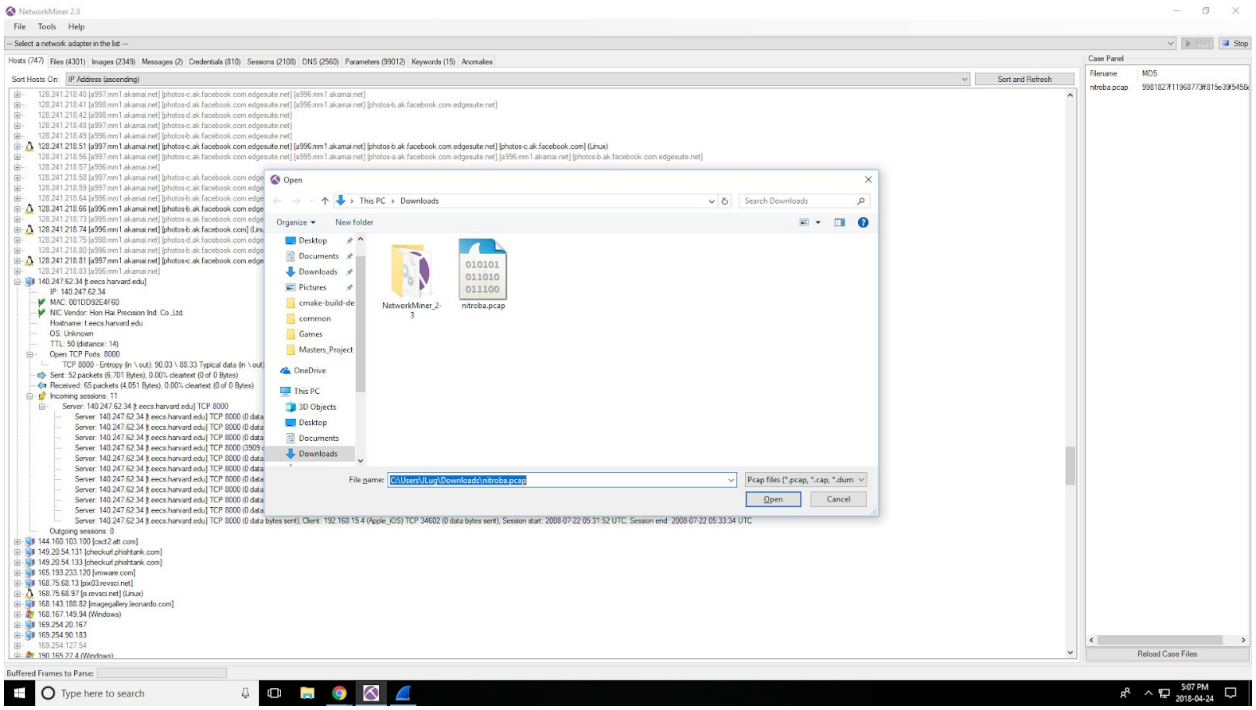
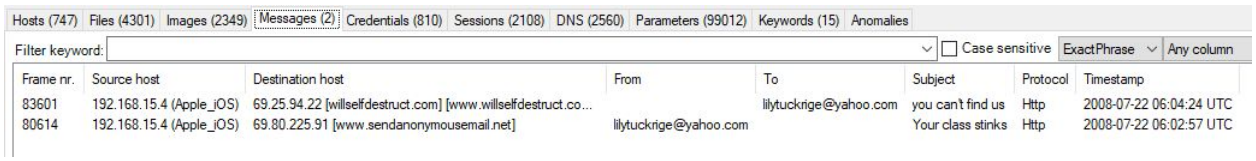
I started by opening the *nitroba.pcap* file in network miner.



I then clicked on the messages tab to see the emails sent from *192.168.15.4 (Apple_iOS)*



I then started looking through the session from the IP address above.

