Fortal Tugas 1

ALVARO AUSTIN - 2106752180

MOHAMMAD FERRY HUSNIL ARIF - 2106709112

RADEN MOHAMAD ADRIAN RAMADHAN HENDAR WIBAWA - 2106750540

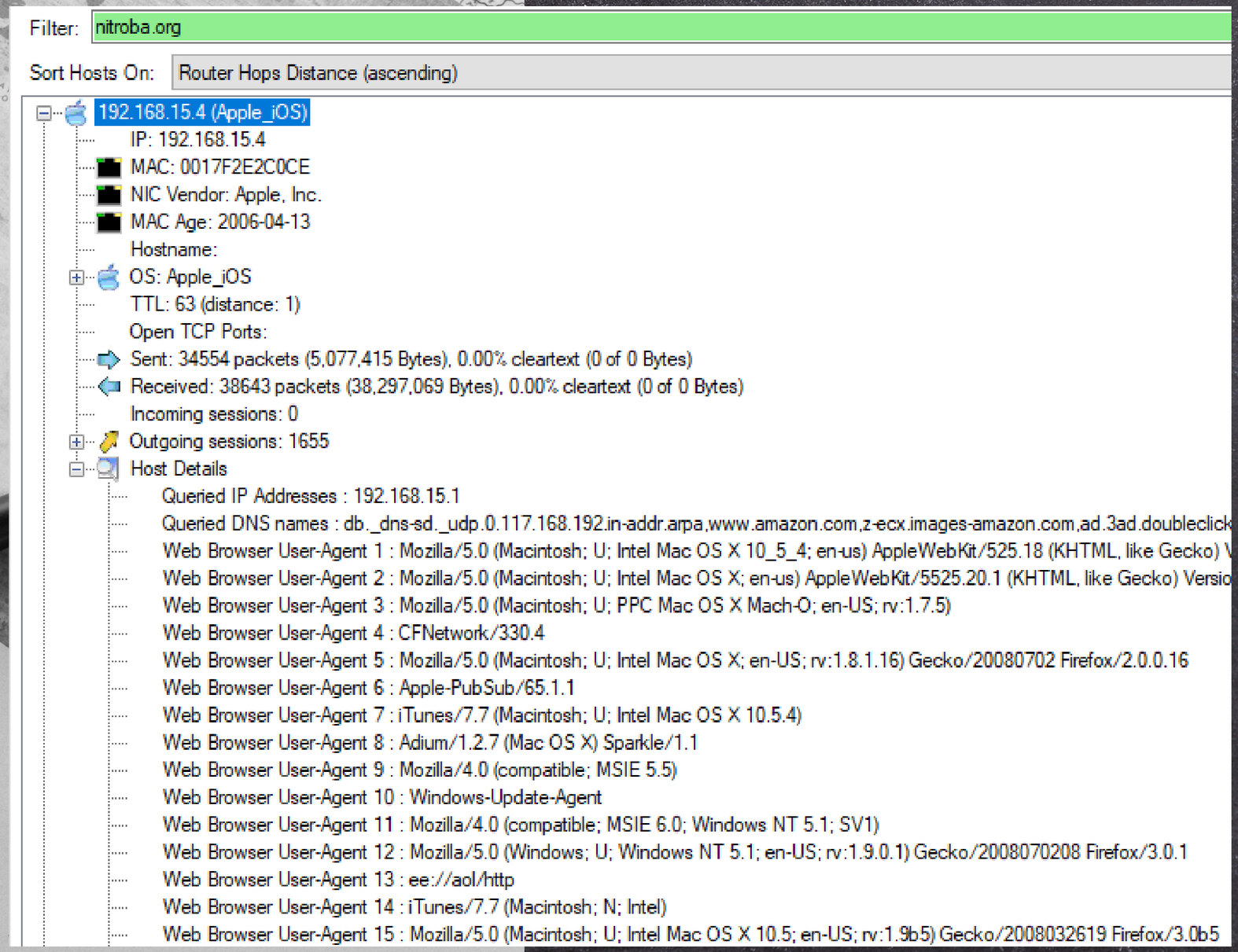
RAHFI ALYENDRA GIBRAN - 2106705764

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 below to the attacker
4. Find information in one of those TCP connections that IDs the attacker.

