Network Forensics Investigation: Tracing Anonymous Emails with Wireshark & NetworkMiner

Cybersecurity Lab Portfolio | Sanitized for Public Sharing

Overview

This lab simulated a digital harassment investigation at Nitroba State University. Using Wireshark and NetworkMiner, I analyzed a packet capture file to trace anonymous emails sent through services like sendanonymousemail.net and willselfdestruct.com. By filtering traffic, reconstructing files, and correlating IP and MAC address data, I identified the suspect device (192.168.15.4), linked to the Gmail account jcoachj@gmail.com, and confirmed its use of the campus dorm network via NAT translation. This exercise strengthened my ability to analyze packet data, investigate malicious activity, and correlate digital evidence in real-world scenarios.

Tools Used

- Wireshark – Packet analysis & traffic filtering
- NetworkMiner – Host analysis & file reconstruction
- Nitroba.pcap – Packet capture for investigation
- Windows environment (Alienware M17 R5)

Methods

- Imported Nitroba.pcap into Wireshark and NetworkMiner for analysis.
- Applied IP filters and searched for domains linked to anonymous email services.
- Correlated timestamps between harassing emails and suspect device activity.
- Extracted host metadata and reconstructed web sessions in NetworkMiner.
- Linked internal IP (192.168.15.4) to public dorm IP (140.247.62.34) using NAT and MAC address data.

Key Results

1. Anonymous Emails Identified
   Filtered Wireshark traffic revealed HTTP activity to anonymous email services at timestamps matching the two harassing emails.

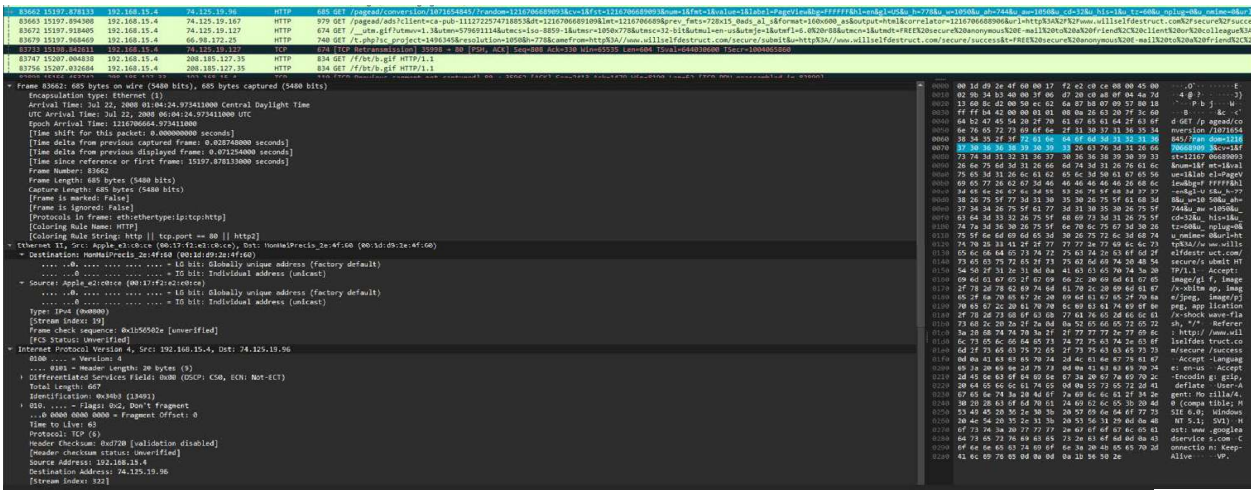

Figure 1 Wireshark HTTP request revealing activity to anonymous email service (simulated lab data).

2. Linking Internal IP to Suspect
   NetworkMiner's Credentials tab identified Gmail login jcoachj@gmail.com from 192.168.15.4 at 06:01 AM – minutes before the emails were sent. Data shown is from a simulated lab environment, not real user accounts.

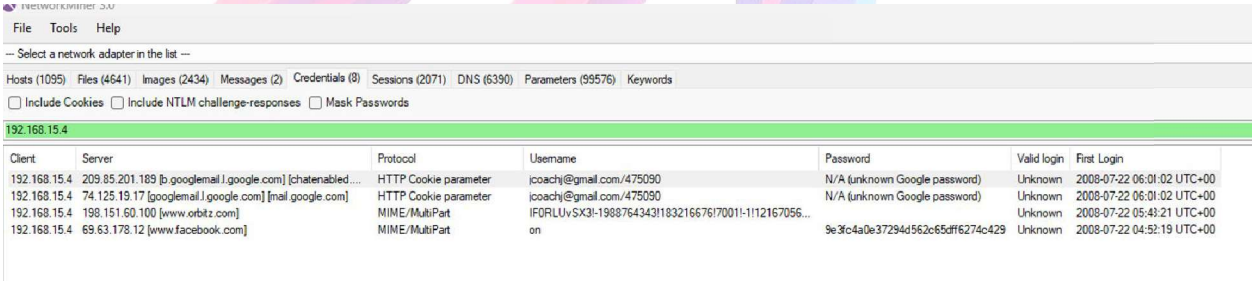

Figure 2 NetworkMiner Credentials tab linking suspect email to internal IP 192.168.15.4,

3. Correlating Internal and External IP
   Wireshark analysis confirmed NAT translation between the suspect IP (192.168.15.4) and the public dorm IP (140.247.62.34).

