CS5332 – 2018, Individual Assignment 3

February 2018

Nitroba University Harassment Scenario

First analysis

To find the device from which the threat originated, do a Wireshark full-text search for `lilytuckrige@yahoo.com`. It was POSTed/sent from:

- MAC: 00:17:f2:e2:c0:ce
- IP: 192.168.15.4

Filtering by the MAC gives ~45MB of packages, filtering by the IP would give much less. So use `File` > `Export Specified Packets` to export the filtered packages and open them in NetworkMonitor. The next part is just a manual search for scraps. Findings:

- in file `index[2].html`, amazon.com greets "Hello, Simson L. Garfinkel"
- signed in with google.com as `jcoachj@gmail.com` (credentials tab)

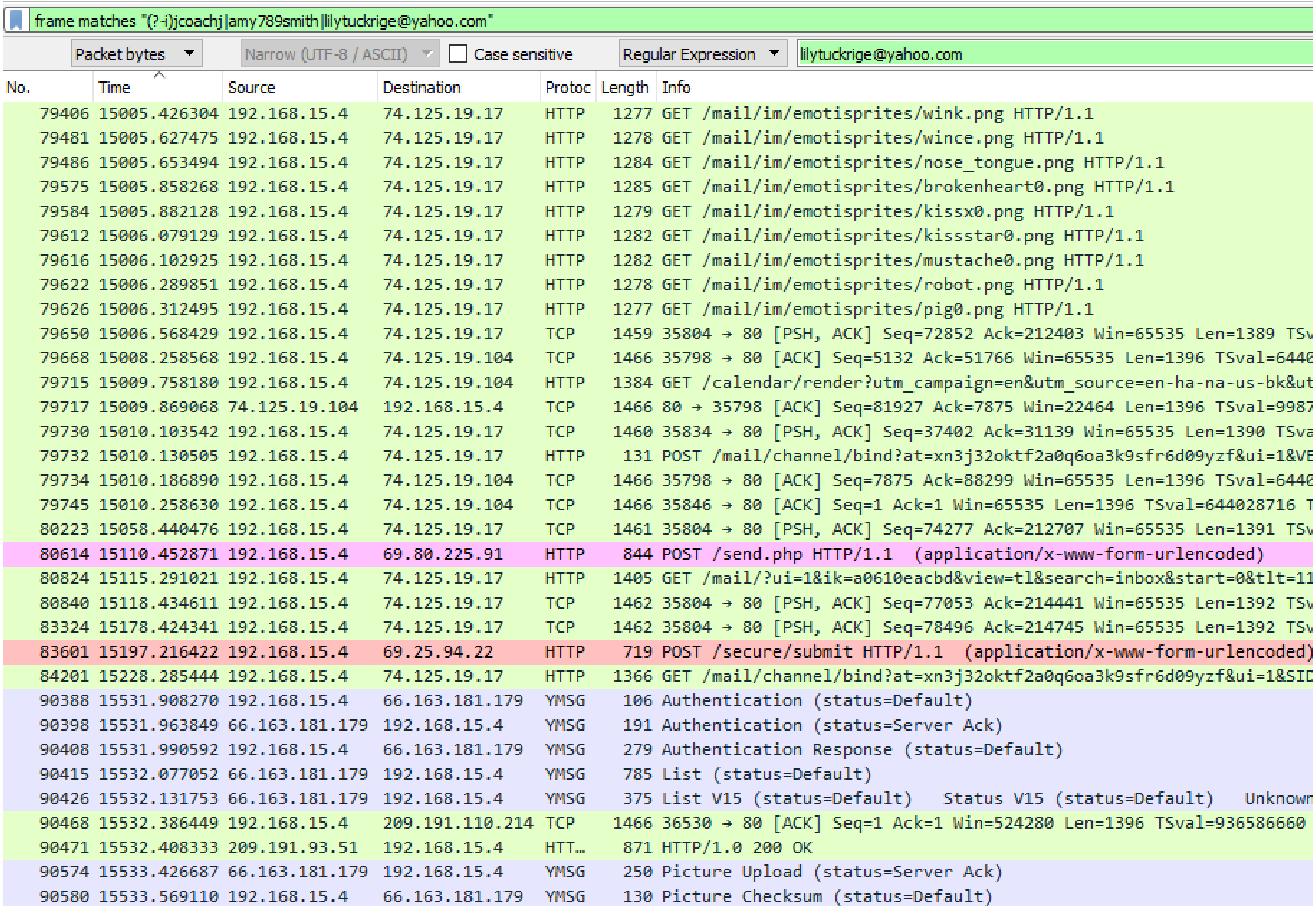
To find additional things, use Wireshark again and search for (RegExp) `Amy|Smith|Burt|Greedom|Tuck|Gorge|Johnny|Coach|Jeremy|Ledvkin|Nancy|Colburne|Tamara|Perkins|Esther|Pringle|Asar|Misrad|Jenny|Kant`. This is quite permissive and also matches a lot of irrelevant packages, but with some patience, one can find the following (in addition to the points above): * [Wireshark]: there is a `Yahoo YMSG Messenger Protocol (Authentication)` message for `amy789smith` and some `YMSG` protocol communication with that name

