

Fortal

Tugas 1

ALVARO AUSTIN - 2106752180

MOHAMMAD FERRY HUSNIL ARIF - 2106709112

RADEN MOHAMAD ADRIAN RAMADHAN HENDAR WIBAWA - 2106750540

RAHFI ALYENDRA GIBRAN - 2106705764

AUSHAAF FADHILAH AZZAH - 2106630063



Pertanyaan:

1. Map out the Nitroba dorm room network.
2. Find who sent email to lilytuckrige@yahoo.com
 - a. Look for a TCP flow that includes the hostile message
 - b. Find information that can tie that message to a particular web browser.
3. Identify the other TCP connections that belong to the attacker
4. Find information in one of those TCP connections that IDs the attacker.



Nitroba Dorm Map

Filter: nitroba.org

Sort Hosts On: Router Hops Distance (ascending)

- 192.168.15.4 (Apple_iOS)
 - IP: 192.168.15.4
 - MAC: 0017F2E2C0CE
 - NIC Vendor: Apple, Inc.
 - MAC Age: 2006-04-13
 - Hostname:
 - + OS: Apple_iOS
 - TTL: 63 (distance: 1)
 - Open TCP Ports:
 - Sent: 34554 packets (5,077,415 Bytes), 0.00% cleartext (0 of 0 Bytes)
 - Received: 38643 packets (38,297,069 Bytes), 0.00% cleartext (0 of 0 Bytes)
 - Incoming sessions: 0
 - + Outgoing sessions: 1655
 - Host Details
 - Queried IP Addresses : 192.168.15.1
 - Queried DNS names : db._dns-sd._udp.0.117.168.192.in-addr.arpa.www.amazon.com.z-ecx.images-amazon.com.ad.3ad.doubleclick.net
 - Web Browser User-Agent 1 : Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_4; en-us) AppleWebKit/525.18 (KHTML, like Gecko) Version/3.1.2 Safari/525.18
 - Web Browser User-Agent 2 : Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-us) AppleWebKit/5525.20.1 (KHTML, like Gecko) Version/3.1.2 S
 - Web Browser User-Agent 3 : Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.7.5)
 - Web Browser User-Agent 4 : CFNetwork/330.4
 - Web Browser User-Agent 5 : Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.16) Gecko/20080702 Firefox/2.0.0.16
 - Web Browser User-Agent 6 : Apple-PubSub/65.1.1
 - Web Browser User-Agent 7 : iTunes/7.7 (Macintosh; U; Intel Mac OS X 10.5.4)
 - Web Browser User-Agent 8 : Adium/1.2.7 (Mac OS X) Sparkle/1.1
 - Web Browser User-Agent 9 : Mozilla/4.0 (compatible; MSIE 5.5)
 - Web Browser User-Agent 10 : Windows-Update-Agent
 - Web Browser User-Agent 11 : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
 - Web Browser User-Agent 12 : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1
 - Web Browser User-Agent 13 : ee://aol/http
 - Web Browser User-Agent 14 : iTunes/7.7 (Macintosh; N; Intel)
 - Web Browser User-Agent 15 : Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9b5) Gecko/2008032619 Firefox/3.0b5

Using NetworkMiner, we can see the list of Clients using the Nitroba dorm network