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
18761	192.168.1.64 (Apple_iOS)	48087	74.125.19.99 [www.l.google.com] [www.google.com]	80	Http	2008-07-22 03:50:10 UTC
18784	192.168.1.64 (Apple_iOS)	37351	66.135.205.13 [ebay.com]	80	Http	2008-07-22 03:50:16 UTC
18820	192.168.15.4	32814	72.21.210.11 [www.amazon.com]	80	Http	2008-07-22 04:29:53 UTC
18840	192.168.15.4	32816	69.22.167.225 [a1248.g.akamai.net] [z-ecx.images-amazon.com.edgesuite.net] [z-ecx.images-amazon.com] (Linux)	80	Http	2008-07-22 04:29:54 UTC
18841	192.168.15.4	32818	69.22.167.225 [a1248.g.akamai.net] [z-ecx.images-amazon.com.edgesuite.net] [z-ecx.images-amazon.com] (Linux)	80	Http	2008-07-22 04:29:54 UTC
18928	192.168.15.4	32822	8.12.217.125 [g-ecx.images-amazon.com.c.footprint.net] [g-ecx.images-amazon.com]	80	Http	2008-07-22 04:29:55 UTC
18929	192.168.15.4	32824	8.12.217.125 [g-ecx.images-amazon.com.c.footprint.net] [g-ecx.images-amazon.com]	80	Http	2008-07-22 04:29:55 UTC
18925	192.168.15.4	32820	216.73.86.52 [ad.3ad.doubleclick.net]	443	Ssl	2008-07-22 04:29:55 UTC
19114	192.168.15.4	32828	8.12.217.125 [g-ecx.images-amazon.com.c.footprint.net] [g-ecx.images-amazon.com]	80	Http	2008-07-22 04:29:55 UTC
19115	192.168.15.4	32830	8.12.217.125 [g-ecx.images-amazon.com.c.footprint.net] [g-ecx.images-amazon.com]	80	Http	2008-07-22 04:29:55 UTC
19112	192.168.15.4	32826	216.73.86.52 [ad.3ad.doubleclick.net]	443	Ssl	2008-07-22 04:29:55 UTC
19133	192.168.15.4	32832	66.119.33.171 [ar.gta.voicefive.com] [ar.voicefive.com]	443	Ssl	2008-07-22 04:29:55 UTC
19169	192.168.15.4	32834	216.73.86.52 [ad.3ad.doubleclick.net]	443	Ssl	2008-07-22 04:29:56 UTC
19261	192.168.15.4	32836	209.84.2.125 [ecx.images-amazon.com.c.footprint.net] [ecx.images-amazon.com]	80	Http	2008-07-22 04:29:56 UTC
19263	192.168.15.4	32838	209.84.2.125 [ecx.images-amazon.com.c.footprint.net] [ecx.images-amazon.com]	80	Http	2008-07-22 04:29:56 UTC
19273	192.168.15.4	32840	209.84.2.125 [ecx.images-amazon.com.c.footprint.net] [ecx.images-amazon.com]	80	Http	2008-07-22 04:29:56 UTC
19303	192.168.15.4	32842	204.2.133.74 [a1794.l.akamai.net] [g-ec2.images-amazon.com.edgesuite.net] [g-ec2.images-amazon.com] (Linux)	80	Http	2008-07-22 04:29:56 UTC
19330	192.168.15.4	32844	209.84.2.125 [ecx.images-amazon.com.c.footprint.net] [ecx.images-amazon.com]	80	Http	2008-07-22 04:29:56 UTC
19394	192.168.15.4	32846	216.73.86.52 [ad.3ad.doubleclick.net] [ad.doubleclick.net]	80	Http	2008-07-22 04:29:56 UTC
19410	192.168.15.4	32848	216.73.86.52 [ad.3ad.doubleclick.net] [ad.doubleclick.net]	80	Http	2008-07-22 04:29:56 UTC
19429	192.168.15.4 (Apple_iOS)	32850	216.73.86.52 [ad.3ad.doubleclick.net] [ad.doubleclick.net]	443	Ssl	2008-07-22 04:29:56 UTC
19591	192.168.15.4 (Apple_iOS)	32854	209.62.186.12 [a509.cd.akamai.net] [m1.2mdn.net] (Linux)	80	Http	2008-07-22 04:29:57 UTC
