Individual Assignment 3

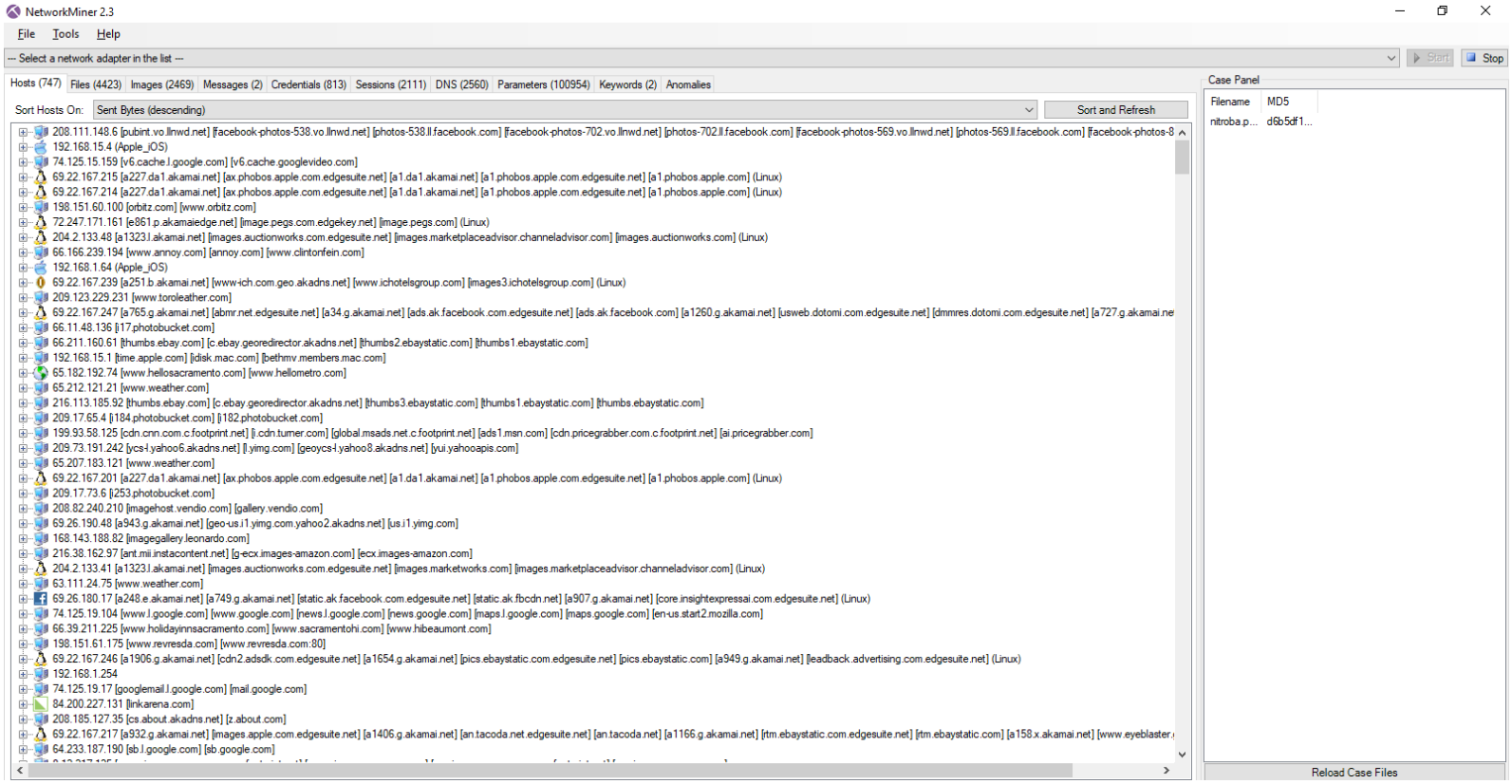
Problem statement: Email harassment to teacher

Evidence: Two harass emails, from the first email, it is able to map the IP to a room with three girls. Those girls are not in Lily's class.

