Fall 2023

Master of Science in Cyber Security Project Report

Computer Science Department

California State University, **Dominguez Hills**

Digital Forensics Incidence Response

A Project

Presented

to the faculty of

California State University, Dominguez Hills

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Cyber Security

---

by

Yahya Sayeed

Fall 2023

DEDICATION

I would like to dedicate this project to

My late father, who always gave utmost importance to education,

My mother for always being there in my adversities and

Last but not least, my beloved wife for her constant support throughout my graduation journey.

ACKNOWLEDGEMENTS

I am grateful that I was given the opportunity to choose this project, which has enhanced my knowledge in so many aspects of digital forensics. I would like to show my gratitude to my course instructor, Dr. Alireza Izaddoost for accepting and guiding me throughout the semester. Special thanks to Dr. Mehrdad Sharbaf, Dr. Bhrigu Celly, Dr. Ashkan Jalooli and Dr. Mohsen Beheshti for supporting me during my time as a student at California State University Dominguez Hills.

AUTHOR’S DECLARATION

I hereby declare that this project consists of the original work which I have authored. This is a true copy of the work, including any required final revisions, as accepted by my committee or course instructor.

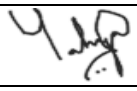
Name	Yahya Sayeed
Signature	
Date	11/19/2023

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

When it comes to cybersecurity, we tend to focus more on the things we should do to avoid a cybersecurity incident.[1] While those things are certainly important, cyberattacks are happening more often and with more sophistication because of which an incident happening in your organization is inevitable. Therefore, we should have a proactive response rather than a reactive response for security incidents. For businesses targeted by a cyberattack, recovery is the top-of-mind concern but beyond getting back up and running, it's also important to understand the how and why behind an incident.[1] This is where traditional incidence response is vulnerable giving rise to Digital Forensics Incidence Response (DFIR). DFIR delivers deeper understanding through a comprehensive and intricate forensic process. DFIR specialists gather and inspect a wealth of information to determine who attacked them, how they got in, the exact steps attackers took to compromise their systems, and what they can do to close those security gaps.[1] The aim of this paper is to focus on various areas where the acquired evidence can be analyzed using digital forensics tools and techniques to find the root cause analysis behind the incident.

Keywords— Cybersecurity, cyberattack, Incidence response, digital forensics incidence response, evidence analysis.

CHAPTER 1

INTRODUCTION

A cyber incident can be defined as any event that compromises information confidentiality, integrity, and/or availability which are the core principles of information security that are often referred to as the "CIA triad." [1] Incident response (IR) is a set of activities planned and designed to get IT infrastructure back up and running as quickly as possible while mitigating the overall damage of an incident.[1]

The primary goal is to minimize the impact of the incident, contain the threat, and restore normal operations as quickly as possible. These frameworks are designed to support recovery efforts. In a broader sense, they also help organizations build cyber maturity and proficiency. This may help enhance defenses, stopping attacks and incidents from affecting businesses in the first place. However, what about the lost data and how do you recover it? Also, how do you prove that a cybercriminal attacked your business and address the resulting impact? The solution is "Digital Forensics Incidence Response (DFIR)". [1]

DFIR fuses traditional incident response (IR) activities with digital forensics techniques. Digital forensics involves collecting, preserving, and analyzing forensic evidence. Incident response involves containing, stopping, and preventing a cyberattack. Digital forensics is a branch of forensic science that focuses on the recovery, investigation, and examination of material found on digital devices. The end goal of digital forensics is to gather and preserve evidence to find the root cause of the security incident occur as well as to find the culprits behind an attack to face criminal charges. [1]

There are generally four major reasons why an organization engages in digital forensics:

- To confirm whether a cyberattack occurred. [1]

- To understand the full impact of a cyber incident. [1]
- To identify the cause behind a cyberattack. [1]
- To collect evidence proving a cyberattack occurred. [1]

Like any forensic investigation, speed is critical, especially if an attack is ongoing. Acting fast can help stop active cyber incidents and reduce the overall damage to a victim organization. Computers, networks, and devices are continuously producing data that may be crucial to an investigation, even while sitting idle. Over time, the risk that this data is deleted, overwritten, or otherwise altered increases. Many forensic artifacts are highly dependent on the state of a computer in the immediate aftermath of an incident. Forensic investigators need to move quickly to ensure they capture all this information before it's lost.

CHAPTER 2

BACKGROUND

The digital forensic process is the accepted method investigators follow to gather and preserve digital evidence, with the express intent of maintaining a chain of custody. It consists of three key steps:

Acquisition [1]

In this step, investigators create an exact duplicate of the media in question, usually using a hard drive duplicator or specialized software tools. The original media is secured to prevent any tampering.[1]

Analysis [1]

Forensic specialists then analyze the duplicated files or technology, logging all the evidence they discover that supports or contradicts a hypothesis. Ongoing analysis is conducted to reconstruct events and actions in an incident, helping them reach conclusions about what happened and how hackers compromised systems. [1]

Reporting [1]

Once a digital forensics investigation is completed, the findings and conclusions analysts uncovered are delivered in a report that non-technical personnel can understand.

These reports are passed on to those who commissioned the investigation and usually wind up in the hands of law enforcement. [1]

During the acquisition phase of the digital forensic process, analysts look for a variety of forensic data to help them in their investigation. As you conduct forensic evidence collection, it is important to preserve the original evidence. Remember that the very conduct of your investigation may alter the evidence you are evaluating. Therefore, when analyzing digital evidence, it’s best to work with a copy of the actual evidence whenever possible. For example,

when investigating the contents of a hard drive, make an image of that drive, seal the original drive in an evidence bag, and then use the disk image for your investigation.

On the other side, Incidence Response follows two industry standards for IR frameworks that go into action when cyber threats are detected. These are the NIST and SANS frameworks. [2]

The NIST Cybersecurity Framework is one of the most popular methodologies for managing cybersecurity risk, part of which is the NIST Computer Security Incident Handling Guide. [2]

The NIST suggests an incident response process that involves these four steps [2]:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Post-Incident Activity

SANS (SysAdmin, Audit, Network and Security) with its sole focus on security, has become an industry standard for many things, one of which is their Incident Handler's Handbook. Like NIST, the SANS incident response process follows six steps [2]:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Figure 1 below portrays steps for Incidence response framework from both NIST as well as SANS.

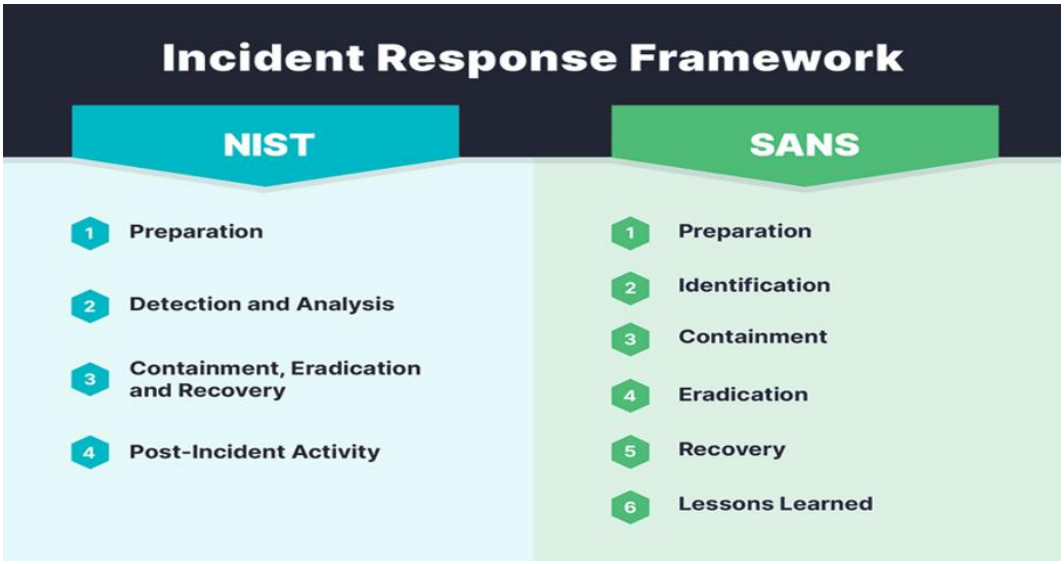


Figure 1:Incidence Response Framework

However, there are challenges in traditional Incidence Response which are as follows.

Preparedness [3]

It is important to have a well-documented and tested incident response plan where all the stakeholders are identified, and everyone understands their role and responsibilities. Without this, teams may struggle to respond promptly and effectively when an incident occurs. [3]

Inadequate Detection Capabilities [3]

Organizations may lack the necessary tools and technologies to detect incidents in real-time. Without robust monitoring and observability tools, suspicious behavior can go undetected for extended periods, putting you at risk for significant damage. [3]

Evidence Collection [3]

Properly preserving and analyzing audit logs is critical for understanding the scope and impact of an incident. [3]

Alert Fatigue [3]

If a trigger is too sensitive, you risk alert fatigue, which can erode confidence or suppress the notification of a real incident. Addressing these challenges requires a proactive approach to

incident response. Organizations should invest in incident response planning, regular training and simulations, and effective communication structures to enhance their incident response capabilities. [3]

In this project, the following digital forensic tools were used. The justification for selecting these tools are twofold. First, these are the most popular tools available in the market. Second, they offer trial versions for research and evaluation purposes.

- NetWitness Investigator [6].
- Wireshark [7].
- Access data Forensic Tool Kit [8]
- Paraben's Electronic Evidence Examiner (E3) [9].

To perform the experiment, the test data was created from my own laptop's selected folders of C: drive to conduct media analysis and memory analysis. For Hardware/Embedded Device Analysis, data acquisition from a mobile device such as smart phone was performed. The test mobile phones were collected from the Forensics Lab. For Network analysis, a sample DOS attack was downloaded from GitHub.

The experiment was performed on a laptop with following hardware configuration:

Processor: 11th Gen Intel(R) Core (TM) i5-1135G7 @ 2.40GHz 1.38 GHz

Installed RAM: 8.00 GB

System type: 64-bit operating system, x64-based processor.

CHAPTER 3

PROPOSED METHOD

As part of Digital Forensics Incidence Response, a comprehensive analysis was conducted using digital forensics tools and techniques.

The first proposed analysis for this project is Network Analysis [4]. Forensic investigators are also often interested in the activity that took place over the network during a security incident. This is often difficult to reconstruct due to the volatility of network data—if it isn't deliberately recorded at the time it occurs, it generally is not preserved. Network forensic analysis, therefore, often depends on either prior knowledge that an incident is under way or the use of preexisting security controls that log network activity. These include:

- Intrusion detection and prevention system logs.
- Network flow data captured by a flow monitoring system.
- Packet captures deliberately collected during an incident.
- Logs from firewalls and other network security devices.

When collecting data directly from a network during a live analysis, forensic technicians should use a SPAN port on a switch (which mirrors data sent to one or more other ports for analysis) or a network tap, which is a hardware device that performs the same function as a SPAN port. Both approaches generate packet dumps without altering the network traffic being exchanged between the two systems. In cases where this is not possible, the analyst may run a software protocol analyzer on one of the communicating systems, but this approach is not as reliable as using a dedicated hardware device. After collecting network packets, they should be treated in the same manner as any other digital evidence. The tools creating the packet capture should write them to forensically prepared media. Analysts should compute cryptographic hashes of the original evidence files and work only with copies of those original

files. The task of the network forensic analyst is to collect and correlate information from these disparate sources and produce as comprehensive a picture of network activity as possible. The digital forensic tools used for network analysis are “RSA Netwitness Investigator” and “Wireshark”.

The second proposed analysis for this project is In-Memory Analysis [4]. Investigators often wish to collect information from the memory of live systems. This is a tricky undertaking since it can be difficult to work with memory without altering its contents. When gathering the contents of memory, analysts should use trusted tools to generate a memory dump file and place it on a forensically prepared device, such as a USB drive. This memory dump file contains all the contents collected from memory and may then be used for analysis. As with other types of digital evidence, the analyst collecting the memory dump should compute a cryptographic hash of the dump file to later prove its authenticity. The analyst should preserve the original collected dump and work from copies of that dump file. The digital forensic tools used for memory analysis is “Paraben’s Electronic Evidence Examiner”.

The third proposed analysis for this project is Media Analysis [4]. Media analysis, a branch of computer forensic analysis, involves the identification and extraction of information from storage media. This may include magnetic media (e.g., hard disks, tapes) or optical media (e.g., CDs, DVDs, Blu-ray discs). Techniques used for media analysis may include the recovery of deleted files from unallocated sectors of the physical disk, the live analysis of storage media connected to a computer system (especially useful when examining encrypted media), and the static analysis of forensic images of storage media. When gathering information from storage devices, analysts should never access hard drives or other media from a live system. Instead, they should power off the system (after collecting other evidence), remove the storage device, and then attach the storage device to a dedicated forensic workstation, using a write blocker. Write blockers are hardware adapters that physically sever the portion of the cable used to

connect the storage device that would write data to the device, reducing the likelihood of accidental tampering with the device. After connecting the device to a live workstation, the analyst should immediately calculate a cryptographic hash of the device contents and then use forensic tools to create a forensic image of the device: a bitwise copy of the data stored on the device. The analyst should then compute the cryptographic hash of that image to ensure that it is identical to the original media contents. After creating and verifying a forensic image, the original image file should be preserved as evidence. Analysts should create copies of that image (verifying the integrity of the hash) and then use those images for any analysis. This careful process reduces the likelihood of error and ensures the preservation of the chain of custody. The digital forensic tools used for media analysis are "AccessData Forensic Tool Kit Imager" and "Paraben's Electronic Evidence Examiner."

The fourth proposed analysis for this project is Hardware/Embedded Device Analysis [4]. Forensic analysts often must review the contents of hardware and embedded devices. This may include a review of:

- Personal computers
- Smartphones
- Tablet computers
- Embedded computers in cars, security systems, and other devices.

Analysts conducting these reviews must have specialized knowledge of the systems under review. An organization may have to call in expert consultants who are familiar with the memory, storage systems, and operating systems of such devices. Because of the complex interactions between software, hardware, and storage, the discipline of hardware analysis requires skills in both media analysis and software analysis. The current project portrays data acquisition and analysis from an Android Smart phone. In this project, digital data from the smartphone will be acquired and analyzed using Paraben's E3.

The proposed method of Digital Forensics Incidence response follows 5 core functions of the NIST Cybersecurity Framework. The Framework's core consists of five elements that work together to achieve desired cybersecurity outcomes. Each of these five functions has a set of actions that can be included in the organization's cybersecurity policy. [5]

Identify [5]

This function lays the foundation for a robust cybersecurity program. It helps organizations improve their understanding of cybersecurity risk management regarding people, systems, assets, and data.

Protect [5]

This function helps the organization take steps to reduce the number of possible attacks, intrusions, or breaches, and limit the damage that can be done if an attack is successful. This involves developing and implementing safeguards to ensure the organization is ready for an attack and has a plan in case safeguards fail.

Detect [5]

This function helps organizations implement appropriate measures to quickly identify cybersecurity incidents. It requires a continuous monitoring solution to detect anomalous activity and other threats to the continuity of operations. Organizations need network visibility to predict network events and have all actionable information that security teams can react to. Continuous monitoring and threat hunting are effective ways to analyze and prevent cyber incidents.

Respond [5]

This function helps contain and minimize the impact of potential cybersecurity incidents by taking appropriate response actions when an incident is detected.

Recover [5]

This function helps the organization restore a function or service affected by cybersecurity incidents to normal operations. A timely recovery is critical to mitigating the impact of cybersecurity incidents.

CHAPTER 4

IMPLEMENTATION

The implementation is first started with Network analysis wherein a sample packet capture is taken and analyzed for any cyber-attacks. By using Wireshark, TCP and UDP packets are investigated to check for any anomalies. In our experiment, a DOS attack is detected because of the anomalies in the TCP handshake. There were humungous TCP packets with 4 SYN and SYN/ACK packets. However, there were over 2000 packets with FIN packets which gave an idea that the TCP handshake was not smooth. On further looking into the issue, there were a lot of redundant FIN, PSH and URG packets originating from various source IP addresses to the same destination at the rate 5 packets at the same time. This hints us for a DDOS attack but the MAC address of all the source IP addresses is the same which leads us to a conclusion that it is DOS attack with spoofed IP addresses. The attacked machine was then disconnected from the network to contain the attack and avoid further spread. The memory analysis is performed on the victim's live machine to capture the memory from non-volatile as well as volatile storage spaces like RAM so that no data is lost. Memory analysis performs physical acquisition which is a bit-by-bit copy of the entire drive from allocated as well as unallocated spaces of the drive. The advantage of copying the memory is that even the deleted files can be recovered from the memory dumps. Sometimes, the memory dumps are difficult to convert to a readable memory format for analysis. Therefore, media analysis was also performed which captures the logical memory of the drive which means only the allocated spaces of the drive. The content in this method is easily readable for analysis. Once the logical memory was capture, a forensic image drive was created using Access Data FTK and saved the image drive in .ad1 format. The investigation was carried out using Paraben's E3 in which email database was also investigated to analyze email headers for any phishing emails. Lastly,

acquisition of data from a smartphone was also portrayed in Embedded/Hardware analysis to analyze the data contacts, SMS, call logs, applications installed on the mobile device.

Network Analysis

The idea of network analysis is to detect the security incident during the attack as part of threat intelligence so that it provides a proactive approach rather than reactive approach.

Network analysis using RSA NetWitness Investigator. NetWitness Investigator is an interactive threat analysis application of the RSA NetWitness product suite. Investigator provides security operations staff, auditors, fraud, and forensics investigators with the power to perform free-form contextual analysis of raw network data. Investigator collects network traffic live or accepts imported .pcap files providing unprecedented detail, interactive navigation, and dynamic analysis across all network layers. [6]

1. To create a collection, first make sure the collections page is visible. On the collection toolbar, click the New Local Collection icon as shown in Figure 2 below.

Figure 2: Creation of new local connection.

2. Enter a unique name for the new collection in the New Local Collection dialog box as shown in Figure 3. Specify a location for the new collection if you want it saved other than the displayed folder by checking the Override Default Location checkbox.