19586	192.168.15.4 (Apple_iOS)	32852	209.85.66.221 [afe.specificclick.net]	80	Http	2008-07-22 04:29:56 UTC
19666	192.168.15.4 (Apple_iOS)	32856	64.79.161.90 [adopt.specificclick.net]	80	Http	2008-07-22 04:29:57 UTC
19679	192.168.15.4 (Apple_iOS)	32858	66.114.50.83 [g1.panthercdn.com] [cdn2.specificmedia.com]	80	Http	2008-07-22 04:29:57 UTC
19708	192.168.15.4 (Apple_iOS)	32806	209.85.171.190	80		2008-07-22 04:30:00 UTC
19895	192.168.15.4 (Apple_iOS)	32866	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:42 UTC
19919	192.168.15.4 (Apple_iOS)	32868	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
19927	192.168.15.4 (Apple_iOS)	32870	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
19935	192.168.15.4 (Apple_iOS)	32872	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
19938	192.168.15.4 (Apple_iOS)	32874	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
19947	192.168.15.4 (Apple_iOS)	32876	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
19951	192.168.15.4 (Apple_iOS)	32878	18.7.7.97 [rss.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
19969	192.168.15.4 (Apple_iOS)	32880	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
19988	192.168.15.4 (Apple_iOS)	32882	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
20033	192.168.15.4 (Apple_iOS)	32888	66.114.48.49 [g1.panthercdn.com] [www.statcounter.com]	80	Http	2008-07-22 04:30:43 UTC
20014	192.168.15.4 (Apple_iOS)	32884	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
20015	192.168.15.4 (Apple_iOS)	32886	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
20039	192.168.15.4 (Apple_iOS)	32890	18.7.21.116 [HILL-OF-BEANS.mit.edu] [counter.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
20054	192.168.15.4 (Apple_iOS)	32892	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:43 UTC
20142	192.168.15.4 (Apple_iOS)	32896	209.85.171.127 [www-google-analytics.l.google.com] [www.google-analytics.com]	80	Http	2008-07-22 04:30:44 UTC
20141	192.168.15.4 (Apple_iOS)	32894	67.15.56.64 [c12.statcounter.com]	80	Http	2008-07-22 04:30:44 UTC
20184	192.168.15.4 (Apple_iOS)	32898	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:46 UTC
20205	192.168.15.4 (Apple_iOS)	32900	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:47 UTC
20206	192.168.15.4 (Apple_iOS)	32902	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:47 UTC
20207	192.168.15.4 (Apple_iOS)	32904	18.7.22.69 [web.mit.edu]	80	Http	2008-07-22 04:30:47 UTC
19877	192.168.15.4 (Apple_iOS)	32798	209.73.191.242	80		2008-07-22 04:30:41 UTC
19878	192.168.15.4 (Apple_iOS)	32796	209.73.191.242	80		2008-07-22 04:30:41 UTC
19879	192.168.15.4 (Apple_iOS)	32794	209.73.191.242	80		2008-07-22 04:30:41 UTC
19880	192.168.15.4 (Apple_iOS)	32792	209.73.191.242	80		2008-07-22 04:30:41 UTC
20545	192.168.15.4 (Apple_iOS)	32914	64.236.91.21 [www.cnn.com]	80	Http	2008-07-22 04:35:15 UTC

