

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. 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.

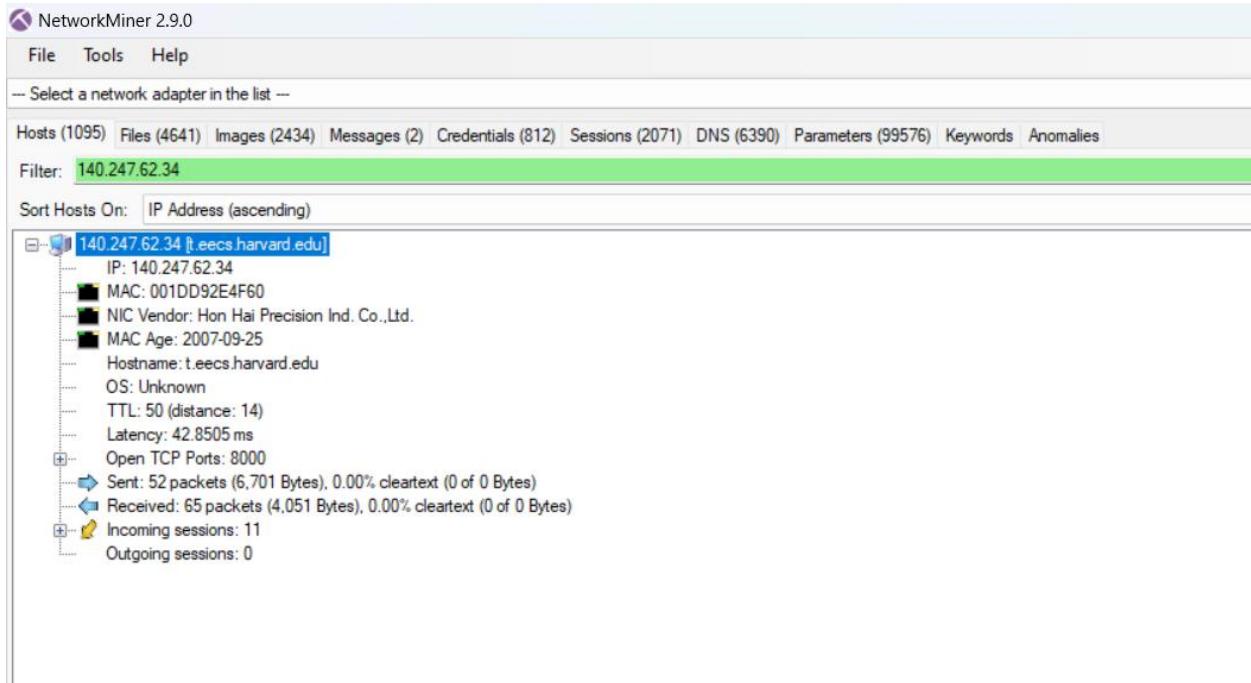
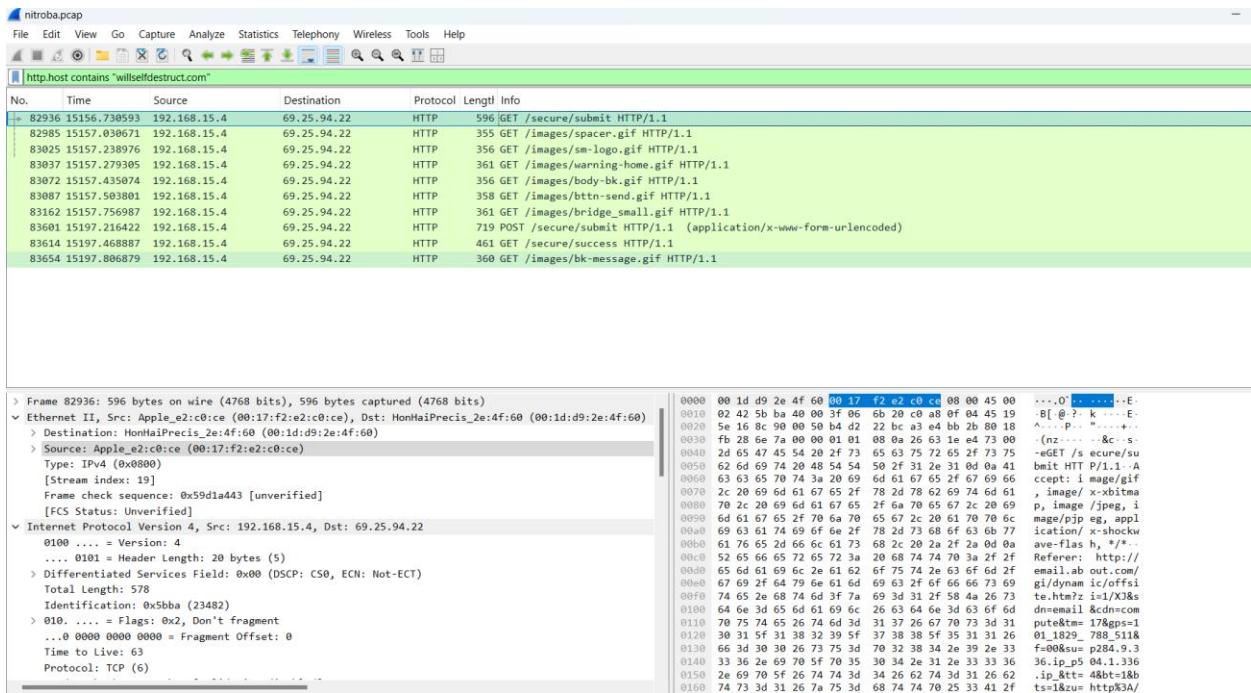
Works Cited

