|  |  |
| --- | --- |
| C:\user-pjpf\Briefcase-SO\so\so-12-13\slides\logo-IST-Tecnico.JPG | INSTITUTO SUPERIOR TÉCNICO  Departamento de Engenharia Informática  Forensics Cyber Security  MEIC / METI 2017-2018 – 1st Semester |

Digital Forensics Report

**Luís Aguiar 80950 & Jorge Pereira 81428 & Filipe Azevedo 82468**

**Index**

[1 Objectives of the investigation 1](#_Toc500589648)

[2 Artifacts for analysis 1](#_Toc500589649)

[3 Evidence to look for 1](#_Toc500589650)

[4 Examination details 2](#_Toc500589651)

[5 Analysis results 5](#_Toc500589652)

[6 Conclusions 5](#_Toc500589653)

# Objectives of the investigation

This report aims to spell out the entire forensic investigation process in the case of the Harassment at Nitroba University. In this case, a teacher in the Chemistry Department, named Lily Tuckrige, has been receiving harassing emails and she suspects that they are being sent by a student in her class Chemistry 109 (CHEM109). After figuring out the dorm from which the emails were being sent, and after obtaining proper legal approval, Nitroba University decides to place a network sniffer on the ethernet tap of that dorm. The objective of the investigation is to figure out if it was one of the students in the class who sent the harassing emails, while providing clear, definite evidence to support our conclusions.

# Artifacts for analysis

We were given screenshots of one of the harassing emails (the *willselfdestruct* email), the list of students from the Chemistry 109 class, and the trace file of the packets that were collected from the network sniffer.

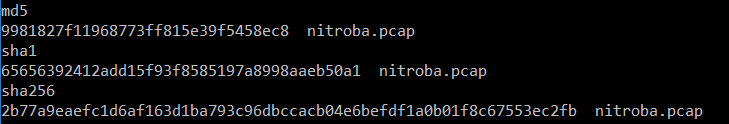
We calculated the hash values for the *nitroba.pcap* (the trace file of the packets) to verify that the file was not changed before it was delivered to us.

Figure 1 - Hash values of the nitroba.pcap file

# Evidence to look for

After having verified the integrity of the files, we started examining the *nitroba.pcap* file, containing the packets collected from the sniffer, using a tool called **Wireshark**, to try and find the packet containing the harassing message that was sent to Lily Tuckrige. We hoped that by analyzing that packet (and others that could appear to be sent by the same person) we would be able to retrieve enough information to draw definite conclusion regarding the author of the emails.

# Examination details

As was said before, we started by analyzing the *nitroba.pcap* file using **Wireshark**. However, since we were having difficulties finding the desired packet (the one with the *willselfdestruct* email) we tried examining the same file but with another tool called **NetworkMiner**.

