

University of Texas at San Antonio

Network Forensics Investigation: Identifying the Perpetrator of Harassing Emails

Daniella Carbuccia

IS 3513: Information Assurance and Security

Prof. John Newsom

05 Dec. 2024

Professor Lily Tuckridge complained to the Nitroba State University's IT department regarding harassing emails. The emails were allegedly sent by a student in her Chemistry 109 class to her personal email account. The originating IP address was identified as 140.247.62.34 which was tied to a student's dorm room with unsecured Wi-Fi. Nitroba's IT team placed a network sniffer on the dorm's Ethernet port to monitor the activity to identify the culprit. After the traffic was captured, our objective was to gather enough findings to conclude who the sender was out of the group of students, what methodologies were used and any network security recommendations which we will uncover.

In the lab we were instructed to use both Wireshark and Network Miner to analyze the packets. To begin, I downloaded and examined the provided PCAP file in Wireshark and decided to start by filtering for the SMTP protocol because we were dealing with emails. Unfortunately, I didn't find any results when I searched for them, so I had to take another approach. At this point I wasn't entirely sure which route to go, and I was stuck, but I saw a few messages in the Discord chat that suggested I head over to Network Miner to look through the Credentials tab. I glanced through the log to see if there were any log in attempts to anything substantial, and I ran across the email [jcoachj@gmail.com](mailto:jcoachj@gmail.com). I went over to the lab instructions, and I noticed one student whose name could possibly be associated with the email address and that was Johnny Coach. When I compared the timestamp to the time the email was sent, I knew there was a possibility he could be the culprit, but I had to narrow down my suspicion. I took the Client IP address from the same line as the email, and I went over to the host tab and looked for it in the log. Once I found his IP address, I expanded the list to show any outgoing sessions. I remembered from the instructions; it showed that the Professor received the email from the web-based service called willselfdestruct.com so I looked through the cookies which showed websites visited in the

session. What I was surprised to find was that he did visit that website as well as another suspicious website called, `sendanonymousemail.net`. To double check, I looked for the IP address of those two websites in the host tab, and looked at the incoming sessions, and once again I saw his IP address in the list with the timestamp. I immediately felt like I found the sender of the email, but I wanted to further confirm and prove it was him that sent the email so to do this I went to the files tab and looked through the log to the specific time these emails were sent. I noticed that the two websites were accessed within minutes of the email being sent as well as some regular email activity right before the incident which I decided I was going to use to prove it was him. To do this, I used the filter `ip.src == 192.168.15.4 || ip.dst == 192.168.15.4` in Wireshark to isolate his IP address as either the source or destination and looked through different packets. I was able to find one TCP packet that confirmed his name matched one of the given names and associated it with the email address. I then went down to the period these incidents happened, and I was able to see HTTP requests to `sendanonymousemail.net` and `willselfdestruct.com` and to even further confirm it, right before these requests happened, he was shown online on his personal email right before visiting the other websites. The time span ranged from 6:00:00 to 6:10:00 and this all matched up with the timeline of his activity. I was also able to confirm it more by finding different files and images in Network Miner that confirmed the emails were sent and some images matched the images in the lab instructions. So, after collecting all this data, I was able to verify that Johnny Coach was indeed the sender of the emails.

The main piece of evidence that pointed to Johnny Coach being the culprit was the time frame he was using the internet as well as his cookies. There were a few times I was stumped depending on what I filtered for because when I searched the suspicious IP address, it wouldn't show anything that could really help me but once I saw his email in the credentials tab, it really

started to make things click and seeing his client IP address and the outgoing sessions, I knew I had pretty much figured it out. Everything lined up in the entire PCAP once I took all filters off and search for the period when things happened, because I could see him connecting to his personal email, then to the anonymous email service and finally to the self-destructing service and everything fell into place. I could also see the sent email and his IP address in the packet when I followed the TCP stream, so it confirmed that he was the one who sent it.

This investigation highlights the effectiveness of Wireshark and Network Miner in uncovering digital evidence. However, it also emphasizes ethical considerations in such cases. While the tools were helpful in identifying the perpetrator, we were instructed to avoid drawing conclusions without concrete evidence. The unsecured Wi-Fi in the dorm presented a challenge, as it allowed multiple potential users, but the timestamps and credentials confirmed who was responsible. To prevent similar incidents in the future I would suggest the dorm networks be password-protected and limit unauthorized access and enhance the monitoring to detect and flag anonymous email services so this won't happen again. However, it was still interesting to see this in action.

Through thorough analysis using Wireshark and Network Miner, Johnny Coach was identified as the sender of the harassing emails. The evidence, including IP addresses, credentials, cookies, and browsing data, established a clear link between his actions and the anonymous email services used to send the emails. This case underscores the importance of secure network practices and the value of forensic tools in resolving cybersecurity incidents. Moving forward, Nitroba State University should implement stronger network security measures and educate students to prevent future incidents.

