DIGITAL FORENSICS INVESTIGATION REPORT

This report was created as part of an independent study in the field of Digital Forensics. Not intended for comercial use.

By : Amar - Independent DFIR Analyst

Digital Forensics Report
Nitroba Harassment

Investigator: Amar
Investigation Date: 17/07/2025
Tools: Wireshark, NetworkMiner 3.0
Document Number: 01.002

1. Executive Summary

This investigation was initiated in response to a cyber harassment complaint filed by Chemistry 109 instructor Lily Tuckrige. Through forensic network analysis of packet captures collected from Nitroba's dormitory network, a specific device was identified as having accessed anonymous email services used to send threatening messages. That device was also used to log into the Gmail account jcoachj@gmail.com, which strongly correlates to student Johnny Coach from the Chemistry 109 class roster.

2. Scope of the Investigation

This report covers the analysis of a packet capture file (nitroba.pcap) to:
- Identify the device responsible for sending harassing emails
- Correlate network behavior with possible student identities
- Determine the timeline and method of message transmission

3. Methodolgy

- Filtered all HTTP traffic originating from the MAC address 00:17:f2:e2:c0:ce, associated with IP 192.168.15.4.
- Identified HTTP POST requests to sendanonymousemail.net andwillselfdestruct.com
- Used Wireshark's "Follow HTTP Stream" to analyze email submission.
- Loaded the .pcap into NetworkMiner and extracted credentials.
- Discovered Gmail login: jcoachj@gmail.com
- Matched the email to student Johnny Coach, listed in the Chemistry 109 class roster.

4. Key Finding

Evidence Type	Details
Device MAC Address	00:17:f2:e2:c0:ce
IP Address	192.168.15.4
Device Vendor	Apple, Inc.
HTTP Activity	POST requests to sendanonymousemail.net and willselfdestruct.com
Credential Found	jcoachj@gmail.com (via HTTP cookie)
Matching Student	Johnny Coach (from class roster)

5. Timeline

Date & Time	Activity
2008-07-13 17:21	Email sent via sendanonymousemail.net to lilytuckrige@yahoo.com
2008-07-21 23:04	Message sent via willselfdestruct.com
Same session	Gmail login to jcoachj@gmail.com from the same device/IP/MAC

6. Conclusion

Through technical analysis of the packet capture and correlation with class roster data, it is evident that the device with MAC address 00:17:f2:e2:c0:ce and IP 192.168.15.4 was used to send harassing emails to Ms. Lily Tuckrige via two anonymizing services. This same device also accessed a Gmail account identified as jcoachj@gmail.com, which corresponds to Johnny Coach the only student in Chemistry 109 with a matching name structure. These findings conclusively tie Johnny Coach to the incident.

7. Appendix

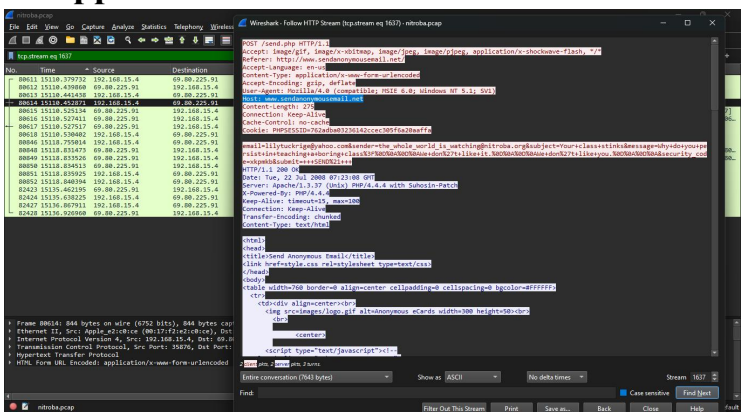

Image 1. IP Use to acces www.sendanonymousemail.net

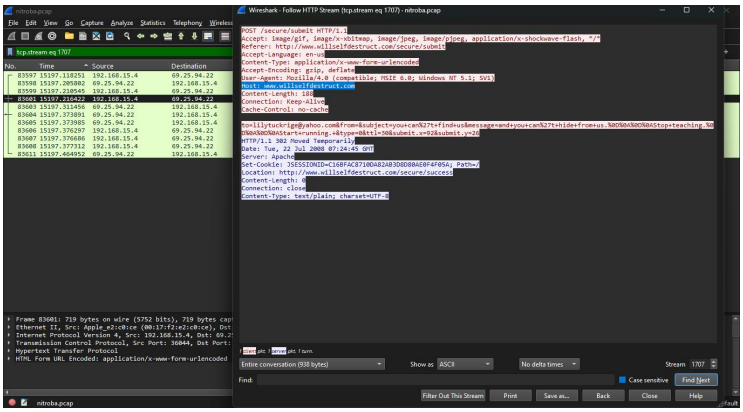

Image 2. IP Use to acces www.willselfdestruct.com

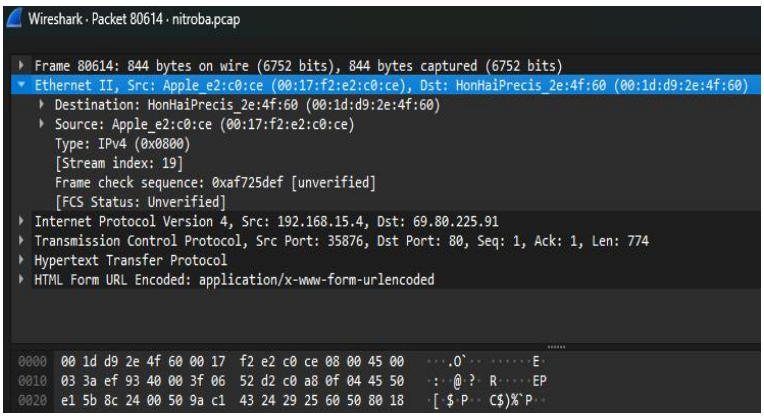

Image 3. MAC Adress

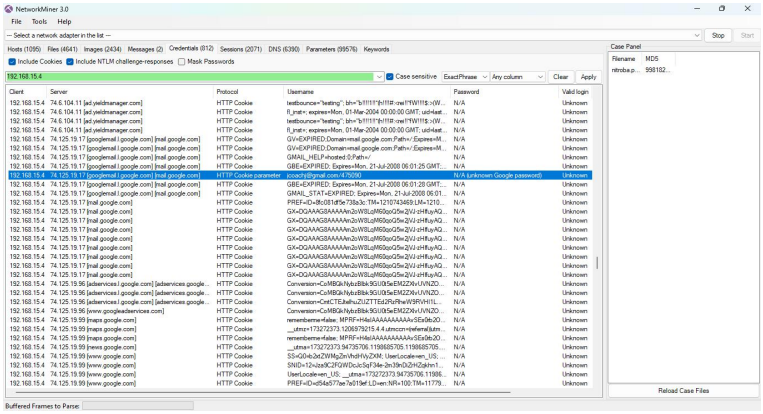

Image 4. Username use for gmail Login

```
Chemistry 109 class list:

Teacher: Lily Tuckrige

Students:
     Amy Smith
     Burt Greedom
     Tuck Gorge
     Ava Book
     Johnny Coach
     Jeremy Ledvkin
     Nancy Colburne
     Tamara Perkins
     Esther Pringle
     Asar Misrad
     Jenny Kant
```

Image 5. Johnny Coach listed in the Chemistry 109 class roster.