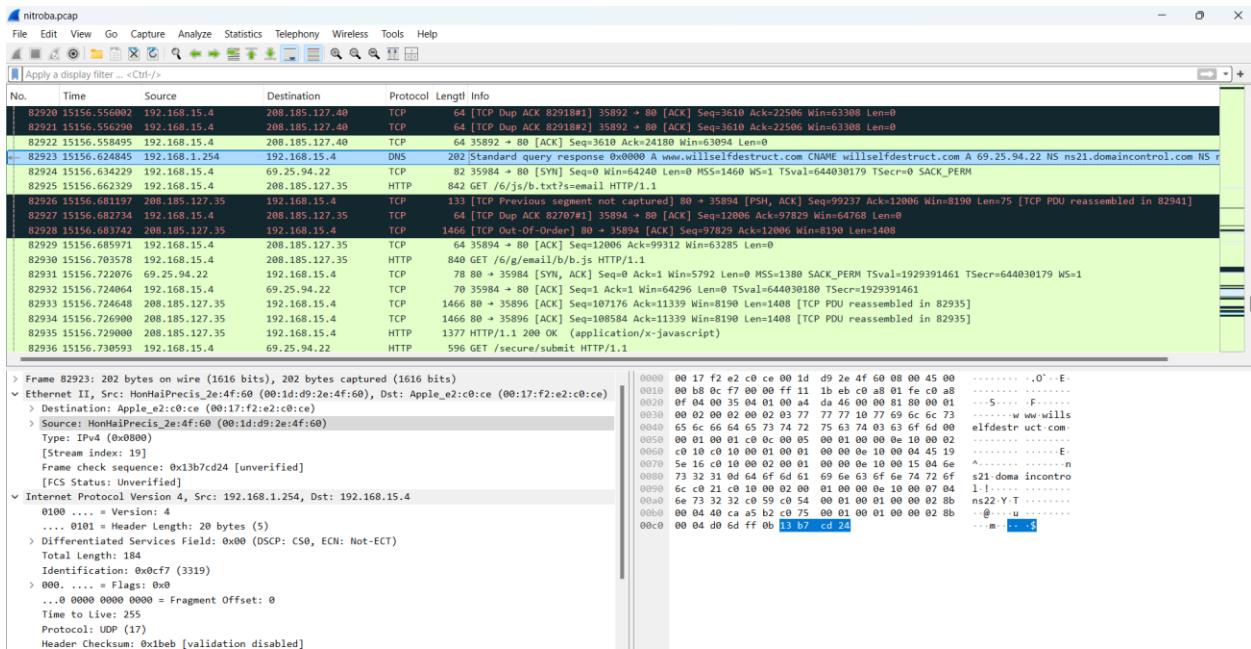
- Forensicxs. “Computer Forensics : Network Case Using Wireshark and NetworkMiner.” *Forensicxs*, 14 Nov. 2020, www.forensicxs.com/computer-forensics-network-case-using-wireshark-and-networkminer/.
- Garn, Damon. “Examine a Captured Packet Using Wireshark: TechTarget.” *Search Networking*, TechTarget, 7 Aug. 2024, www.techtarget.com/searchnetworking/tutorial/Examine-a-captured-packet-using-Wireshark.
- 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.
- 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/.
- Kinzie, Kody. “How to Use Wireshark: Comprehensive Tutorial + Tips.” *Varonis*, Varonis, 19 Aug. 2022, www.varonis.com/blog/how-to-use-wireshark.

