

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.

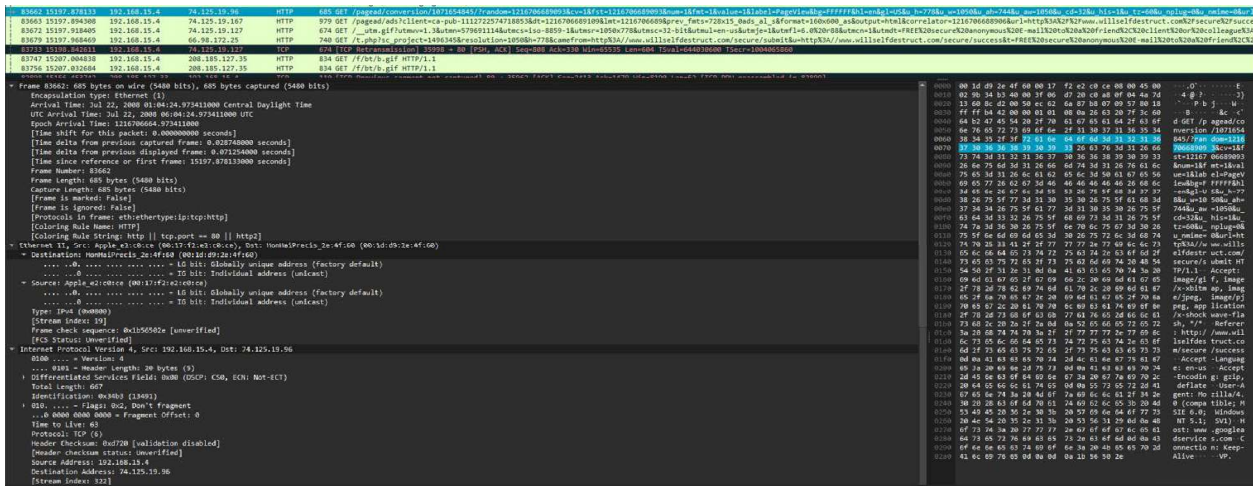


Figure 1 Wireshark HTTP request revealing activity to anonymous email service (simulated lab data).

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.

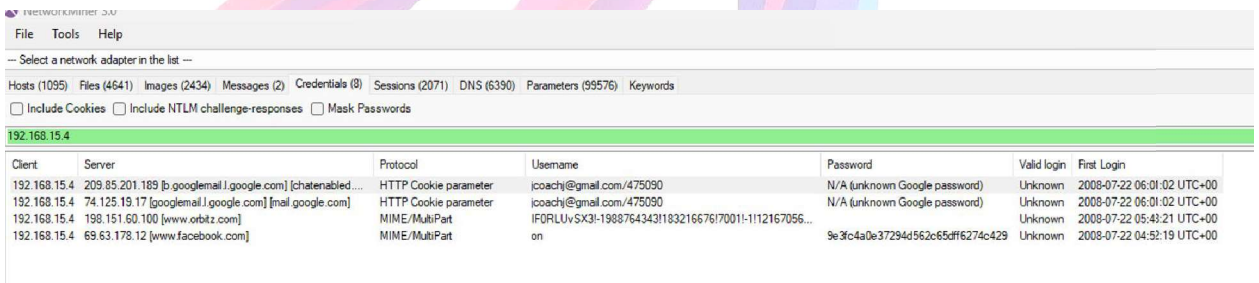


Figure 2 NetworkMiner Credentials tab linking suspect email to internal IP 192.168.15.4,