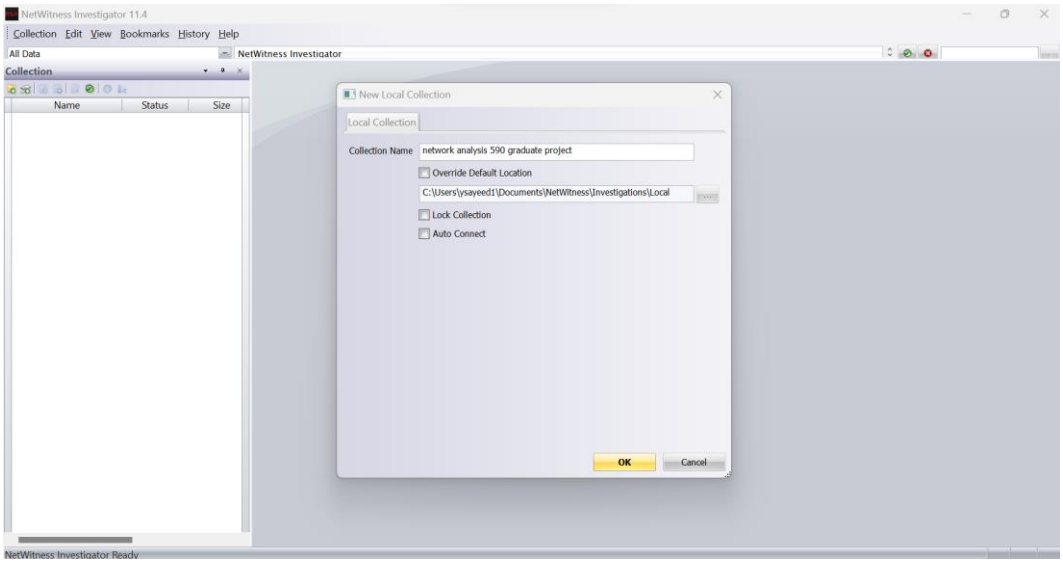


Figure 3:Local Collection wizard

3. Check the Lock Collection checkbox if you want to prevent the collection from being deleted or used for future capture/import. Check the Auto Connect checkbox if you want the collection to open each time you open Investigator.

4. To import a packet file (.pcap, .tcp, etc.) into one of your collections, click the row in the Collections Page that corresponds with the collection into which the packets will be imported.

5. Click on the Import Packets from the File menu as shown in Figure 4 to bring up a Windows Explorer dialog and find the packet file(s) you wish to import. Press "Open" to import the packet capture file as shown in the Figure 5.

Figure 4:Import captured packets.

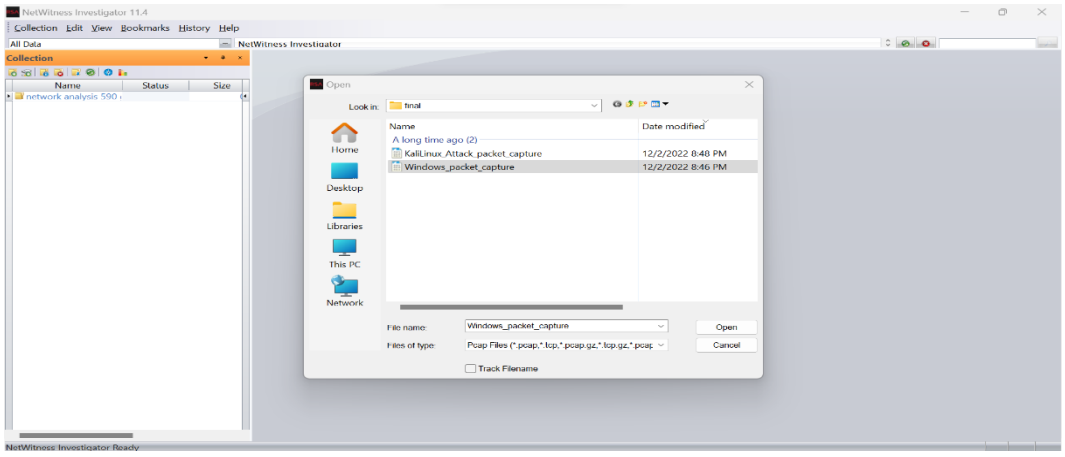


Figure 5:Open packet capture file in NetWitness Investigator

6. You should now see a progress bar in the collection row indicating status of import of your packet files. This is depicted in Figure 6 below:

Figure 6:Packet import status bar

7. Once the import is finished and the collection is "Ready" you can begin interacting with the newly imported packets. Refer Figure 7 below:

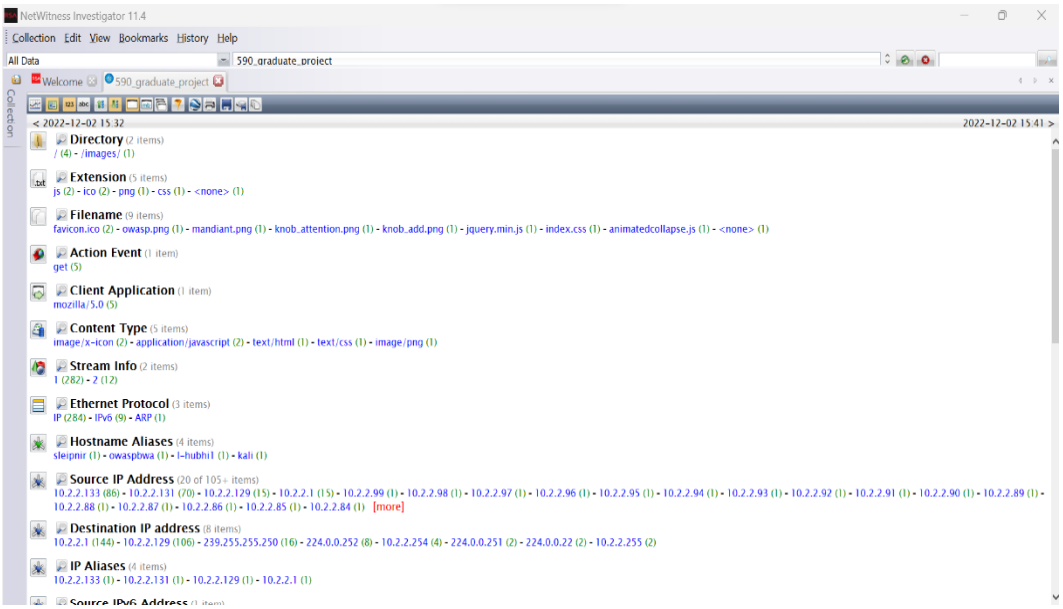


Figure 7:Default view of imported packet capture file.

8. Click Toggle Timeline to monitor the traffic as shown in Figure 8. You can see a steep rise in traffic in Figure 9 for a certain period on the time graph.

Figure 8: Toggle Timeline

Figure 9: Timeline graph of network traffic

9. Select the above highlighted timeline to inspect deeper into the traffic for anomalies. This is depicted in Figure 10 below with a zoomed in view.

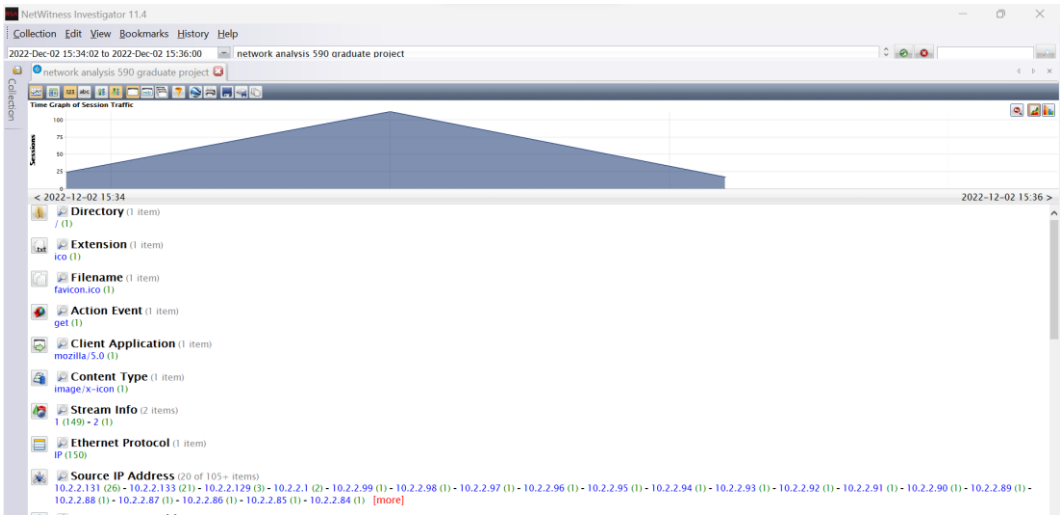


Figure 10: Zoomed in view Time graph of network traffic.

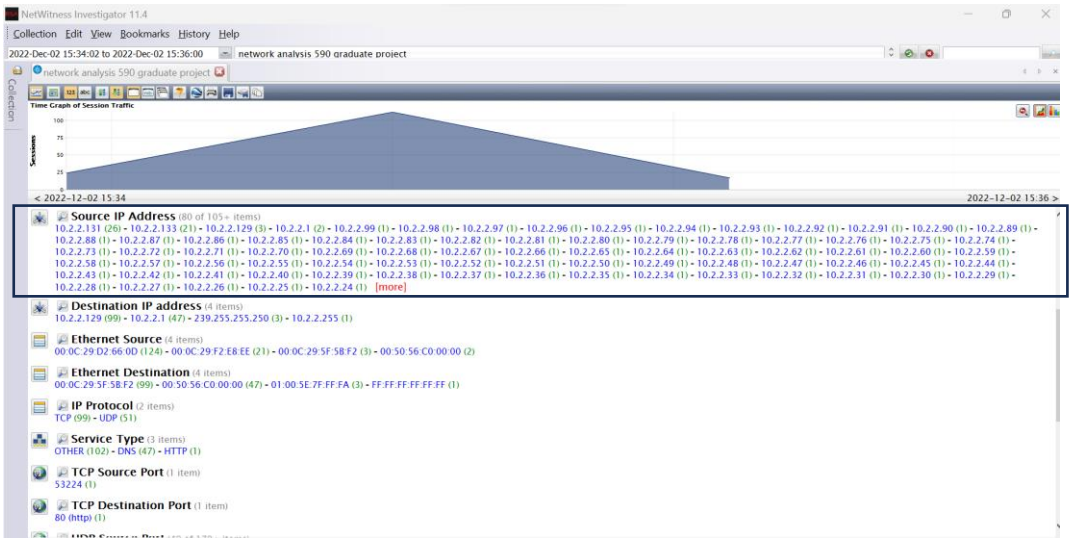


Figure 11:Source IP address entries.

10. From the above Figure 11, we observe that there are 102 source IP addresses with different IP addresses. However, there are few different destination IP addresses predominantly to 10.2.2.129 (99 hits) and 10.2.2.1(47 hits). This is portrayed in Figure 12.

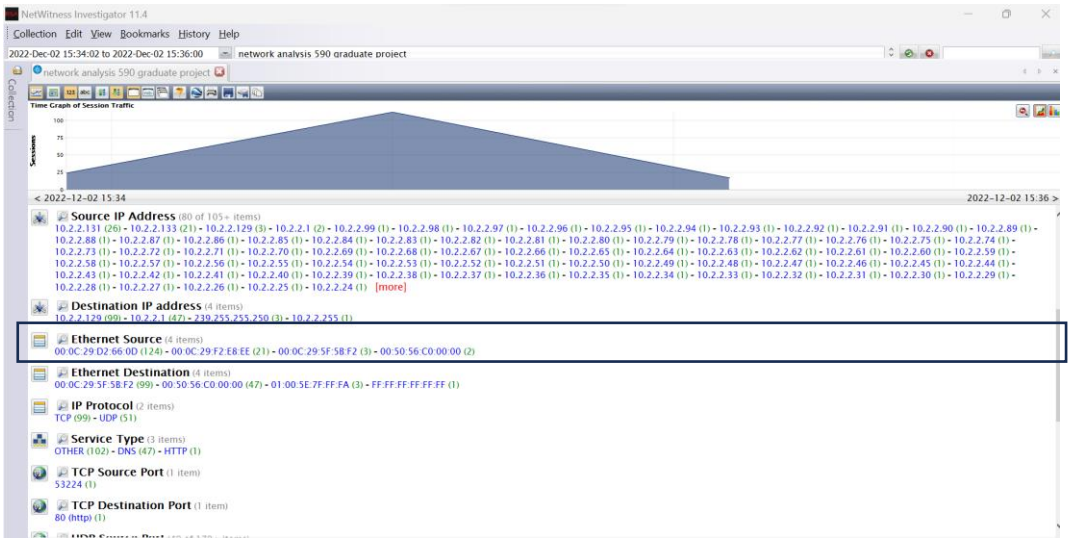


Figure 12: Destination IP address entries.

11. 47 hits for 10.2.2.1 are packets for various host looking up for its domain name from the DNS server. Couple of such packets are shown in Figure 13 and Figure 14 below for instance:

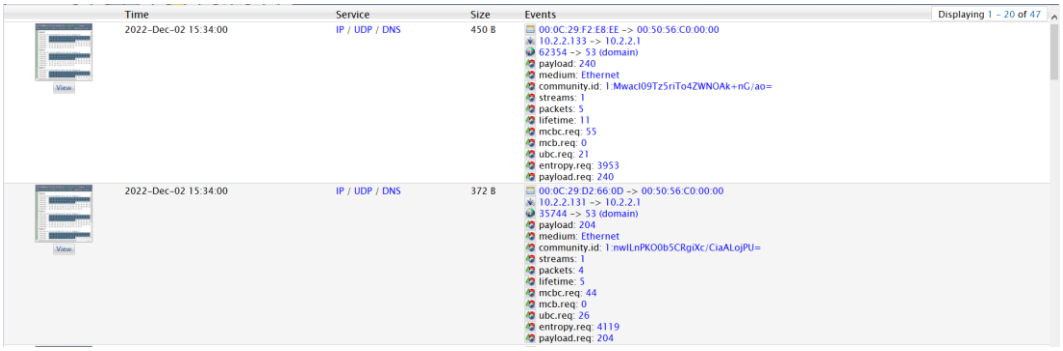


Figure 13: DNS packets for couple of instances

12. 99 hits for 10.2.2.129 is interesting. Only 1 packet is in regard to HTTP connection.

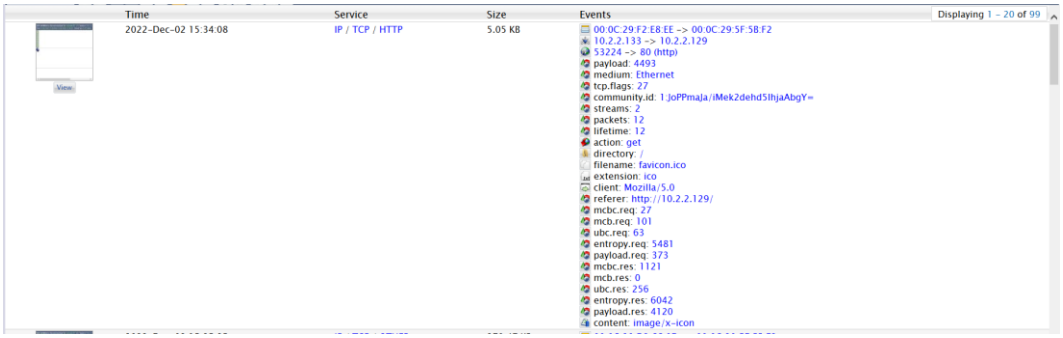


Figure 14: TCP packet for an instance

13. Rest all packets seems to be fake redundant packets at the rate of around 7 packets sent to the server at the “same time” from the same MAC address but different IP address. Refer below Figure 15.

Figure 15: Fake Redundant packets

14. The above scenario proves that this is DOS attack with spoofed IP addresses onto 10.2.2.129. Escalate to the SOC engineers and upward management to confirm the security incident so that the incident can be contained during the incident itself. This can be done by disconnecting the host 10.2.2.129 from the network to contain damage so that attackers don’t attack other hosts on the network.

15. Next, I won’t shut down the host computer since we want to recover any data loss not only from ROM but also from volatile RAM. Now, we move on to the in-memory analysis.

Network analysis using Wireshark. The steps are as follows:

1. Import the packet capture file into Wireshark as shown in Figure 16:

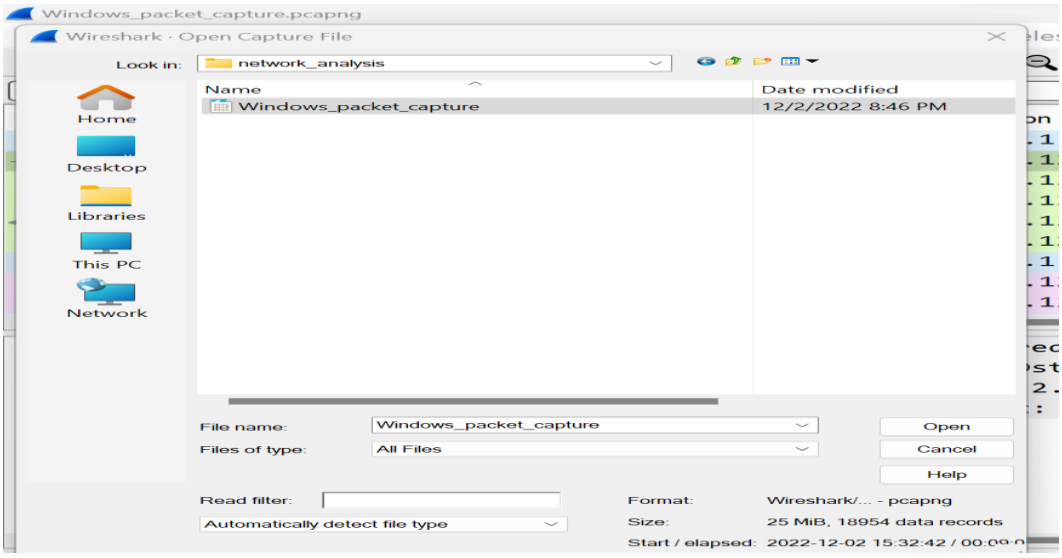


Figure 16: Importing packet capture file in Wireshark.

