(kindly notice page 7-10 are appendices of Part 2)

PART 1 - Forensics Process

Starting the investigation into alleged art fraud in Portsmouth calls for a thoughtful digital forensics strategy. I intend to navigate this case using systematic steps, closely adhering to digital forensic principles outlined in Lecture 1 [1].

1. Identification:

As the Forensics Lead on the case, my initial focus would be on systematically analysing symptoms associated with the art fraud case. Delving into the incident's nature and understanding concerns and probing motives behind the production and distribution of these pieces will be essential. Additionally, establishing a chronological timeline outlining key activities associated with the alleged art fraud will provide a comprehensive overview.

In alignment with the identification principle, my focus will be on ensuring accurate recognition and categorization of digital evidence while strictly adhering to digital evidence principles. [2] (Casey, E. 2011)

2. Preservation & Collection:

My immediate priority is to preserve the crime scene, ensuring that no unauthorised access or alterations occur. This includes meticulously collecting evidence, such as suspicious paintings and digital devices including an iPhone 11, a 9th generation iPad, and a Dell laptop running Windows 10.

Adherence to **chain of custody principles** is crucial to maintaining the integrity of seized items. Here are the specific steps:
- Place the digital devices in a Faraday bag to prevent remote communication.
- Store the device in a secure evidence room with controlled access.
- Assign a unique identification number for tracking in the chain of custody.

3. Examination:

Recognizing the diversity of digital devices, I will tailor the examination process to each device, ensuring a comprehensive analysis. My approach will prioritise preserving data without alterations, assigning qualified and experienced staff if necessary, emphasising **the competency in accessing data principle**. Here's an examination plan for collected digital devices: [3] (Michael B. 2008)

3.1 Documentation:

- Record device details including IMEI, serial number, hardware serial number and software version etc.
- Document the physical condition, noting any visible damage or alterations.
- Capture photographs of the device from different angles.

3.2 Forensic Imaging:

- Use write-blocking and imaging tools to create a forensically sound image of the device.
- Hash the image and verify its integrity through hash comparison.
- Document the extraction process and hash values in the case log.

4. Analysis:

Analysing network activity will be crucial to identifying potential connections to counterfeit artwork production or distribution. I will trace online activities related to the alleged art fraud, explicitly aligning with the creation of an **audit trail principle** and digital evidence principles.

5. Reporting:

The final step involves preparing a comprehensive report outlining the results of the digital forensics examination. Meticulous documentation of every step will be prioritised. Emphasis on the **overall responsibility principle** will be maintained. Since legal challenges may arise, the report will be structured to provide not only technical details but also a narrative that is easily understandable in a courtroom setting.

In summary, this plan ensures a meticulous digital forensics process, with each step guided by established principles to facilitate a robust investigation into the alleged art fraud.

Reference

[1] Introduction to Digital Forensics (lecture content)
[2] Casey, E. (2011), Digital evidence and computer crime : forensic science, computer and the Internet, 3rd Edition, London: Academic Press.
[3] Michael B. (2008), Electronic CSI A Guide for First Responders, 2nd Edition, National Institute of Justice

PART 2 - Forensics Report

Forensics Report: Investigation into Alleged Arson

Prepared by Yan Kong

1 Introduction

This forensic report details the examination of a suspect's laptop, belonging to a Maplewood resident suspected of involvement in a series of recent house fires. The objective is to identify digital evidence shedding light on the suspect's potential role in these unsettling arson incidents.

1.1 Statement of compliance

As an expert witness, I acknowledge my duty to provide an unbiased opinion within my area of expertise. [1] (Digital Forensic Report Sample)

2 Forensic Preparation and Examination

2.1 Chain of custody

We are provided with a digital image of Jack's laptop. In case the image was stored in a USB device, we'll need to properly fill in the chain of custody. (omitted here for brevity)

2.2 Tools

The forensic tools employed in the performance of this investigation were:

- Autopsy
- FTK imager

2.3 Data Acquisition

A digital image of Jack C's laptop was acquired from a USB stick using a Writeblocker, and FTK imager verified the hash code (Appendix Figure 1) to preserve evidence integrity.