## Works Cited

Forensics. "Computer Forensics : Network Case Using Wireshark and NetworkMiner."

*Forensics*, 14 Nov. 2020, [www.forensics.com/computer-forensics-network-case-using-wireshark-and-networkminer/](http://www.forensics.com/computer-forensics-network-case-using-wireshark-and-networkminer/).

Garn, Damon. "Examine a Captured Packet Using Wireshark: TechTarget." *Search Networking*,

TechTarget, 7 Aug. 2024, [www.techtarget.com/searchnetworking/tutorial/Examine-a-captured-packet-using-Wireshark](http://www.techtarget.com/searchnetworking/tutorial/Examine-a-captured-packet-using-Wireshark).

Guevarra, Raleigh. "Packet Filtering in Wireshark: A Focus on Display Filters." *Medium*,

Medium, 16 Nov. 2023, [medium.com/@raleighguevarra/packet-filtering-in-wireshark-a-focus-on-display-filters-27d9951808c6](https://medium.com/@raleighguevarra/packet-filtering-in-wireshark-a-focus-on-display-filters-27d9951808c6).

Hjelmvik, Erik. "Intro to NetworkMiner." *Weberblog*, Weberblog, 20 Nov. 2019,

<https://weberblog.net/intro-to-networkminer/>. Accessed 6 Dec. 2024.

Jangid, Kaushal. "NetworkMiner - for Network Forensic Analysis Hackers Online Club -."

*Hackers Online Club*, 6 Nov. 2020, [hackersonlineclub.com/networkminer-for-network-forensic-analysis/](http://hackersonlineclub.com/networkminer-for-network-forensic-analysis/).

Kinzie, Kody. "How to Use Wireshark: Comprehensive Tutorial + Tips." *Varonis*, Varonis, 19

Aug. 2022, [www.varonis.com/blog/how-to-use-wireshark](http://www.varonis.com/blog/how-to-use-wireshark).



nitroba.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.host contains "willselfdestruct.com"

No.	Time	Source	Destination	Protocol	Length	Info
82936	15156.730593	192.168.15.4	69.25.94.22	HTTP	596	GET /secure/submit HTTP/1.1
82985	15157.030671	192.168.15.4	69.25.94.22	HTTP	355	GET /images/spacer.gif HTTP/1.1
83025	15157.238976	192.168.15.4	69.25.94.22	HTTP	356	GET /images/sm-logo.gif HTTP/1.1
83037	15157.279305	192.168.15.4	69.25.94.22	HTTP	361	GET /images/warning-home.gif HTTP/1.1
83072	15157.435074	192.168.15.4	69.25.94.22	HTTP	356	GET /images/body-bk.gif HTTP/1.1
83087	15157.503801	192.168.15.4	69.25.94.22	HTTP	358	GET /images/bttn-send.gif HTTP/1.1
83162	15157.756987	192.168.15.4	69.25.94.22	HTTP	361	GET /images/bridge_small.gif HTTP/1.1
83601	15197.216422	192.168.15.4	69.25.94.22	HTTP	719	POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)
83614	15197.468887	192.168.15.4	69.25.94.22	HTTP	461	GET /secure/success HTTP/1.1
83654	15197.806879	192.168.15.4	69.25.94.22	HTTP	360	GET /images/bk-message.gif HTTP/1.1

> Frame 82936: 596 bytes on wire (4768 bits), 596 bytes captured (4768 bits)

▼ Ethernet II, Src: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60)

> Destination: HonHaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60)

> Source: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce)

Type: IPv4 (0x0800)

[Stream index: 19]

Frame check sequence: 0x59d1a443 [unverified]

[FCS Status: Unverified]

▼ Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.25.94.22

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 578

Identification: 0x5bba (23482)

> 010 .... = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 63

Protocol: TCP (6)