2. There are in total 18954 packets in this pcap file. Refer below Figure 17.

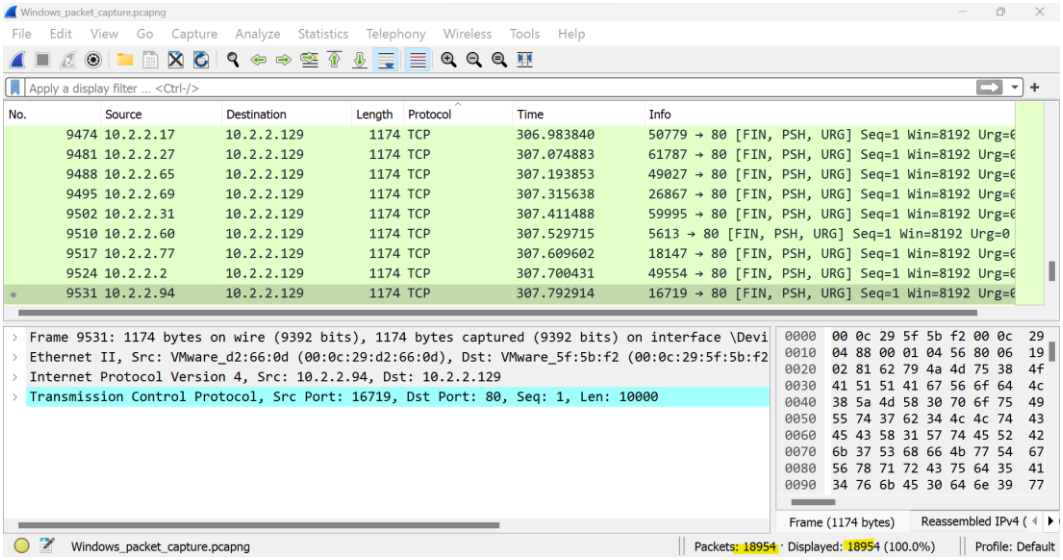


Figure 17: Default view of Wireshark

3. Enter tcp.flags filter to view the TCP packets. This is depicted in Figure 18.

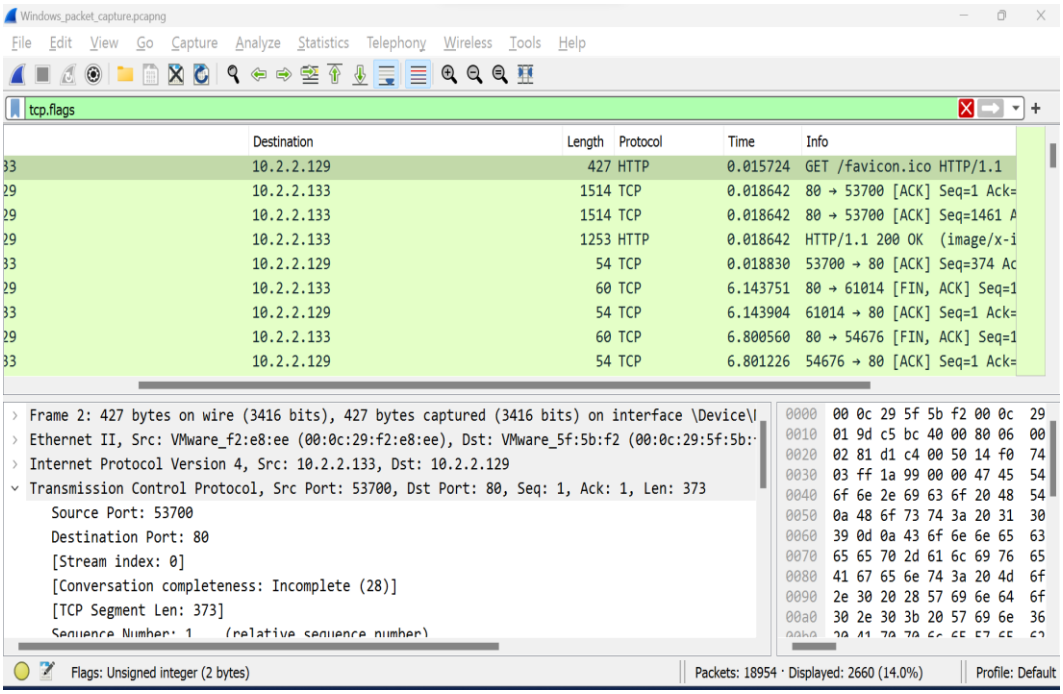


Figure 18: TCP flags filter

4. Now let's check how many TCP handshakes were successful. We can count the number of SYN and ACK packets to tally it from Figures 19 and 20 respectively.

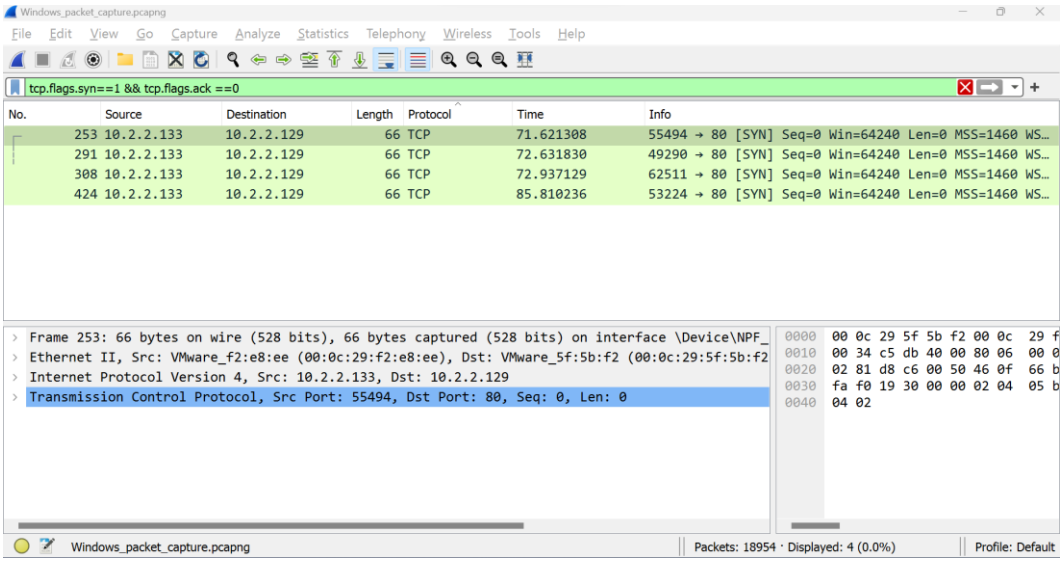


Figure 19: TCP SYN packets

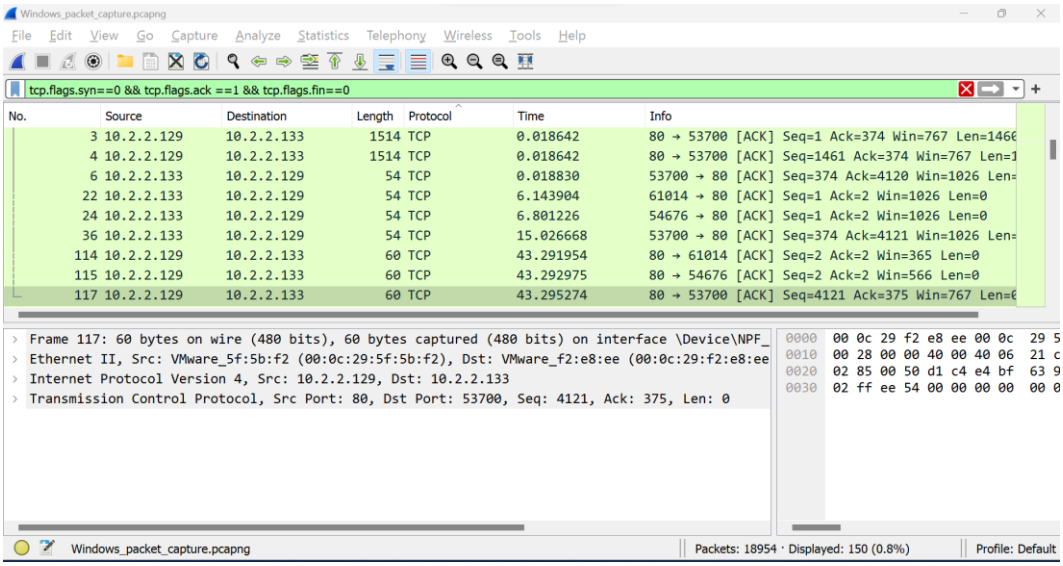


Figure 20: TCP ACK packets

5. There were 4 SYN packets sent but 150 ACK received. This means that the TCP handshake was not smooth.

6. The other flags we can check here are PSH, RST to gain deeper insight. Refer below Figure 21.

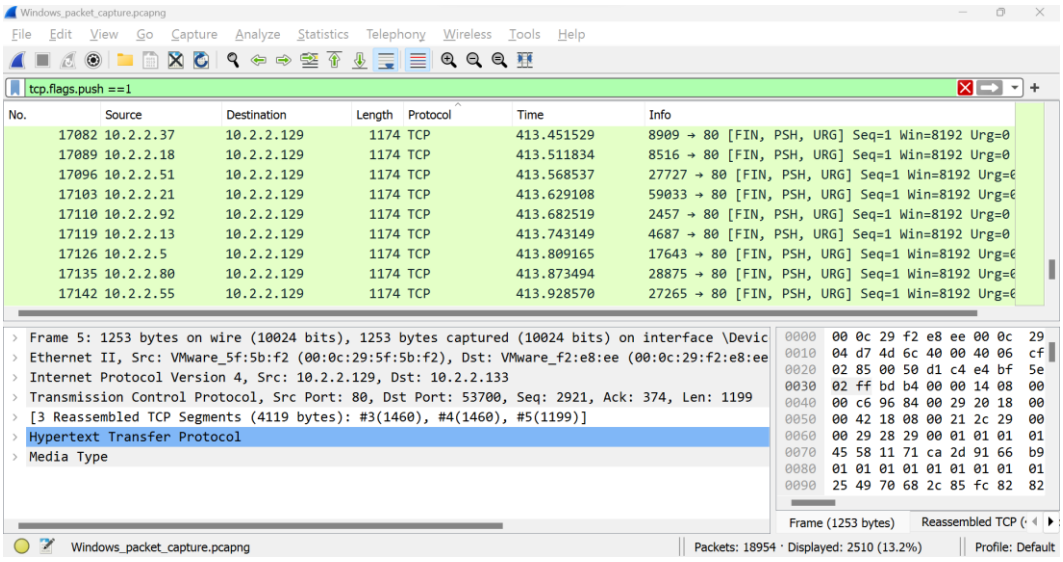


Figure 21: TCP FIN, PSH, URG packets

7. There were no RST hits. However, there were 2510 PSH hits for only 4 packets of SYN, SYN/ACK and 150 packets of FIN. Moreover, these were FIN, PSH and URG packets which look to be coming from various source IP addresses but to the same destination i.e., 10.2.2.129.

FIN packets are used to gracefully terminate the connection. If they want to communicate again, they will start from the beginning, that is, from the three-way handshake process.

PSH packets indicate that the incoming data should be passed on directly to the application instead of getting buffered. To state this simply, the other host should receive data without waiting for it.

URG packets indicate that the data that the packet is carrying should be processed immediately by the TCP stack and the urgent pointer field should be examined if it is set.

8. In addition, we observed that these packets have the same length, similar time interval, same destination address and also same MAC address but originating from various different IP addresses. Refer Figure 22 below:

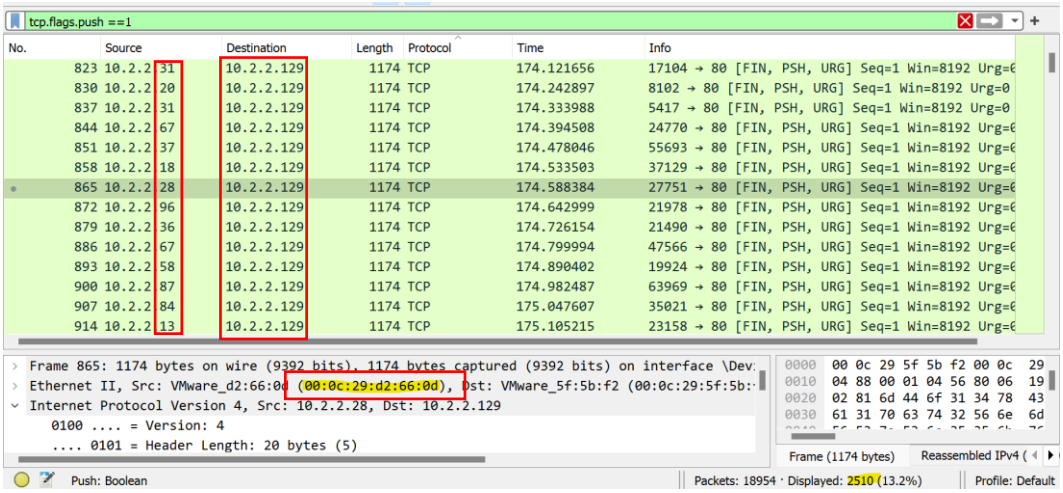


Figure 22: Spoofed source IP address

9. The last octet of the source IP address seems to be spoofed. The redundant fake FPU tcp packets for only 4 SYN packets with same MAC address throughout confirms this to be a DOS attack. This needs to be escalated to SOC engineer and upward management for further DFIR steps to contain the incident. The team should immediately look for segregating the victim machine from the network.

In-Memory Analysis

In this project, I conducted the memory analysis from a live workstation wherein my own laptop's C: drive was used to perform the experiment.

In-memory analysis using Paraben's E3. The E3 Forensic Platform seamlessly adds a large variety of evidence into a single interface to be able to search, parse, review, and report on the

digital data from most digital sources. It allows processing of all types of digital evidence quickly with an Easy interface, Efficient engines, and Effective workflow [9]. The step-by-step process are as follows:

1. Launch Paraben's Electronic Evidence Examiner and click "Add Evidence" as shown in Figure 23 below:

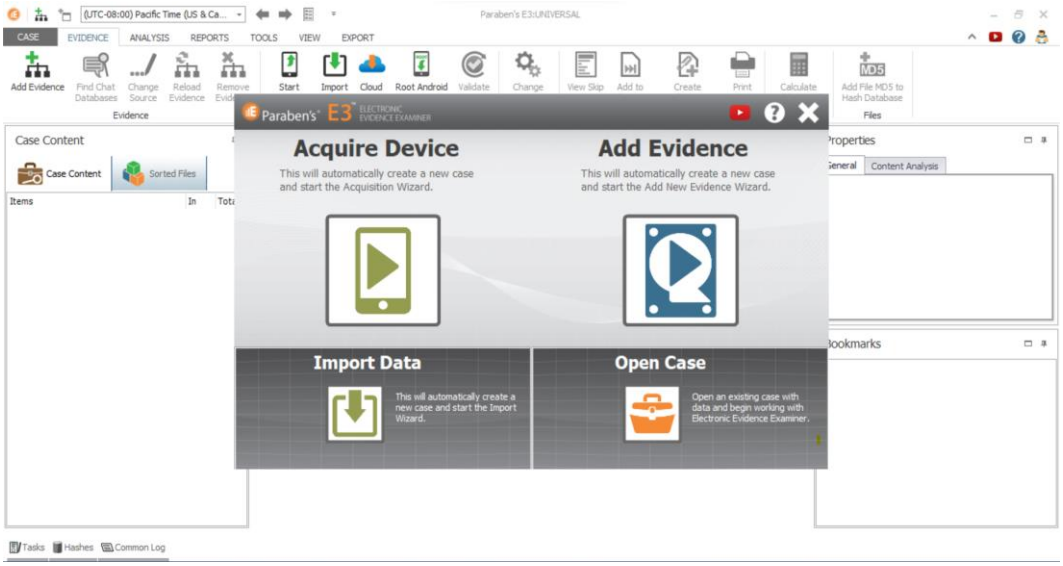


Figure 23: Launch view of Paraben's E3

2. Enter the Case name and location where you want to store the memory dump post-acquisition. This is portrayed in Figure 24.

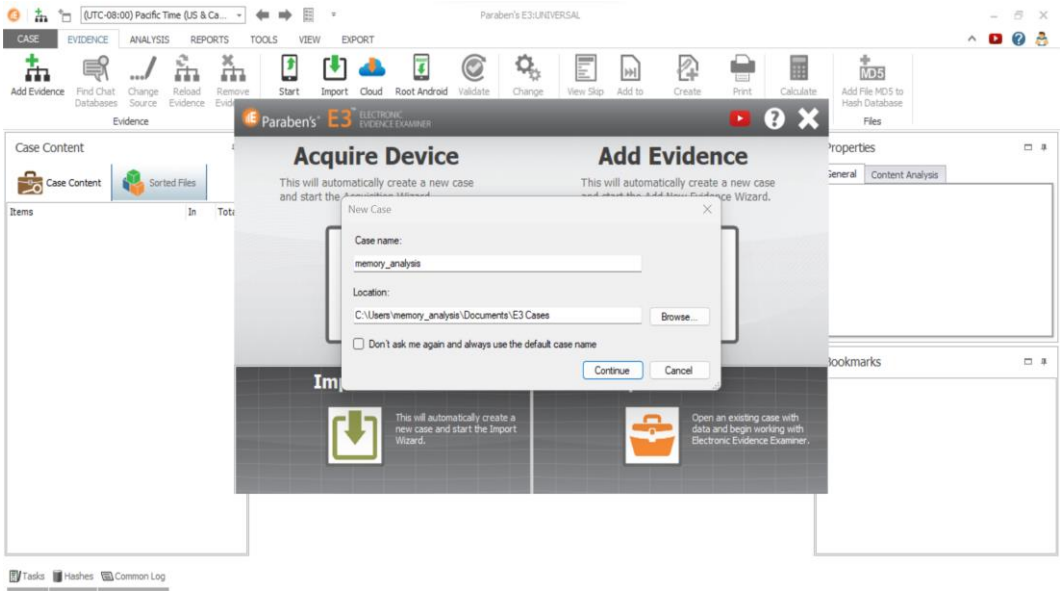


Figure 24: Case details name and location.

3. Select Logical drive or Folder and click C: drive as source type as shown in Figure 25 below:

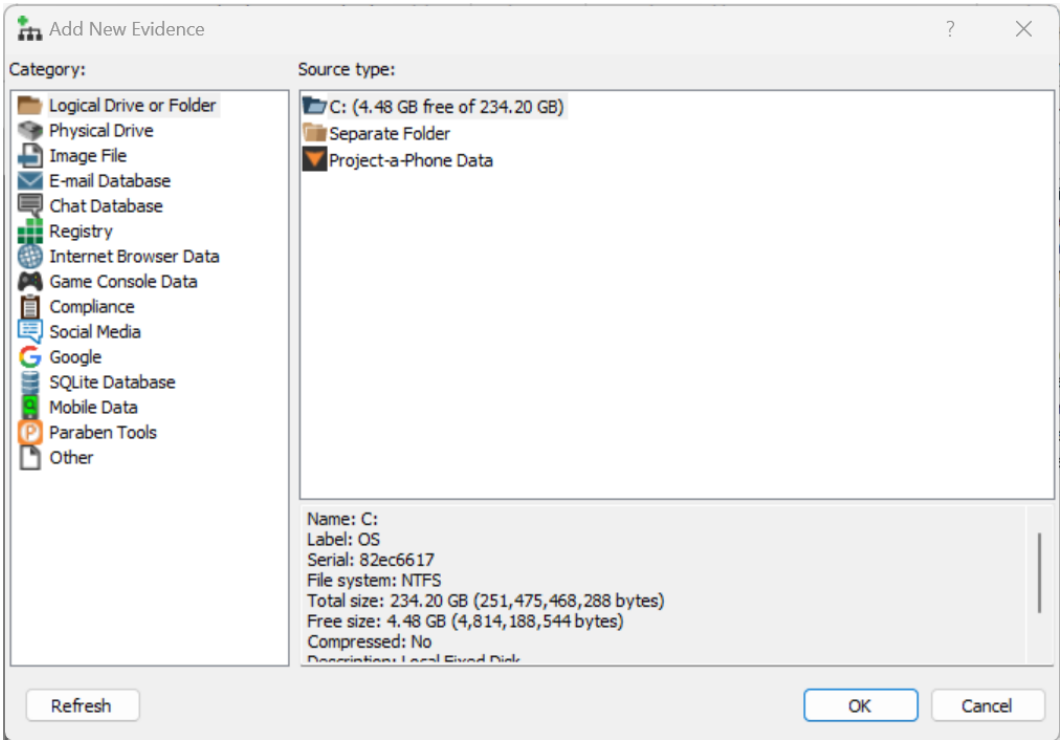


Figure 25: Adding C: drive as evidence.

