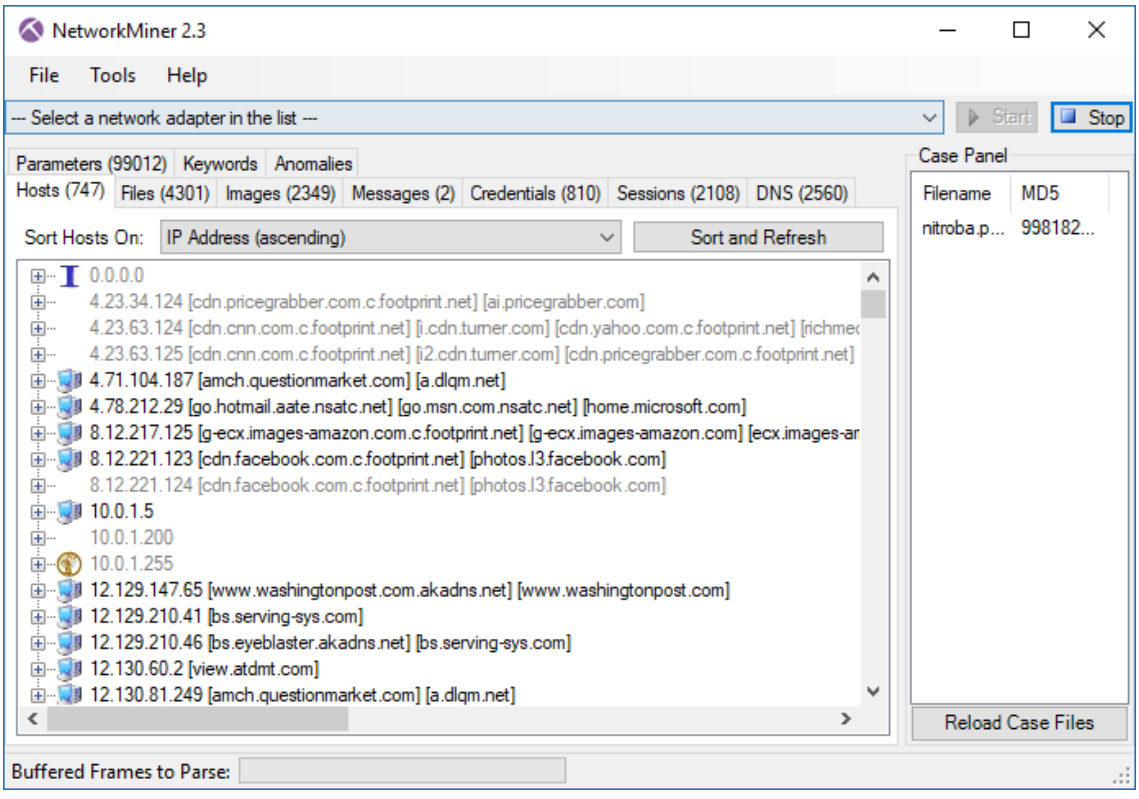
CS 5332 Digital Forensics
Texas Tech University Spring 2018