Solution:

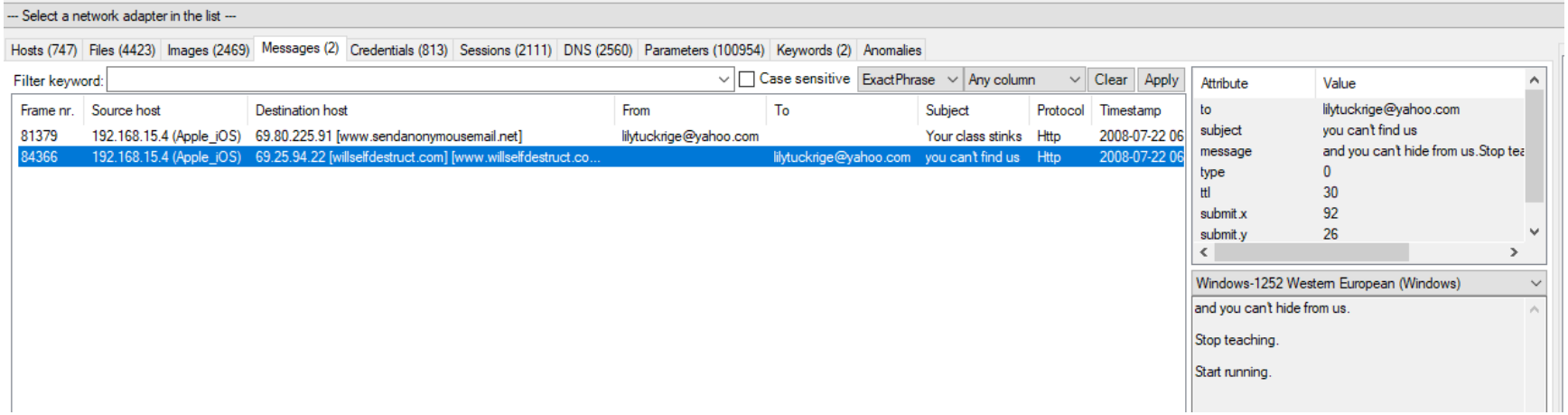
In this assignment, we will use NetworkMiner to solve the problem.

1. First Load the given Pcap file then you will be given the layout as shown below



The first screen or layout provides us with a lot of information, it's difficult to start from here. One thing we could do at this step is to filter out which ip address performs a lot of actions by Sort Host on bytes sent.

2. A very good starting point to this problem is going to the "Message" tab.



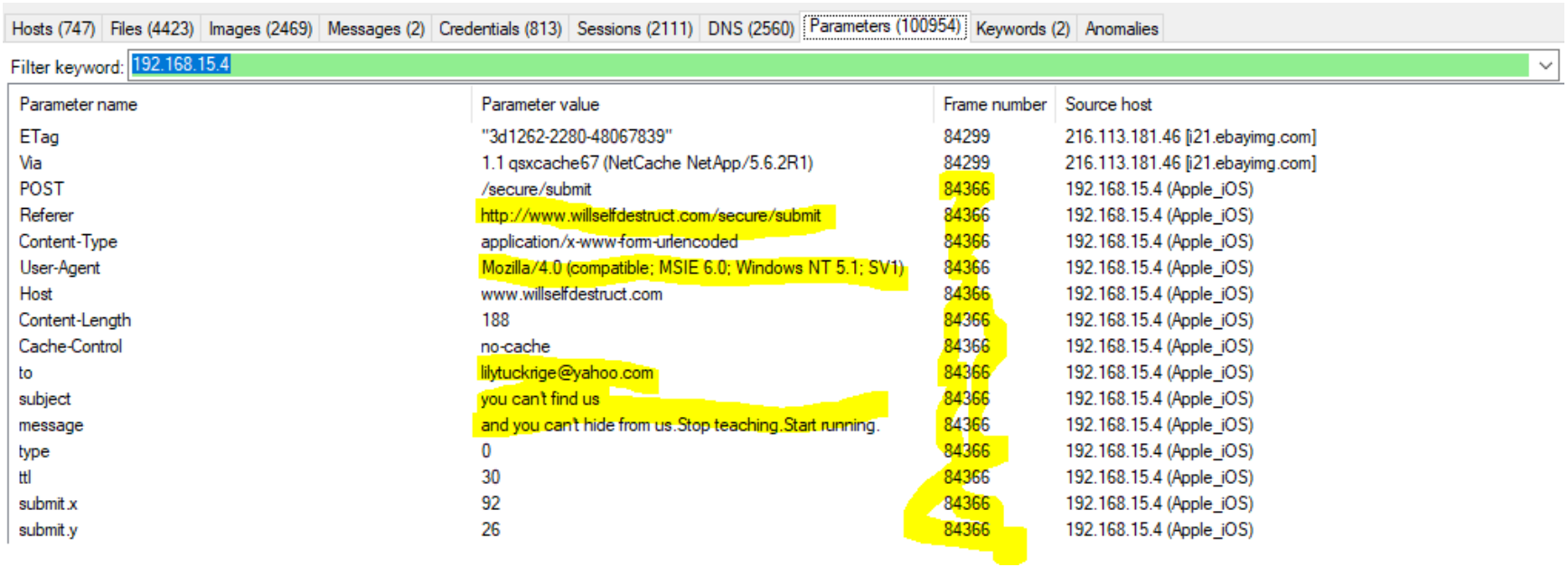
There are two messages here, the most important message is the second one since it is exactly what Lily received. We can start from here.