4. Select Search for deleted files and folders in NTFS settings and click OK as shown in Figure 26.

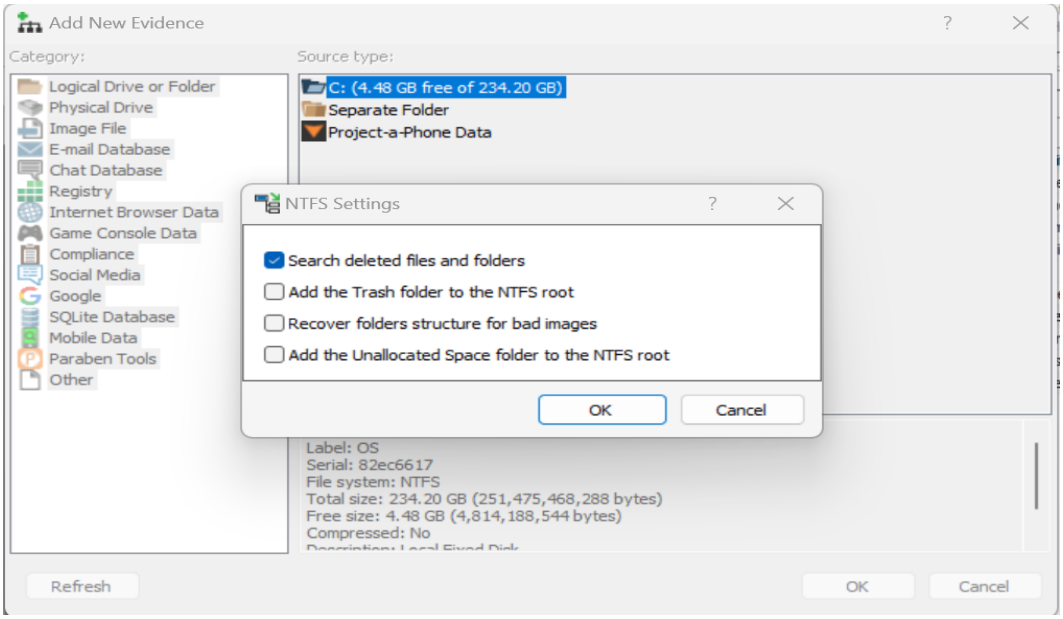


Figure 26: NTFS settings

5. Expand the added evidence on the left pane from Case Content tab and expand Data Triage folder. Refer Figure 27 below:

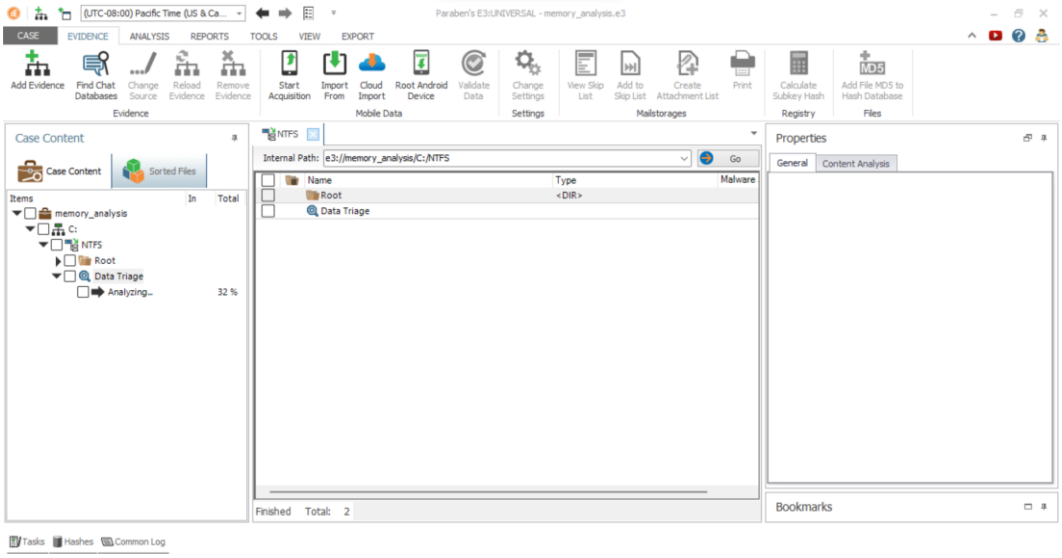


Figure 27: Case Content Tab with Data Triage

6. The hard drive has various memory sectors on which NTFS file system is responsible to organizes the files on each partition of the hard drive. For every deletion of the file the master table will be updated by the NTFS of its new location. The file is not deleted entirely until any new data overwrites the new location of the deleted file on the hard drive. That is why a forensic analyst should first acquire the data and transfer the dumps into USB or external hard drive and work on the copy for further investigation to collect as much data as possible from the memory.

7. Moving further, the data triage folder contains all the files including the deleted files from the drive. The files in the red font in Figure 28 are the ones which are deleted.

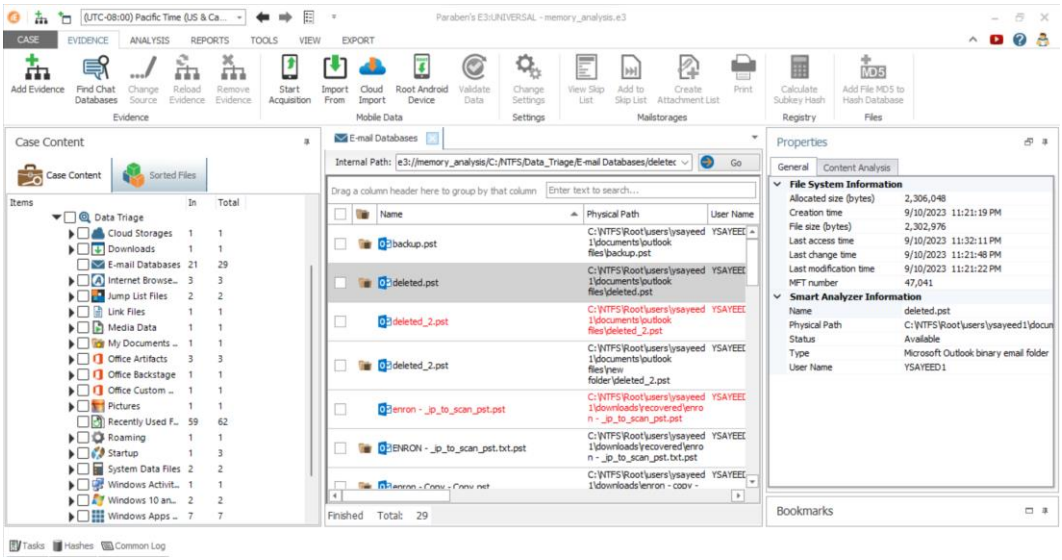


Figure 28: Data Triage view with contents of sub-folders.

8. The forensic tool is able to recover the deleted files because performs a physical acquisition which means the data is captured from the memory of the drive. The beauty of in-memory analysis is that it recovers even the deleted files which may be deliberately deleted by the culprit.

9. Apart from the recovery, cryptographic hash values and metadata values are also extracted by Paraben's E3. There's also option for performing Optical Character Recognition which extracts text from the acquired files to cater indexing and searching across the added evidence.

10. The deleted files can be exported as shown in Figure 29 below.

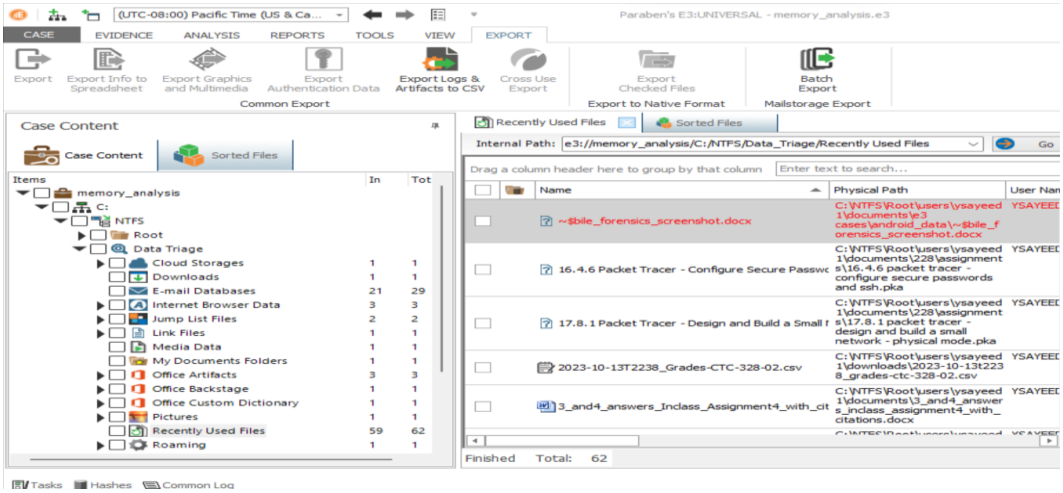


Figure 29: Deleted files extracted by Paraben's E3

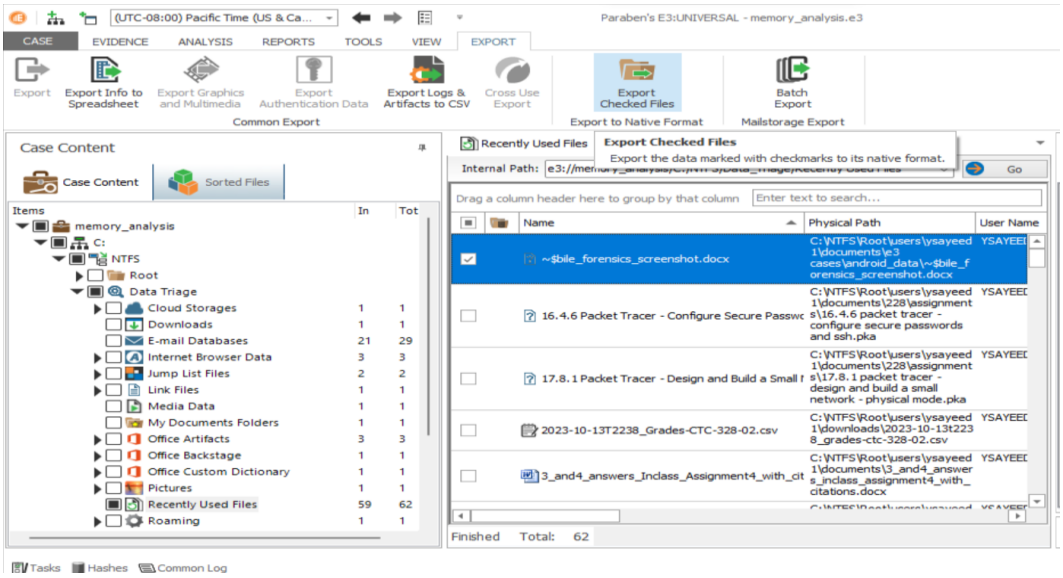


Figure 30: Export of files from Paraben's E3

11. The data can be selected and exported to the same location as specified in Step2. This can be observed in Figure 30 above.

Media Analysis

The media analysis for this project will be divided into two parts in this section: Firstly, a forensic image file will be created from selected folders of my own C: drive. Secondly, the created forensic image file will be mounted in Access FTK to view the contents of the image file. Also, the same image file will also be imported into Paraben's E3 to view the contents of the image file from within the tool itself. The steps are as follows:

1. To create a forensic image file, launch AccessData FTK Imager tool and select Create Disk Image from the File menu in the toolbar. Refer Figure 31 below:

Figure 31: Create Disk Image option.

1. Select the evidence type as shown in Figure 32 below:

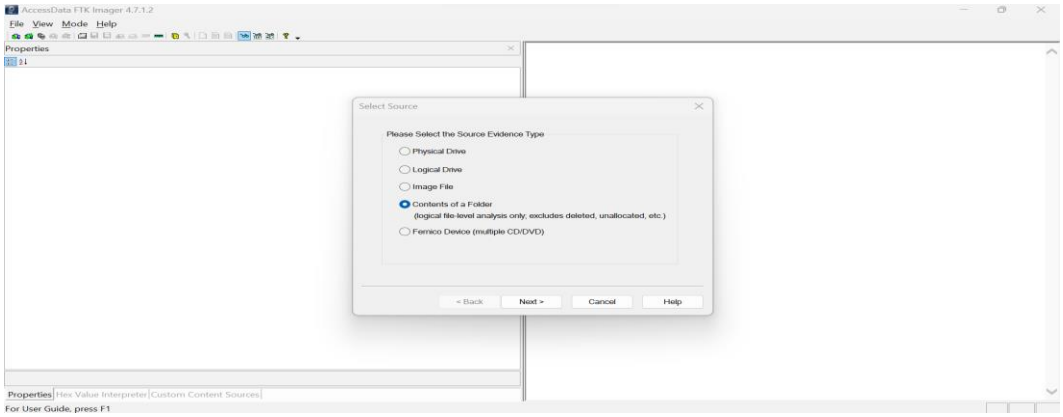


Figure 32: Source selection for forensic image creation

2. Specify the source path which needs to be imaged. In this experiment only selected folder of the C: drive has been acquired to avoid memory issues. This is shown in Figure 33 below. In real time however, the whole disk is generally imaged.

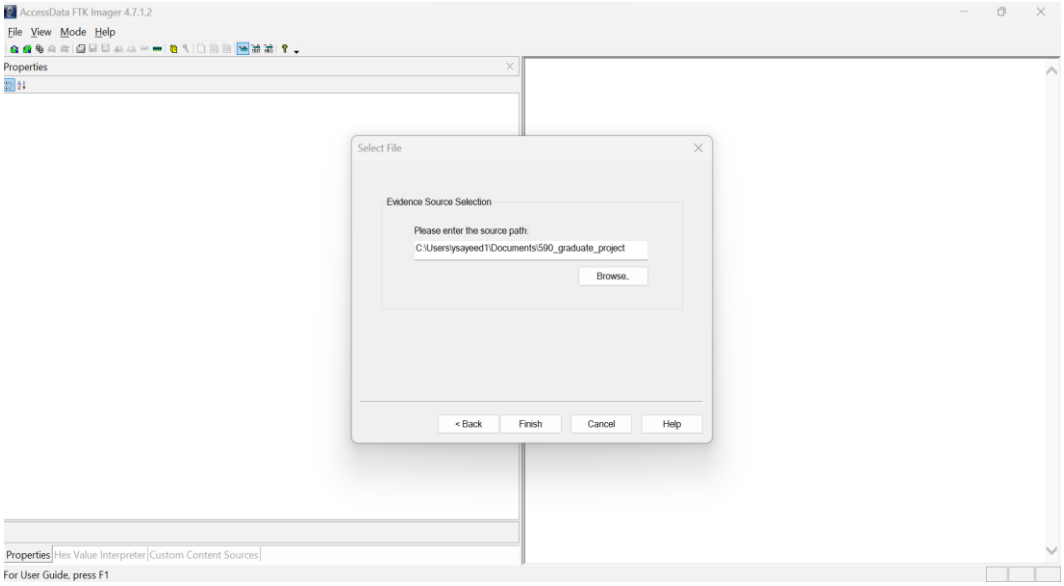


Figure 33: Source path specification

3. Enter the name of the image and destination path where the forensic image file will be saved. Refer Figure 34.

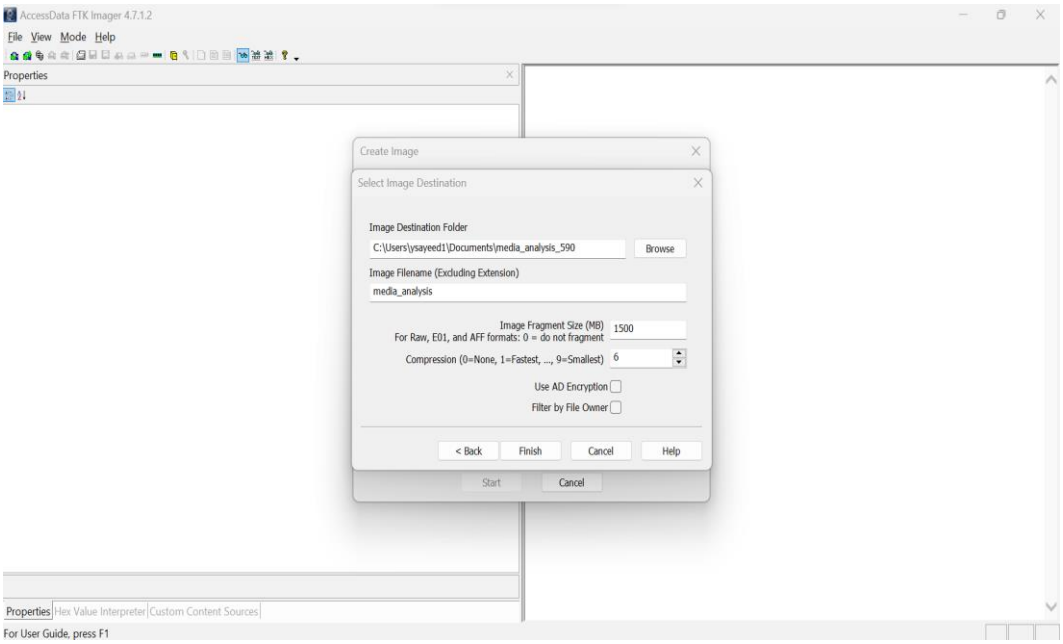


Figure 34: Image name and destination path

4. Click Finish and the tool starts creating image in .ad1 format. This is depicted in Figure 35.

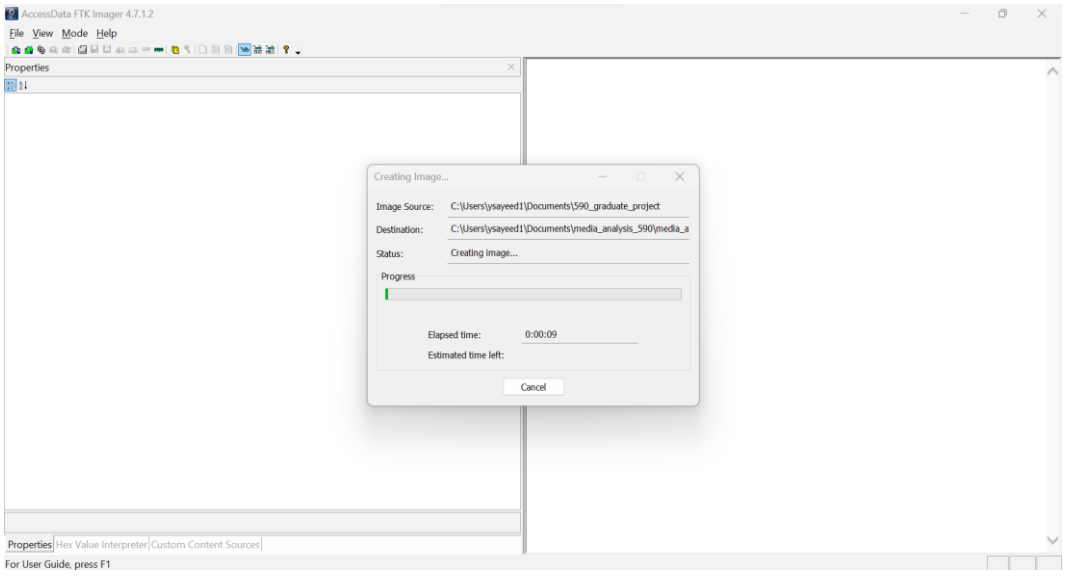


Figure 35: Image creation status

5. Close the dialogue box once the image is successfully created.

6. Note and save the cryptographic hash values which mark the authenticity of the evidence from any alterations. This is depicted in Figure 36.