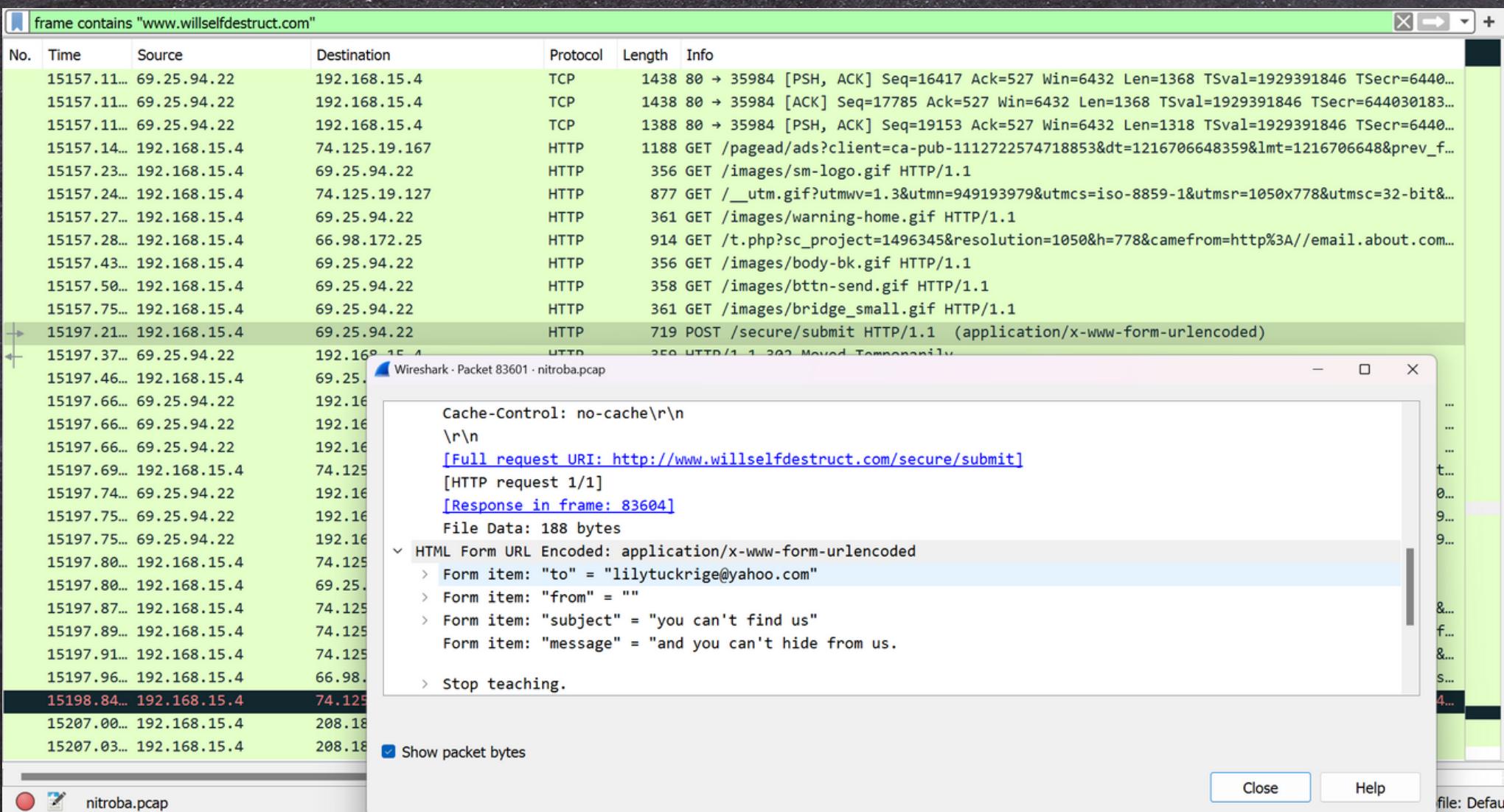


**WHO SENT THE
EMAIL?**

EVIDENCE

1

We need to find the packet that is related to
www.willselfdestruct.com



We found out that it was sent from IP 192.168.15.4

EVIDENCE

2

From previous evidence, we found out that the source IP Address is from 192.168.15.4. We then could check which frame contains lilytuckrige@yahoo.com as destination of the email.



```
frame contains "lilytuckrige@yahoo.com"
No. Time Source Destination Protocol Length Info
15110.45... 192.168.15.4 69.80.225.91 HTTP 844 POST /send.php HTTP/1.1 (application/x-www-form-urlencoded)
15197.21... 192.168.15.4 69.25.94.22 HTTP 719 POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)

Wireshark - Packet 80614 · nitroba.pcap
Hypertext Transfer Protocol
POST /send.php HTTP/1.1\r\n
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
Referer: http://www.sendanonymousemail.net/\r\n
Accept-Language: en-us\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
Host: www.sendanonymousemail.net\r\n
Content-Length: 275\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
Cookie: PHPSESSID=762adba03236142ccec305f6a20affa\r\n
\r\n
[Full request URI: http://www.sendanonymousemail.net/send.php]
[HTTP request 1/2]
[Response in frame: 80617]
[Next request in frame: 80846]
File Data: 275 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "email" = "lilytuckrige@yahoo.com"
Form item: "sender" = "the_whole_world_is_watching@nitroba.org"
Form item: "subject" = "Your class stinks"
Form item: "message" = "Why do you persist in teaching a boring class?
We don't like it.
We don't like you.

e: Default
```

Turns out there was another attempt of sending email from another website called www.sendanonymousemail.net.