Individual Assignment 3
Nitroba University Harassment Scenario

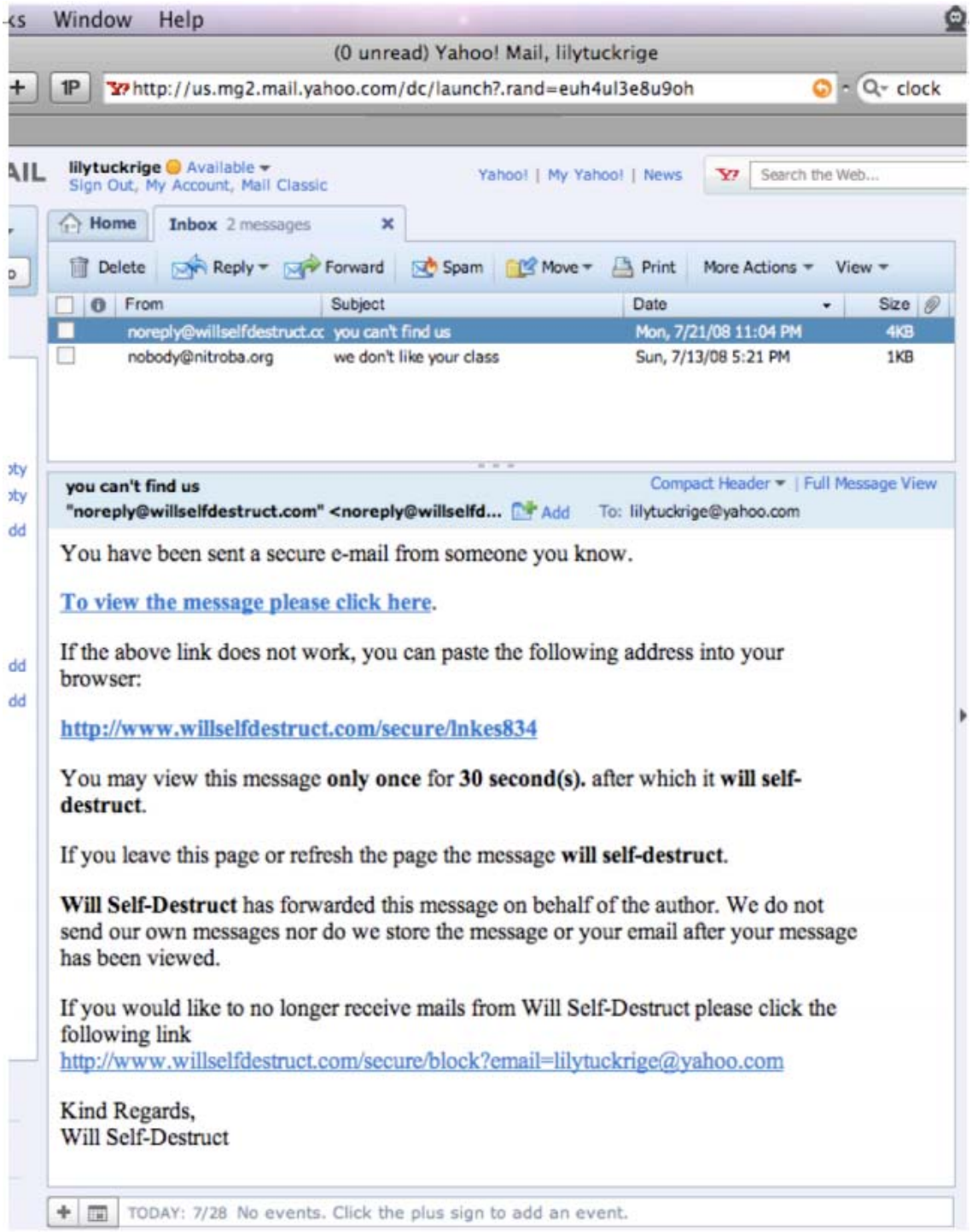
[redacted]

You have been given the screen shots, the packets that were collected from the Ethernet tap, and the Chem 109 roster. Your job is to determine if one of the students in the class was responsible for the harassing email and to provide clear, conclusive evidence to support your conclusion.

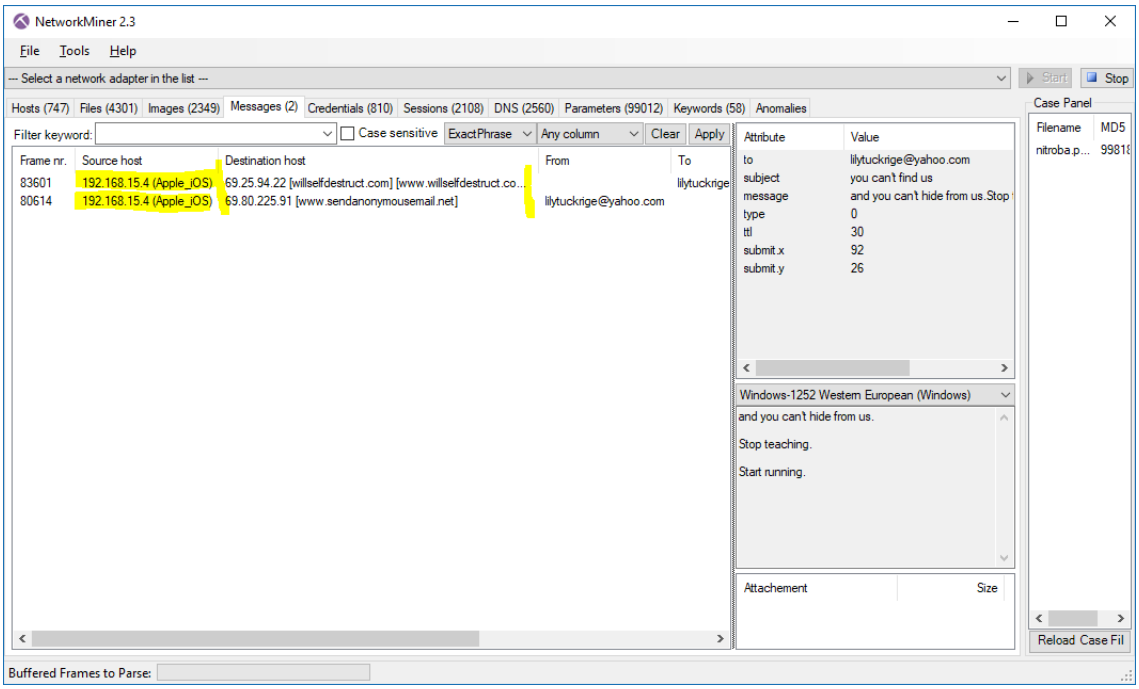
To find the student who responsible for harassment. I opened the pcap file with NetworkMiner (http://www.netresec.com/?page=NetworkMiner)