Carbuccia 6

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						
<input checked="" type="checkbox"/> Show Cookies <input checked="" type="checkbox"/> Show NTLM challenge-response <input type="checkbox"/> Mask Passwords						
Client	Server	Protocol	Username	Password	Valid login	First Login
192.168.15.4	74.125.19.102 [calendar.google.com]	HTTP Cookie	PREF=ID=8c081df5e738a3c;TM=1210743469;LM=1210...	N/A	Unknown	2008-07-22 06:00:45 UTC
192.168.15.4	74.125.19.104 [www.google.com] [ne...	HTTP Cookie	CAL=DQAAAG8AAAAApUrUkgsFp1wFwiIILZowqnpAeq-KS...	N/A	Unknown	2008-07-22 06:00:45 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	PREF=ID=8c081df5e738a3c;TM=1210743469;LM=1210...	N/A	Unknown	2008-07-22 06:00:53 UTC
192.168.15.4	74.125.19.17 [googlemail.google.com] [mail.google.com]	HTTP Cookie	GV=EXPIRED;Domain=mail.google.com;Path=/;Expires=M...	N/A	Unknown	2008-07-22 06:00:53 UTC
192.168.15.4	66.151.146.194 [e-2d6wymioicjaq.stats.esomniture.com] [...]	HTTP Cookie	s_vi_7x7fx3Cx7Cx0Dx2Bx7fx21xDx3Ax0Dx2Bx60x0Dx...	N/A	Unknown	2008-07-22 06:00:56 UTC
192.168.15.4	74.125.19.17 [googlemail.google.com] [mail.google.com]	HTTP Cookie	GV=EXPIRED;Domain=mail.google.com;Path=/;Expires=M...	N/A	Unknown	2008-07-22 06:00:57 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:00:57 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:00:58 UTC
192.168.15.4	74.125.19.17 [googlemail.google.com] [mail.google.com]	HTTP Cookie	GMAIL_HELP=hosted:0;Path=/	N/A	Unknown	2008-07-22 06:00:58 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:00:58 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:01:01 UTC
192.168.15.4	74.125.19.17 [googlemail.google.com] [mail.google.com]	HTTP Cookie	GBE=EXPIRED;Expires=Mon, 21-Jul-2008 06:01:25 GMT;...	N/A	Unknown	2008-07-22 06:01:01 UTC
192.168.15.4	74.125.19.17 [googlemail.google.com] [mail.google.com]	HTTP Cookie parameter	icoachj@gmail.com/475090	N/A (unknown Google password)	Unknown	2008-07-22 06:01:02 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:01:02 UTC
192.168.15.4	209.85.201.189 [b.googlemail.google.com] [chattenabled....]	HTTP Cookie parameter	icoachj@gmail.com/475090	N/A (unknown Google password)	Unknown	2008-07-22 06:01:02 UTC
192.168.15.4	209.85.201.189 [chattenabled.mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:01:02 UTC
192.168.15.4	74.125.19.104 [www.google.com]	HTTP Cookie	PREF=ID=8c081df5e738a3c;TM=1210743469;LM=1210...	N/A	Unknown	2008-07-22 06:01:02 UTC
192.168.15.4	74.125.19.104 [www.google.com] [ne...	HTTP Cookie	PREF=ID=8c081df5e738a3c;TM=1210743469;LM=1216...	N/A	Unknown	2008-07-22 06:01:02 UTC
192.168.15.4	209.85.201.189 [b.mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:01:02 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:01:04 UTC
192.168.15.4	209.85.201.189 [b.mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:01:05 UTC
192.168.15.4	74.125.19.17 [googlemail.google.com] [mail.google.com]	HTTP Cookie	GBE=EXPIRED;Expires=Mon, 21-Jul-2008 06:01:28 GMT;...	N/A	Unknown	2008-07-22 06:01:05 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:01:05 UTC