The output provides us three information

- The message is sent with a frame number: 84366 so we can start from this frame number backward to save time
- The source host is 192.168.15.4, we can filter only activities related to this address
- The operating system on the source host is Apple (Apple_iOS).

3. The next step, we would like to know which browser the attacker uses to send the message. The reason to look for this information can give us two things:
    a. Some credential information might be used if we look at this browser
    b. Other related activities may reveal some information

After playing around with all other tabs, I found the "**Parameters"** tab to be the most relevant tab to answer my question since it includes information such as Frame Number, Brower type or iOS. First, we filter out the activities related to ip address 192.168.15.4 then scroll down and look for frame number 84366



To interpret the browser, we simply put the whole parameter value on Google

`Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)` =>

Internet Explorer 6 on Windows XP SP2

So we can think that, the attacker may use Virtual Machine installed with Windows XP SP2 and use IE to send the message.

4. The next step is a very long and it consumes a lot of time because we have to trace back around 95000 packets. To make it's easier we need to filter out only activities related to this Browser.

Hosts (747) | Files (4423) | Images (2469) | Messages (2) | Credentials (813) | Sessions (2111) | DNS (2560) | Parameters (100954) | Keywords (2) | Anomalies

Filter keyword: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) | Case sensitive | ExactPhrase | Parameter value | Clear | Apply

Parameter name	Parameter value	Frame number	Source host	Source port	Destination host
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83774	192.168.15.4 (Apple_iOS)	TCP 35990	194.129.79.21 [view.atdmt.com]
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83776	192.168.15.4 (Apple_iOS)	TCP 35880	74.125.19.167 [pagead.l.google.com] [pagead2.googlesyndicatio
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83790	192.168.15.4 (Apple_iOS)	TCP 35992	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Lin
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83792	192.168.15.4 (Apple_iOS)	TCP 35998	74.125.19.127 [www-google-analytics.l.google.com] [www.google
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83802	192.168.15.4 (Apple_iOS)	TCP 35994	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Lin
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83803	192.168.15.4 (Apple_iOS)	TCP 35996	66.98.172.25 [c14.statcounter.com]
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83837	192.168.15.4 (Apple_iOS)	TCP 36000	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Lin
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83852	192.168.15.4 (Apple_iOS)	TCP 36002	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Lin
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83884	192.168.15.4 (Apple_iOS)	TCP 35976	69.22.167.249 [a867.g.akamai.net] [www.wired.com.edgesuite.n
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83885	192.168.15.4 (Apple_iOS)	TCP 35950	4.71.104.187 [amch.questionmarket.com] [a.dlqm.net]
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	83927	192.168.15.4 (Apple_iOS)	TCP 36008	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Lin
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	84091	192.168.15.4 (Apple_iOS)	TCP 35804	74.125.19.17 [googlemail.l.google.com] [mail.google.com]
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	84366	192.168.15.4 (Apple_iOS)	TCP 36044	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com] (Lin

Right above the frame 84366 is the frame 84091 which uses this browser to perform mail activity, this email activity may give us who logins.