Evaluation

Amy Smith (`amy789smith`) and Johnny Coach (`jcoachj@gmail.com`) are both students in the class. "Simson L. Garfinkel" is not.

Apparently, two people from that class used the device from which the threat-mail originated. It seems more likely that Johnny used Amys Laptop to check his mails then that Amy used Johnnys Laptop and signed in to the Yahoo Messenger program, which just happened to be installed on his computer. It should be pretty easy to find out who actually owns that device, either by analysing more traffic or by sizing the device.

But the more interesting question is who actually used the device at the time the message was sent. To answer this question, it might be useful to look at the timeline of all packages mentioning either `jcoachj`, `amy789smith` or `lilytuckrige@yahoo.com`:



frame matches "(?-i)jcoachj|amy789smith|lilytuckrige@yahoo.com"

Packet bytes ▾ | Narrow (UTF-8 / ASCII) ▾ | □ Case sensitive | Regular Expression ▾ | lilytuckrige@yahoo.com

No.	Time	Source	Destination	Protoc	Length	Info
79406	15005.426304	192.168.15.4	74.125.19.17	HTTP	1277	GET /mail/im/emotisprites/wink.png HTTP/1.1
79481	15005.627475	192.168.15.4	74.125.19.17	HTTP	1278	GET /mail/im/emotisprites/wince.png HTTP/1.1
79486	15005.653494	192.168.15.4	74.125.19.17	HTTP	1284	GET /mail/im/emotisprites/nose_tongue.png HTTP/1.1
79575	15005.858268	192.168.15.4	74.125.19.17	HTTP	1285	GET /mail/im/emotisprites/brokenheart0.png HTTP/1.1
79584	15005.882128	192.168.15.4	74.125.19.17	HTTP	1279	GET /mail/im/emotisprites/kissx0.png HTTP/1.1
79612	15006.079129	192.168.15.4	74.125.19.17	HTTP	1282	GET /mail/im/emotisprites/kissstar0.png HTTP/1.1
79616	15006.102925	192.168.15.4	74.125.19.17	HTTP	1282	GET /mail/im/emotisprites/mustache0.png HTTP/1.1
79622	15006.289851	192.168.15.4	74.125.19.17	HTTP	1278	GET /mail/im/emotisprites/robot.png HTTP/1.1
79626	15006.312495	192.168.15.4	74.125.19.17	HTTP	1277	GET /mail/im/emotisprites/pig0.png HTTP/1.1
79650	15006.568429	192.168.15.4	74.125.19.17	TCP	1459	35804 → 80 [PSH, ACK] Seq=72852 Ack=212403 Win=65535 Len=1389 TSv
79668	15008.258568	192.168.15.4	74.125.19.104	TCP	1466	35798 → 80 [ACK] Seq=5132 Ack=51766 Win=65535 Len=1396 TSval=6440
79715	15009.758180	192.168.15.4	74.125.19.104	HTTP	1384	GET /calendar/render?utm_campaign=en&utm_source=en-ha-na-us-bk&ut
79717	15009.869068	74.125.19.104	192.168.15.4	TCP	1466	80 → 35798 [ACK] Seq=81927 Ack=7875 Win=22464 Len=1396 TSval=9987
79730	15010.103542	192.168.15.4	74.125.19.17	TCP	1460	35834 → 80 [PSH, ACK] Seq=37402 Ack=31139 Win=65535 Len=1390 TSva
79732	15010.130505	192.168.15.4	74.125.19.17	HTTP	131	POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VE
79734	15010.186890	192.168.15.4	74.125.19.104	TCP	1466	35798 → 80 [ACK] Seq=7875 Ack=88299 Win=65535 Len=1396 TSval=6440
79745	15010.258630	192.168.15.4	74.125.19.104	TCP	1466	35846 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=1396 TSval=644028716 T
80223	15058.440476	192.168.15.4	74.125.19.17	TCP	1461	35804 → 80 [PSH, ACK] Seq=74277 Ack=212707 Win=65535 Len=1391 TSv