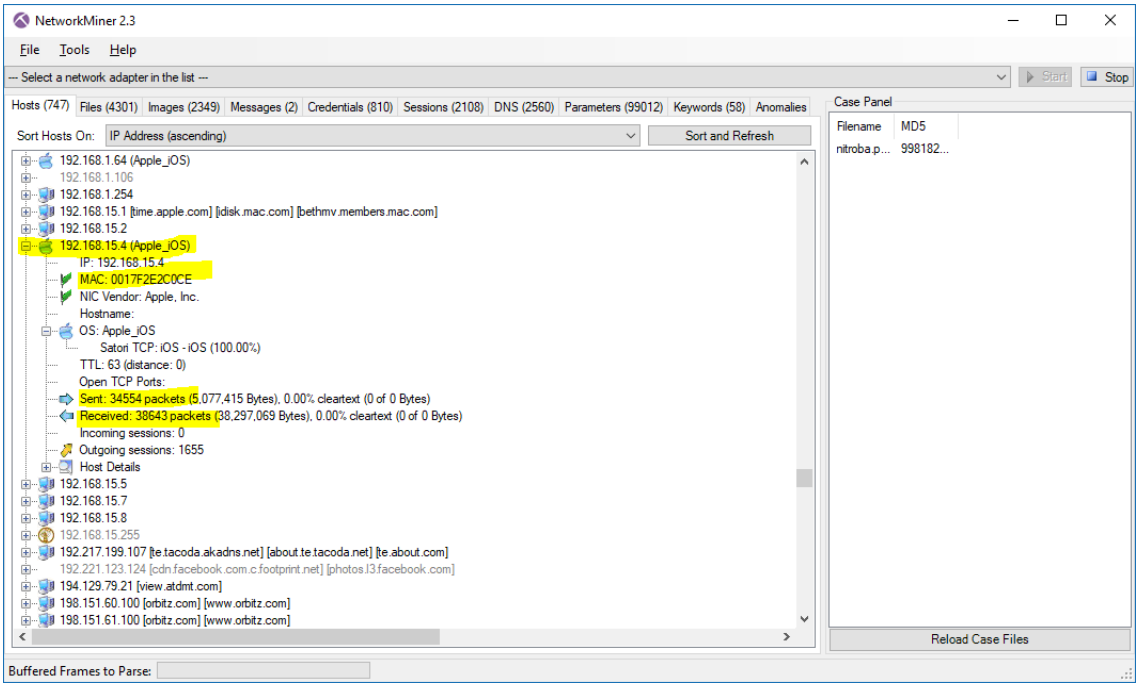
There are a lot of packets in the pcap file but first we need to find the captured harassing email.



NetworkMiner can capture two messages that send from ip 192.168.15.4 (Apple_iOS) to two website that provide message self destruct and anonymous email services.