2.4 Data Examination

Examining locations of interest in Linux and employing skills from the lecture on Operating Systems Forensics (Linux)[2], I conducted keyword searches, and revealed

the following findings. [3] Due to word constraints, the evidence is presented solely by file names, excluding file hash, metadata, and dates.

2.4.1 Evidence Class 1

Web browsing history related to arson (Appendix Figure 2)

- "How to start a fire with nothing else besides a bunch of sticks" on Quora
- Search for the historical reference to a serial arsonist burning Addison school in the 1920s
- The search for gloves on eBay

Analysis: Jack C's web browsing history reveals searches like "How to start a fire with nothing else besides a bunch of sticks" on Quora, indicating potential preparation for arson-related activities. Searches for historical arson cases and gloves on eBay suggest concerning interests.

2.4.2 Evidence Class 2

House images in Maplewood (Appendix Figure 3)

- For_viewing_mapplewood.jpg
- Acquired.jpg
- a1.jpg

Analysis: Jack C may be gathering information on specific properties or individuals. The images might be used for reconnaissance, planning of the suspected arsons.

2.4.3 Evidence Class 3

User credit card, address, social media records (Appendix Figure 4, 5)

- womens_day.xlsx: a list of women with credit card number and address
- socialMedia.xlsx: activities of someone posted on various social media platforms
- Plane_Tickets_20220315.csv: clients' plane tickets information

Analysis: These files suggest a coordinated effort to compile comprehensive profiles for potential identity theft or fraud. The presence of credit card numbers indicates successful acquisition or potential victim account information, heightening concerns about the misuse of sensitive financial data.

2.4.4 Evidence Class 4

A large collection of advanced hacker tools. (Appendix Figure 6, 7)

- ➢ Tools_list.doc: a list of hacker tools and manual
- ➢ Linux bash history: commands to install virtual-box and delete user account
- ➢ A bunch of hacker tools are found installed on /usr/bin /usr/lib, like openvpn, openssh, cracklib etc.

Analysis: The evidence strongly indicates Jack C's likely engagement in illicit cyber activities. VirtualBox and OpenVPN installations suggest efforts to conceal malicious actions, while deleted user accounts raise concerns about covering digital tracks. The list of hacker tools underscores a significant contrast between his amiable demeanour and unexpected technical proficiency.

2.4.5 Evidence Class 5

Client’s information collection activity (Appendix Figure 8)

- ➢ Hotel reservation record
- ➢ Travel plan
- ➢ Email

Analysis: Jack C's role as a travel agent introduces concerns regarding potential exploitation of client information for identity theft. Records of hotel reservations, travel plans, and email communications indicate access to personal details that could be misused.

2.4.5 Evidence Class 6

DigitalOcean bookmark and some saved HTML files (Appendix Figure 9, 10)

- ➢ Firefox bookmark
- ➢ Website1.html

- ➢ contact_us.html

Analysis: It suggests Jack's potential involvement in phishing. As a web host provider, Digitocean could facilitate hosting malicious websites, with the saved HTML files indicating active efforts in crafting potentially harmful web content.

2.4.5 Evidence Class 7

Significant financial gains found from deleted files through keyword search (Appendix Figure 11)

- ➢ Unaloc_459210_11314135040_12888047616 (deleted file)

Analysis: The substantial income, comprising both dollars and bitcoins, discovered through a keyword search in deleted files is inconsistent with Jack C's role as a travel agent. Furthermore, the use of Bitcoin collections as a form of payment in illicit industries is noteworthy. Bank receipts attached to project progress emails and the subtle use of the term "deliverable" in the text suggest Jack C's potential involvement in a partnership with someone experienced in such operations.

3 Summary of Conclusion Reached

The evidence strongly suggests Jack C's involvement in criminal activities, combining cyber expertise, suspicious web behaviour, and the collection of customer data. An urgent and thorough inquiry is necessary to understand the full extent of Jack C's activities and the risks associated with his potential involvement in a criminal network.