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).

```

nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==192.168.15.4 and ip.addr==140.247.62.34

No. Time Source Destination Protocol Length Info
51309 13353.262718 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34602 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352236794 TSecr=734639525
51305 13352.696728 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34600 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352236288 TSecr=734639520
51311 13353.618844 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34598 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352237289 TSecr=734639529
51189 13226.882357 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34588 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351104512 TSecr=734638283
50985 12807.987781 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34569 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351731485 TSecr=734639080
50963 12807.503236 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34558 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351791821 TSecr=734635075
50970 12808.562255 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34556 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351792088 TSecr=734635086
50902 12869.599230 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34554 [FIN, ACK] Seq=3910 Ack=572 Min=6912 Len=0 TSval=351753111 TSecr=734634712
50979 12808.577463 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34544 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351793895 TSecr=734635091
51007 13099.258929 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34528 [FIN, ACK] Seq=1 Ack=6 Win=5888 Len=0 TSval=351812807 TSecr=734634051
51066 13099.258751 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34528 [FIN, ACK] Seq=1 Ack=6 Win=5888 Len=0 TSval=351812807 TSecr=734634051
51085 13099.258647 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34528 [FIN, ACK] Seq=1 Ack=6 Win=5888 Len=0 TSval=351812807 TSecr=734634051
51084 13099.258196 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34528 [FIN, ACK] Seq=1 Ack=6 Win=5888 Len=0 TSval=351812807 TSecr=734634051
50554 12823.804845 140.247.62.34 192.168.15.4 TCP 70 [TCP Retransmission] 8000 -> 34526 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351707388 TSecr=734634233
51093 13099.264179 192.168.15.4 140.247.62.34 TCP 70 [TCP Retransmission] 34528 -> 8000 [FIN, ACK] Seq=9 Ack=2 Win=65612 Len=0 TSval=734637048 TSecr=351928207
51002 13099.263084 192.168.15.4 140.247.62.34 TCP 70 [TCP Retransmission] 34528 -> 8000 [FIN, ACK] Seq=9 Ack=2 Win=65612 Len=0 TSval=734637048 TSecr=351928207
51091 13099.263117 192.168.15.4 140.247.62.34 TCP 70 [TCP Retransmission] 34528 -> 8000 [FIN, ACK] Seq=6 Ack=2 Win=65612 Len=0 TSval=734637048 TSecr=351928207
51098 13099.352381 140.247.62.34 192.168.15.4 TCP 70 [TCP Dup ACK 51094#3] 8000 -> 34528 [ACK] Seq=2 Ack=7 Win=5888 Len=0 TSval=351982900 TSecr=734637048
51096 13099.350928 140.247.62.34 192.168.15.4 TCP 70 [TCP Dup ACK 51094#2] 8000 -> 34528 [ACK] Seq=2 Ack=7 Win=5888 Len=0 TSval=351982900 TSecr=734637048
51095 13099.350157 140.247.62.34 192.168.15.4 TCP 70 [TCP Dup ACK 51094#1] 8000 -> 34528 [ACK] Seq=2 Ack=7 Win=5888 Len=0 TSval=351982900 TSecr=734637048
51089 13099.262376 192.168.15.4 140.247.62.34 TCP 70 [TCP Dup ACK 51088#1] 34528 -> 8000 [ACK] Seq=6 Ack=2 Win=65612 Len=0 TSval=734637048 TSecr=351982807
50877 12853.506156 140.247.62.34 192.168.15.4 TLSv1 1466 Server Hello
50884 12853.643734 192.168.15.4 140.247.62.34 TLSv1 268 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
50875 12853.302148 192.168.15.4 140.247.62.34 SSLv2 188 Client Hello
50886 12853.744678 140.247.62.34 192.168.15.4 TLSv1 129 Change Cipher Spec, Encrypted Handshake Message
50852 12853.596708 140.247.62.34 192.168.15.4 TLSv1 764 Certificate, Server Key Exchange, Server Hello Done
50896 12864.667051 192.168.15.4 140.247.62.34 TLSv1 144 Application Data, Application Data
50893 12862.650983 192.168.15.4 140.247.62.34 TLSv1 144 Application Data, Application Data
50890 12858.571431 192.168.15.4 140.247.62.34 TLSv1 176 Application Data, Application Data
50897 12864.753338 140.247.62.34 192.168.15.4 TLSv1 139 Application Data
50894 12862.797342 140.247.62.34 192.168.15.4 TLSv1 123 Application Data
50891 12858.658855 140.247.62.34 192.168.15.4 TLSv1 139 Application Data
50888 12853.830492 140.247.62.34 192.168.15.4 TLSv1 139 Application Data
51207 13245.897411 140.247.62.34 192.168.15.4 TCP 78 8000 -> 34662 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=3512120471 TSecr=734648512 WS=128
51300 13347.264196 140.247.62.34 192.168.15.4 TCP 70 8000 -> 34662 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352238854 TSecr=734639525
51206 13245.896180 140.247.62.34 192.168.15.4 TCP 78 8000 -> 34600 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=3512120469 TSecr=734648512 WS=128
51298 13346.758077 140.247.62.34 192.168.15.4 TCP 70 8000 -> 34600 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352238348 TSecr=734639520
51192 13238.144624 140.247.62.34 192.168.15.4 TCP 78 8000 -> 34598 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=3512121717 TSecr=734638435 WS=128
51302 13347.678580 140.247.62.34 192.168.15.4 TCP 70 8000 -> 34598 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352231269 TSecr=734639529

* Frame 50877: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface 0
  Encapsulation type: Ethernet (1)
    Arrival Time: Jul 22, 2008 00:25:20.601434000 Central Daylight Time
    UTC Arrival Time: Jul 22, 2008 05:25:20.601434000 UTC
    Epoch Arrival Time: 1216704320.601434000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.116959000 seconds]
    [Time delta from previous displayed frame: 0.116959000 seconds]
    [Time since reference or first frame: 12853.506156000 seconds]
  Frame Number: 50877
  Frame Length: 1466 bytes (11728 bits)
  Capture Length: 1466 bytes (11728 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in Frame: ethertype:ip:tcp:tls]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  * Ethernet II, Src: NonHmiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60), Dst: Apple_e2:c0:cc (00:17:f2:e2:c0:cc)
    * Destination: Apple_e2:c0:cc (00:17:f2:e2:c0:cc)
      ....0. .... .. .. . LG bit: Globally unique address (factory default)
      ....0. .... .. .. . IG bit: Individual address (unicast)
    * Source: NonHmiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
      ....0. .... .. .. . LG bit: Globally unique address (factory default)
      ....0. .... .. .. . IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 19]

```

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.