0000 00 1d d9 2e 4f 60 00 17 f2 e2 c0 ce 08 00 45 00 ....0 ..E  
 0010 02 42 5b ba 40 00 3f 06 6b 20 c0 a8 0f 04 45 19 :B[ @-? k ...E  
 0020 5a 16 8c 90 00 5b d2 22 bc a3 e4 bb 2b 80 18 A...P...+..  
 0030 fb 28 6e 7a 00 00 01 01 08 0a 26 63 1e e4 73 00 (nz....&c:s  
 0040 2d 65 47 45 54 20 2f 73 65 63 75 72 65 2f 73 75 -eGET /s ecur/su  
 0050 62 6d 69 74 20 48 54 54 50 2f 31 2e 31 0d 0a 41 bmit HT P/1.1-A  
 0060 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 67 69 66 ccept: i mage/gif  
 0070 2c 20 69 6d 61 67 65 2f 78 2d 78 62 69 74 6d 61 , image/ x-xbitma  
 0080 70 2c 20 69 6d 61 67 65 2f 2f 6a 70 65 67 2c 20 69 p, image /jpg, i  
 0090 6d 61 67 65 2f 70 6a 70 65 67 2c 20 61 70 70 6c mage/pjp es, appl  
 00a0 69 63 61 74 69 6f 6e 2f 78 2d 73 68 6f 63 6b 77 ication/ x-shockw  
 00b0 61 76 65 2d 66 6c 61 73 68 2c 20 2a 2f 2a 0d 0a ave-flas h, /\*..  
 00c0 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f Referer: http://  
 00d0 65 6d 61 69 6c 2e 61 62 6f 75 74 2e 63 6f 6d 2f email.ab out.com/  
 00e0 67 69 2f 64 79 6e 61 6d 69 63 2f 6f 66 66 73 69 gi/dynam ic/offai  
 00f0 74 65 2e 68 74 6d 3f 7a 69 3d 31 2f 58 4a 26 73 te.htm?z i=1/X38s  
 0100 64 6e 3d 65 6d 61 69 6c 26 63 64 6e 3d 63 6f 6d dneemail &cdn=com  
 0110 70 75 74 65 26 74 6d 3d 31 37 26 67 70 73 3d 31 pute&= 17&gps=1  
 0120 30 31 5f 31 38 32 39 5f 37 38 38 5f 35 31 31 26 01.1829\_ 788.511&  
 0130 66 3d 30 30 26 73 75 3d 70 32 38 34 2e 39 2e 33 f=00&su= p284.9.3  
 0140 33 36 2e 69 70 5f 70 35 30 34 2e 31 2e 33 33 36 3e.ip\_p5 04.1.336  
 0150 2e 69 70 5f 26 74 74 3d 34 26 62 74 3d 31 26 62 .ip.&tt= 4&bt=1&b  
 0160 74 73 3d 31 26 7a 75 3d 68 74 70 25 33 41 2f ts=1&zu= http&3A/

NetworkMiner 2.9.0

File Tools Help

-- Select a network adapter in the list --

Hosts (1095) Files (4641) Images (2434) Messages (2) Credentials (812) Sessions (2071) DNS (6390) Parameters (99576) Keywords Anomalies

Filter: 140.247.62.34

Sort Hosts On: IP Address (ascending)

140.247.62.34 [t.eecs.harvard.edu]

- IP: 140.247.62.34
- MAC: 001DD92E4F60
- NIC Vendor: Hon Hai Precision Ind. Co.,Ltd.
- MAC Age: 2007-09-25
- Hostname: t.eecs.harvard.edu
- OS: Unknown
- TTL: 50 (distance: 14)
- Latency: 42.8505 ms
- Open TCP Ports: 8000
- Sent: 52 packets (6,701 Bytes), 0.00% cleartext (0 of 0 Bytes)
- Received: 65 packets (4,051 Bytes), 0.00% cleartext (0 of 0 Bytes)
- Incoming sessions: 11
- Outgoing sessions: 0

nitroba.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... «Ctrl-F»

No.	Time	Source	Destination	Protocol	Length	Info
82920	15156.556002	192.168.15.4	208.185.127.40	TCP	64	[TCP Dup ACK 8291081] 35892 → 80 [ACK] Seq=3610 Ack=22506 Win=63308 Len=0
82921	15156.556290	192.168.15.4	208.185.127.40	TCP	64	[TCP Dup ACK 8291082] 35892 → 80 [ACK] Seq=3610 Ack=22506 Win=63308 Len=0
82922	15156.558495	192.168.15.4	208.185.127.40	TCP	64	35892 → 80 [ACK] Seq=3610 Ack=24180 Win=63094 Len=0
82923	15156.624845	192.168.1.254	192.168.15.4	DNS	202	Standard query response 0x0000 A www.willselfdestruct.com CNAME willselfdestruct.com A 69.25.94.22 NS ns21.domaincontrol.com NS r
82924	15156.634229	192.168.15.4	69.25.94.22	TCP	82	35984 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=1 TSval=644030179 TSecr=0 SACK_PERM
82925	15156.662329	192.168.15.4	208.185.127.35	HTTP	842	GET /6/js/b.txt?s=email HTTP/1.1
82926	15156.681197	208.185.127.35	192.168.15.4	TCP	133	[TCP Previous segment not captured] 80 → 35894 [RST, ACK] Seq=39227 Ack=12006 Win=8190 Len=75 [TCP PDU reassembled in 82941]
82927	15156.682734	192.168.15.4	208.185.127.35	TCP	64	[TCP Dup ACK 8270741] 35894 → 80 [ACK] Seq=12006 Ack=97829 Win=64768 Len=0
82928	15156.681742	208.185.127.35	192.168.15.4	TCP	1466	[TCP Out-Of-Order] 80 → 35894 [ACK] Seq=87829 Ack=12006 Win=8190 Len=1408
82929	15156.685971	192.168.15.4	208.185.127.35	TCP	64	35894 → 80 [ACK] Seq=12006 Ack=99312 Win=63285 Len=0
82930	15156.703578	192.168.15.4	208.185.127.35	HTTP	840	GET /6/g/email/b/b.js HTTP/1.1
82931	15156.722076	69.25.94.22	192.168.15.4	TCP	78	80 → 35984 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM TSval=1929391461 TSecr=644030179 WS=1
82932	15156.724064	192.168.15.4	69.25.94.22	TCP	70	35984 → 80 [ACK] Seq=1 Ack=1 Win=64296 Len=0 TSval=644030180 TSecr=1929391461
82933	15156.724648	208.185.127.35	192.168.15.4	TCP	1466	80 → 35896 [ACK] Seq=107176 Ack=11339 Win=8190 Len=1408 [TCP PDU reassembled in 82935]
82934	15156.726900	208.185.127.35	192.168.15.4	TCP	1466	80 → 35896 [ACK] Seq=108584 Ack=11339 Win=8190 Len=1408 [TCP PDU reassembled in 82935]
82935	15156.729000	208.185.127.35	192.168.15.4	HTTP	1377	HTTP/1.1 200 OK (application/x-javascript)
82936	15156.730593	192.168.15.4	69.25.94.22	HTTP	596	GET /secure/submit HTTP/1.1