Date: Dec 11, 2023
Signature: Yan Kong

Reference

[1] Digital Forensic Report- sample PDF
[2] Operating Systems Forensics - Linux (lecture content)
[3] Digital Forensics with Autopsy : Part 2
(https://www.hackercoolmagazine.com/digital-forensics-with-autopsy-part-2/)

Appendices

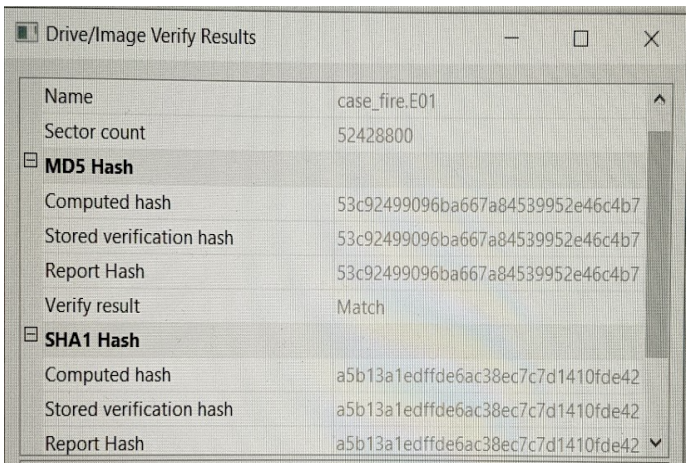


Figure 1 - Hash check using FTK imager

Title	Program Name	Domain
starting fire with sticks - Google Search	FireFox	google.com
	FireFox	google.com
How to Start a Fire with Sticks (with Pictures) - wikiHow	FireFox	wikihow.com
	FireFox	google.com
How to start a fire with nothing else besides a bunch of stic...	FireFox	quora.com
arsonist in 1920 - Google Search	FireFox	google.com
	FireFox	google.com
In 1920s serial arsonist burned Addison school	FireFox	lenconnect.com
fire accelerant - Google Search	FireFox	google.com
fire accelerant - Google Search	FireFox	google.com
	FireFox	google.com
Detecting Arson Accelerants For Fire/Arson Investigators	FireFox	ionscience.com
Electronics, Cars, Fashion, Collectibles & More | eBay	FireFox	ebay.com
thick gloves for sale | eBay	FireFox	ebay.com
thick rubbergloves for sale | eBay	FireFox	ebay.com

Figure 2 - Web search history

Figure 3 - Images of house in Maplewood

First Name	Last Name	Credit Card No.	Address
Ermentrude	Kirman	3.56965676605679E+15	16
Lauretta	Rosentholer	6.77144449073011E+16	78246
Idelle	Goodban	6.33487264304233E+15	68
Betta	Ossipenko	5.01012790406945E+15	19
Molly	Dono	3.55876279271824E+15	40
Lorie	Ropcke	3.52811741213172E+15	516
Tanya	Baudino	5.1001771538027E+15	44
Ronna	Hakeworth	5.52440006741465E+15	1
Dacie	Gobel	3.53385771751886E+15	26159
Aida	Tombling	6.30438858650439E+16	871
Blair	Tadlow	201641507054219	2245
Ophelie	Bronger	201589466923579	5
Cleopatra	Gillott	4.02655975766547E+15	4144
Kassi	Ondra	201592583903227	1
Liana	Crocumbe	3.55959244223616E+15	68584
Lissy	Schaumann	5.60221128483211E+16	694
Veronica	Lingard	5.60222303726585E+17	25
Harlie	Francesconi	3.53448382096263E+15	2
Jeanie	Bates	6.75932800269167E+18	4054
Charo	Bernade	3.58597619663384E+15	79

Figure 4 - Women's name, address and credit card no.