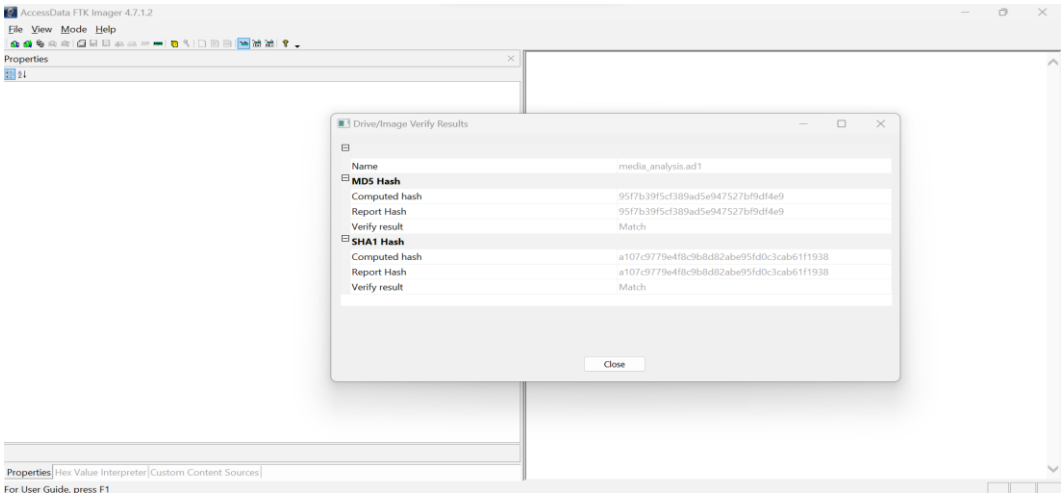


Figure 36: Image results with hash verification

7. The image drive will be saved in the destination path along with a text file which consists of the information about the start/end date and time of the acquisition. It also saves the hash values for the investigator to cross-check the authenticity as shown in the Figures 37 and 38 below:

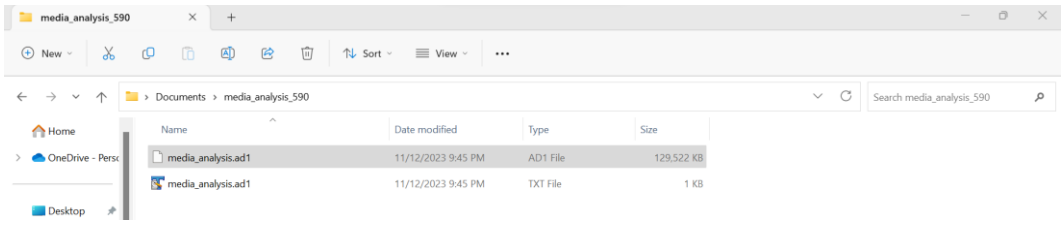


Figure 37: Destination directory

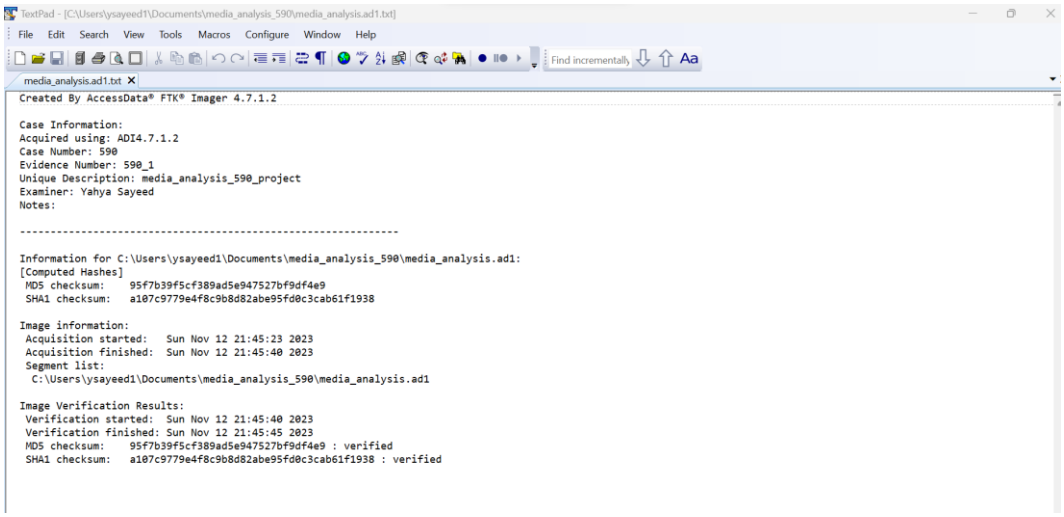


Figure 38: Case information results

8. The contents of the image file can also be viewed by mounting on mapping to a free drive. Select Image mounting from the File menu as shown in Figure 39 below.

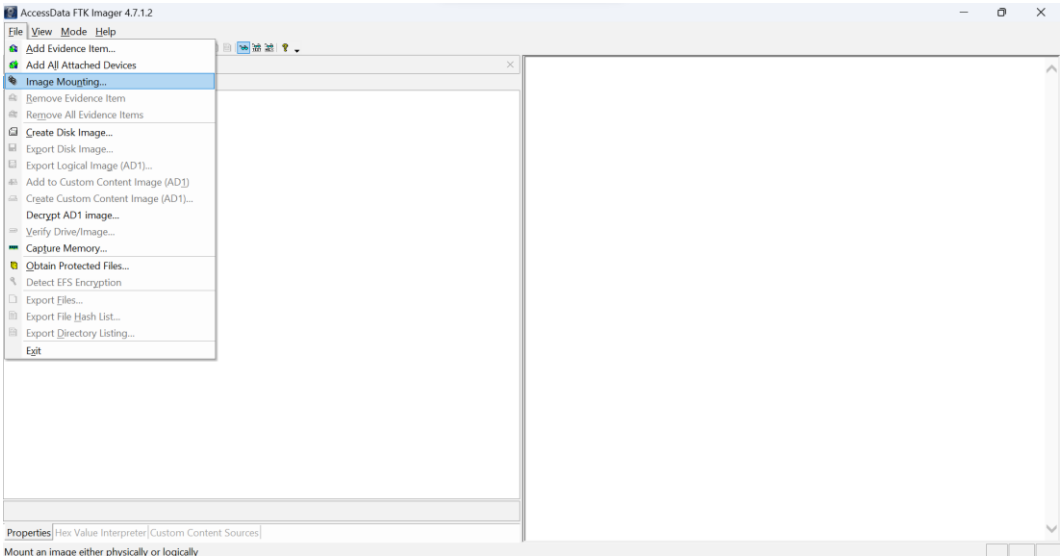


Figure 39: Image mounting in Access Data FTK

9. Select the image drive and map it to a free drive (D: drive in this case). Refer Figure 40 below:

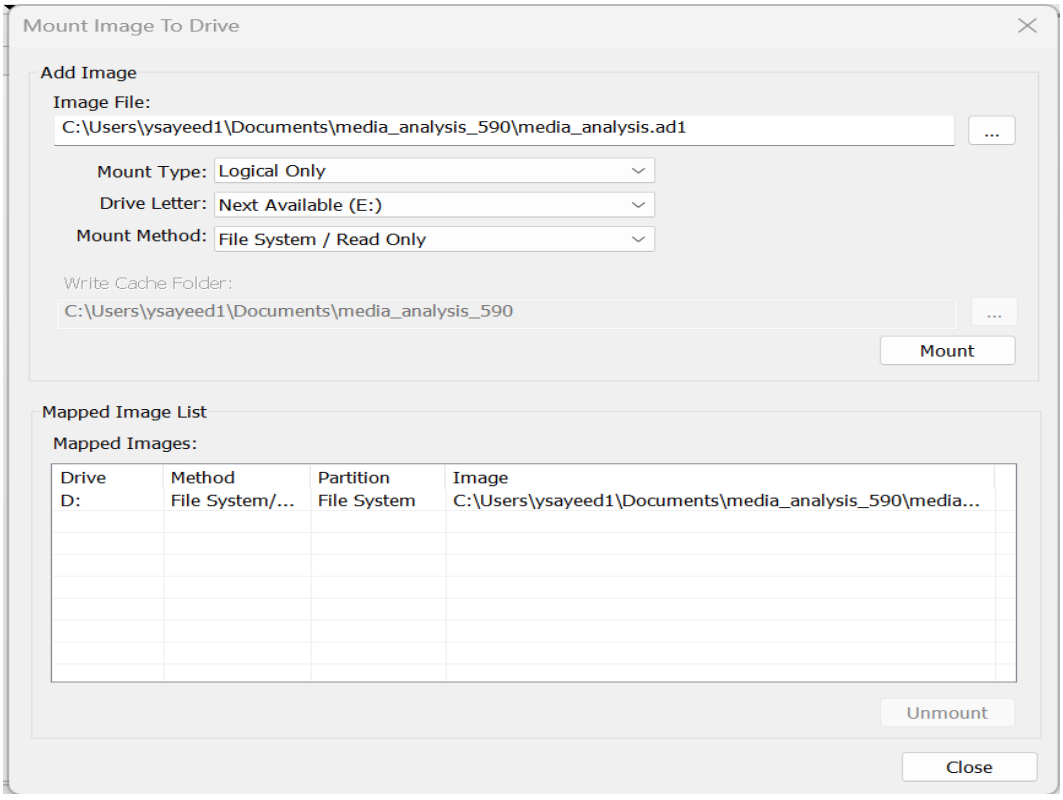


Figure 40: Image mount mapping to free drive

10. Once mounted, you can open the mapped drive directory, D: drive in this case and view all the files and folders of the image drive as shown in Figure 41 below:

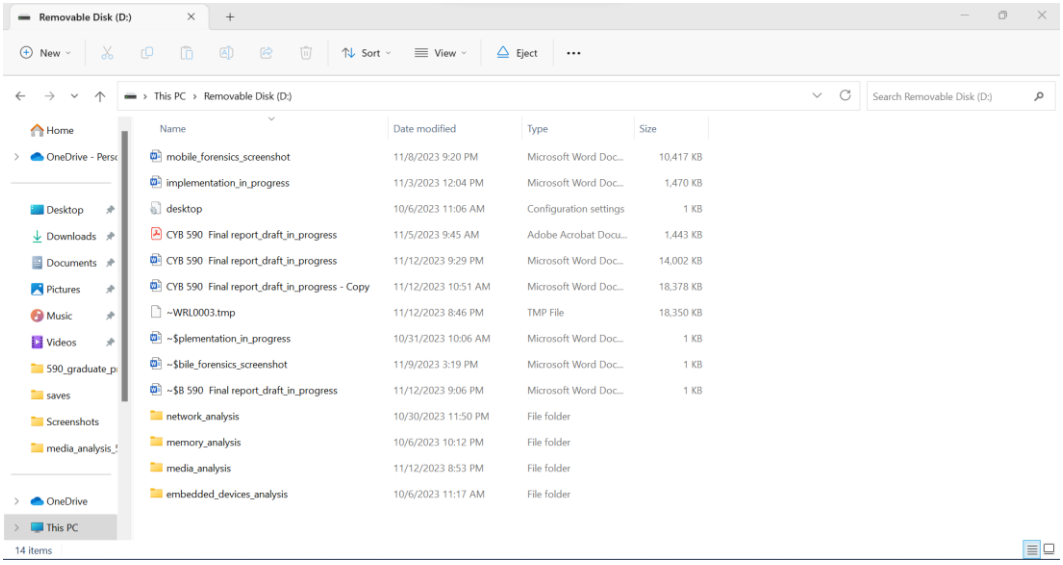


Figure 41: Image mounted output directory.

11. We can also view the contents of the image drive without mapping onto your drive by using Paraben's E3. Launch Paraben's E3 and click "Add Evidence". Refer Figure 42 below:

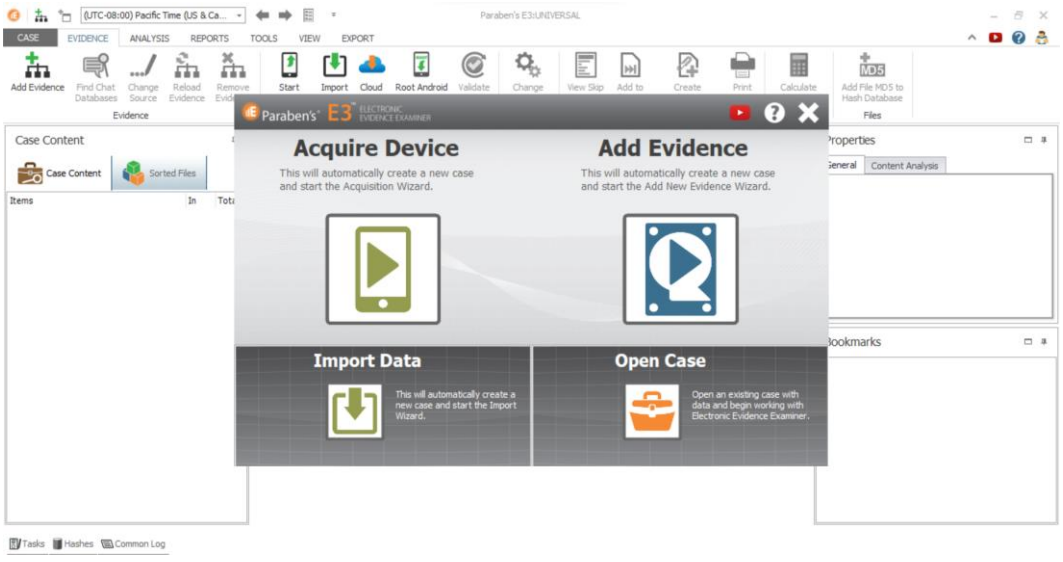


Figure 42: Launch window of Paraben's E3 for adding evidence.

12. Select the image file which you have created through Access Data FTK Imager and open it. This is portrayed in Figure 43.

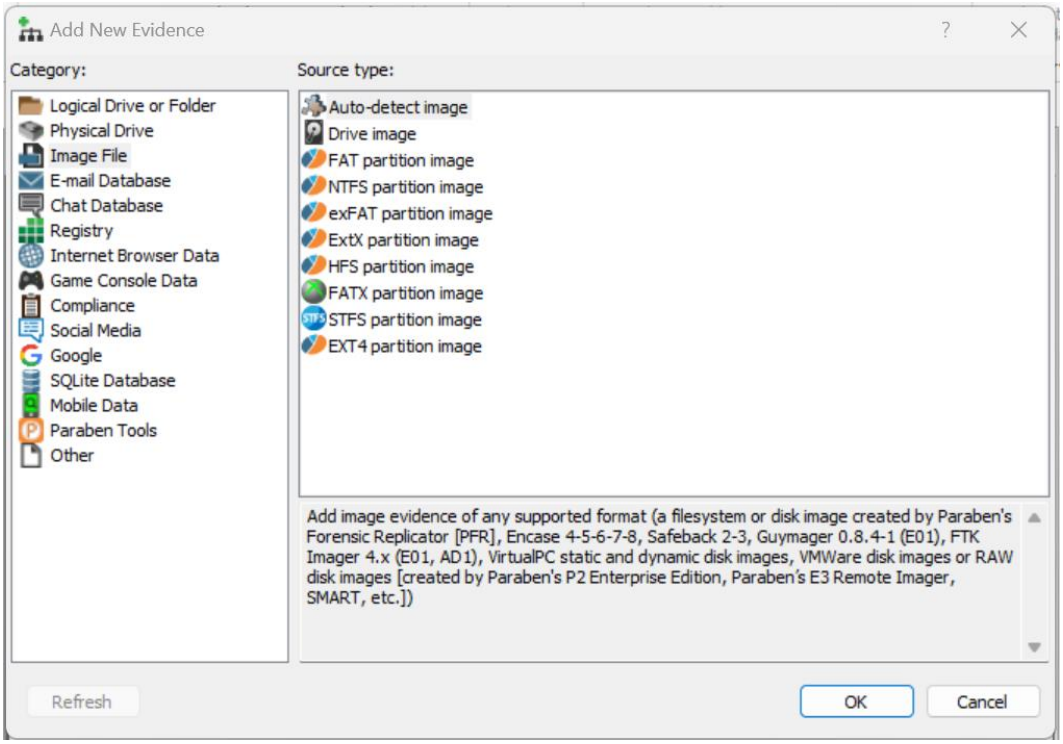


Figure 43: Image file evidence selection

13. All the files and folders can be viewed post adding the evidence as shown in Figure 44. Also, further investigation can be done by analyzing the metadata extracted by E3.

