Lab 7

Packet Capture Analysis

Mina Salehi

University of Maryland Baltimore County

CYBR 642 Introduction to Digital Forensics

Presented to: Gina Scaldaferri

04/09/2025

Introduction

In the realm of digital forensics and incident response (DFIR), network packet analysis serves as a vital tool in uncovering unauthorized or suspicious activity. The increasing sophistication of cyber threats has made it essential for analysts to interpret raw packet data to identify malicious systems, reconstruct events, and extract potential indicators of compromise (IOC). As cybercriminals continue to exploit network vulnerabilities to exfiltrate data or communicate covertly, forensic analysts must rely on packet capture (PCAP) files to track threat actors and understand their methods (APNIC, 2022; Corelight, n.d.).

This lab simulates a real-world scenario in which a DFIR team is tasked with analyzing a provided PCAP file to assist in a criminal investigation. The scenario follows Ann Dercover, a suspect recently released on bail, who has since disappeared. Authorities believe that clues to her whereabouts may lie within her network communications, particularly potential exchanges with a mysterious accomplice, Mr. X. Through detailed packet analysis, the forensic team aims to determine the presence of any malicious systems on the network and extract relevant files embedded in the traffic, thereby reconstructing Ann's digital footprint and uncovering her possible escape plans.

This exercise will involve scrutinizing network flows, identifying anomalies, and carving files from the data stream. The ultimate goal is to develop a coherent narrative of the network activity that occurred prior to Ann Dercover's disappearance, leveraging digital forensics best practices and analytic tools such as Wireshark and NetworkMiner

(Forensicxs, 2020; Alblas, 2025). The analysis underscores the critical role that packet inspection plays in modern cyber investigations, particularly in tracking fugitives, detecting covert communications, and enhancing situational awareness for law enforcement agencies.

Network Forensics Methodology: The OSCAR Model

To conduct a structured and effective network forensic investigation, the OSCAR methodology provides a reliable and repeatable framework. OSCAR is an acronym for Obtain information, Strategize, Collect evidence, Analyze, and Report**,** five critical stages designed to guide investigators through complex digital forensic cases. (Dropzone AI, 2023)

Obtain Information

Initially, investigators gather background information about the case. In this scenario, law enforcement suspects that Ann Dercover communicated with an individual named Mr. X prior to her disappearance. These interactions are believed to be found in a packet capture (PCAP) file obtained during surveillance. Key information such as the timeframe of monitoring, involved devices, and suspected activity helps narrow the scope of the investigation (Varonis, 2023).

Strategize

Once the context is established, the investigative team develops a tactical plan. This includes selecting appropriate tools such as Wireshark for packet-level inspection and

NetworkMiner for file and artifact extraction (Netresec, 2024). Wireshark is known for its deep packet inspection features, while NetworkMiner excels in carving files and reconstructing sessions from PCAP data.

Collect Evidence

The core of network forensics lies in the collection of digital evidence. In this case, the primary source is the PCAP file, which contains captured packets from Ann Dercover's monitored network activity.

Analyze

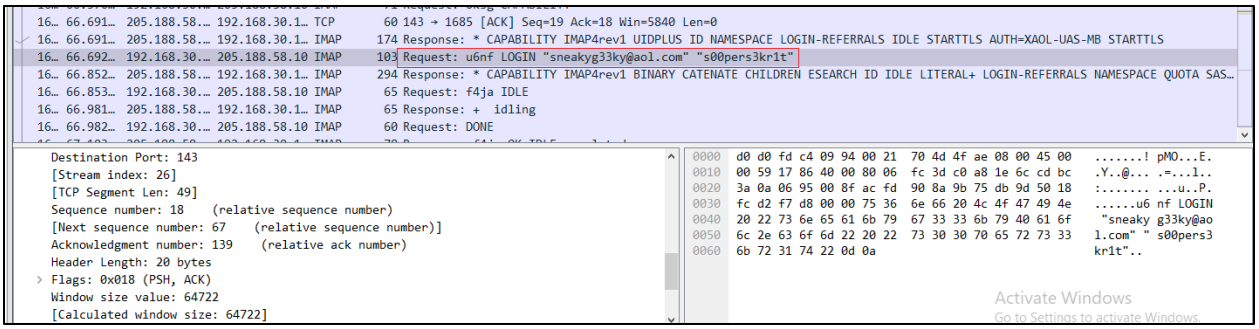
This phase involves a deep examination of the packet data to uncover any hidden communication, file transfers, or malicious activity. Investigators can use tools to reconstruct TCP streams, analyze DNS queries, identify protocols used, and extract payloads.