192.168.15.4	66.151.146.194 [e-2d6wymioicjaq.stats.esomniture.com] [...]	HTTP Cookie	s_vi_7x7fx3Cx7Cx0Dx2Bx7fx21xDx3Ax0Dx2Bx60x0Dx...	N/A	Unknown	2008-07-22 06:01:06 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2VJ-zHfuyAQ...	N/A	Unknown	2008-07-22 06:01:06 UTC
192.168.15.4	66.151.146.194 [e-2d6wymioicjaq.stats.esomniture.com] [...]	HTTP Cookie	GMAIL_STAT=EXPIRED;Expires=Mon, 21-Jul-2008 06:01...	N/A	Unknown	2008-07-22 06:01:08 UTC
192.168.15.4	74.125.19.17 [mail.google.com]	HTTP Cookie	s_vi_7x7fx3Cx7Cx0Dx2Bx7fx21xDx3Ax0Dx2Bx60x0Dx...	N/A	Unknown	2008-07-22 06:01:13 UTC
192.168.15.4	74.125.19.104 [www.google.com]	HTTP Cookie	_utma=173272373.890237978.1216706402.1216706402...	N/A	Unknown	2008-07-22 06:01:15 UTC
192.168.15.4	74.125.19.104 [www.google.com] [www.google.com] [ne...	HTTP Cookie	OL_SESSION=icoachj@gmail.com-ca...	N/A	Unknown	2008-07-22 06:01:16 UTC
192.168.15.4	74.125.19.104 [www.google.com] [www.google.com] [ne...	HTTP Cookie	CAL=DQAAAG8AAAAApUrUkgsFp1wFwiIILZowqnpAeq-KS...	N/A	Unknown	2008-07-22 06:01:17 UTC
192.168.15.4	74.125.19.104 [www.google.com]	HTTP Cookie	PREF=ID=8c081df5e738a3c;TM=1210743469;LM=1216...	N/A	Unknown	2008-07-22 06:01:20 UTC
192.168.15.4	74.125.19.104 [www.google.com] [ne...	HTTP Cookie	SS=0=Z29vZzlxIGHnbGVuZGFy; PREF=ID=8c081df5e...	N/A	Unknown	2008-07-22 06:01:24 UTC
192.168.15.4	74.125.19.104 [www.google.com] [www.google.com] [ne...	HTTP Cookie	SS=Q0=c2VuZCBhb9ueW1vdXMbWFpbA; path=/search	N/A	Unknown	2008-07-22 06:01:24 UTC
192.168.15.4	67.15.76.53 [c20.statcounter.com]	HTTP Cookie	session_2147602=1216706294%;260	N/A	Unknown	2008-07-22 06:01:27 UTC
192.168.15.4	69.80.225.91 [www.sendanonymousemail.net]	HTTP Cookie	PHPSESSID=762adba03236142cec30f6a20affa; path=/	N/A	Unknown	2008-07-22 06:01:27 UTC
192.168.15.4	67.15.76.53 [c20.statcounter.com]	HTTP Cookie	session_2134460=1216706510%;260; expires=Sun, 21-Jul-...	N/A	Unknown	2008-07-22 06:01:27 UTC
192.168.15.4	66.151.146.194 [e-2d6wymioicjaq.stats.esomniture.com] [...]	HTTP Cookie	s_vi_7x7fx3Cx7Cx0Dx2Bx7fx21xDx3Ax0Dx2Bx60x0Dx...	N/A	Unknown	2008-07-22 06:01:38 UTC
192.168.15.4	66.151.146.194 [e-2d6wymioicjaq.stats.esomniture.com] [...]	HTTP Cookie	s_vi_7x7fx3Cx7Cx0Dx2Bx7fx21xDx3Ax0Dx2Bx60x0Dx...	N/A	Unknown	2008-07-22 06:02:05 UTC
192.168.15.4	66.151.146.194 [e-2d6wymioicjaq.stats.esomniture.com] [...]	HTTP Cookie	s_vi_7x7fx3Cx7Cx0Dx2Bx7fx21xDx3Ax0Dx2Bx60x0Dx...	N/A	Unknown	2008-07-22 06:02:31 UTC
192.168.15.4	69.80.225.91 [www.sendanonymousemail.net]	HTTP Cookie	PHPSESSID=762adba03236142cec30f6a20affa	N/A	Unknown	2008-07-22 06:02:57 UTC
192.168.15.4	67.15.76.53 [c20.statcounter.com]	HTTP Cookie	session_2147602=1216706294%;260; session_2134460=1...	N/A	Unknown	2008-07-22 06:02:57 UTC
192.168.15.4	67.15.76.53 [c20.statcounter.com]	HTTP Cookie	session_2134460=1216706601%;260; session_2147602=...	N/A	Unknown	2008-07-22 06:02:57 UTC