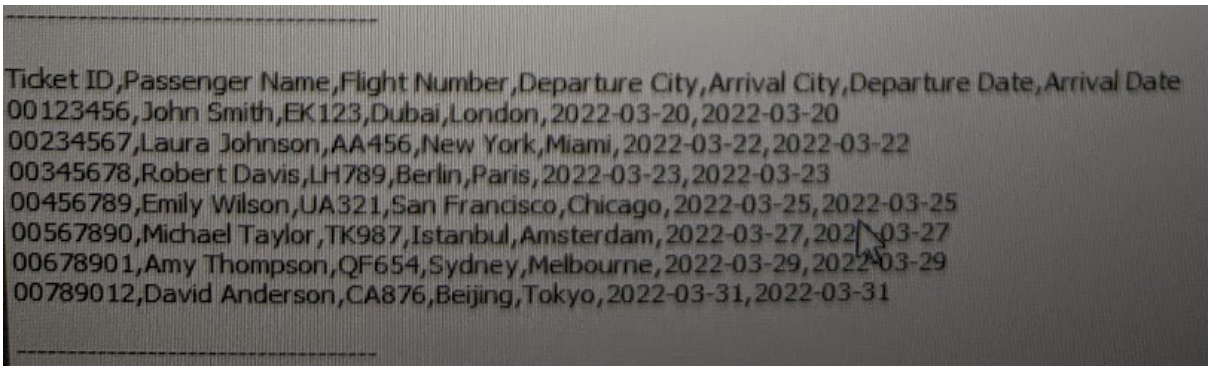


Figure 5 - Plane tickets

5	sudo apt-get update
6	sudo apt-get install -y build-essential linux-headers-$(uname -r)
7	sudo apt-get install virtualbox-guest-utils
8	sudo adduser $(whoami) vboxsf
9	su
10	cat /etc/passwd | cut -d: -f1
11	sudo userdel sammy1
12	cat /etc/passwd | cut -d: -f1
13	sudo userdel sammy
14	cat /etc/passwd | cut -d: -f1
15	sudo userdel sammy1
16	cat /etc/passwd | cut -d: -f1
17	sudo userdel kane24
18	cat /etc/passwd | cut -d: -f1
19	cat /etc/passwd | cut -d f1
20	cat /etc/passwd | cut -d f1
21	cat /etc/passwd | cut -d: f1
22	cat /etc/passwd | cut -d: -f1
23	sudo userdel ruby04

Figure 6 - Linux bash log

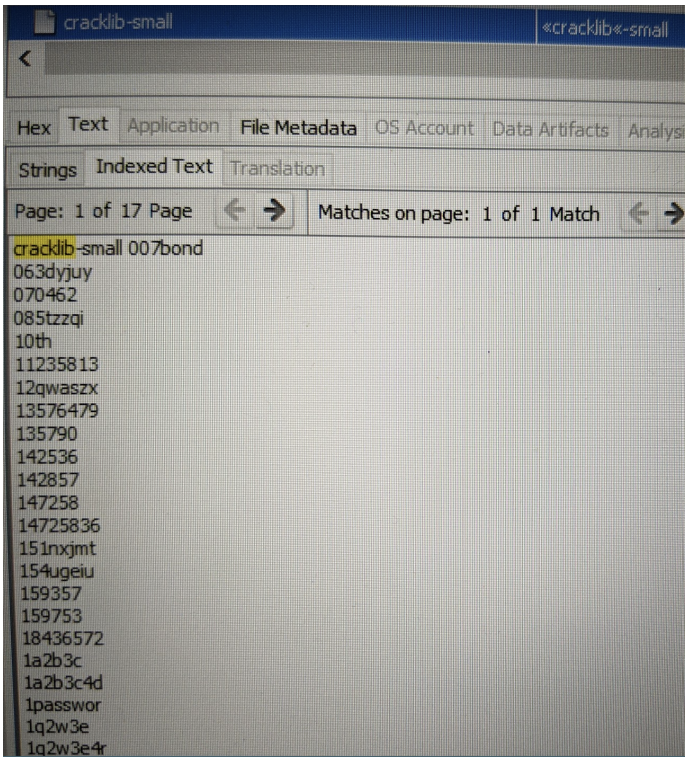
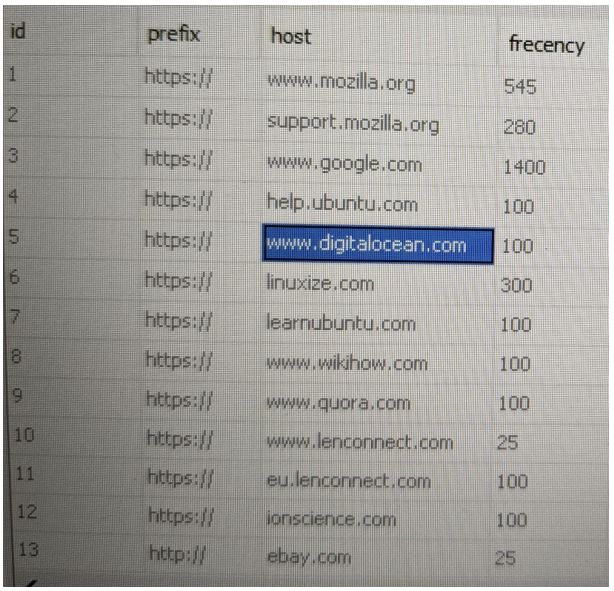