How Packet Captures Work

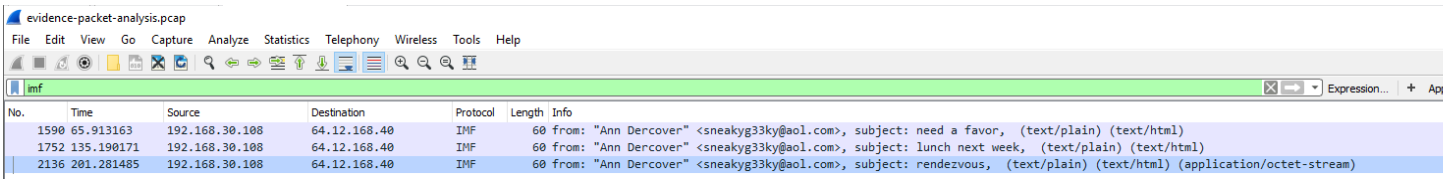
Packet captures are typically collected using network monitoring tools such as tcpdump, Wireshark, or TShark, often run on a device connected to a network hub, switch with port mirroring, or a tap. These tools place the NIC in promiscuous mode, enabling it to capture all packets on the network segment, not just those addressed to the host device. Captured packets are saved in a PCAP format, which retains detailed information about each packet's source, destination, protocol, and payload data. This allows forensic analysts to replay and scrutinize the network traffic for investigative purposes (Alharbi et al., 2011).

Packet Capture Analysis

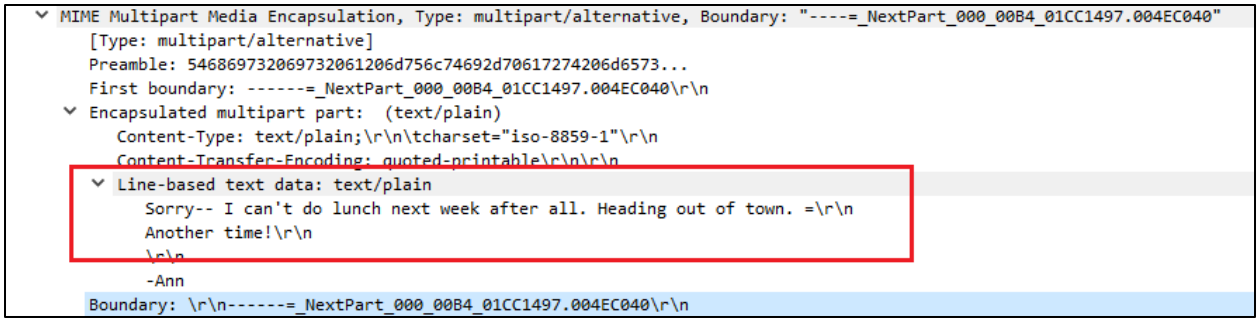
- Provide any online aliases or addresses and corresponding account credentials that may be used by the suspect under investigation.
    - Account used by the suspect is "sneakyg33ky" and password is "s00pers3kr1t"