Nitroba Dorm Map



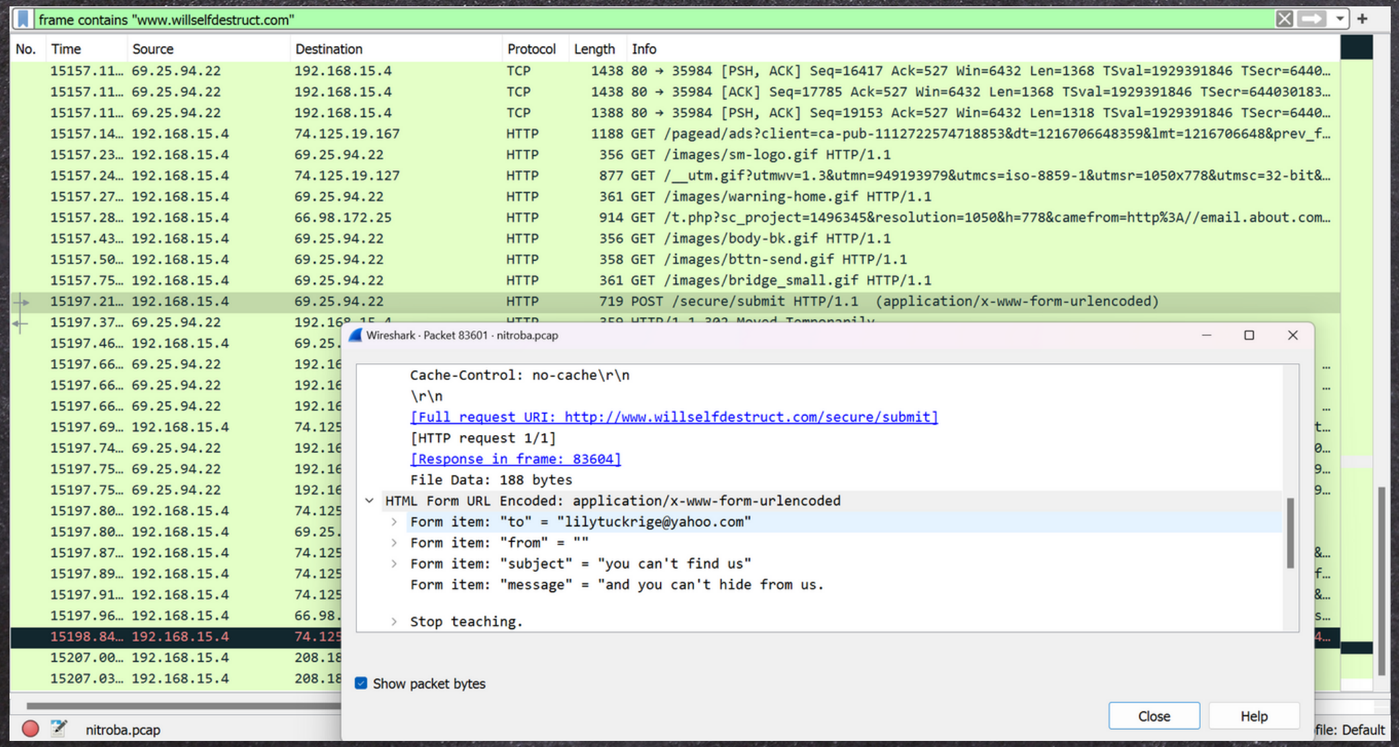
Using Networkminer, we can see the list of Clients using the Nitroba dorm network

WHO SENT THE EMAIL?