Figure 7 - Cracklib and password library

Figure 8 - Hotel booking via covert operation



id	prefix	host	frecency
1	https://	www.mozilla.org	545
2	https://	support.mozilla.org	280
3	https://	www.google.com	1400
4	https://	help.ubuntu.com	100
5	https://	www.digitalocean.com	100
6	https://	linuxize.com	300
7	https://	learnubuntu.com	100
8	https://	www.wikihow.com	100
9	https://	www.quora.com	100
10	https://	www.lenconnect.com	25
11	https://	eu.lenconnect.com	100
12	https://	ionscience.com	100
13	http://	ebay.com	25

Figure 9 - Online host website

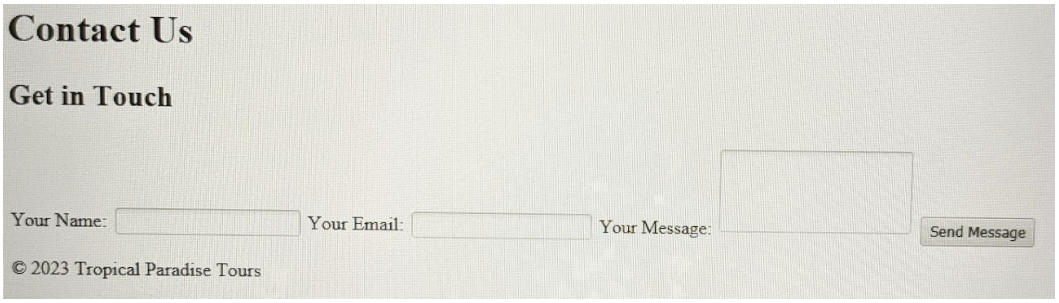


Figure 10 - Self crafted contact form in phishing website

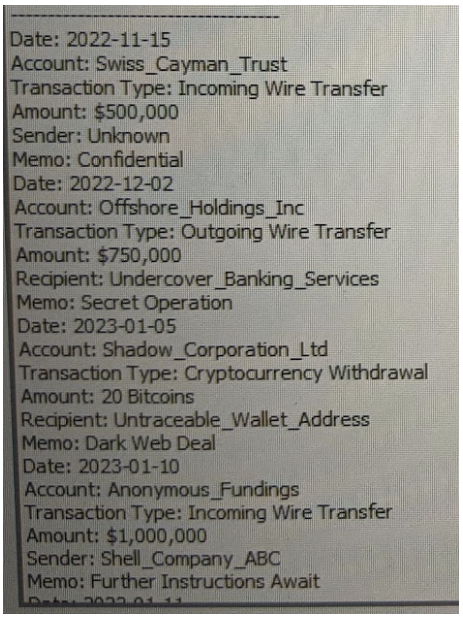


Figure 11 - Significant financial gains

PART 3 - Incident Handling

As the forensics analyst leading the case for BGP Forensics, my initial focus would be on a meticulous examination of the 2 x 2TB hard drive disk images provided by colleagues. These images, serving as the primary source of digital evidence, require delicate handling to preserve forensic integrity.