Parameter name	Parameter value	Frame number	Source host
count	1	84091	192.168.15.4 (Apple_iOS)
req0_type	i	84091	192.168.15.4 (Apple_iOS)
req0_time	172110	84091	192.168.15.4 (Apple_iOS)
req0_evtype	7	84091	192.168.15.4 (Apple_iOS)
GX	DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHlfuyAQ3G...	84091	192.168.15.4 (Apple_iOS)
S	gmail=L5hb7hHJ9B97n6StWA4FvA:gmail_yj=-OoenmU7qT...	84091	192.168.15.4 (Apple_iOS)
GMAIL_AT	xn3j32oktf2a0q6oa3k9sfr6d09yzf	84091	192.168.15.4 (Apple_iOS)
gmailchat	jcoachj@gmail.com/475090	84091	192.168.15.4 (Apple_iOS)
PREF	ID=8fc081df5e738a3c:TM=1210743469:LM=1216706486:...	84091	192.168.15.4 (Apple_iOS)
NID	13=tJ7LtEc6z12iH4BP_IPyV0gGhi4aLcZoJcjAf7l-9JQ2Aeo...	84091	192.168.15.4 (Apple_iOS)
__utmx	173272373.000009831923099282 71:2:	84091	192.168.15.4 (Apple_iOS)
__utmxx	173272373.000009831923099282 71:1216706401:2592000	84091	192.168.15.4 (Apple_iOS)
SID	DQAAAGwAAACH8Y_j5izp1fdbDJzwdRFDGtU3aaeZKWg...	84091	192.168.15.4 (Apple_iOS)
TZ	-60	84091	192.168.15.4 (Apple_iOS)
GMAIL_HELP	hosted:0	84091	192.168.15.4 (Apple_iOS)

At this point we have evidence that joachj@gmail or Johnny Coach may be the one who sent the harassment email to Lily but we need more evidence to close the case.

There are several frames related to **willselfdestruct.com** that sent before and after the frame number 84091, this is a good point to say that the attacker keeps these connections open. Next we found another email

POST	/send.php	81379	192.168.15.4
Referer	http://www.sendanonymousemail.net/	81379	192.168.15.4
Content-Type	application/x-www-form-urlencoded	81379	192.168.15.4
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	81379	192.168.15.4
Host	www.sendanonymousemail.net	81379	192.168.15.4
Content-Length	275	81379	192.168.15.4
Cache-Control	no-cache	81379	192.168.15.4
Cookie	PHPSESSID=762adba03236142ccec305f6a20aaffa	81379	192.168.15.4
email	lilytuckrige@yahoo.com	81379	192.168.15.4
sender	the_whole_world_is_watching@nitroba.org	81379	192.168.15.4
subject	Your class stinks	81379	192.168.15.4
message	Why do you persist in teaching a boring class?We don't like it.We don't like you.	81379	192.168.15.4
security_code	xkpmkb	81379	192.168.15.4
submit	SEND!	81379	192.168.15.4
PHPSESSID	762adba03236142ccec305f6a20aaffa	81379	192.168.15.4

If we keep looking all the frames sent by this browser, we can get a very interesting activity at the frame number 75685

Parameter name	Parameter value	Frame number	Source host
wmpv	9	75682	192.168.15.4 (Apple_iOS)
res	0	75682	192.168.15.4 (Apple_iOS)
B	drcsgu548atoe&b=3&s=2p	75685	192.168.15.4 (Apple_iOS)
answers	rPr8rbs2YDe6N_jmMp5o.r1Pj5AUjPzHt7_utliCPH92P1POs...	75685	192.168.15.4 (Apple_iOS)
GET	/search/search_result;_ylt=A9FJui4Od4VIL5QANivD7BR.;...	75685	192.168.15.4 (Apple_iOS)
Referer	http://answers.yahoo.com/question/index?qid=20080606...	75685	192.168.15.4 (Apple_iOS)
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	75685	192.168.15.4 (Apple_iOS)
Host	answers.yahoo.com	75685	192.168.15.4 (Apple_iOS)
Cookie	B=drcsgu548atoe&b=3&s=2p; answers=rPr8rbs2YDe6N_jm...	75685	192.168.15.4 (Apple_iOS)
p	can I go to jail for harassing my teacher?	75685	192.168.15.4 (Apple_iOS)
GET	/us.yimg.com/i/geo/advan/spacer.gif	75705	192.168.15.4 (Apple_iOS)