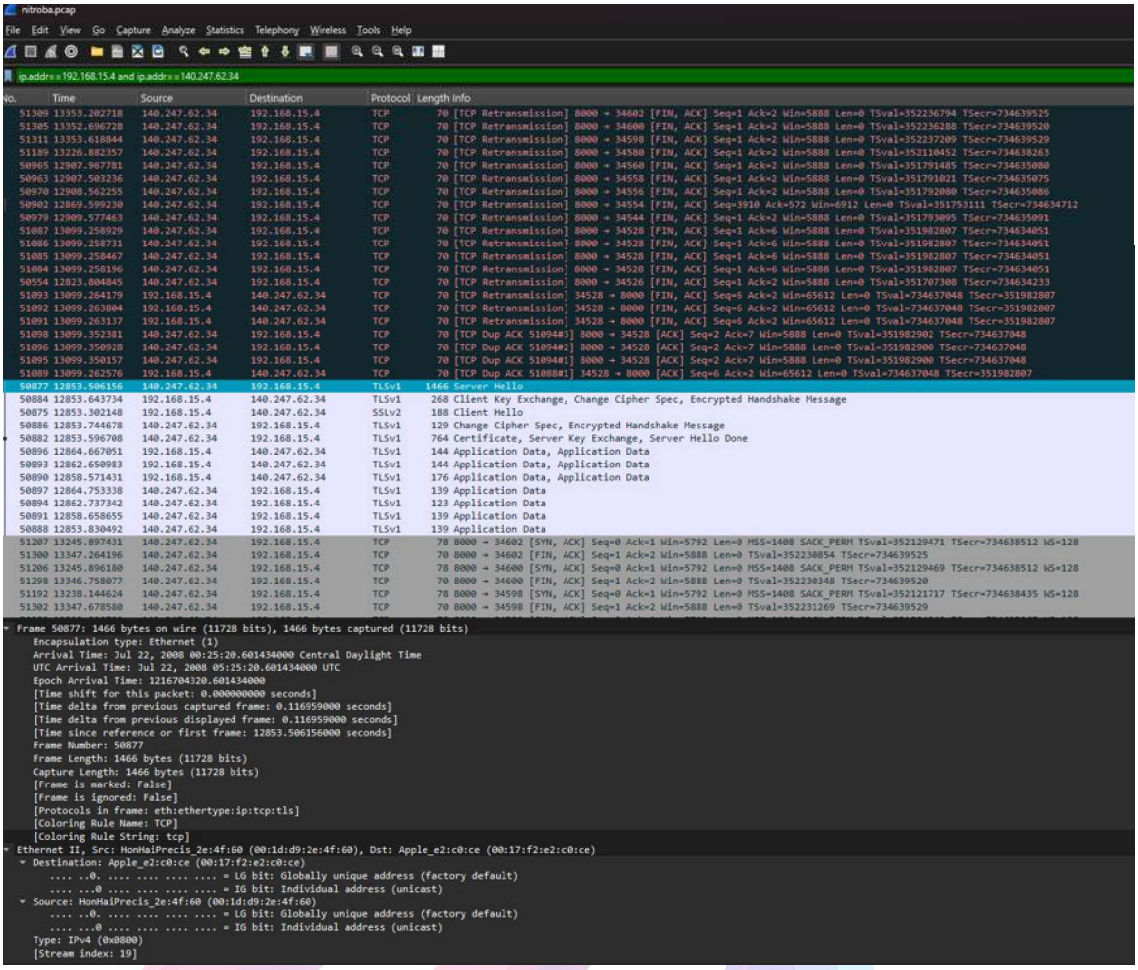

Figure 3 Wireshark packet details showing connecting between suspect device and dorm IP via NAT (simulated lab data).

Discussion

This lab highlights how network forensics techniques uncover evidence hidden behind NAT and public IP addresses. By correlating multiple data points – IP addresses, timestamps, session logs, and reconstructed files – I build a strong case tying activity to a specific user. Real-world investigations often involve similar challenges, such as working through anonymizing services and shared networks, making these skills critical for incident response and legal proceedings.

Key Takeaways

- Demonstrated the use of Wireshark filters to isolate malicious activity.
- Reconstructed web sessions and artifacts in NetworkMiner to validate evidence.

- Mapped internal and external IPs using NAT analysis.
- Identified digital footprints leading to a specific account under investigation.
- Reinforced ethical considerations when analyzing potentially sensitive data.