nitroba.pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
udp.stream eq 412						
No.	Time	Source	Destination	Protocol	Length	Info
82802	15140.583190	192.168.1.254	192.168.15.4	DNS	485	Standard query response 0x0000 A spe.atdmtd.com CNAME spe.atdmtd.com.edgesuite.net CNAME a1521.x.akamai.net A 69.22.167.249 A 69.22.
82814	15140.677589	192.168.1.254	192.168.1.254	DNS	77	Standard query 0x0000 A rmd.atdmtd.com
82818	15140.693974	192.168.1.254	192.168.15.4	DNS	484	Standard query response 0x0000 A rmd.atdmtd.com CNAME rmd.atdmtd.com.edgesuite.net CNAME a898.x.akamai.net A 69.22.167.217 A 69.22.
82912	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
83015	15157.185326	192.168.1.254	192.168.1.254	DNS	83	Standard query 0x0000 A 14.statcounter.com
83016	15157.198815	192.168.1.254	192.168.15.4	DNS	281	Standard query response 0x0000 A c14.statcounter.com A 66.98.172.25 NS ns4.dnsmadeeasy.com NS ns3.dnsmadeeasy.com NS ns1.dnsmade
83017	15157.205164	192.168.1.254	192.168.15.4	DNS	97	Standard queru 0x0000 A www.google-analytics.l.google.com





```
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
```