When the attacker performs a search on yahoo with the keywords: **Can I go to jail for harassing my teacher?**
And If we go back more at the frame number: 75095 then we get another search: **I want to harass my teacher**

SS	Q0=c2VuZGluZyBhbm9ueW1vdXMgbWFpbA	75095	192.168.15.4 (Apple_iOS)	
PREF	ID=8fc081df5e738a3c:TM=1210743469:LM=1210743469:...	75095	192.168.15.4 (Apple_iOS)	
NID	13=tJ7LtEc6z12iH4BP_IPyV0gGhi4aLcZoJcjAf7l-9JQ2Aeo...	75095	192.168.15.4 (Apple_iOS)	
GET	/search?hl=en&q=i+want+to+harass+my+teacher	75095	192.168.15.4 (Apple_iOS)	
Referer	http://www.google.com/search?hl=en&q=sending+anony...	75095	192.168.15.4 (Apple_iOS)	
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	75095	192.168.15.4 (Apple_iOS)	
Host	www.google.com	75095	192.168.15.4 (Apple_iOS)	
Cookie	SS=Q0=c2VuZGluZyBhbm9ueW1vdXMgbWFpbA; PREF=...	75095	192.168.15.4 (Apple_iOS)	
hl	en	75095	192.168.15.4 (Apple_iOS)	
q	i want to harass my teacher	75095	192.168.15.4 (Apple_iOS)	

And more: **sending anonymous email**

PREF	ID=8fc081df5e738a3c:TM=1210743469:LM=1210743469:S=PiBsyJkS6cu-UEXV	74864	192.168.15.4
NID	12=mIYIMwRy7BkT_gh2VmeAozfrsxDxGoeUEh5jRx5FdCdsWS5Pnoe8cOm8j0ldtXvd9o7ngti0HdeDoQXD...	74864	192.168.15.4
GET	/verify/EAAAAIUqq8kMrLib5yGXYL5Cjn8.gif	74864	192.168.15.4
Referer	http://www.google.com/search?hl=en&q=sending+anonymous+mail	74864	192.168.15.4
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	74864	192.168.15.4
Host	www.google.com	74864	192.168.15.4
Cookie	SNID=13=D8mxrhvS1jq_nwQH8uWqEzoUHeqRFcoFcMd5lsrI=2d0abKT-cu9-Q7Gg; PREF=ID=8fc081df5...	74864	192.168.15.4

And: **How to annoy people**

PREF	ID=8fc081df5e738a3c:TM=1210743469:LM=1210743469:S=PiBsyJkS6cu-UEXV	72597	192.168.15.4
NID	12=mIYIMwRy7BkT_gh2VmeAozfrsxDxGoeUEh5jRx5FdCdsWS5Pnoe8cOm8j0ldtXvd9o7ngti0HdeDoQXD...	72597	192.168.15.4
GET	/search?hl=en&q=how+to+annoy+people	72597	192.168.15.4
Referer	http://www.google.com/	72597	192.168.15.4
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	72597	192.168.15.4
Host	www.google.com	72597	192.168.15.4
Cookie	PREF=ID=8fc081df5e738a3c:TM=1210743469:LM=1210743469:S=PiBsyJkS6cu-UEXV; NID=12=mIYIM...	72597	192.168.15.4
hl	en	72597	192.168.15.4
q	how to annoy people	72597	192.168.15.4

At this point we can conclude that Johnny Coach is the attacker because of the following evidence.

- He performs a series of searches related to annoy, harassment, anonymous message
- He is the only one who uses IE 6.0 in Virtual Machine (other browsers run in Mac OS)
- The sessions or frame number connects to "**willselfdestruct.com**" occurs simultaneously when he logins to his Gmail account which means that he performs this connection (because it uses the same browser) in such a short time.