> Frame 82923: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits)

▼ Ethernet II, Src: HontaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60), Dst: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce)

> Destination: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce)

> Source: HontaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60)

Type: IPv4 (0x0800)

[Stream index: 19]

Frame check sequence: 0x13b7cd24 [unverified]

[FCS Status: Unverified]

▼ Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.15.4

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 184

Identification: 0x0cf7 (3319)

> 0000. .... = Flags: 0x0

... 0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 255

Protocol: UDP (17)

Header Checksum: 0x1beeb [validation disabled]

0000 00 17 f2 e2 c0 ce 00 1d d9 2e 4f 60 08 00 45 00 .....0'.....E:  
0010 00 10 0c f7 00 00 ff 11 1b eb c0 a0 01 fe c0 a8 .....5.....F.....  
0020 0f 04 00 35 04 01 00 a4 da 46 00 00 81 80 00 01 .....w.wills  
0030 00 02 00 02 00 02 03 77 77 77 10 77 69 6c 6c 73 .....elfdestr uct:com  
0040 65 6c 66 64 65 73 74 72 75 63 74 03 63 6f 6d 00 .....s21 doma incontro  
0050 00 01 00 01 c0 0c 00 05 00 01 00 00 0e 10 00 02 .....l i.....  
0060 c0 10 c0 10 00 01 00 01 00 00 0e 10 00 04 45 19 .....ns22:Y.T.....  
0070 5e 16 c0 10 00 02 00 01 00 00 0e 10 00 15 04 6e .....-@.....  
0080 73 32 31 0d 64 6f 6d 61 69 6e 63 6f 6e 74 72 6f .....m.....  
0090 6c c0 21 c0 10 00 02 00 01 00 00 0e 10 00 07 04 .....  
00a0 6e 73 32 c0 59 c0 54 00 01 00 01 00 00 02 8b .....  
00b0 00 04 40 ca a5 b2 c0 75 00 01 00 01 00 00 02 8b .....  
00c0 00 04 0d 6d ff 0b 13 b7 cd 24

```
rNtKTTB36PHXZM_gowk1-6JXuYxw0Vx0dtx3GeHiG9jMFjCF0gqNK0f; TZ=-60; GMAIL_HELP=hosted:0
```

```
count=1&req0_type=i&req0_time=2531&req0_evtype=-1&
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Content-Type: text/html; charset=UTF-8
ETag:
Content-Encoding: gzip
Content-Length: 140
Date: Tue, 22 Jul 2008 06:01:29 GMT
Server: GFE/1.3
```

```
183
[[0,["c","67F8DC1634D9D313","b"]
],
[1,["b"]
],
[2,["ud","jcoachj@gmail.com","Jonny Coach","Jonny Coach","Jonny"]
],
[3,["ast","",0]
],
[4,["acc",0]
],
[5,["ef",1]
],
[6,["cu",0]
],
]
```

```
GET /mail/im/available_ltblue1.gif HTTP/1.1
```

Server: 69.22.167.223 [a1906.g.akamai.net] [cdn2.adsdk.com.edgesuite.net] [cdn2.adsdk.com] [a34.g.akamai.net] [ads.ak.facebook.com.edgesuite.net] [a802.g.akamai.net] [include.ebaystatic.com.edgesuite.net] [a1174.g.akamai.net]