Carbuccia 9

Server: 69.22.167.223 [a1906.g.akamai.net] [cdn2.ad sdk.com.edgesuite.net] [cdn2.ad sdk.com] [a34.g.akamai.net] [ads.ak.facebook.com.edgesuite.net] [a802.g.akamai.net] [include.ebaystatic.com.edgesuite.net] [a1174.g.akamai.net] [z-ecx.images-amazon.com.edgesuite.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.channeladviso...]
 Server: 69.22.167.225 [a1248.g.akamai.net] [z-ecx.images-amazon.com.edgesuite.net] [z-ecx.images-amazon.com.edgesuite.net] [a1812.g.akamai.net] [img.shopping.com.edgesuite.net] [di1.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.edgesuite.net] [a1812.g.akamai.net] [img.shopping.com.edgesuite.net] [img.shopping.com] [di1.shopping.com] [a811.g.akamai.net] [base.shared.live.com]
 Server: 69.22.167.245 [a1906.g.akamai.net] [cdn2.ad sdk.com.edgesuite.net] [a1654.g.akamai.net] [pics.ebaystatic.com.edgesuite.net] [pics.ebaystatic.com] [a949.g.akamai.net] [feedback.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] [dmres.dotomi.com.edgesuite.net] [a1654.g.akamai.net] [www.abmr.net] [a765.g.akamai.net] [pics.ebaystatic.com.edgesuite.net] [a802.g.akamai.net] [include.ebaystatic.com.edgesuite.net] [include.ebaystatic.com.edgesuite.net] [a158.x.akamai.net] [www.eyeblast.georedirector.com]
 Server: 69.22.167.249 [a867.g.akamai.net] [www.wired.com.edgesuite.net] [www.wired.com.edgesuite.net] [a727.g.akamai.net] [j.shoebuy.com.edgesuite.net] [j.shoebuy.com] [ds.serving-sys.com] [a158.x.akamai.net] [www.eyeblast.georedirector.com]
 Server: 69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] [TCP 80]
 Server: 69.25.152.120 [jar.worthathousandwords.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.g.akamai.net] [a749.g.akamai.net] [static.ak.facebook.com.edgesuite.net] [static.ak.facebook.com.edgesuite.net] [a907.g.akamai.net] [core.insightexpress.com.edgesuite.net] [TCP 443]
 Server: 69.26.180.17 [a248.g.akamai.net] [a749.g.akamai.net] [static.ak.facebook.com.edgesuite.net] [static.ak.fbcdn.net] [a907.g.akamai.net] [core.insightexpress.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.insightexpress.com.edgesuite.net] [core.insightexpress.com] [TCP 80]
 Server: 69.26.190.48 [a943.g.akamai.net] [geo-us1.yimg.com.yahoo2.akadns.net] [us1.yimg.com] [TCP 80]
 Server: 69.28.150.204 [lcn.vo.lnwd.net] [lcn.vo.lnwd.net] [TCP 80]
 Server: 69.28.176.41 [wc.vo.lnwd.net] [image.weather.com] [TCP 80]
 Server: 69.28.176.65 [wc.vo.lnwd.net] [image.weather.com] [TCP 80]
 Server: 69.28.176.68 [wc.vo.lnwd.net] [image.weather.com] [TCP 80]
 Server: 69.28.178.68 [wc.vo.lnwd.net] [image.weather.com] [TCP 80]
 Server: 69.39.67.98 [theprivacyplace.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 [ykids.yahoo6.akadns.net] [ykids.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-extermal-1.amazonaws.com] [img.auctiva.com] [TCP 80]
 Server: 72.21.207.136 [s3-extermal-1.amazonaws.com] [scimg.auctiva.com] [TCP 80]
 Server: 72.21.210.11 [www.amazon.com] [TCP 80]
 Server: 72.21.211.101 [s3-extermal-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.ysm.yahoo.com] [rc12.overture.com] [TCP 80]