80614	15110.452871	192.168.15.4	69.80.225.91	HTTP	844	POST /send.php HTTP/1.1 (application/x-www-form-urlencoded)
80824	15115.291021	192.168.15.4	74.125.19.17	HTTP	1405	GET /mail/?ui=1&ik=a0610eacbd&view=tl&search=inbox&start=0&tlt=11
80840	15118.434611	192.168.15.4	74.125.19.17	TCP	1462	35804 → 80 [PSH, ACK] Seq=77053 Ack=214441 Win=65535 Len=1392 TSv
83324	15178.424341	192.168.15.4	74.125.19.17	TCP	1462	35804 → 80 [PSH, ACK] Seq=78496 Ack=214745 Win=65535 Len=1392 TSv
83601	15197.216422	192.168.15.4	69.25.94.22	HTTP	719	POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)
84201	15228.285444	192.168.15.4	74.125.19.17	HTTP	1366	GET /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&SID
90388	15531.908270	192.168.15.4	66.163.181.179	YMSG	106	Authentication (status=Default)
90398	15531.963849	66.163.181.179	192.168.15.4	YMSG	191	Authentication (status=Server Ack)
90408	15531.990592	192.168.15.4	66.163.181.179	YMSG	279	Authentication Response (status=Default)
90415	15532.077052	66.163.181.179	192.168.15.4	YMSG	785	List (status=Default)
90426	15532.131753	66.163.181.179	192.168.15.4	YMSG	375	List V15 (status=Default) Status V15 (status=Default) Unknown
90468	15532.386449	192.168.15.4	209.191.110.214	TCP	1466	36530 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=1396 TSval=936586660
90471	15532.408333	209.191.93.51	192.168.15.4	HTT…	871	HTTP/1.0 200 OK
90574	15533.426687	66.163.181.179	192.168.15.4	YMSG	250	Picture Upload (status=Server Ack)
90580	15533.569110	192.168.15.4	66.163.181.179	YMSG	130	Picture Checksum (status=Default)

Figure 1: **Time line**: times in seconds since capture start; green: HTTP traffic with `jcoachj`; pink: threat originated, do a to `lilytuckrige@yahoo.com`; blue: Yahoo Messenger (`amy789smith`)

Observations: * The HTTP traffic involving `jcoachj` starts at 14976 seconds (not displayed) and keeps sending packets quite rapidly until 15010 seconds * There are actually tow threat originated, do a essages sent from the device, the first one (not delivered?) sent 15110 and the second one at 15197, 1.6 and 3 minutes after the bulk of `jcoachj` traffic * There is a picture upload on the Yahoo Messenger at 15533, 5.5 minutes after the second threat originated, do a as sent

Conclusion

One possible interpretation/explanation would be, that Johnny did indeed use Amys deice to check his mails and do some browsing between seconds 14976 and 15010, then forgot to sign out. It is pretty likely that Amy used her device at second 15533 to send a picture vi the Yahoo Messenger. There is no indication that Johnny used the device after 15010, and if we assume that the device is Amys and she used it at 15533, it seems more likely that she sent the threat. If Johnny used Amys device to send the threat to hide his trail, but signed in with his account first, he would be a true moron.

It should be noted though that this is based mostly on assumptions and would hardly be court-worthy.