Server: 69.22.167.224 [a1248.g.akamai.net] [z-ecx.images-amazon.com.edgesuite.net] [a1166.g.akamai.net] [itm.ebaystatic.com.edgesuite.net] [a1817.g.akamai.net] [images.channeladvisor.com.edgesuite.net] [images.channeladvisor.com]

Server: 69.22.167.225 [a1248.g.akamai.net] [z-ecx.images-amazon.com.edgesuite.net] [z-ecx.images-amazon.com] [a1812.g.akamai.net] [img.shopping.com.edgesuite.net] [d1.shopping.com] [a1260.g.akamai.net] [usweb.dotomi.com]

Server: 69.22.167.230 [a1174.g.akamai.net] [content.yieldmanager.edgesuite.net] TCP 80

Server: 69.22.167.232 [a867.g.akamai.net] [www.wired.com.edgesuite.net] [www.wired.com] [a1812.g.akamai.net] [img.shopping.com.edgesuite.net] [img.shopping.com] [d1.shopping.com] [a811.g.akamai.net] [base.shared.live.com]

Server: 69.22.167.239 [a251.b.akamai.net] [www.ich.com.geo.akadns.net] [www.ichotelsgroup.com] [images3.ichotelsgroup.com] TCP 80

Server: 69.22.167.246 [a1906.g.akamai.net] [cdn2.adsdk.com.edgesuite.net] [a1654.g.akamai.net] [pics.ebaystatic.com.edgesuite.net] [pics.ebaystatic.com] [a949.g.akamai.net] [leadback.advertising.com.edgesuite.net] TCP 80

Server: 69.22.167.247 [a765.g.akamai.net] [abmr.net.edgesuite.net] [a34.g.akamai.net] [ads.ak.facebook.com.edgesuite.net] [ads.ak.facebook.com] [a1260.g.akamai.net] [usweb.dotomi.com.edgesuite.net] [dmmres.dotomi.com.edgesuite.net]

Server: 69.22.167.248 [a943.g.akamai.net] [a765.g.akamai.net] [abmr.net.edgesuite.net] [www.abmr.net] [a1654.g.akamai.net] [pics.ebaystatic.com.edgesuite.net] [pics.ebaystatic.com] [a802.g.akamai.net] [include.ebaystatic.com.edgesuite.net] [include.ebaystatic.com]

Server: 69.22.167.249 [a867.g.akamai.net] [www.wired.com.edgesuite.net] [www.wired.com] [a727.g.akamai.net] [i.shoebuy.com.edgesuite.net] [i.shoebuy.com] [ds.serving-sys.com] [a158.x.akamai.net] [www.eyebliaster.georedirector.com]

Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80

Server: 69.25.152.120 [jar.worthousandwords.com] TCP 80

Server: 69.26.180.8 [a867.g.akamai.net] [www.wired.com.edgesuite.net] [www.wired.com] [a1248.g.akamai.net] [z-ecx.images-amazon.com.edgesuite.net] [z-ecx.images-amazon.com] TCP 80

Server: 69.26.180.17 [a248.e.akamai.net] [a749.g.akamai.net] [static.ak.facebook.com.edgesuite.net] [static.ak.fbcdn.net] [a907.g.akamai.net] [core.insightexpressai.com.edgesuite.net] TCP 443

Server: 69.26.180.17 [a248.e.akamai.net] [a749.g.akamai.net] [static.ak.facebook.com.edgesuite.net] [static.ak.fbcdn.net] [a907.g.akamai.net] [core.insightexpressai.com.edgesuite.net] TCP 80

Server: 69.26.180.23 [a34.g.akamai.net] [ads.ak.facebook.com] TCP 80

Server: 69.26.180.24 [a907.g.akamai.net] [core.insightexpressai.com.edgesuite.net] [core.insightexpressai.com] TCP 80

Server: 69.26.190.48 [a943.g.akamai.net] [geo-us11.yimg.com.yahoo2.akadns.net] [us11.yimg.com] TCP 80