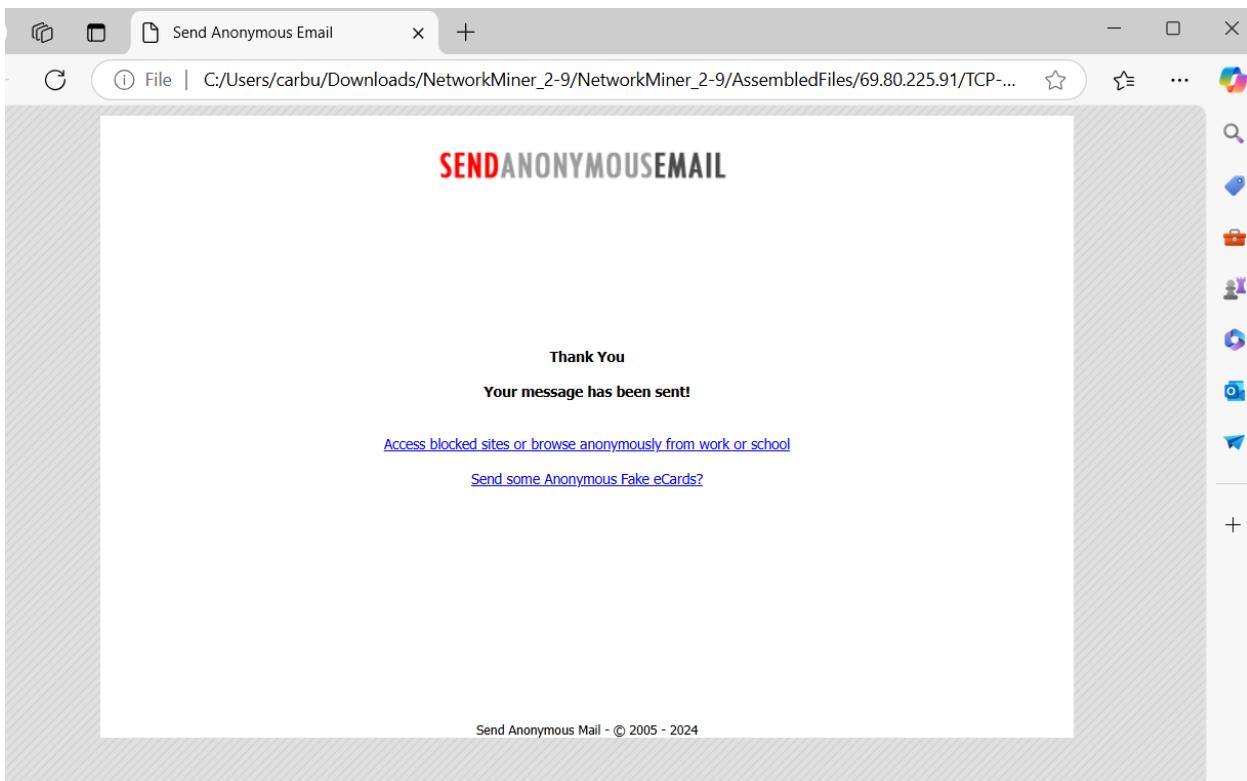
Server: 69.63.176.174 [0.channel14.facebook.com] [TCP 443]
 Server: 69.63.176.174 [0.channel14.facebook.com] [TCP 80]
 Server: 69.63.178.11 [facebook.com] [TCP 80]
 Server: 69.63.178.12 [www.facebook.com] [TCP 80]
 Server: 69.63.178.23 [login.facebook.com] [TCP 443]
 Server: 69.80.200.254 [secure-us.imrworldwide.com] [TCP 80]
 Server: 69.80.225.91 [www.sendanonymousemail.net] [TCP 80]
 Server: 69.147.71.20 [ykids.yahoo6.akadns.net] [ykids.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-extermal-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.ysm.yahoo.com] [rc12.overture.com] [TCP 80]

69.80.225.91 [www.sendanonymousemail.net]
 IP: 69.80.225.91
 MAC: 001D092E4F60
 NIC Vendor: Hon Ha 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

```

A 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 (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 (42632 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 (209 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

```



FREE secure anonymous E-mail to +

File | C:/Users/carbu/Downloads/NetworkMiner_2-9/NetworkMiner_2-9/AssembledFiles/69.25.94.22/TCP-8...

[Secure Anonymous Email - WillSelfDestruct.com](#)