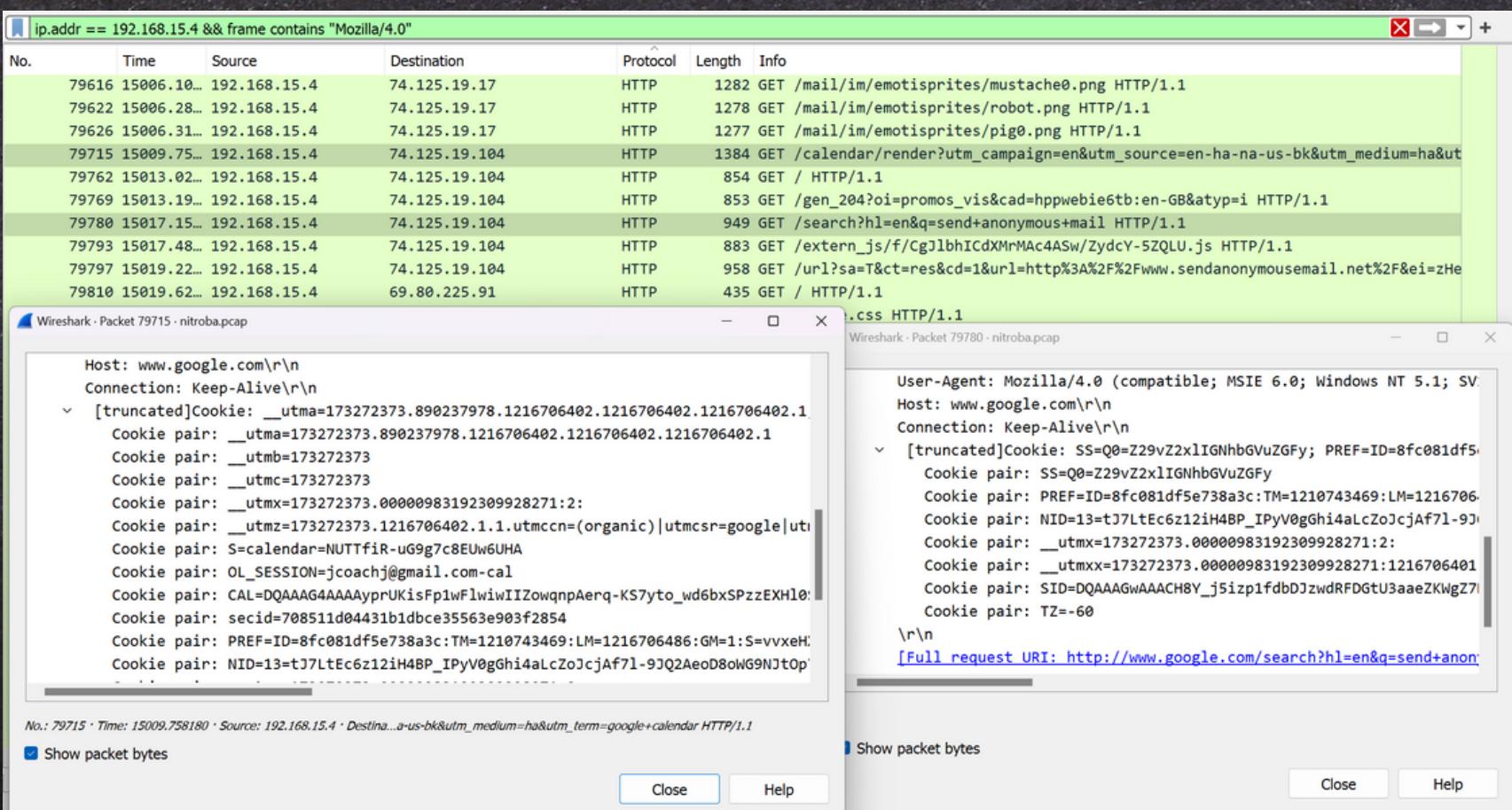
We could also see the similarity between user agent (Mozilla/4.0).

There was also an email explicitly mentioned (the_whole_world_is_watching@nitroba.org). But it wasn't a useful evidence, if we tried to filter the same email.

3

EVIDENCE

Afterwards, we have to find the user that sent these email. We could try to find few packages that is around the time the email was sent. Luckily, in wireshark, we could see the time of when packages were captured. We do know that the attacker is connected to IP 192.168.15.4 and using Mozilla/4.0 as the browser. We can use that information to filter in wireshark. Not only that, we also need to to match the time between attacker attack.



As you can see we could use the cookie from informations that we got from few packets between attacker attack.

Right before the attacker search for “send anonymous email”, it uses referrer from www.google.com which came from a packet that contains cookie regarding the email of the user, which is jcoachj@gmail.com-cal

From that email, we can identify the attacker with a simple identification. The identity of attacker is Johnny Coach

THANK
YOU