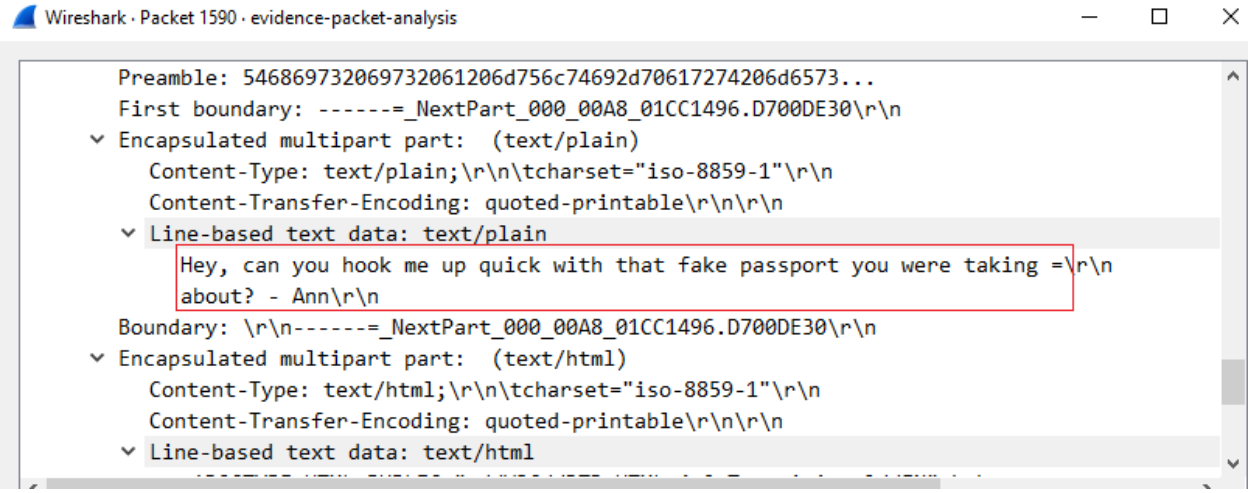
- Who did Ann communicate with? Provide a list of email addresses and any other identifying information.
    - For this task I searched using ip.addr==192.168.30.108 , this will show all the communication from Ann Dercover IP address