Send Message | FAQ | Blog | Feedback | B2B | Legalese

Secure Anonymous Email - WillSelfDestruct.com

**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](#).



nitroba.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1637

No.	Time	Source	Destination	Protocol	Length
80611	2008-07-22 06:02:57.475010	192.168.15.4	69.80.225.91	TCP	82
80612	2008-07-22 06:02:57.535138	69.80.225.91	192.168.15.4	TCP	82
80613	2008-07-22 06:02:57.536716	192.168.15.4	69.80.225.91	TCP	70
80614	2008-07-22 06:02:57.548149	192.168.15.4	69.80.225.91	HTTP	844
80615	2008-07-22 06:02:57.620412	69.80.225.91	192.168.15.4	TCP	1466
80616	2008-07-22 06:02:57.622689	69.80.225.91	192.168.15.4	TCP	1466
80617	2008-07-22 06:02:57.622795	69.80.225.91	192.168.15.4	HTTP	329
80618	2008-07-22 06:02:57.625680	192.168.15.4	69.80.225.91	TCP	70
80846	2008-07-22 06:03:05.850292	192.168.15.4	69.80.225.91	HTTP	438
80848	2008-07-22 06:03:05.926751	69.80.225.91	192.168.15.4	TCP	1466
80849	2008-07-22 06:03:05.928804	69.80.225.91	192.168.15.4	TCP	1466
80850	2008-07-22 06:03:05.929791	69.80.225.91	192.168.15.4	HTTP	752
80851	2008-07-22 06:03:05.931203	192.168.15.4	69.80.225.91	TCP	70
80852	2008-07-22 06:03:05.935672	192.168.15.4	69.80.225.91	TCP	70
82423	2008-07-22 06:03:22.557473	69.80.225.91	192.168.15.4	TCP	70
82424	2008-07-22 06:03:22.733583	192.168.15.4	69.80.225.91	TCP	70
82427	2008-07-22 06:03:23.963189	192.168.15.4	69.80.225.91	TCP	70

Frame 80614: 844 bytes on wire (6752 bits), 844 bytes captured (6752 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: 0xf725def [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 (DS2P: CS0, ECN: Not-ECT)

Total Length: 826

Identification: 0xef93 (61331)

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

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

Time to Live: 63

Protocol: TCP (6)

Header Checksum: 0x52d2 [validation disabled]

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

Accept-Charset: utf-8;q=1, *;q=0

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=762adb03236142ccce305f6a0aafffa

email:lytuckrige@yahoo.com&sender=the_whole_world_is_watching@nitroba.org&subject=Your+class+stinks&message=why+do+you+spersist+in+teaching+a+boring+class%3F#000000A000%0A#0e+don%27t+like+it.%300%0A%000%0A#0e+don%27t+like+you.%300%0A%000%0A&secure_ty_code=on&mb=b&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

<html>

<head>

<title>Send Anonymous Email</title>

<link href="style.css" rel="stylesheet" type="text/css">

</head>

<body>

<table width=760 border=0 align=center cellpadding=0 cellspacing=0 bgcolor="#FFFFFF">

<tr>

<td><div align=center>

</center>

Packet 80617.2 client ptkts, 2 server ptkts, 2 turns. Click to select.

Entire conversation (7643 bytes) Show as ASCII No delta times Stream 16:

Find: Case sensitive Find Next

tcp.stream eq 1620					Time	Source	Destination	Protocol	Length
o.									
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	06:04:44.528919	209.85.201.189			209.85.201.189		TCP	

```

GET /mail/channel/test?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&at=x
v&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=DQAAAG8AAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvvcv4N9vQ6lW
wOo-H5ktrUCM822cati0c7NMWnq3dfja63nj2FKE1FpHQqfs2we; S=gmail=L5hb7I
oxy=6uatNcZZmB8; gmproxy_yj=FRV17ZyWhh8:gmproxy_yj_sub=bzg0W0bARA;
gmailchat=jcoachj@gmail.com/475090; GMAIL_STAT=lt=500&js=251&dw=62&
REF=ID=8fc081df5e738a3c:TM=1210743469:LM=1216706486:GM=1:S=vvxehX0c
f71-9JQ2AeoD8oWG9NJtOp7T5tuskkNgEKMRAngP49vI4Easp6lpBuJWaDr5pEv4yh
92309928271:2; __utmx=173272373.00000983192309928271:1216706401:_
WgZ7DwUjYpLoqh7F1_E-X5taC4l0uvzXtrVeE6Zq1gcoQt50MC7lgOfv5YtK9GsvrN
TZ=-60; GMAIL_HELP=hosted:0
HTTP/1.1 200 OK

```