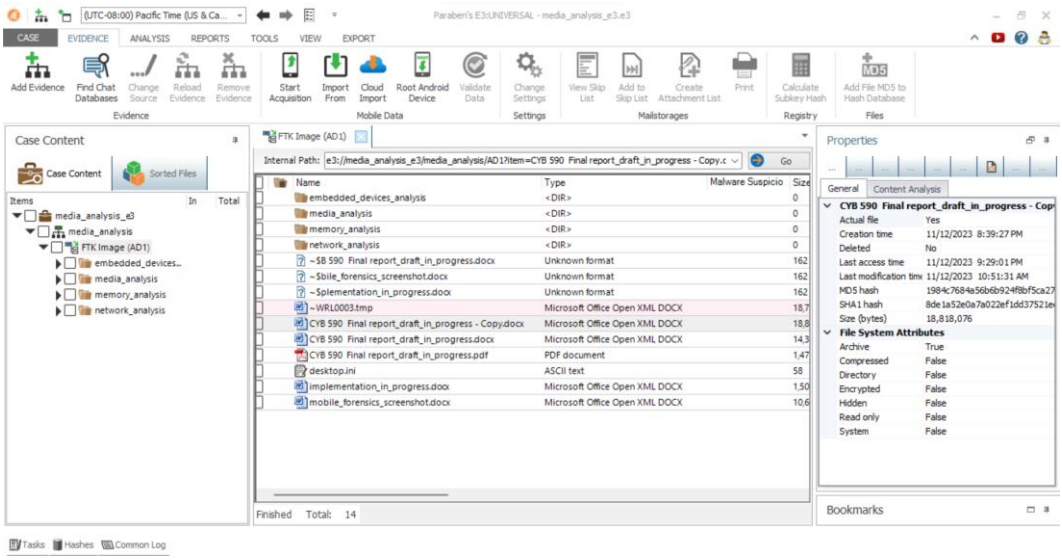


Figure 44: Imported Image file in Paraben's E3

14. Expand the image drive to view different categories of information. One such instance is the mailbox of the victim's machine as shown in Figure 45.

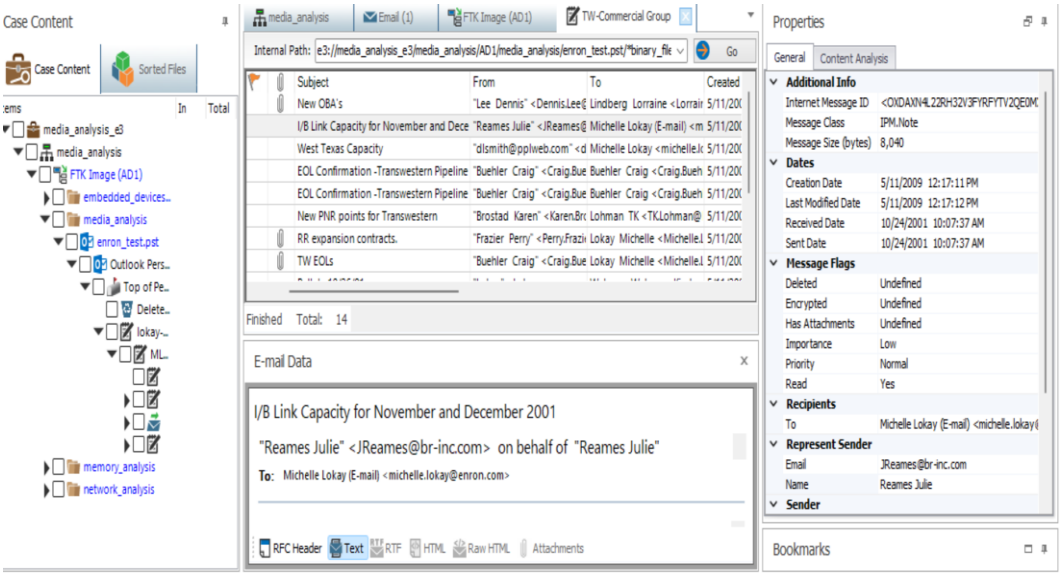


Figure 45: Case content tab with expanded folders.

15. The tool also recovers deleted email items from the email servers in case where the email files have been deleted deliberately from email client such as “Microsoft Outlook.”

16. Additionally, email headers can also be analyzed to verify if the message is legitimate to rule out the possibilities of phishing email scams. Refer below Figure 46 to view the header details of an email.

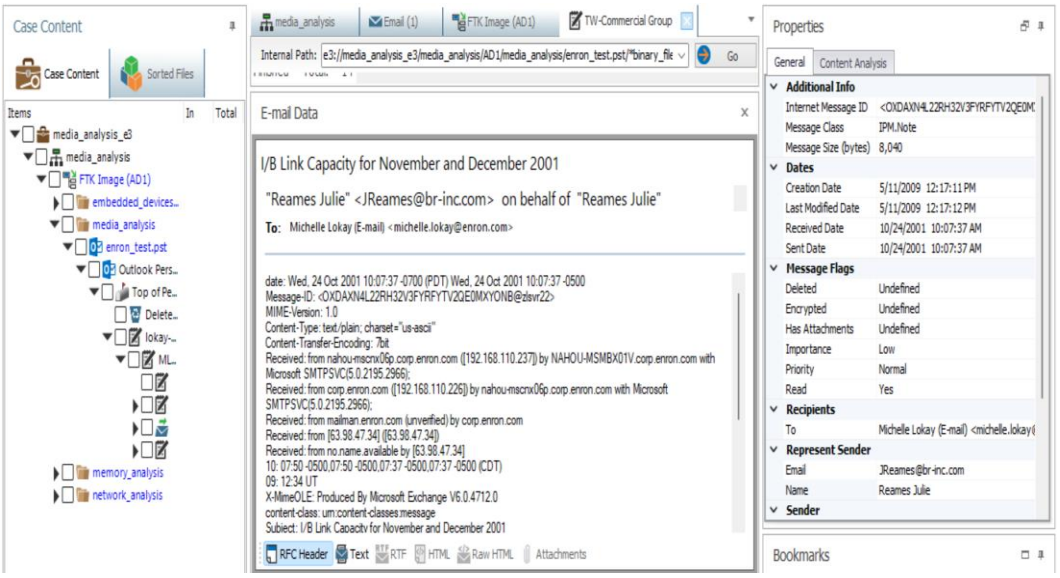


Figure 46: Email headers and properties view

17. During investigation, reports can be exported as well as shown in the figure 47 below:

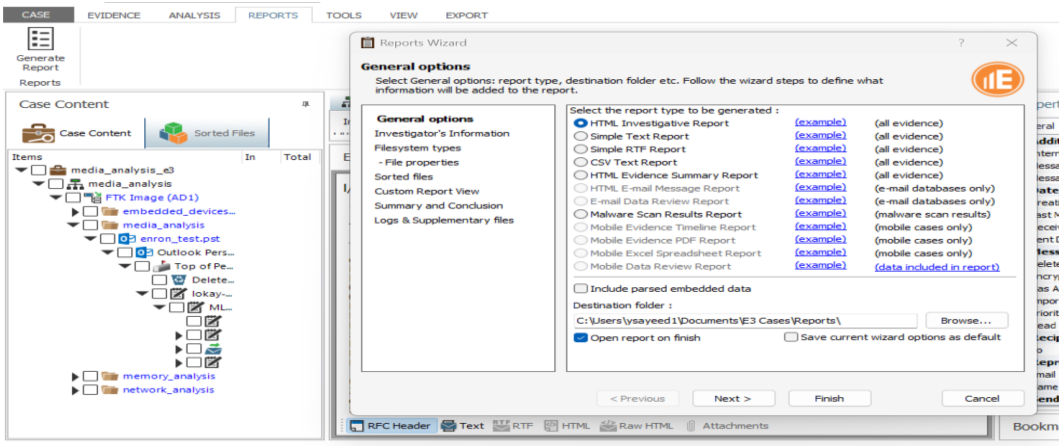


Figure 47: Exporting reports feature.

Embedded/Hardware Analysis

For Hardware/Embedded Device Analysis, data acquisition from a mobile device such as smart phone was performed using Paraben's E3. The E3 Forensic Platform seamlessly guides you through the process of Adding Evidence, Parsing the data, and carving artifacts such as Smartphones, Computers, Cloud Data, IoT data as well as OSINT data.[9]

1. Connect Android mobile device which needs to be acquired in USB debugging mode and launch Paraben's Electronic Evidence Examiner. The following screenshot will pop-up post the launch as shown in Figure 48.

Figure 48: Launch window for mobile data acquisition

2. Enter the case details and specify the directory to which acquired data will be saved. Click 'Continue' to land into the Acquisition Wizard window as shown in Figure 49 below:

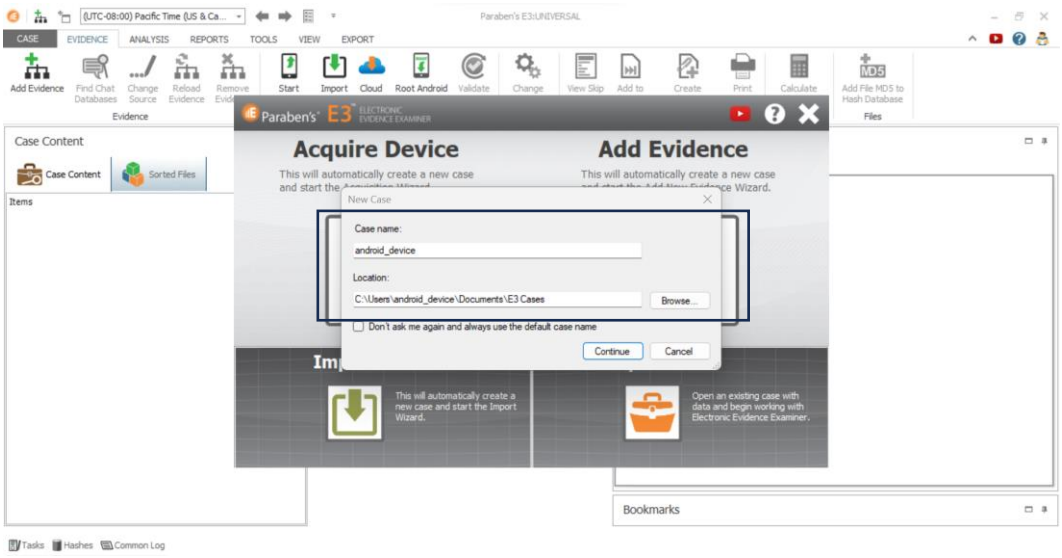


Figure 49: Case name and location.

3. Select Android as shown in Figure 50 below and click Next.

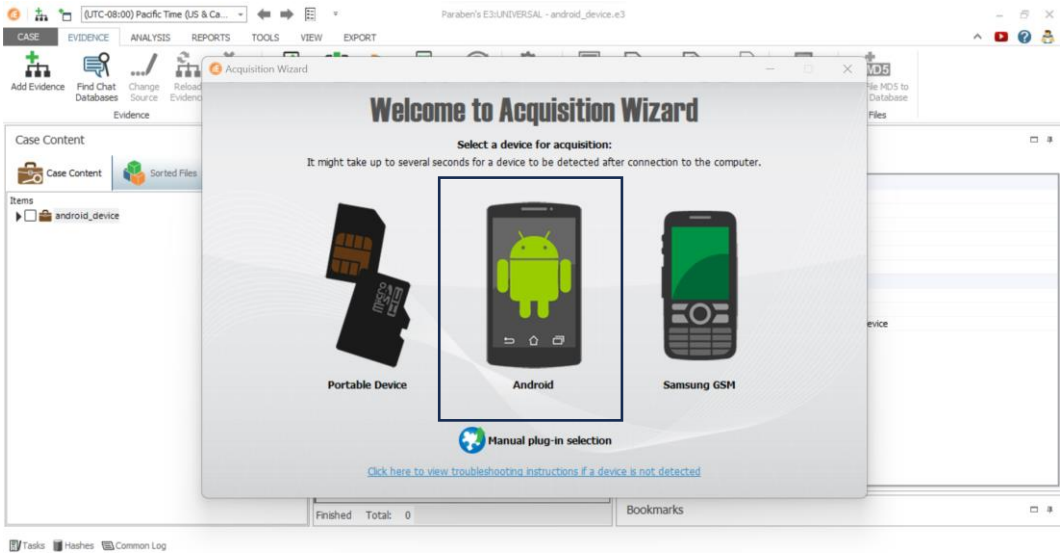


Figure 50: Acquisition wizard

4. There are 4 types of data acquisition in Paraben's E3. This is depicted in Figure 51 below.

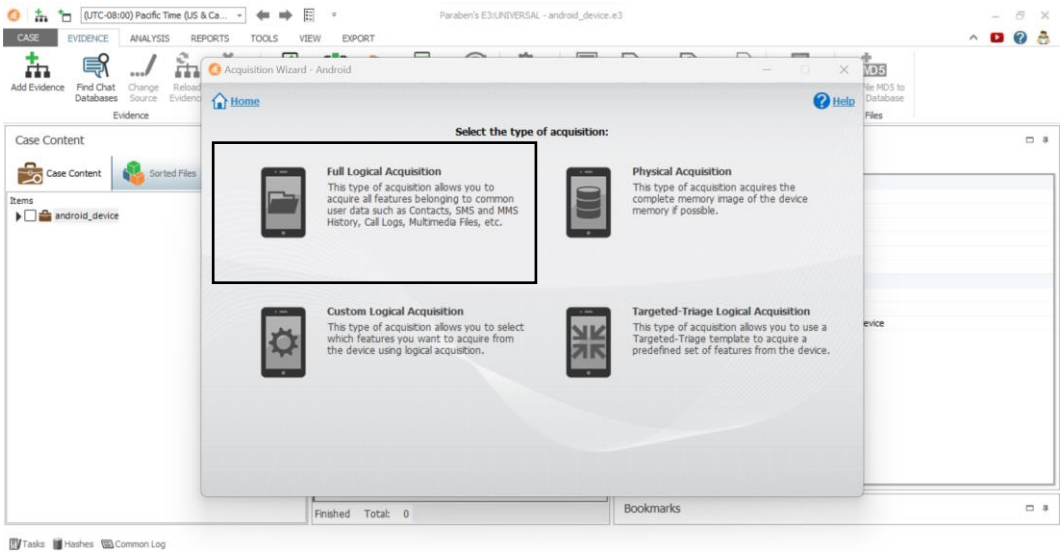


Figure 51: Types of mobile data acquisition.

5. Click Full Logical acquisition. The tool now starts the bit-by-bit acquisition from the allocated section of the memory.

6. Unlock the file system and hit ‘Start Acquisition’. Follow the instructions along the process for successful connection and acquisition as shown in Figure 52 and Figure 53.

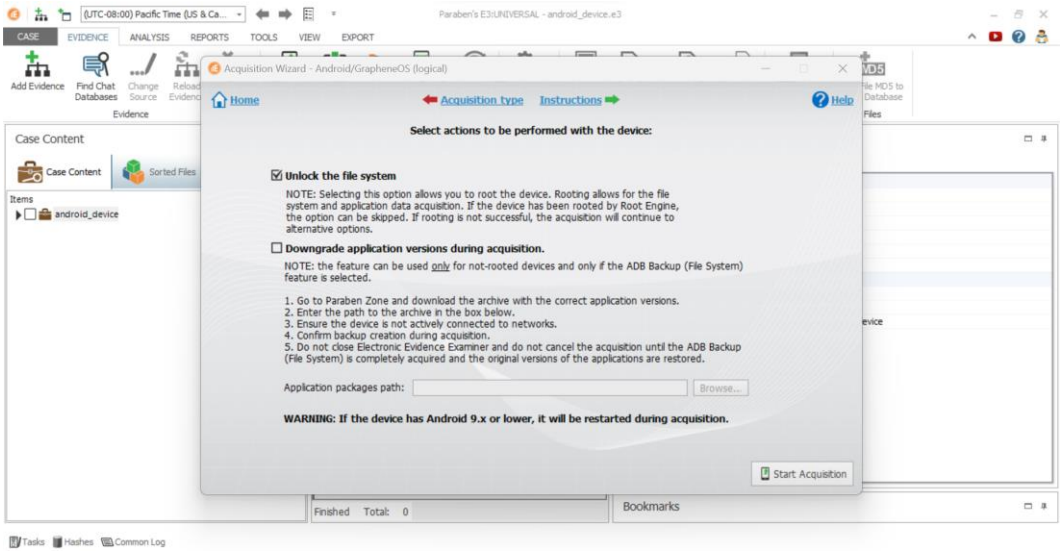


Figure 52: Unlock file system.

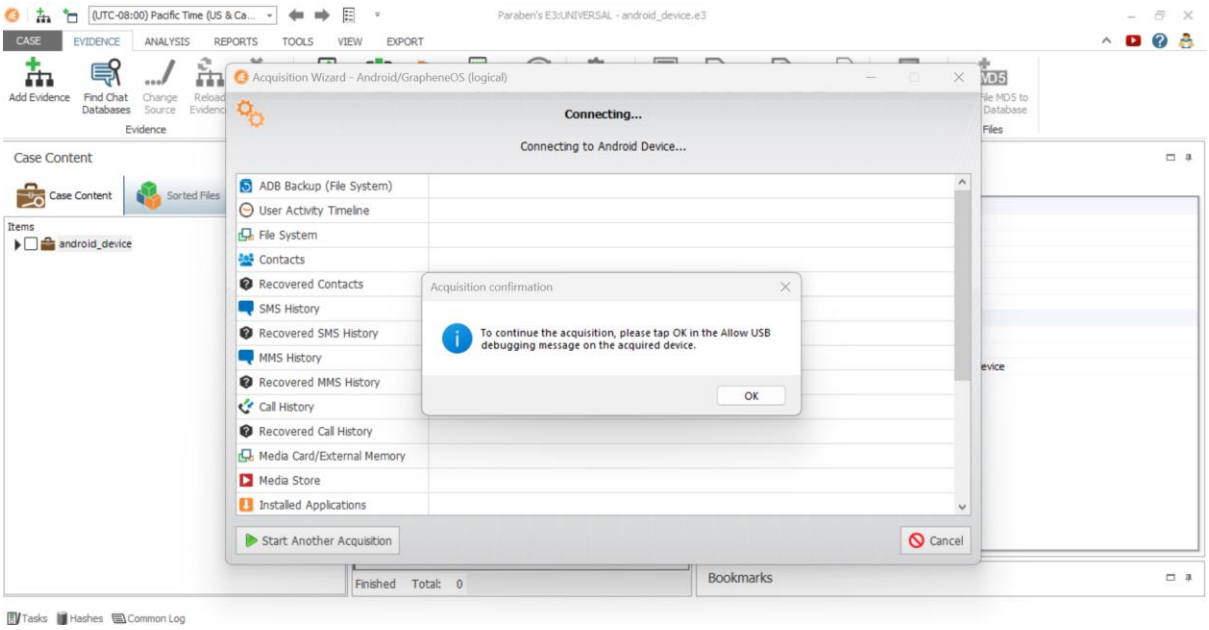


Figure 53: Acquisition progress wizard.