    - Communication with D4rktangent@gmail.com



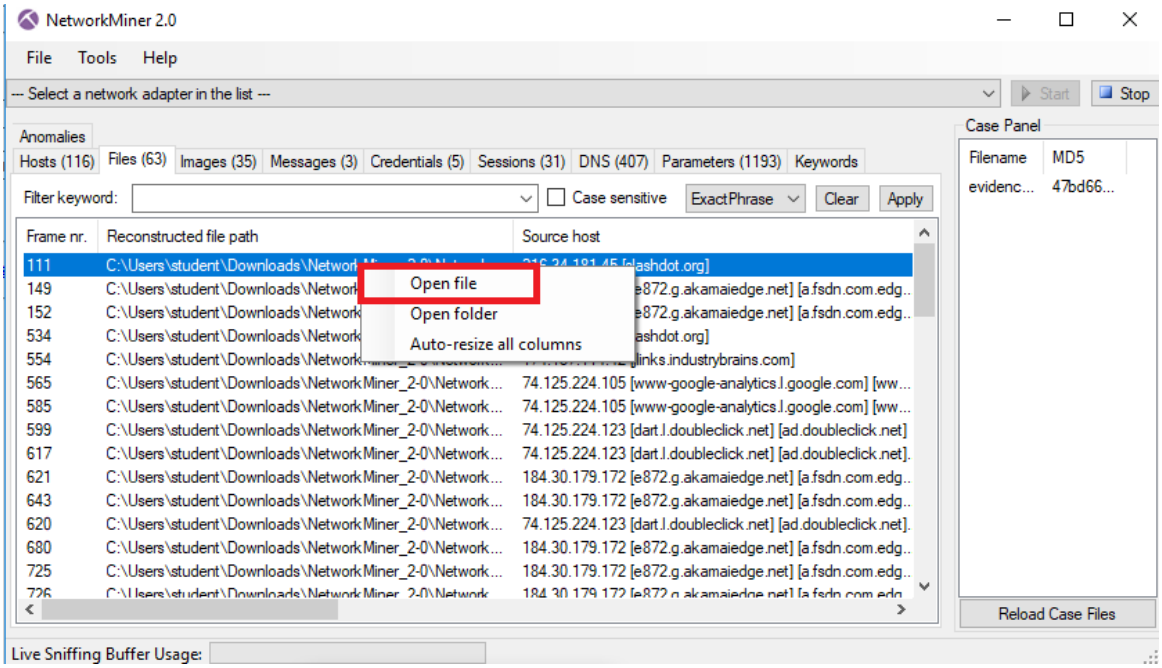
- Communication with Inter0pt1c@aol.com

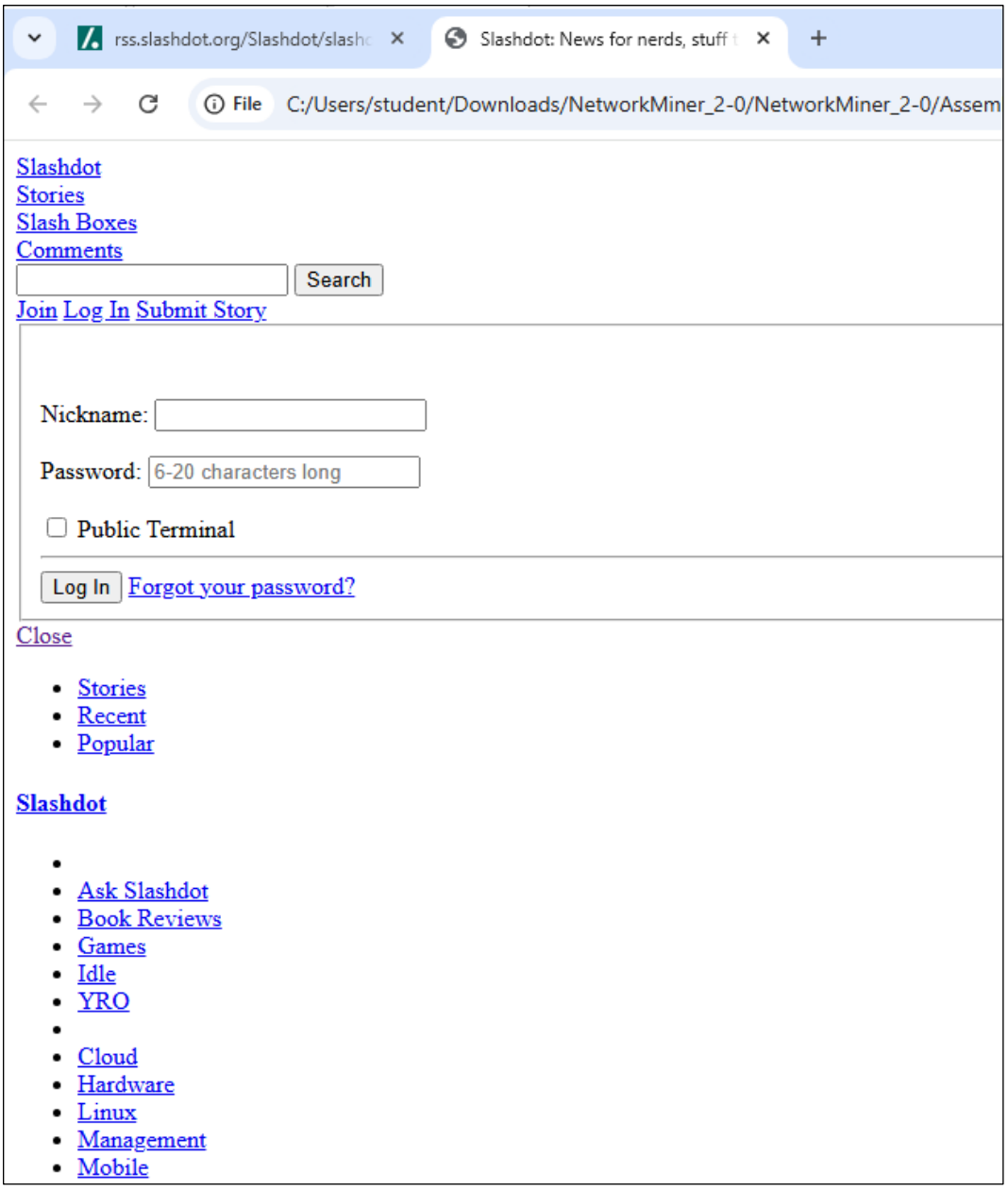


- Communication with Mistersekritx@aol.con

If Ann transferred or received any files of interest, recover them.