In the Preparation stage of the CREST Incident Response Framework[1] (Jason Creasey, 2013), I would prioritise establishing clear communication channels within the team. Effective coordination is essential to streamline efforts. Simultaneously, I would initiate engaging training sessions for company staff, not only enhancing their awareness of potential cyber threats but also ensuring they understand their roles in the incident response plan.

Moving to the Identification stage, a thorough analysis of the incident involves validating and reporting details. I would delve into the threatening email received on January 7th and the website defacement on January 9th. Preliminary interviews would go beyond data collection, serving as an educational opportunity for stakeholders regarding usernames, passwords, and security schemes.

With the disk images in hand, the Initial Search of the Scene is conducted meticulously. This step includes a comprehensive inspection for signs of unauthorised access, malware, or malicious activities. The electronic crime scene is documented through photography and sketching, providing a visual record that aids in analysis and stakeholder communication.

In the Containment stage, isolating affected systems is not just about prevention; it's also about minimising disruption. Communication strategies are implemented to assure stakeholders, emphasising the protective measures in place. The Order of Volatility is adhered to, prioritising the collection of evidence to ensure critical data is preserved promptly. [1] (Jason Creasey, 2013)

Eradication involves a strategic effort to remove identified malware, utilising standard anti-virus tools. To prevent future incidents, security measures are bolstered through the enabling of firewalls and router filters.

Recovery, the pivotal stage for minimising downtime, involves a meticulous determination of actions. System categorization based on criticality allows for the prioritised restoration of essential functions. A 'Road to Recovery' infographic is shared with stakeholders, providing a visual representation of progress and expected timelines.

In the Follow-up stage, policies and procedures are revised and innovatively communicated. A short, engaging video or infographic summarises key findings and

actions, creating a memorable impact. A detailed cost analysis considers the extent of disruptions, data loss, and damaged hardware, providing a comprehensive view of the incident's impact. [1] (Jason Creasey, 2013)

This holistic and detailed approach ensures the capture of digital evidence, maintains forensic integrity, minimises downtime through effective communication, and engages stakeholders in a clear manner.

Reference

[1] Jason Creasey, Cyber Security Incident Response Guide, Version 1, 2013
Published by: CREST

PART 4 - Network forensics

Since we don't know which device the network packet was captured on, it could have been captured on a computer on the 11.3.X.X network segment or on a device such as a router or firewall. And, based on my personal experience (I've had some experience working with windows networking), packet capturing on network devices may results in packet loss, and the behaviour of the firewall itself is difficult to discover by capturing packets on a single device, so the following analysis contains some speculation, and to clarify the attack, it may need to be combined with other relevant evidence.

Tools:
1. Wireshark
2. DynamiteLab - online PCAP viewer and analyzer

Examination:
1. Use wireshark with filters for ip address, protocol and statistic function, I got the following observations:

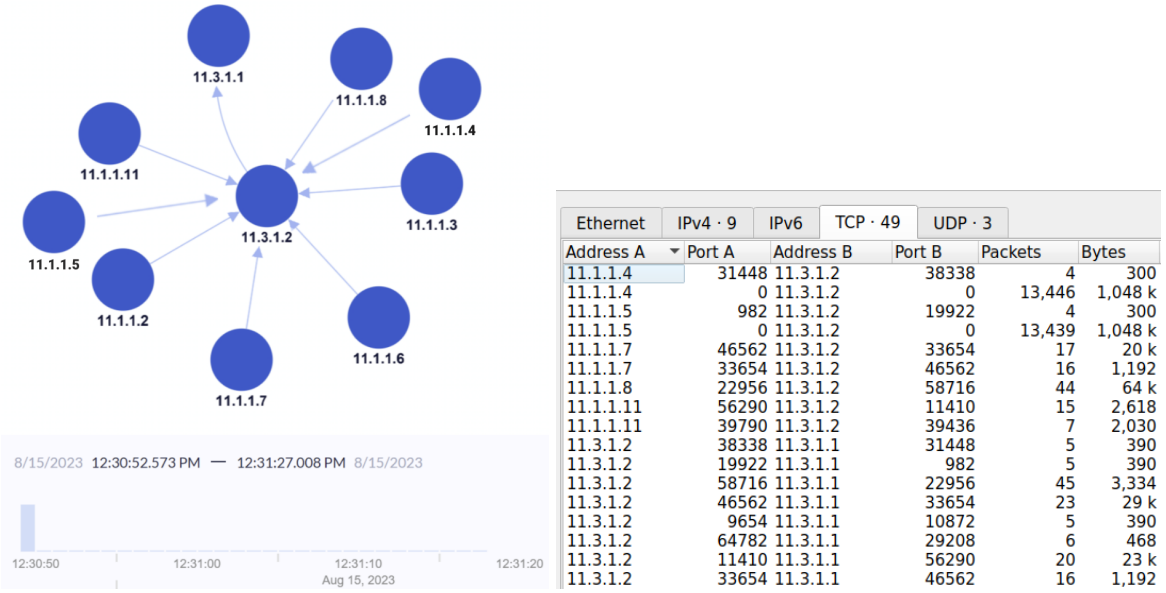
1) 11.1.1.2, 11.1.1.3 and 11.1.1.6 each send 660+ UDP packets to 11.3.1.2 without any responses from 11.3.1.2

2) 11.1.1.3 and 11.1.1.4 each send around 13400+ TCP packets to 11.3.1.2 (0 length, from port 0 to 0) without any responses from 11.3.1.2

3) 11.1.1.7, 11.1.1.8 and 11.1.1.11 each send 20-50 TCP packets to 11.3.1.2 with retransmissions and no any responses from 11.3.1.2

4) 11.3.1.1 did not send out any packets, instead it only received 274 TCP packets with retransmissions from 11.3.1.2

2. Use the online tool DynamiteLab to get a visualisation of the network flow.



Address A	Port A	Address B	Port B	Packets	Bytes
11.1.1.4	31448	11.3.1.2	38338	4	300
11.1.1.4	0	11.3.1.2	0	13,446	1,048 k
11.1.1.5	982	11.3.1.2	19922	4	300
11.1.1.5	0	11.3.1.2	0	13,439	1,048 k
11.1.1.7	46562	11.3.1.2	33654	17	20 k
11.1.1.7	33654	11.3.1.2	46562	16	1,192
11.1.1.8	22956	11.3.1.2	58716	44	64 k
11.1.1.11	56290	11.3.1.2	11410	15	2,618
11.1.1.11	39790	11.3.1.2	39436	7	2,030
11.3.1.2	38338	11.3.1.1	31448	5	390
11.3.1.2	19922	11.3.1.1	982	5	390
11.3.1.2	58716	11.3.1.1	22956	45	3,334
11.3.1.2	46562	11.3.1.1	33654	23	29 k
11.3.1.2	9654	11.3.1.1	10872	5	390
11.3.1.2	64782	11.3.1.1	29208	6	468
11.3.1.2	11410	11.3.1.1	56290	20	23 k
11.3.1.2	33654	11.3.1.1	46562	16	1,192

Figure 12 - Simple network topology indicating directions of packets flow

There are several indications of suspicious activity on the network. Here's a breakdown of the anomalies:

1. **Anomaly**: 11.3.1.2 only sent out packets to 11.3.1.1 in the same network segment, while didn't respond to any hosts outside the network.
   Analysis: Local firewalls may have blocked the packets from/to other network segments. However, if the packets are captured in a Windows PC, the Windows Filtering Platform - WFP component could interfere with the capturing component of the Npcap library used by capturing tools.