7. Once the acquisition is completed, click finish as shown in Figure 54 below.

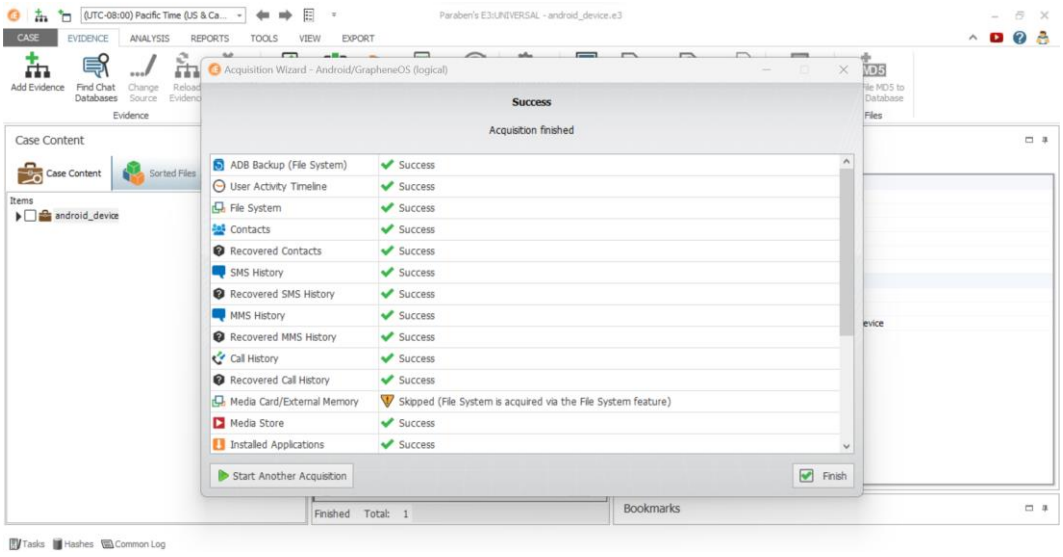


Figure 54: Acquisition status completion.

8. Expand the Case Content tab in the left pane to view various types of data residing in the device. This is depicted in Figure 55.

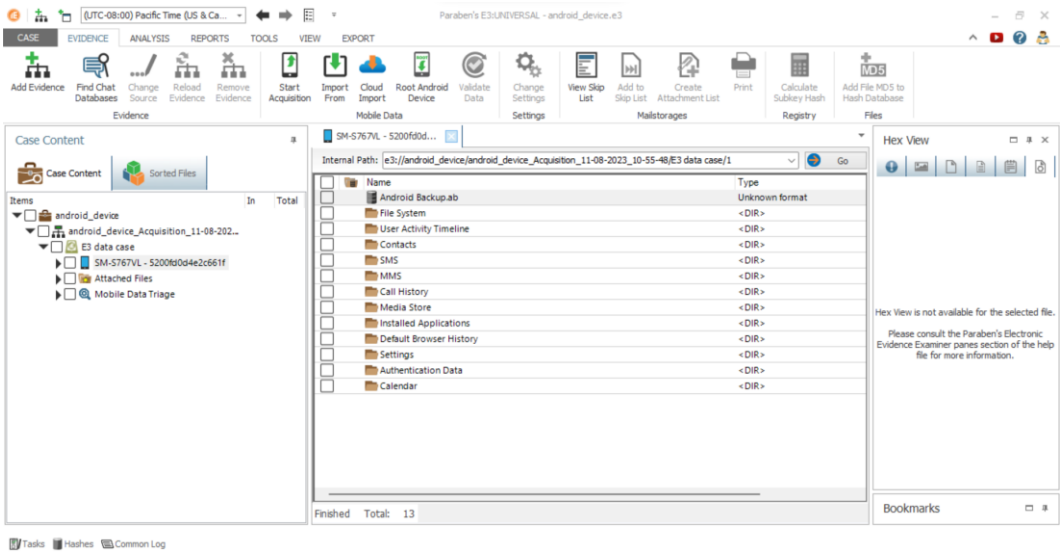


Figure 55: Case content view of mobile data.

9. For instance, below 2 Figures 56 and 57 portray the contact and call logs details respectively.

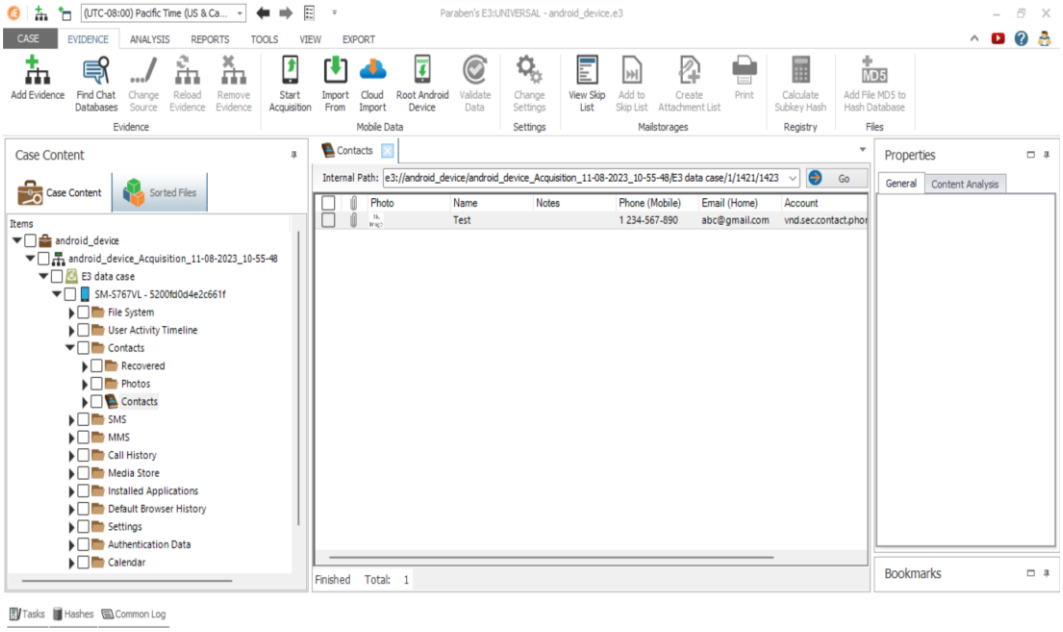


Figure 56: Phone contact view of mobile data.

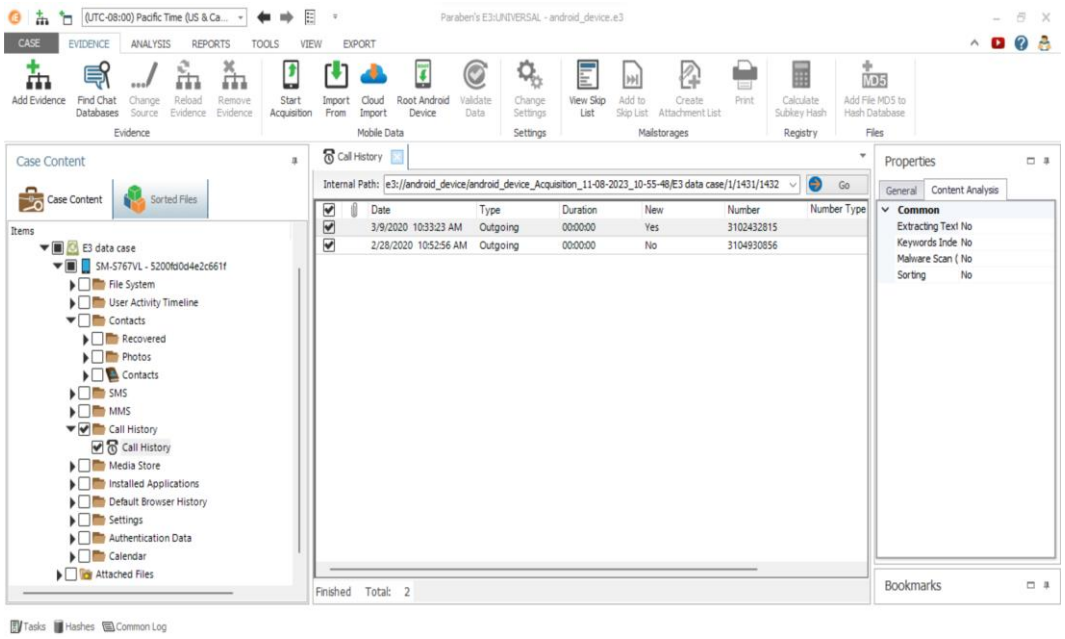


Figure 57: Call logs of mobile data.

10. The tool also captures all the information of the device as well as the applications installed on the device. This is depicted in the figures 58 and 59 below:

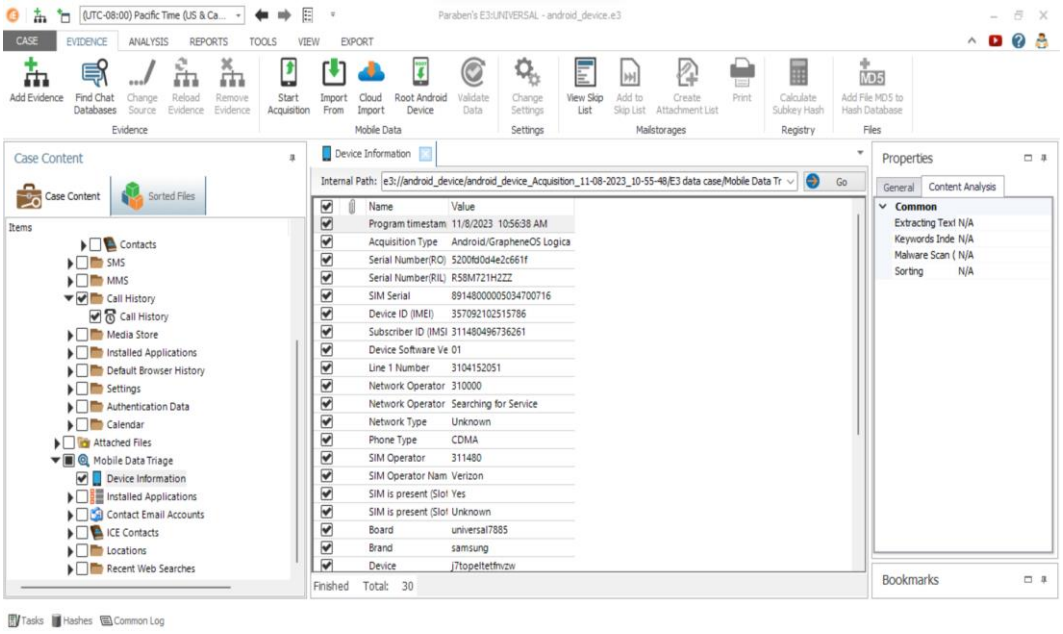


Figure 58: Acquired device information.

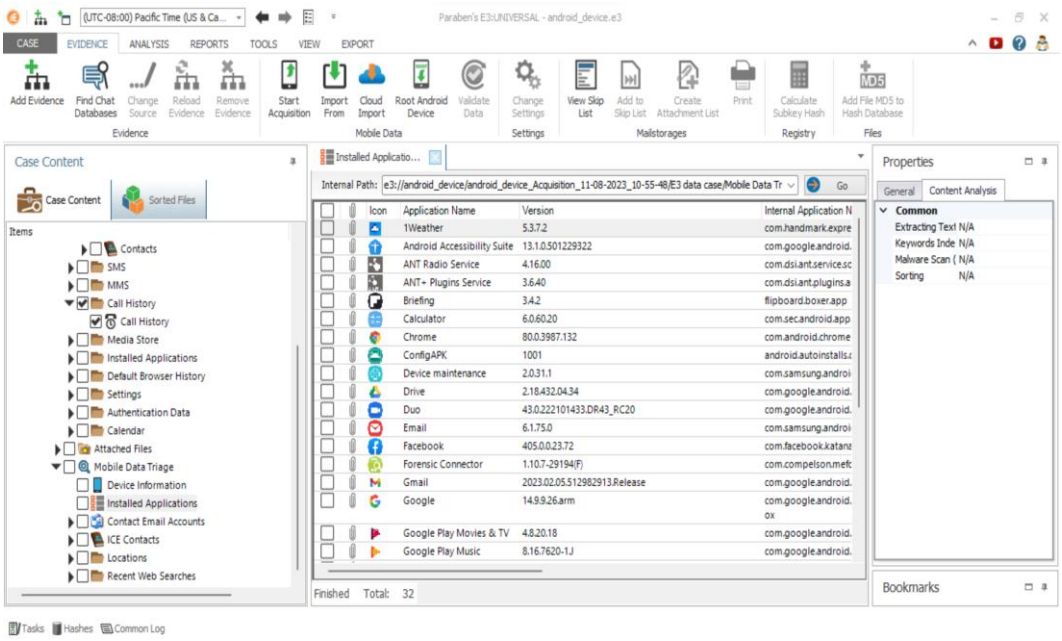


Figure 59: Applications installed on the acquired device.

11. Right click on the root folder to select the ‘Content Analysis’ and ‘Sort Data’ option. This will process the data that calculates cryptographic hash values, index keywords and run OCR for a quicker search and deeper analysis. This is portrayed in Figures 60, 61 and 62.

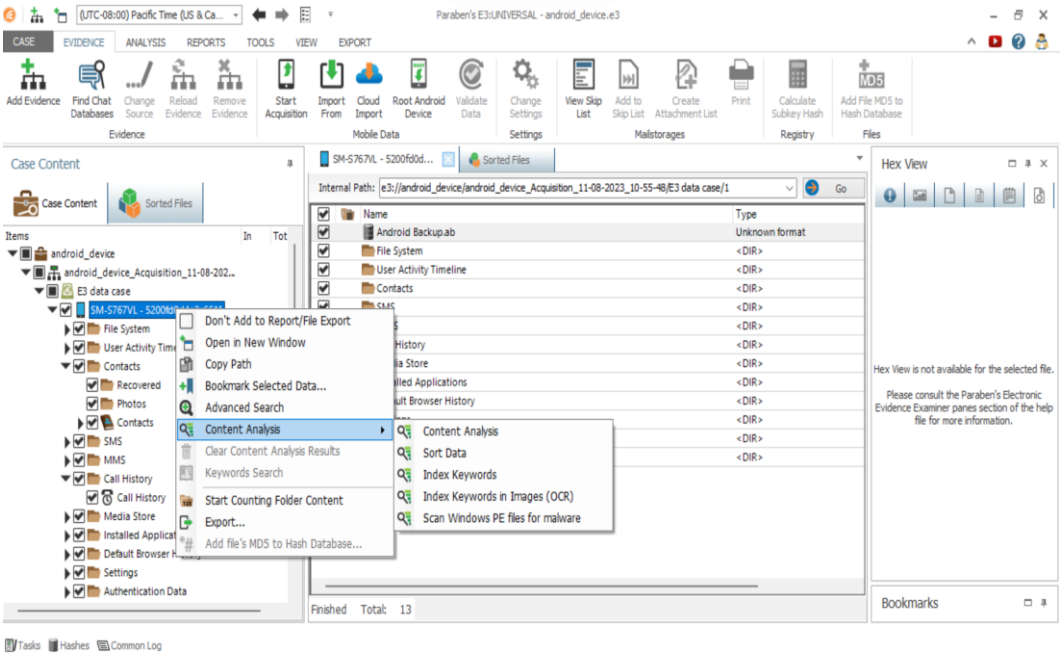


Figure 60: Content Analysis and Sort Data feature.

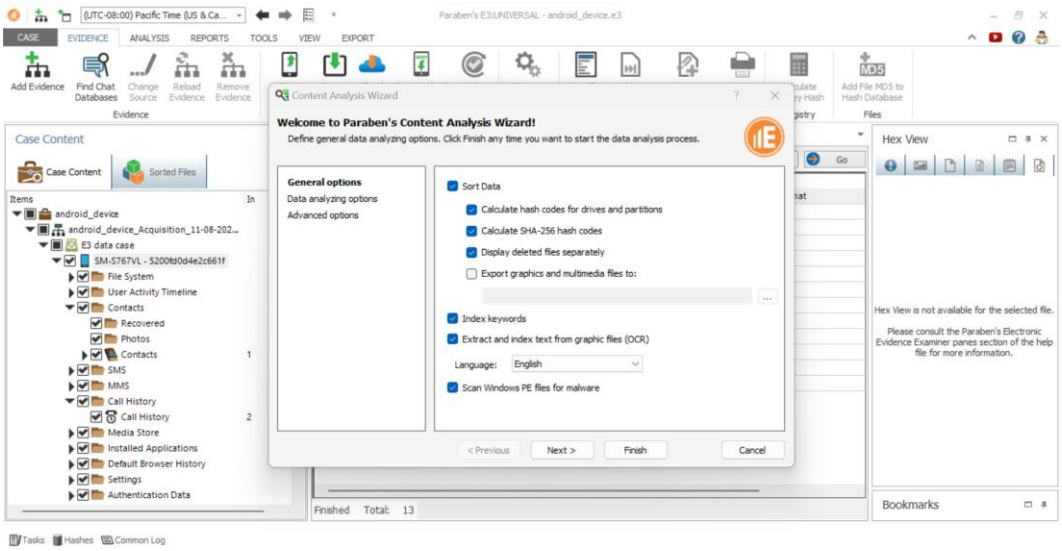


Figure 61: Sort Data options wizard.

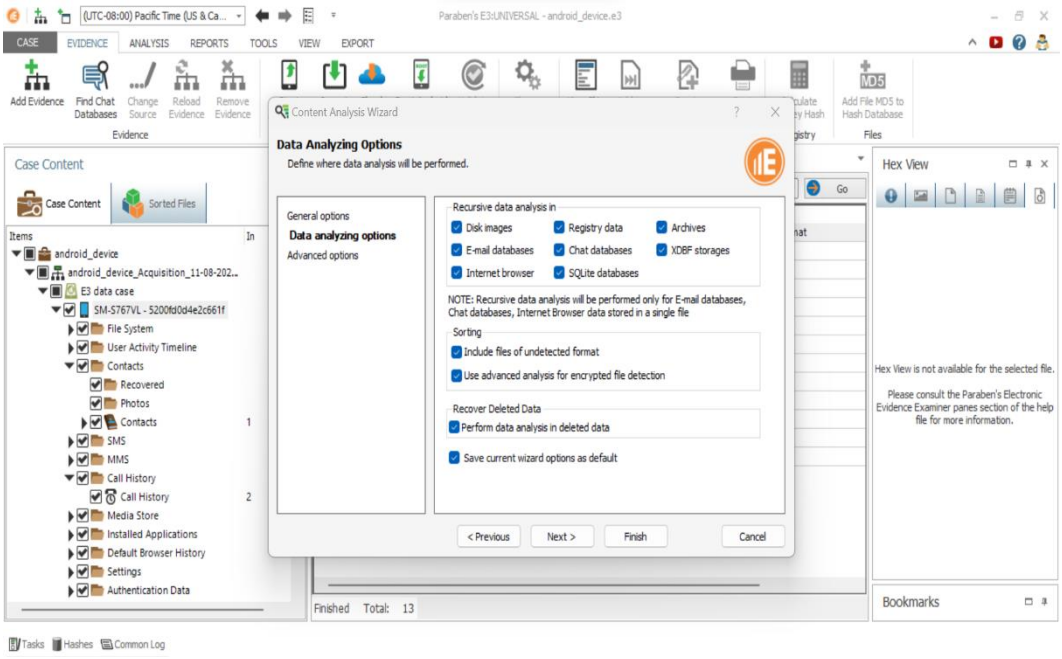


Figure 62: Content Analysis Data options wizard

.