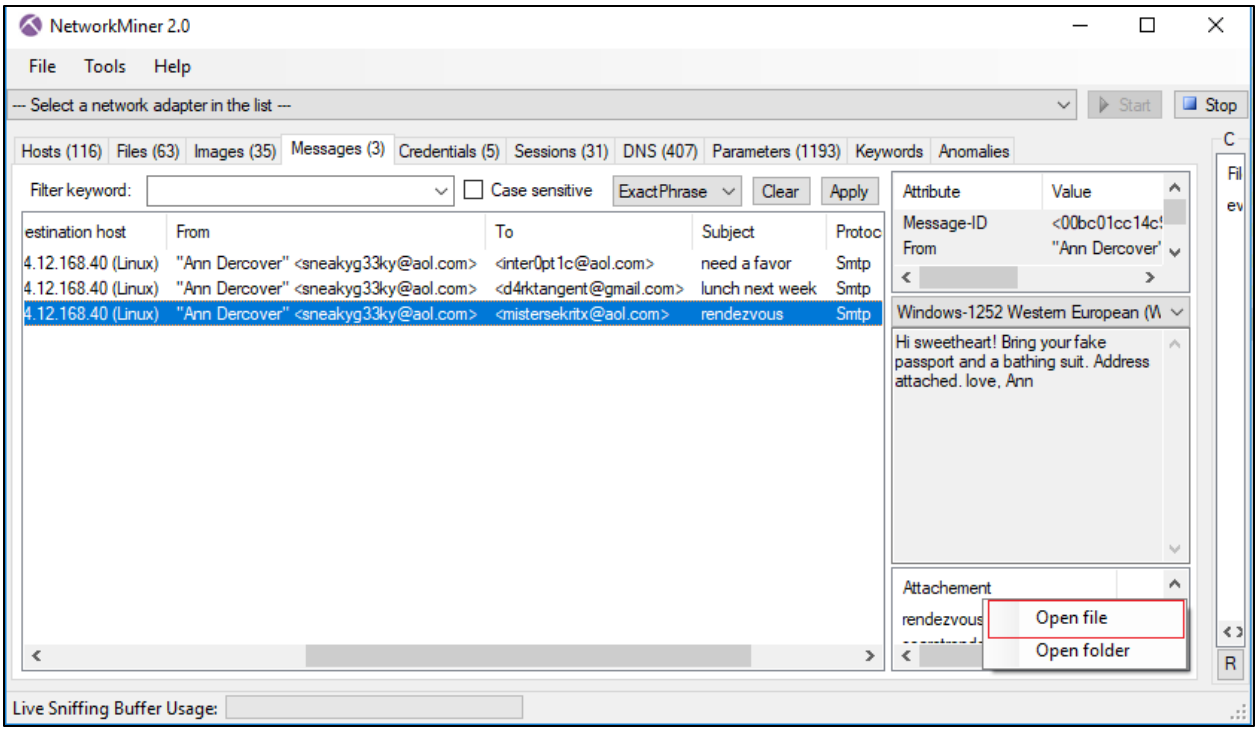
For this section, I utilized NetworkMiner