EVIDENCE

7

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

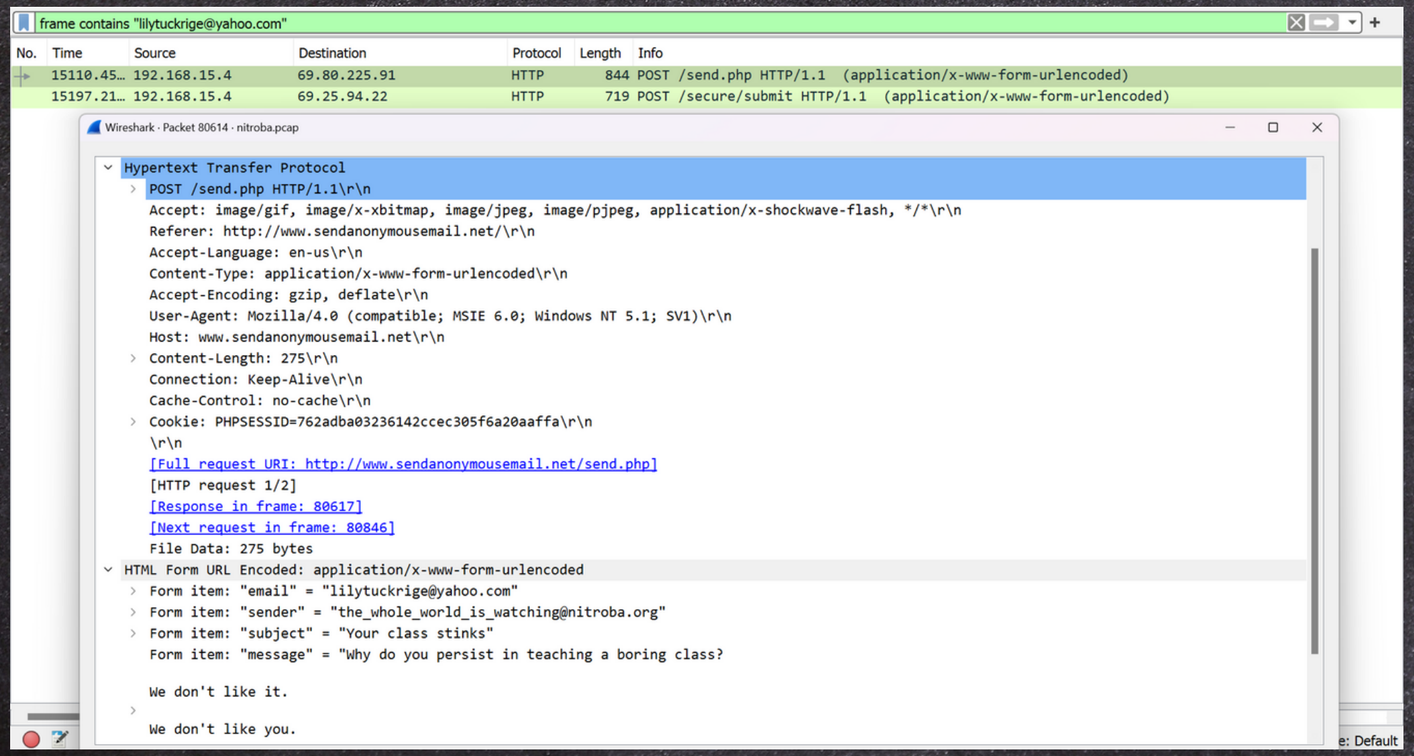


We found out that it was sent from IP 192.168.15.4

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.



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

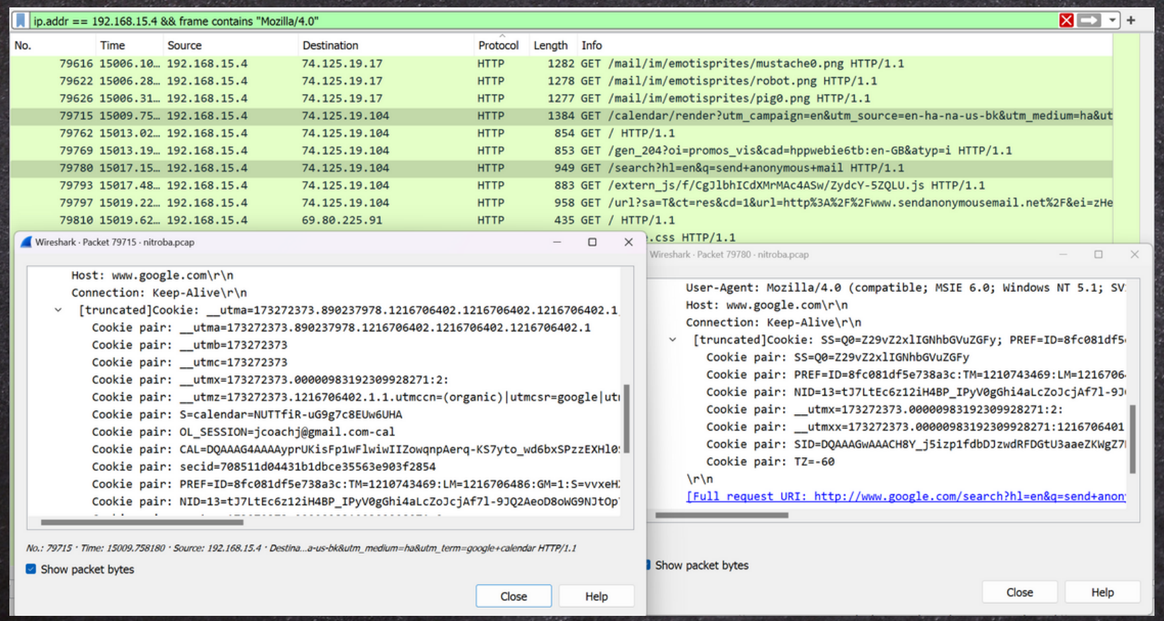
We could also see the similarity between user agent (Mozzila/4.0).

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.

EVIDENCE

3

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 Mozzila/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