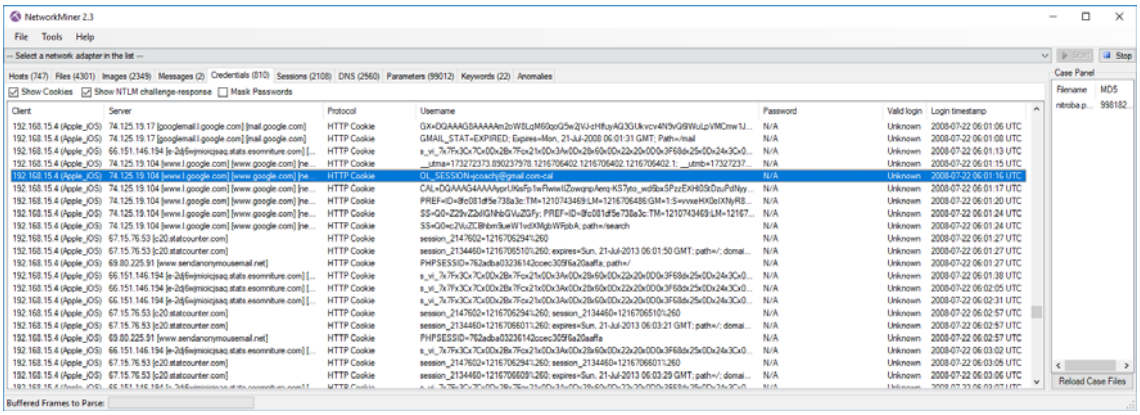


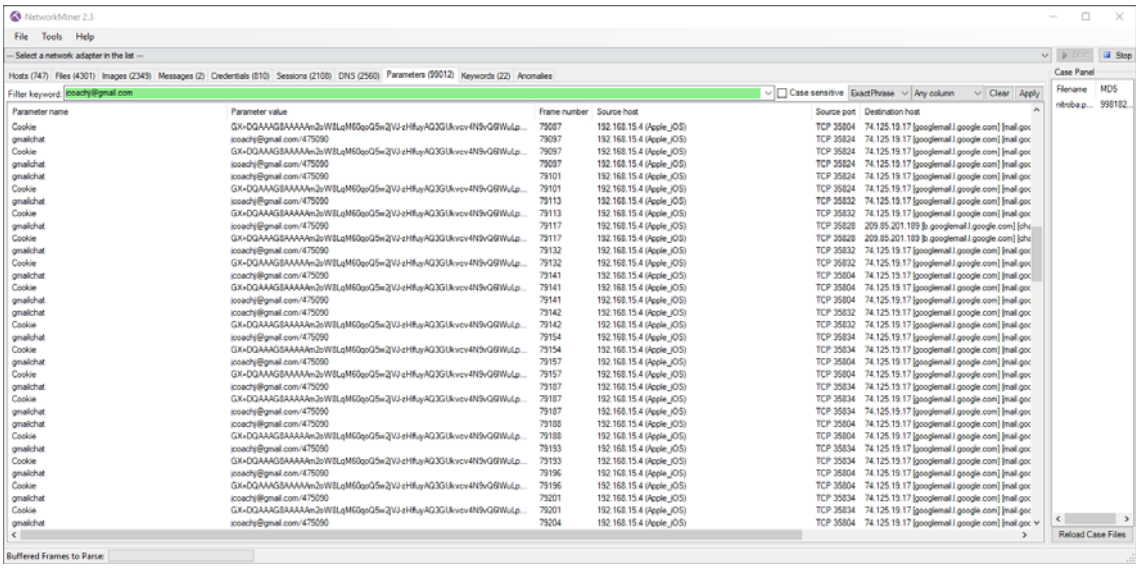
We want to know who own this devices so look for information about this and we found the MAC address 0017F2E2C0CE of this devices and some other informations.



The problem now is to identify the owner of this device. The easiest way is to find the physical Apple IOS device and see who is the owner. However to find this information from the pcap file I putted every students' name into Keyword search and try to find who is the one related to this device.

On the credentials, NetworkMiner capture the email jcoachj@gmail.com credentail from the device 192.168.15.4 (Apple_iOS) and when searching this email on the Parameters the result shows a lot of parameters relating email jcoachj@gmail.com with device ip 192.168.15.4 (Apple_iOS)





My conclusion is the owner of the device with ip 192.168.15.4 (Apple_iOS) is the owner of jcoachj@gmail.com which points to **Johnny Coach** who take Chemistry 109.