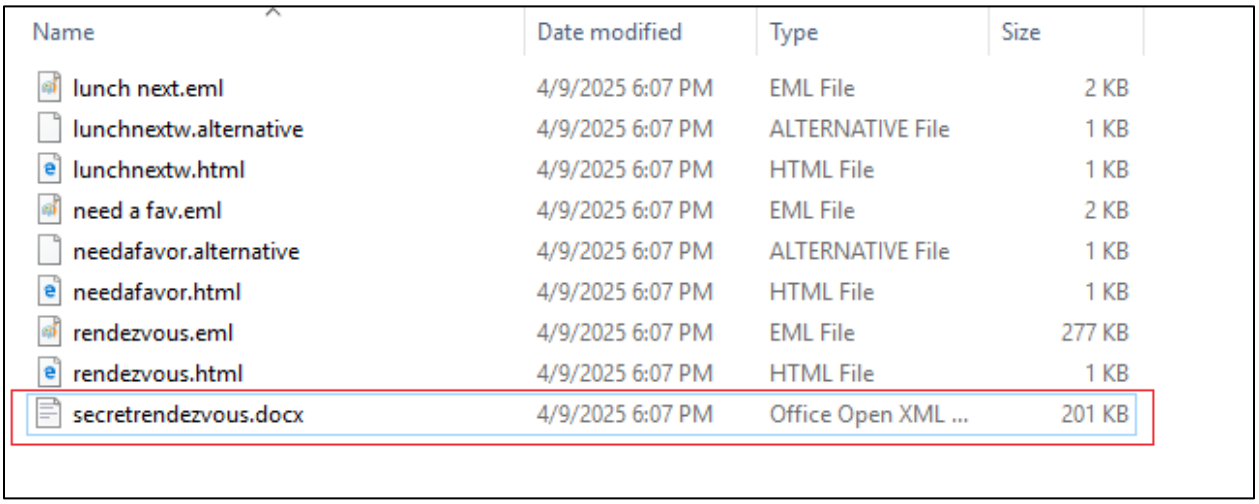


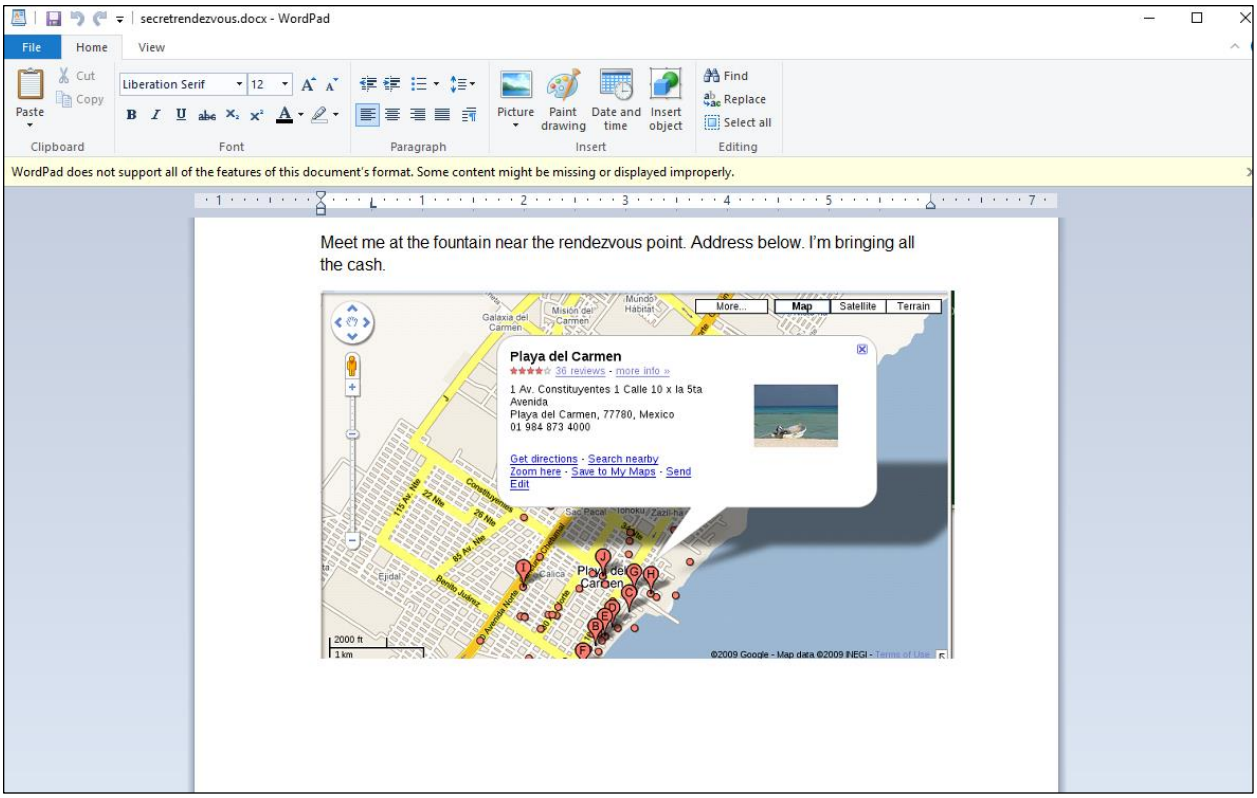


Are there any indications of Ann's physical whereabouts? If so, provide supporting evidence.