2. **Anomaly:** The sending of numerous TCP packets with zero-length payloads (0 bytes) from 11.1.1.3 and 11.1.1.4 to 11.3.1.2 .
   Analysis: These 0 payload packets look like they are artificially generated and do not behave like regular applications. Sending a large volume of them raises concerns about potential malicious activity. [1] (Ke Meng, 2015)

3. **Anomaly**: The repeated transmission of TCP packets with retransmissions from 11.1.1.7, 11.1.1.8, and 11.1.1.11 to 11.3.1.2.
   Analysis: It indicates a possible connection establishment attempt. However, the lack of responses from 11.3.1.2 suggests that these devices are repeatedly trying to connect to a non-responsive or unavailable server.

4. **Anomaly**: The complete lack of outgoing packets from 11.3.1.1, coupled with the hundreds of incoming packets with retransmissions from 11.3.1.2.
   Analysis: It suggests that 11.3.1.1 is either malfunctioning or under attack. The retransmissions from 11.3.1.2 could indicate that it's trying to respond to these connections, but the lack of responses from 11.3.1.1 implies that it's unable to process or respond to the incoming traffic.

5. **Anomaly**: UDP packets to 11.3.1.2 with consistent size.
   Analysis: The constant 1460 packet size and the absence of response packets may indicate a covert channel or data exfiltration attempt. It could also suggest a potential UDP flood attack which aims to overwhelm the target device or network with excessive UDP traffic.

These observations point towards a potential malicious activity targeting these devices on the network. The combination of UDP floods, zero-length TCP packets, repeated TCP retransmissions, and an unresponsive target device suggests that the network is under attack or experiencing a significant disruption.

One possible scenario is that machines in the 11.1.X.X network segment are infected and used to attack machines in the 11.3.X.X network segment. Machines in segment 11.3.X.X may be in a DMZ protected by a firewall and may not be able to respond, or may have their packets intercepted by the firewall and not be reflected in the capture.

Further investigation is necessary to determine the specific nature of the attack and its potential impact. This may involve capturing packets from the hosts that are sending the packets, and inspect which program triggered the network activity. Also go to 11.3.1.2 and check its local firewall log, netstat, to figure out why it stopped responding to those hosts.

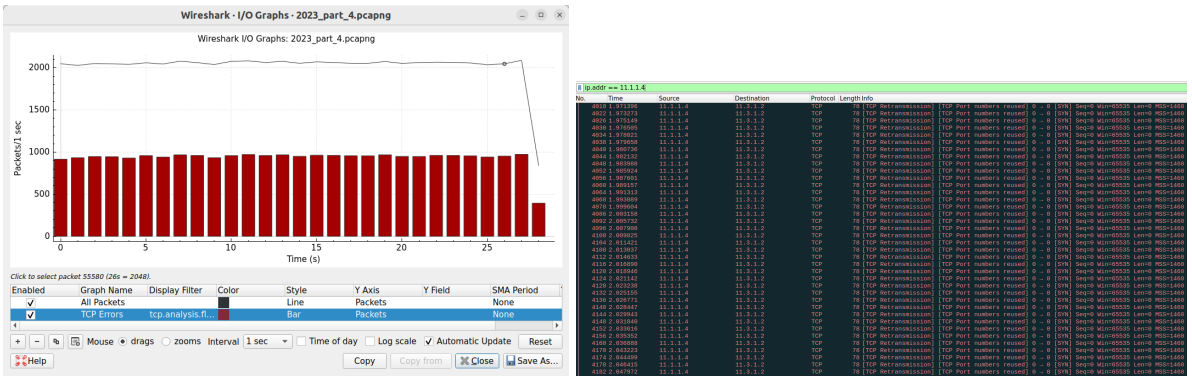


Figure 13 - consistent TCP retransmission errors

Reference

[1] Ke Meng, 2015, Network forensics analysis using Wireshark, Research Gate