Server: 69.28.150.204 [cnn.vollnwd.net] [i.cnn.net] TCP 80

Server: 69.28.176.41 [twc.vollnwd.net] [image.weather.com] TCP 80

Server: 69.28.176.65 [twc.vollnwd.net] [image.weather.com] TCP 80

Server: 69.28.176.68 [twc.vollnwd.net] [image.weather.com] TCP 80

Server: 69.28.176.68 [twc.vollnwd.net] [image.weather.com] TCP 80

Server: 69.39.67.98 [heprivacyplace.org] TCP 80

Server: 69.63.176.11 [apps.facebook.com] TCP 80

Server: 69.63.176.40 [www.facebook.com] TCP 80

Server: 69.63.176.44 [login.facebook.com] TCP 443

Server: 69.63.176.174 [0.channel14.facebook.com] TCP 80

Server: 69.63.178.11 [facebook.com] TCP 80

Server: 69.63.178.12 [www.facebook.com] TCP 80

Server: 69.63.178.23 [login.facebook.com] TCP 443

Server: 69.80.200.254 [secure-us.imrworldwide.com] TCP 80

Server: 69.80.225.91 [www.sendanonymousemail.net] TCP 80

Server: 69.147.71.20 [kids.yahoo6.akadns.net] [kids.yahoo.com] TCP 80

Server: 70.42.153.135 [sales.liveperson.net] TCP 80

Server: 72.14.253.125 [talk.l.google.com] [talk.google.com] TCP 5222

Server: 72.21.202.98 [s3-external-1.amazonaws.com] [img.auctiva.com] TCP 80

Server: 72.21.207.136 [s3-external-1.amazonaws.com] [scimg.auctiva.com] TCP 80

Server: 72.21.210.11 [www.amazon.com] TCP 80

Server: 72.21.211.101 [s3-external-1.amazonaws.com] [scimg.auctiva.com] TCP 80

Server: 72.21.211.145 [s3-external-1.amazonaws.com] [scimg.auctiva.com] TCP 80

Server: 72.30.33.114 [rc12.g.ym.yahoo.com] [rc12.overture.com] TCP 80

Server: 69.63.176.174 [0.channel14.facebook.com] TCP 80

Server: 69.63.178.11 [facebook.com] TCP 80

Server: 69.63.178.12 [www.facebook.com] TCP 80

Server: 69.63.178.23 [login.facebook.com] TCP 443

Server: 69.80.200.254 [secure-us.imrworldwide.com] TCP 80

Server: 69.80.225.91 [www.sendanonymousemail.net] TCP 80

Server: 69.147.71.20 [kids.yahoo6.akadns.net] [kids.yahoo.com] TCP 80

Server: 70.42.153.135 [sales.liveperson.net] TCP 80

Server: 72.14.253.125 [talk.l.google.com] [talk.google.com] TCP 5222

Server: 72.21.202.98 [s3-external-1.amazonaws.com] [img.auctiva.com] TCP 80

Server: 72.21.207.136 [s3-external-1.amazonaws.com] [scimg.auctiva.com] TCP 80

Server: 72.21.210.11 [www.amazon.com] TCP 80

Server: 72.21.211.101 [s3-external-1.amazonaws.com] [scimg.auctiva.com] TCP 80

Server: 72.21.211.145 [s3-external-1.amazonaws.com] [scimg.auctiva.com] TCP 80

Server: 72.30.33.114 [rc12.g.ym.yahoo.com] [rc12.overture.com] TCP 80

69.80.225.91 [www.sendanonymousemail.net]

IP: 69.80.225.91

MAC: 001DD92E4F60

NIC Vendor: Hon Hai Precision Ind. Co., Ltd.

MAC Age: 2007-09-25

Hostname: www.sendanonymousemail.net

OS: Unknown

TTL: 55 (distance: 9)

Latency: 30.064 ms

Open TCP Ports: 80 (HTTP)

Sent: 29 packets (24,876 Bytes), 0.00% cleartext (0 of 0 Bytes)

Received: 52 packets (5,365 Bytes), 0.00% cleartext (0 of 0 Bytes)

Incoming sessions: 4

Server: 69.80.225.91 [www.sendanonymousemail.net] TCP 80

Server: 69.80.225.91 [www.sendanonymousemail.net] TCP 80 (15860 data bytes sent), Client: 192.168.15.4 TCP 35848 (955 data bytes sent), Session start: 2008-07-22 06:01:26 UTC, Session end: 2008-07-22 06:01:44 UTC

Server: 69.80.225.91 [www.sendanonymousemail.net] TCP 80 (947 data bytes sent), Client: 192.168.15.4 TCP 35850 (540 data bytes sent), Session start: 2008-07-22 06:01:26 UTC, Session end: 2008-07-22 06:02:00 UTC

Server: 69.80.225.91 [www.sendanonymousemail.net] TCP 80 (6525 data bytes sent), Client: 192.168.15.4 TCP 35876 (1142 data bytes sent), Session start: 2008-07-22 06:02:57 UTC, Session end: 2008-07-22 06:03:23 UTC

Server: 69.80.225.91 [www.sendanonymousemail.net] TCP 80 (0 data bytes sent), Client: 192.168.15.4 TCP 35850 (0 data bytes sent), Session start: 2008-07-22 06:10:31 UTC, Session end: 2008-07-22 06:10:31 UTC

Outgoing sessions: 0

Host Details

69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)