The recovered file reveals Ann's physical location. As shown in the image below, she is meeting mistersekritx@aol.com at the fountain near Playa del Carmen


NetworkMiner 2.0
File
Tools
Help
-- Select a network adapter in the list ---
Start
Stop
Hosts (116)
Files (63)
Images (35)
Messages (3)
Credentials (5)
Sessions (31)
DNS (407)
Parameters (1193)
Keywords
Anomalies
Filter keyword:
Case sensitive
ExactPhrase
Clear
Apply
estination host
From
To
Subject
Protoc
4.12.168.40 (Linux)
"Ann Dercover" <sneakyg33ky@aol.com>
<inter0pt1c@aol.com>
need a favor
Smtp
4.12.168.40 (Linux)
"Ann Dercover" <sneakyg33ky@aol.com>
<d4rktangent@gmail.com>
lunch next week
Smtp
4.12.168.40 (Linux)
"Ann Dercover" <sneakyg33ky@aol.com>
<mistersekritx@aol.com>
rendezvous
Smtp
Attribute
Value
Message-ID
<00bc01cc14c
From
"Ann Dercover'
Windows-1252 Western European (W
Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann
Attachement
rendezvous
Open file
Open folder
Live Sniffing Buffer Usage:


Name
Date modified
Type
Size
lunch next.eml
4/9/2025 6:07 PM
EML File
2 KB
lunchnextw.alternative
4/9/2025 6:07 PM
ALTERNATIVE File
1 KB
lunchnextw.html
4/9/2025 6:07 PM
HTML File
1 KB
need a fav.eml
4/9/2025 6:07 PM
EML File
2 KB
needafavor.alternative
4/9/2025 6:07 PM
ALTERNATIVE File
1 KB
needafavor.html
4/9/2025 6:07 PM
HTML File
1 KB
rendezvous.eml
4/9/2025 6:07 PM
EML File
277 KB
rendezvous.html
4/9/2025 6:07 PM
HTML File
1 KB
secretrendezvous.docx
4/9/2025 6:07 PM
Office Open XML ...
201 KB



Conclusion

This lab successfully demonstrates the critical importance of network forensics in modern digital investigations, particularly through the structured application of the OSCAR methodology. By following the stages of obtaining information, strategizing, collecting evidence, analyzing packet data, and reporting, investigators can piece together digital narratives that aid in both criminal investigations and cybersecurity incident response. The case of Ann Dercover highlights how tools such as Wireshark and NetworkMiner can be leveraged to uncover hidden communications, extract files, and identify patterns of suspicious activity.

Glossary

DFIR (Digital Forensics and Incident Response): A field within cybersecurity focused on investigating and responding to cyber incidents and breaches.

Packet Analysis: The process of capturing, inspecting, and interpreting data packets that travel across a network to identify potential security threats.

PCAP (Packet Capture): A file format used to capture and store data packets for later analysis.

Carving Files: Extracting embedded files or data from a larger dataset, such as a network stream or hard disk image.

Indicators of Compromise (IOC): Artifacts or evidence on a system or network that indicate a potential intrusion.

References

APNIC. (2022, March 31). *How to: Detect and prevent common data exfiltration attacks*. https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/

Corelight. (n.d.). *Packet Capture: What Is PCAP in Network Security?* https://corelight.com/resources/glossary/packet-capture-pcap

Dropzone AI. (2023, August 22). *Why SOCs rely on OSCAR: A proven investigative framework*. https://www.dropzone.ai/blog/why-socs-rely-on-oscar-a-proven-investigative-framework

Forensicxs. (2020, November 20). *Network Case using Wireshark and NetworkMiner*. https://www.forensicxs.com/computer-forensics-network-case-using-wireshark-and-networkminer/

Infosec Institute. (2021, February 10). *Network Forensics Tools*. https://www.infosecinstitute.com/resources/digital-forensics/network-forensics-tools/

Netresec. (2024). *NetworkMiner*. https://www.netresec.com/?page=NetworkMiner

Varonis. (2023, July 10). *What is packet capture? A complete guide*. https://www.varonis.com/blog/packet-capture