Afeefah Manzoor

ITN261

Project Part 2: Who Did it?

1. Start by describing your approach to solving this mystery in terms of the key terms, what you will check, and what pieces of information make link together.

I first check what the scenario gave. I wrote down the time and dates that the attack happened on-to check that on the nmap, and plan to look through emails and any similar messaging and websites that they visited since they used a self-destruct website and I am sure they looked at other similar websites or even social media.

1. Map out the dorm room network.

Roommates: Alice, Barbara, Candice

Kenny is Barbara boyfriend.

Who are friends with them?

1. Find who sent email to [lilytuckrige@yahoo.com](mailto:lilytuckrige@yahoo.com)

• Look for a TCP flow that includes the hostile message  
• Find information that can tie that message to a particular web browser.

Jonny Coach sent the email.

1. Identify the other TCP connections that belong to the attacker
2. Find information in one of those TCP connections that IDs the attacker.
3. At what point in time was the self-destruct message sent?

2:02:57EST

1. Has the sender's IP address been used by one or several computers?

The IP was used by several different devices. I can tell this by the different screen resolutions(1280x800,1680x1050,1050x778).

1. What online services (webmail / social media / instant messaging etc.) has the user of this IP address been logged into?

Hotmail, facebook, itunes, ebay, yahoo messages, gmail,

1. List all devices that are associated with Apple.  Explain how you know for each device.

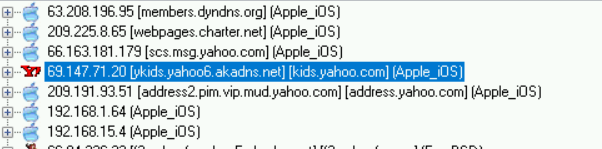
IP addr 63.203.196.95, 209.225.8.65, 66.163.181.179, 69.147.71.20, 209.191.93.51, 192.168.1.64, 192.168.15.4

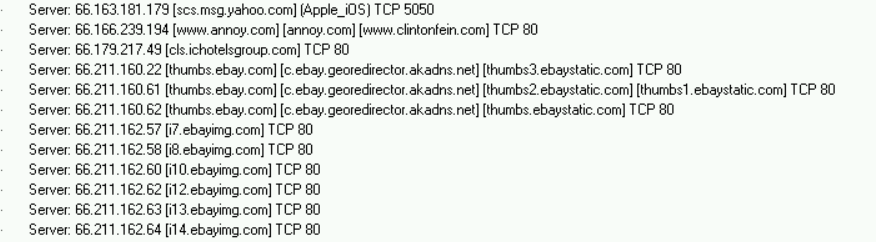
Network Miner ID them as a Apple IOS device.

1. Which book did Lisa See write?

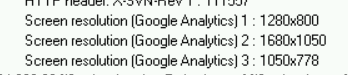
Peony In Love

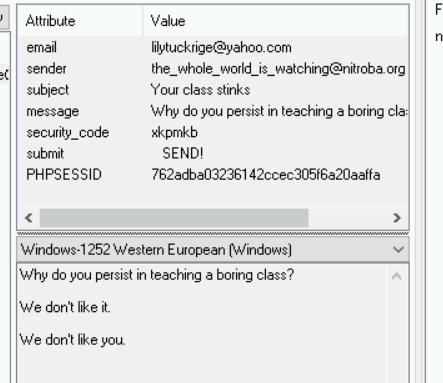


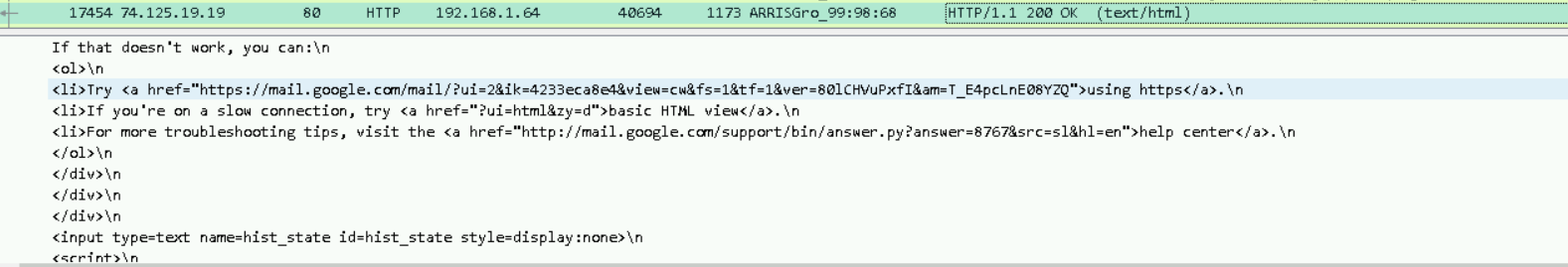


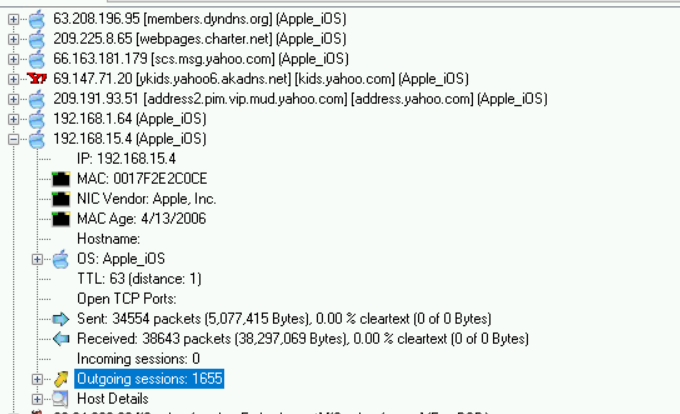
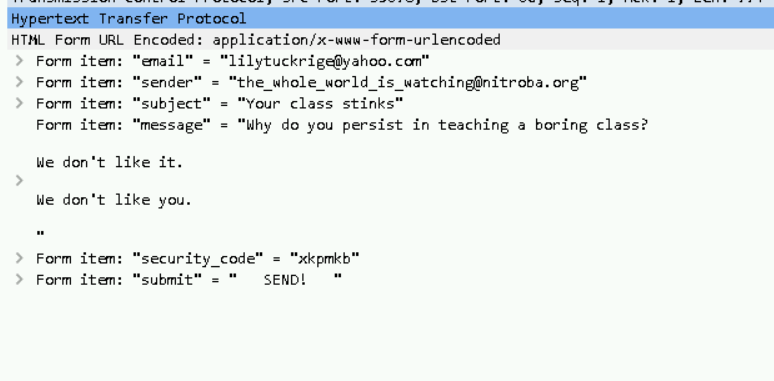
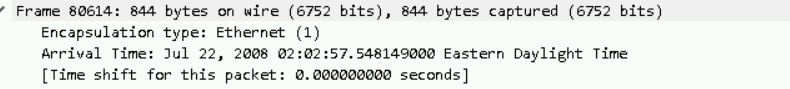










 J Coach = Jonny Coach