- IP: 69.25.94.22
- MAC: 001DD92E4F60
- NIC Vendor: Hon Hai Precision Ind. Co., Ltd.
- MAC Age: 2007-09-25
- Hostname: willselfdestruct.com, www.willselfdestruct.com
- OS: Linux
- TTL: 54 (distance: 10)
- Latency: 43.9235 ms
- Open TCP Ports: 80 (HTTP)
- Sent: 106 packets (91,924 Bytes), 0.00% cleartext (0 of 0 Bytes)
- Received: 101 packets (8,955 Bytes), 0.00% cleartext (0 of 0 Bytes)
- Incoming sessions: 10

Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80

- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (20475 data bytes sent), Client: 192.168.15.4 TCP 35984 (526 data bytes sent), Session start: 2008-07-22 06:03:43 UTC, Session end: 2008-07-22 06:03:44 UTC
- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (253 data bytes sent), Client: 192.168.15.4 TCP 35988 (285 data bytes sent), Session start: 2008-07-22 06:03:44 UTC, Session end: 2008-07-22 06:03:44 UTC
- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (1380 data bytes sent), Client: 192.168.15.4 TCP 35992 (286 data bytes sent), Session start: 2008-07-22 06:03:44 UTC, Session end: 2008-07-22 06:03:44 UTC
- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (3427 data bytes sent), Client: 192.168.15.4 TCP 35994 (291 data bytes sent), Session start: 2008-07-22 06:03:44 UTC, Session end: 2008-07-22 06:03:44 UTC
- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (22632 data bytes sent), Client: 192.168.15.4 TCP 36000 (286 data bytes sent), Session start: 2008-07-22 06:03:44 UTC, Session end: 2008-07-22 06:03:44 UTC
- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (1167 data bytes sent), Client: 192.168.15.4 TCP 36002 (288 data bytes sent), Session start: 2008-07-22 06:03:44 UTC, Session end: 2008-07-22 06:03:44 UTC
- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (823 data bytes sent), Client: 192.168.15.4 TCP 36008 (291 data bytes sent), Session start: 2008-07-22 06:03:44 UTC, Session end: 2008-07-22 06:03:44 UTC
- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (289 data bytes sent), Client: 192.168.15.4 TCP 36044 (649 data bytes sent), Session start: 2008-07-22 06:04:24 UTC, Session end: 2008-07-22 06:04:24 UTC
- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (16167 data bytes sent), Client: 192.168.15.4 TCP 36046 (391 data bytes sent), Session start: 2008-07-22 06:04:24 UTC, Session end: 2008-07-22 06:04:24 UTC
- Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] TCP 80 (19719 data bytes sent), Client: 192.168.15.4 TCP 36048 (290 data bytes sent), Session start: 2008-07-22 06:04:24 UTC, Session end: 2008-07-22 06:04:24 UTC

Outgoing sessions: 0

Host Details

Send Anonymous Email

File | C:/Users/carbu/Downloads/NetworkMiner\_2-9/NetworkMiner\_2-9/AssembledFiles/69.80.225.91/TCP...

**SENDANONYMOUSEMAIL**

**Thank You**

**Your message has been sent!**

[Access blocked sites or browse anonymously from work or school](#)

[Send some Anonymous Fake eCards?](#)

Send Anonymous Mail - © 2005 - 2024

The screenshot shows a web browser window displaying the 'Secure Anonymous Email - WillSelfDestruct.com' website. The page has a header with navigation links: 'Send Message', 'Faq', 'Blog', 'Feedback', 'B2B', and 'Legalese'. The main content area features a large red box with the text 'Will Self-Destruct is For Sale' and a paragraph stating: 'We've had a lot of fun with it over the years but we are moving to pastures green. If you are interested in buying it you can either visit [ebay](#) or [contact us](#) directly.' Below this is a link 'Mission Impossible Version'. The page also includes a section titled 'Self Destruct Message Sent.' with instructions on how to view and send messages.

Overlaid on the bottom of the browser window is a Wireshark packet capture window showing the HTTP stream. The packet list on the left shows a series of TCP and HTTP packets. The selected packet (80614) is an HTTP POST request to '/send.php'. The packet details pane shows the request headers and body, including the 'Accept' header, 'Referer', 'Content-Type', 'Content-Encoding', 'User-Agent', 'Host', 'Content-Length', 'Connection', 'Cache-Control', and 'Cookie'. The packet bytes pane shows the raw data of the request.

**Secure Anonymous Email - WillSelfDestruct.com**

Send Message | Faq | Blog | Feedback | B2B | Legalese

**Will Self-Destruct is For Sale**

We've had a lot of fun with it over the years but we are moving to pastures green. If you are interested in buying it you can either visit [ebay](#) or [contact us](#) directly.

[Mission Impossible Version](#)

**Self Destruct Message Sent.**

The recipient has been sent an e-mail with a link to your secret message.

Once they click on the link the message will be deleted, and they will no longer be able to view the message.

If you would like to send the same message to another e-mail then [click here](#).

If you would like to send a new message then [click here](#).