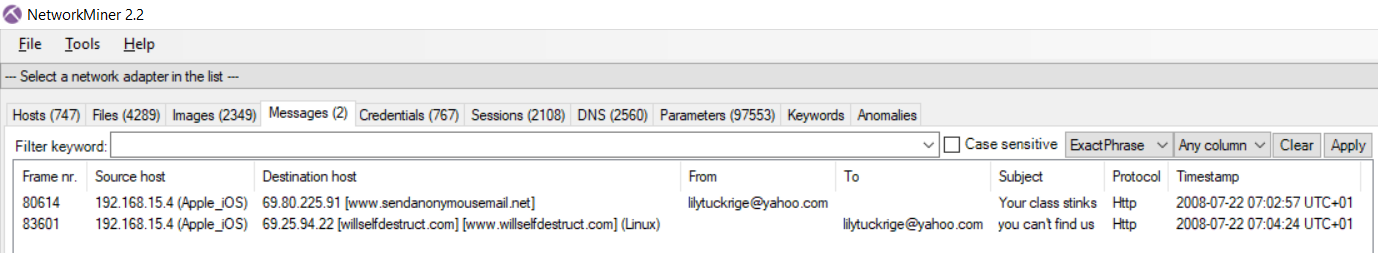
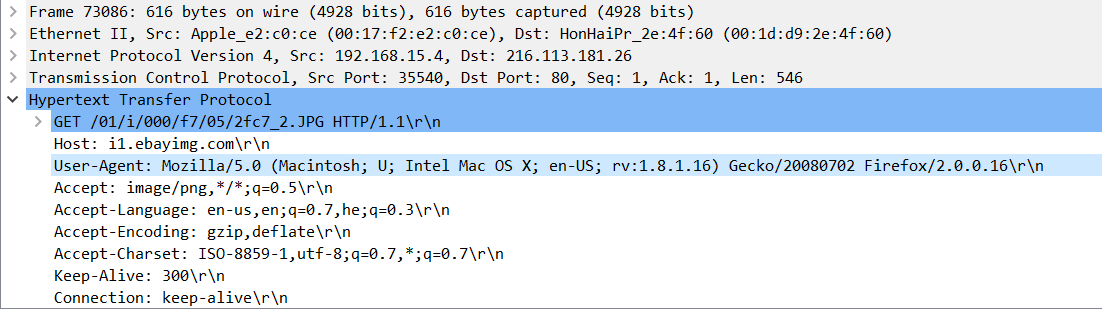
In the **NetworkMiner** tool, we went to the ‘Messages’ tab and it was there that we found 2 messages: one using the site *sendanonymousemail.net*, not mentioned in the assignment, and the email sent using the *willselfdestruct.com* website.

Figure 2 - Messages found in the NetworkMiner tool

With this new information, we were able to figure out the IP address from which these two messages were sent: 192.168.15.4, by looking at the ‘Source host’ field. But since the packet sniffer is in a local area network, any device inside that network could have that IP address at any point in time, provided it is not already taken by some other device. With this in mind, we needed to find more information to link a culprit to the device that had the IP address 192.168.15.4 at the time the harassing emails were sent.

We turned again to Wireshark to examine the packets that contained the IP address 192.168.15.4 as its source IP. Here we performed a technique called Device Fingerprinting, which consists in collecting information about a device by looking at the information sent in the network packets, to check if the IP address in question was used by one or several devices. Just by analyzing the ‘User-Agent’ field of the ‘HTTP’ protocol on some packets in Wireshark we found at least 2 different devices that at one point in time used the 192.168.15.4 IP address: one being a Macintosh computer running Mac OS X as its operating system, and a PC running Windows XP.

Figure 3 - The ‘User-Agent’ field highlighted, showing that the device is a Macintosh computer, running Mac OS X operating system, among other useful information.



However, since these conclusions were just made by us looking through some of the packet and we wanted to be sure that we were on the right track, we used a tool called **p0f** that performs the Device Fingerprinting technique on packets.

After taking a look at all the packets with ‘HTTP’ protocol that contained the IP address of the harassing emails as its source IP, we found 13 different ‘User-Agent’ fields. However, after further analyzing the ‘User-Agent’ field with the help of the p0f tool, only 2 of the devices were running Windows operating systems, both being Windows XP (since both have the ‘Windows NT 5.1’ token).