I applied a filter for *willselfdestruct.com* and *sendanonymousemail.net* within the ‘Sessions’ tab to see if more information could be found.

Filter keyword: willselfdestruct.com

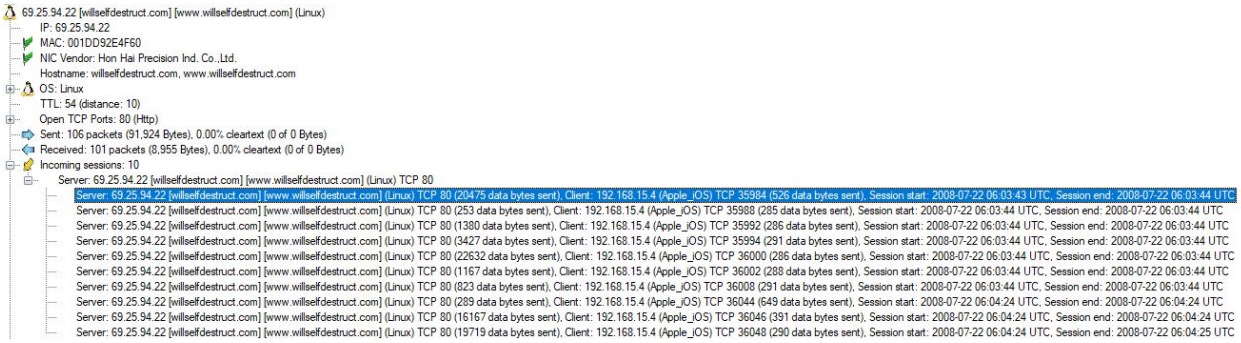
Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
82924	192.168.15.4 (Apple_iOS)	35984	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:03:43 UTC
82969	192.168.15.4 (Apple_iOS)	35988	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:03:44 UTC
83010	192.168.15.4 (Apple_iOS)	35992	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:03:44 UTC
83013	192.168.15.4 (Apple_iOS)	35994	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:03:44 UTC
83051	192.168.15.4 (Apple_iOS)	36000	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:03:44 UTC
83067	192.168.15.4 (Apple_iOS)	36002	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:03:44 UTC
83105	192.168.15.4 (Apple_iOS)	36008	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:03:44 UTC
83597	192.168.15.4 (Apple_iOS)	36044	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:04:24 UTC
83609	192.168.15.4 (Apple_iOS)	36046	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:04:24 UTC
83633	192.168.15.4 (Apple_iOS)	36048	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Linux)	80	Http	2008-07-22 06:04:24 UTC

Filter keyword: sendanonymousemail.net

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
79807	192.168.15.4 (Apple_iOS)	35848	69.80.225.91 [www.sendanonymousemail.net]	80	Http	2008-07-22 06:01:26 UTC
79816	192.168.15.4 (Apple_iOS)	35850	69.80.225.91 [www.sendanonymousemail.net]	80	Http	2008-07-22 06:01:26 UTC
80611	192.168.15.4 (Apple_iOS)	35876	69.80.225.91 [www.sendanonymousemail.net]	80	Http	2008-07-22 06:02:57 UTC
93362	192.168.15.4 (Apple_iOS)	35850	69.80.225.91 [www.sendanonymousemail.net]	80		2008-07-22 06:10:31 UTC

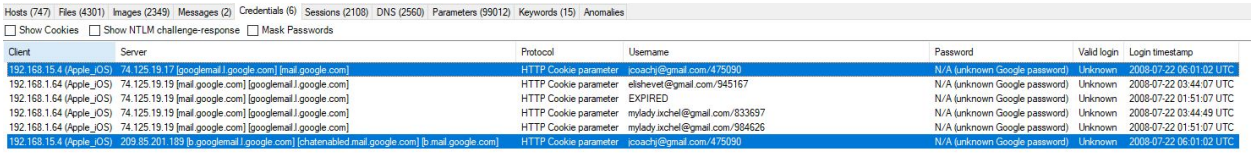
I noticed the server host IP addresses (*69.25.94.22* and *69.80.225.91*). I also noticed the start time of the sessions. All start times are around 0600 UTC on July 22, 2008.

Below are the sessions for *69.25.94.22*



** For some reason, I could not open the sessions for *69.80.225.91*. **

In the ‘Credentials’ tab, I found who was using the machine at the same time the email messages were sent.



It appears that the user with the email address *jcoachj@gmail.com* was using the Apple iOS machine with IP *192.168.15.4* at 0601 on July 22, 2008.

Using the name list provided by the Assignment slides…

So who did it?

```
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
```

We can see there is a student by the name of **Johnny Coach**. He is the one who was sending the emails to Mrs. Tuckrige.