**Wireshark - Follow HTTP Stream (tcp.stream eq 1637) - nitroba.pcap**

POST /send.php HTTP/1.1

Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, \*/\*

Referer: http://www.sendanonymousemail.net/

Accept-Language: en-us

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Host: www.sendanonymousemail.net

Content-Length: 275

Connection: Keep-Alive

Cache-Control: no-cache

Cookie: PHPSESSID=762adba03236142ccec305f6a20aaffa

email=lilytuckrige@yahoo.com&sender=the\_whole\_world\_is\_watching@nitroba.org&subject=Your+class+stinks&message=why+do+you+persist+in+teaching+a+boring+class&3f300d0a30050a0e+don%27t+like+it.%30050a30050a0e+don%27t+like+you.%300d0a30050a0e+securi+ty\_code=xpmb&submit=+++SEND%21+++

HTTP/1.1 200 OK

Date: Tue, 22 Jul 2008 07:23:08 GMT

Server: Apache/1.3.37 (Unix) PHP/4.4.4 with Suhosin-Patch

X-Powered-By: PHP/4.4.4

Keep-Alive: timeout=15, max=100

Connection: Keep-Alive

Transfer-Encoding: chunked

Content-Type: text/html

Packet 80614: 844 bytes on wire (6752 bits), 844 bytes captured (6752 bits) on interface 0

Ethernet II, Src: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60)

Destination: HonHaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60)

Source: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce)

Type: IPv4 (0x0800)

[Stream index: 19]

Frame check sequence: 0xaf725def [unverified]

[FCS Status: Unverified]

Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.80.225.91

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 826

Identification: 0xaf93 (61331)

010. .... = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 63

Protocol: TCP (6)

Header Checksum: 0x5d2d [validation disabled]

tcp.stream eq 1620					
o.	Time	Source	Destination	Protocol	L
79928	2008-07-22 06:01:34.295940	192.168.15.4	209.85.201.189	TCP	
79929	2008-07-22 06:01:34.296219	192.168.15.4	209.85.201.189	TCP	
79972	2008-07-22 06:02:00.599380	209.85.201.189	192.168.15.4	TCP	
79973	2008-07-22 06:02:00.714112	192.168.15.4	209.85.201.189	TCP	
80276	2008-07-22 06:02:27.920017	209.85.201.189	192.168.15.4	TCP	
80277	2008-07-22 06:02:28.053908	192.168.15.4	209.85.201.189	TCP	
80605	2008-07-22 06:02:55.186810	209.85.201.189	192.168.15.4	TCP	
80606	2008-07-22 06:02:55.393687	192.168.15.4	209.85.201.189	TCP	
82425	2008-07-22 06:03:23.793219	209.85.201.189	192.168.15.4	TCP	
82426	2008-07-22 06:03:23.962267	192.168.15.4	209.85.201.189	TCP	
83230	2008-07-22 06:03:49.834305	209.85.201.189	192.168.15.4	TCP	
83233	2008-07-22 06:03:50.073348	192.168.15.4	209.85.201.189	TCP	
83562	2008-07-22 06:04:17.743738	209.85.201.189	192.168.15.4	TCP	
83563	2008-07-22 06:04:18.027425	192.168.15.4	209.85.201.189	TCP	
83842	2008-07-22 06:04:44.528919	209.85.201.189	192.168.15.4	TCP	
83843	2008-07-22 06:04:44.752746	192.168.15.4	209.85.201.189	TCP	

```

GET /mail/channel/test?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&at=xv&DOMAIN=mail.google.com&t=1 HTTP/1.1
Accept: */*
Referer: http://mail.google.com/mail/?ui=1&view=page&name=js&ver=1
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Host: b.mail.google.com
Connection: Keep-Alive
Cookie: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3Gukvcv4N9vQ6lWwOo-HSktRUCM8z2caTi0C7NMWnqJdfJa63rj2FKElFpHQqf52we; S=gmail=L5hb7l oxy=6uatNcZZmB8:gmproxy_yj=FRV17ZyWnh8:gmproxy_yj_sub=bzgoW0ybARA; gmailchat=jcoachj@gmail.com/475090; GMAIL_STAT=lt=500&js=251&dw=62l REF=ID=8fc081df5e738a3c; TM=1210743469; LM=1216706486; GM=1; S=vvxeHX0; f71-9JQ2AeoD8oWG9NjtOp7T5tuskkNgEKMRA9P49vI4Easp6NpBuJWaDr5pEv4yhi 923099928271:2; __utmxx=173272373.000009831923099928271:1216706401.: WgZ7DwUjYpLoqH7F1_E-X5taC4l0uvzXtrVeE6Zq1gcoQt50MC7lgQFv5YtK9GsvrN TZ=-60; GMAIL_HELP=hosted:0

```

```
HTTP/1.1 200 OK
```