student name: Andrew Simon

Blue Team Midterm Achievement

Either: `Make a Copy of this in your personal Google Drive`

Or: `Download this template as .docx locally`

Use it to complete the Scenario and Scripting Challenges and document your work. When you have finished, export your document as a **.pdf** in the following syntax:

```
cohortNumber_lastName_firstName.pdf
```

Scenario

A professor reports a harassing email from an unknown sender. You investigate, and find the source IP to be a student dorm room. You set up a network tap to collect any traffic from that room's wifi network, in the hopes of catching the culprit. Some time later, a second malicious email is sent!

Answer the following questions, and document what steps you took to determine the information (ex. which wireshark searches did you run, which display filters did you use, and which packet numbers contained the information.)

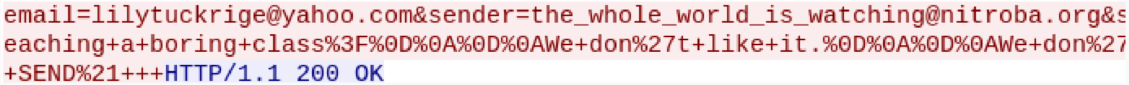
Here is the Pcap

Here is the Email

Scenario Questions

1. Search for an identifier associated with the harassing email. What steps did you take in Wireshark?

answer: The identifier I chose to work with was looking in the TCP streams for content including “lilytuckrige” (the email of the professor). This gave me info on the second email sent. (Packet # 80614)

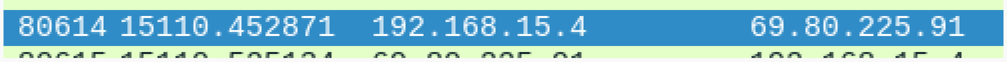


```
email=lilytuckrige@yahoo.com&sender=the_whole_world_is_watching@nitroba.org&s
eaching+a+boring+class%3F%0D%0A%0D%0AWe+don%27t+like+it.%0D%0A%0D%0AWe+don%27
+SEND%21+++HTTP/1.1 200 OK
```

This gives me the email contents, likely source IP of the sender, which browser they used, and the site they sent it from.
I used tcp contains ‘lilytuckrige’

2. Which IP address likely sent the emails?

answer:

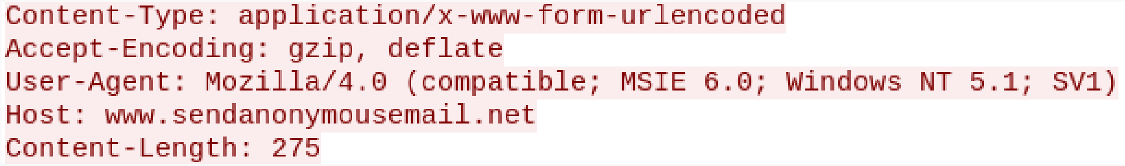


```
80614 15110.452871   192.168.15.4            69.80.225.91
```

The filter used in the previous question that pulled the second email had the source IP of 192.168.15.4

3. From that request, what browser was used to send the second harassing email?

answer:

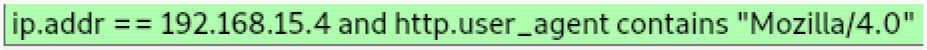


```
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.sendanonymousemail.net
Content-Length: 275
```

From the filter used in Question 1, the second email was sent through Mozilla Firefox. I know this from the User-Agent: Mozilla/4.40 line in the TCP stream of Packet # 80614

4. Create a display filter for that IP source and browser. (Hint: use "http.user_agent")

answer:

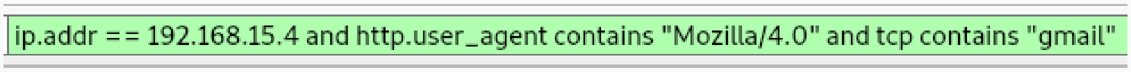


```
ip.addr == 192.168.15.4 and http.user_agent contains "Mozilla/4.0"
```

This searches for Packets that fit both conditions of being from IP 192.168.15.4 and a user agent containing Mozilla/4.0

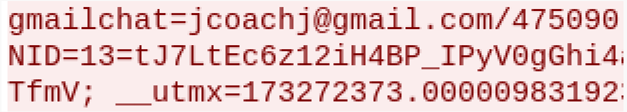
5. What @gmail.com account is associated with that IP/browser pair?

answer:



```
ip.addr == 192.168.15.4 and http.user_agent contains "Mozilla/4.0" and tcp contains "gmail"
```

The filter combination used in Question 4 still had way too many Packets, so I used this filter to look for anything by him/her that included “gmail” in the tcp stream to try and find the gmail account.



```
gmailchat=jcoachj@gmail.com/475090
NID=13=tJ7LtEc6z12iH4BP_IPyV0gGhi4
TfmV; __utmx=173272373.00000983192
```

Several instances (This is from Packet #79732) have shown the email: jcoachj@gmail.com all throughout the tcp streams. We got him!

Scripting Challenges

Use this log file to answer the following questions. **You do NOT need to explain how you arrived at your conclusions.** These headers might help you parse the log file:

```
frame.number;frame.time;ip.src;tcp.srcport;ip.dst;tcp.dstport;ip.proto;ip.len;Proto;Info
```

1. How many times does the most common source IP address appear in the log? **Give the count, NOT the IP address!**

answer:
16,163

2. Which IP address (source or destination) appears most commonly in the log? *Hint: It appears over 42,000 times.*

answer:
131.243.2.12

15,466 as a source
26,824 as a destination
42,290 total

3. What is the most common (sent the most number of packets) FTP **client** IP address?

answer:
157.231.148.18

Both 131 IPs are servers. This client IP made the most number of requests to those servers.