12. Once processed, the data will be available in the Sorted Files tab in the left pane as shown in Figure 63.

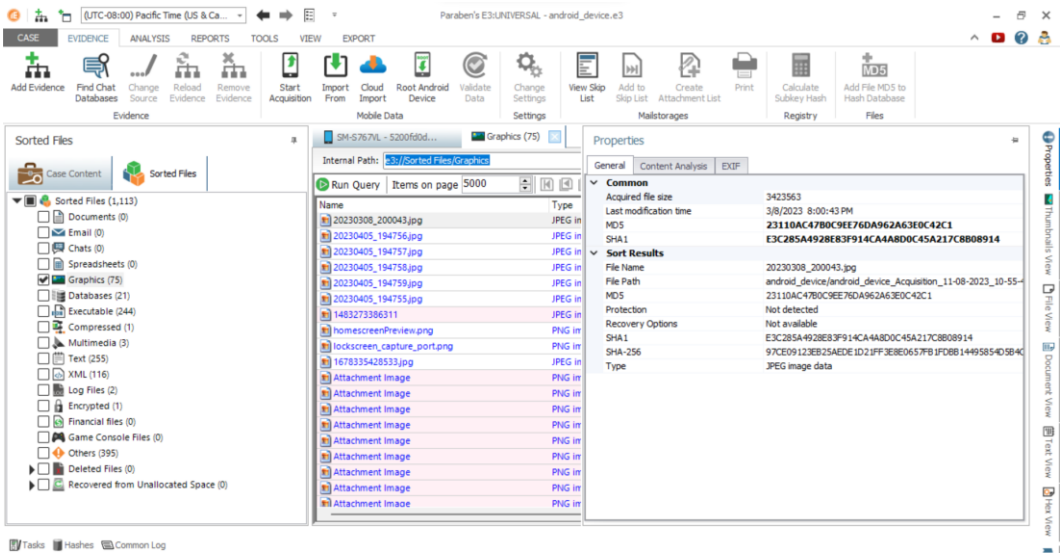


Figure 63: Sorted Files Tab

13. The tool extracts the native view, text view, Hex view, and properties with hash values along metadata for investigation purposes. This is shown from Figures 64 to 67.

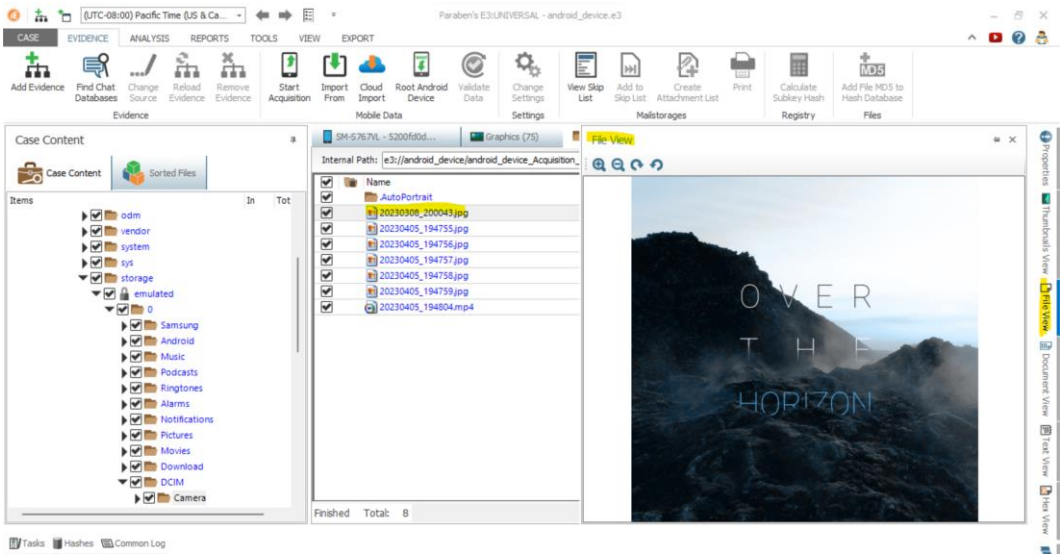


Figure 64: Native view

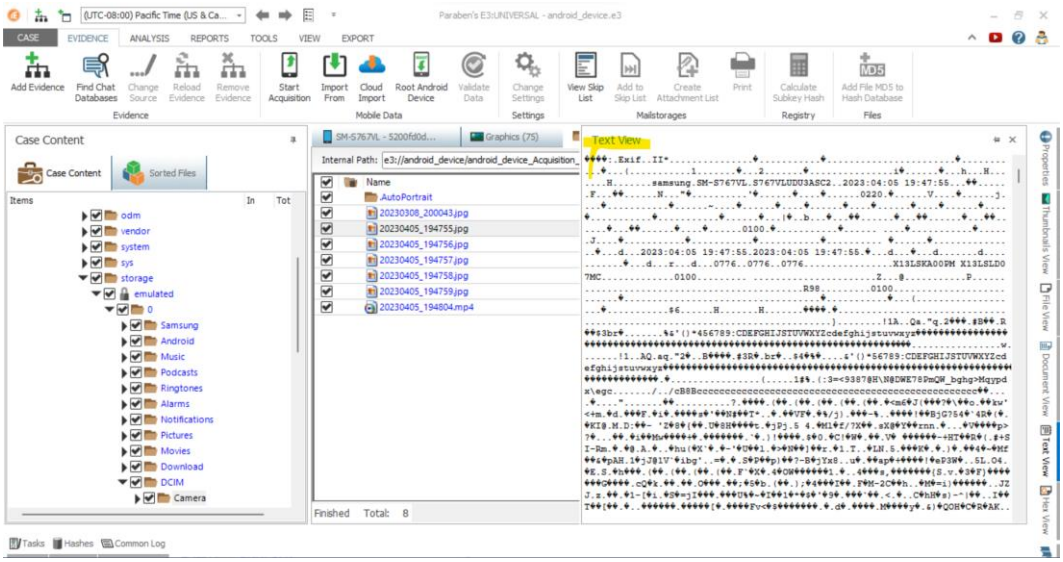


Figure 65: Text view

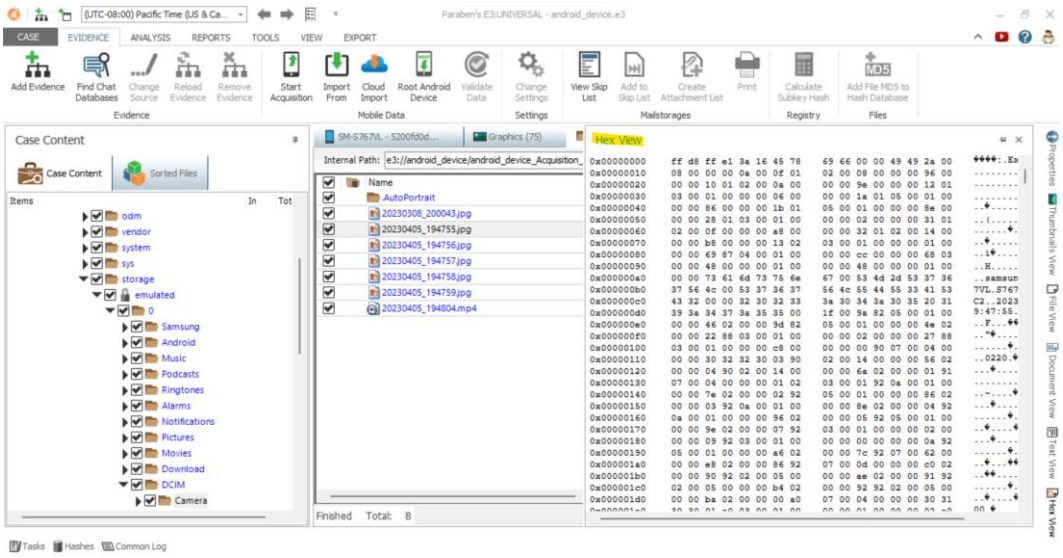


Figure 66: Hex view

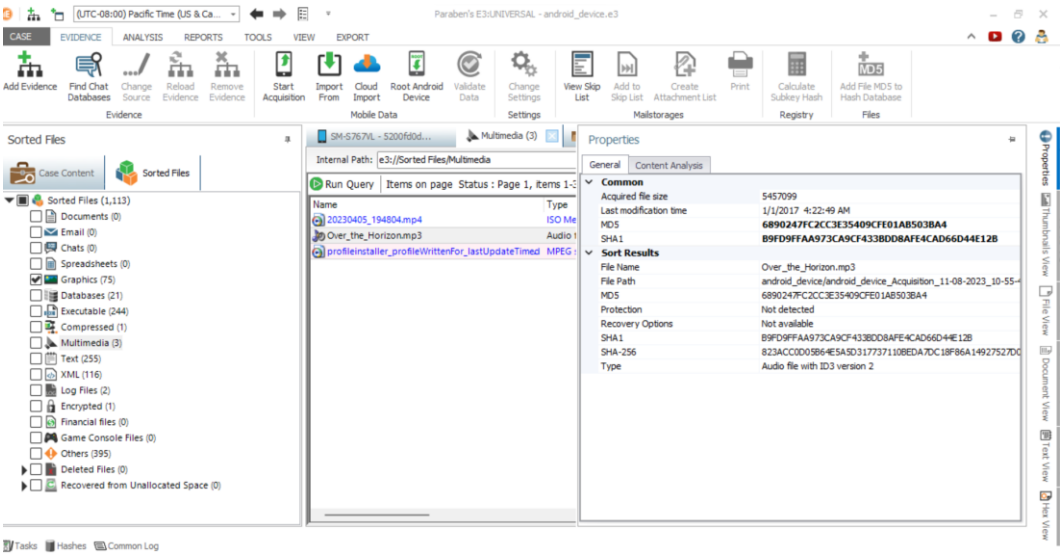


Figure 67: General file properties

14. Export the acquired data by selecting 'Export' option from the tool bar on the top by providing the destination path. This is shown in Figure 68 and Figure 69 below:

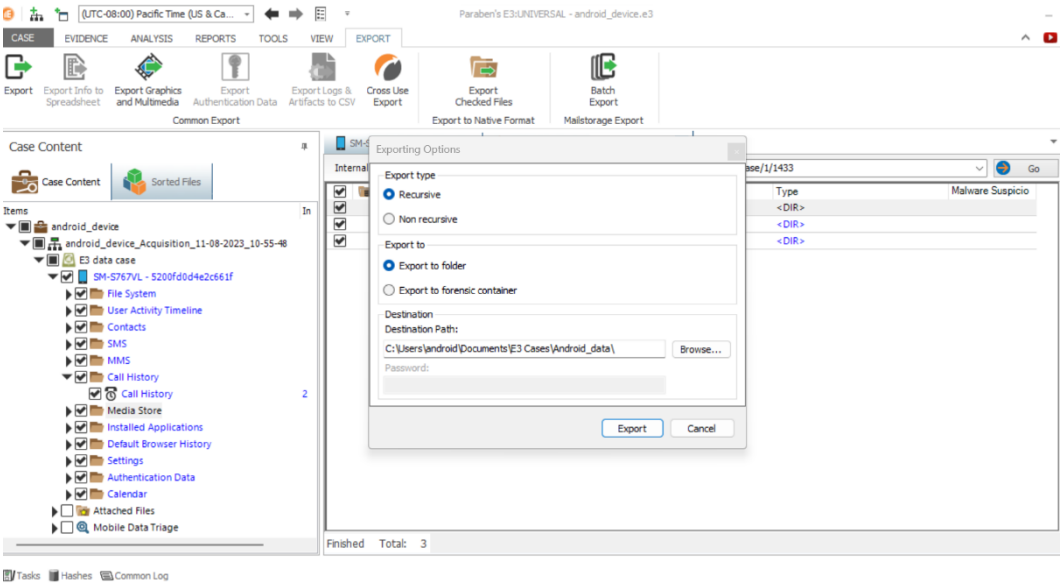


Figure 68: Data export options

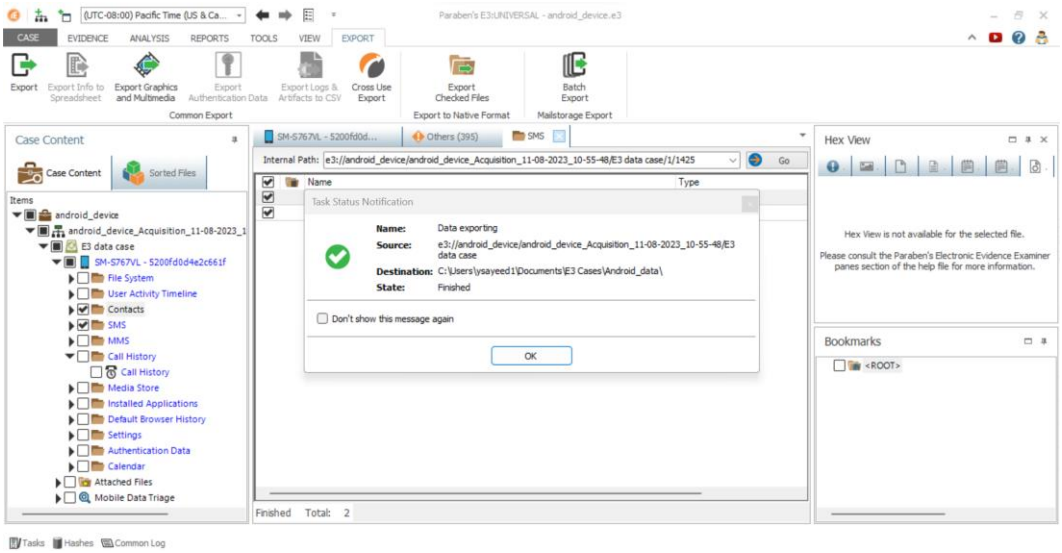


Figure 69: Data export status and details

CHAPTER 5

RESULTS AND DISCUSSION

In this project, the digital forensics incidence response was initiated with a proactive approach of threat detection by performing packet analysis using Netwitness Investigator and Wireshark respectively. DOS attack was confirmed, and the victim's machine was figured out through destination IP address on which the attack was staged. That machine was then disconnected from the network to avoid further spread.

In the second phase, live in-memory analysis of the victim's C: drive was performed using Paraben's E3 to recover files from non-volatile as well as volatile memory. This facilitates the tool to recover even the deleted files on the drive. This way if any file was deliberately deleted by the culprit can be recovered.

In the third phase, media analysis was performed by creating a forensic image file of the C: drive using Access Data Forensic Tool Kit Imager. Then the image file was imported into Paraben's E3 for further investigation of the data on the image drive. The imaged drive consisted of various categories of digital data such Documents, email data, chats, databases, multimedia files etc. The tool also extracted cryptographic hash values, metadata, and various important properties for investigation.

In the fourth and final phase, data acquisition was performed from an Android smartphone as part of Hardware/Embedded analysis to further collect the evidence such as short message service, emails, chat, call logs, calendar entries, applications, media etc. Mobile phones contain a plethora of information and extracting digital data without altering is crucial for evidence preservation. Moreover, analyzing the data extracted will play a vital role while conducting the investigation.

CHAPTER 6

CONTRIBUTION

The main contribution of this project was to portray how organizations can benefit from the use of digital forensics tools when they encounter cyber incidents. By having an in-house team of DFIR professionals, team can utilize these software's to expedite the process of evidence collection and analysis so that they not only contain the incident through traditional incidence response but also find the root cause of the issue along with finding the culprits of the security incident. These tools can optimize the whole incident response by extending it from incident management to problem management where the root cause analysis can be performed thoroughly. The project covered open-source tools such as Wireshark, Netwitness Investigator (Freeware version) and Access Data FTK Imager. It also covered commercial tools like Paraben's E3 which is a versatile tool for conducting various collection and analysis of evidence. However, if the organization is a start-up, even they can have the benefit of using these free tools even though they have limited features. At least, they can detect the attack early on and quickly focus on not only containing but also recovering the lost digital data. While a large organization should have all the mentioned tools readily available, which is worth spending than spending in any litigation later post a security incident.

CHAPTER 7

CONCLUSION AND FUTURE WORK

In conclusion, by implementing digital forensics incidence response, teams can address lack of skills and mismanagement with “Centralized” and “Distributed” model. They will also be able to communicate with the right people in the right way by approaching the centralized DFIR team wherein the first level help desk activities can even preserve critical evidence through proper training which should be a bare minimum skill set in every organization. Proper “intelligence” in the threat intelligence is provided to incident responders by using Digital Forensics Incident response tools which are adequate, managed, tested, and efficiently utilized. This will also provide deeper understanding through a very comprehensive and intricate forensic process by gathering wealth of information to determine who attacked them, how they got in, the exact steps attackers took to compromise their systems, and what they can do to close those security gaps. This will result in improving resiliency against future attacks. Moreover, it also caters in finding evidence you need to press charge against the criminals who targeted your operations or support a cyber insurance claim. Finally, DFIR provides a structured and systematic approach to handling security incidents, helping the organization ensure the protection of sensitive data and assets.

For future work, investigators can further improvise automated methods for acting swiftly to threats. Artificial intelligence (AI) tools can be applied to the process with a variety of techniques that allow the tool to improve performance over time. For example, applying machine learning methods to automate network analysis section wherein all the logs and packet captures should be periodically cleaned and transformed into data frames. From these data frames, AI algorithms can be used to plot the analysis in the form of data visualization to detect the alert swiftly in an optimized manner.

REFERENCES

[1] Ben Filipkowski. (2023, April 20). Digital Forensics and Incident Response. https://fieldeffect.com/blog/digital-forensics-incident-response

[2] Sara Jelen. (2023, June 29). Incident Response in Cybersecurity: Preparing for a Security Breach. https://securitytrails.com/blog/incident-response

[3] Fazila Malik. (2023, July 31). Writing Your Security Incident Response Policy. https://www.strongdm.com/blog/writing-your-security-incident-response-policy

[4] Chapple, M., Stewart, J. M., & Gibson, D. (2021). (ISC)² CISSP Certified Information Systems Security Professional Official Study Guide (9th ed.).

[5] Cynet. (n.d.). NIST Cybersecurity Framework: A Comprehensive Guide. Cynet. https://www.cynet.com/nist-cybersecurity-framework/

[6] NetWitness Investigator, https://www.netwitness.com/

[7] Wireshark, https://www.wireshark.org/

[8] Access data Forensic Tool Kit, https://www.exterro.com/forensic-toolkit

[9] Paraben's Electronic Evidene Examiner (E3), https://paraben.com/