the warrant must specify the reasoning for warrant against Mr Hager.

As per the report released by the IPCA [3] it states that the warrant was made under special circumstances where the reasonable grounds was due to Mr Hager being suspected to having committed the offense of accessing data for dishonest purposes. The warrant also specified the seizure of all documents, records, storage devices and other items related to Mr Hagers work.

Task B

Summarize the argument as to why the search warrant was not specific enough in nature and what part of the Act relates to the need for a special warrant (also consider production orders)?

The argument against the search warrant is that the 'reasonable grounds' stated for the warrant was not specific enough in nature, and in-turn failed to comply with the requirements of the Search and Surveillance Act 2012. The report by IPCA deemed the act of seizing all belongings relating to Mr Hagers work too broad and as per the above statement, the special circumstances of seizure were not sufficiently met.

As per section 148 of the Search and Surveillance Act, it states that in regards to the seizure of material from journalists there is a requirement for a special warrant of which in this case was not properly met.

References

[1] Anders, F., Inger, S., Ausra, D., Jeff, H., Jens, S., Petter, B., Katrin, F., Stefan, A., 23rd May 2017. Digital forensics. https://onlinelibrary.wiley.com/doi/book/10.1002/9781119262442, accessed: 01/03/2023.

[2] ICO Europe, 25th May 2018. The general data protection regulation. https://gdpr-info.eu/, accessed: 10/03/2023.

[3] IPCA Government, 20th August 2019. Unlawful search of journalist nicky hager's property. https://www.ipca.govt.nz/Site/publications-and-media/2019-reports-on-investigations/2019-aug-20-unlawful-search-hager-privilege.aspx, accessed: 02/04/2023.

[4] Network Development Group, 1996. Ndg netlab+. https://netlab.ecs.vuw.ac.nz/, accessed: 01/03/2023.

[5] Parliamentary Counsel Office, 28th August 1990. The new zealand bill of rights act 1990. https://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html, accessed: 10/03/2023.

[6] Parliamentary Counsel Office, 5th April 2012. The new zealand search and surveillance act 2012. https://www.legislation.govt.nz/act/public/2012/0024/latest/DLM2136536.html, accessed: 10/03/2023.