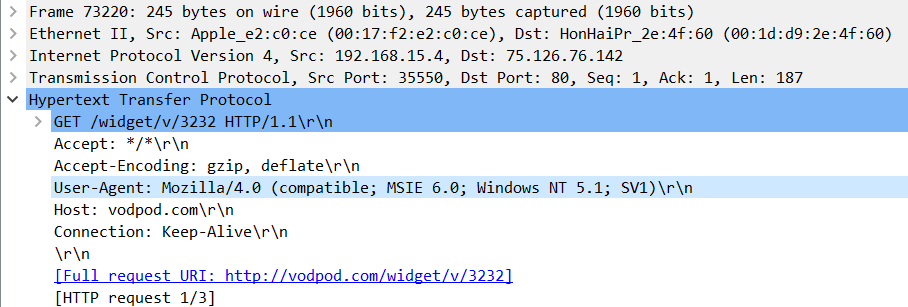
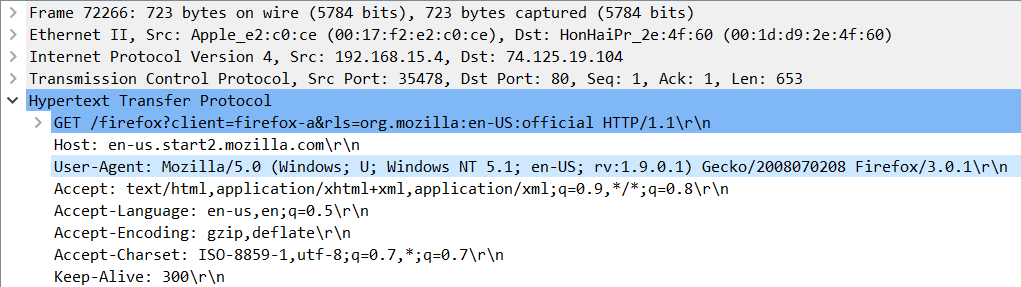


Figure 5 - Second Windows device using the web browser Mozilla/5.0

Figure 4 - First Windows device using the web browser Mozilla/4.0

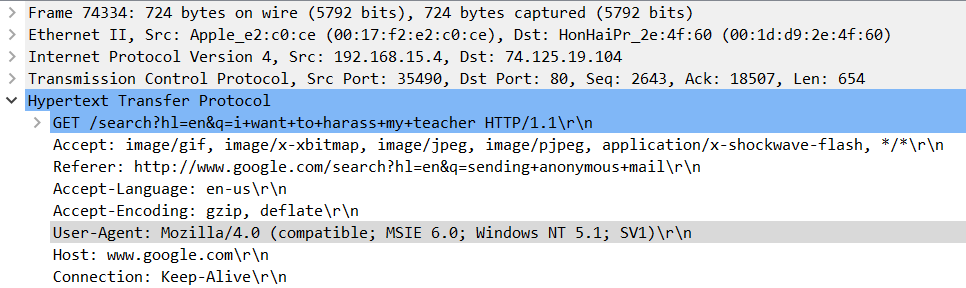
Despite there being 2 devices running Windows in the time frame given, one of them used the web browser Mozilla/4.0 and the other used Mozilla/5.0. This does not mean that the devices are necessarily different, but there’s a good chance that that is the case. In addition to this, the device that sent the 2 harassing emails found with the **NetworkMiner** tool, had the same ‘User-Agent’ filed as the first Windows device listed above. We were also able to find a google search connected to this device with the keywords “I want to harass my teacher”, and a yahoo search with the keywords “can I go to jail for harassing my teacher”.

Figure 6 - The frame containing the "i want to harass my teacher" search

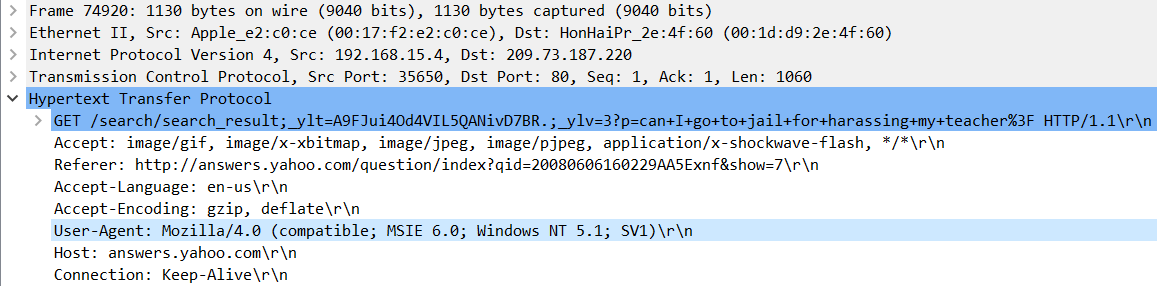


Figure 7 - The frame containing the "can i go to jail for harassing my teacher" search

With all this new information, we only needed to find some sort of personal information in the packets sent or received by this device to identify the author of the harassing emails.

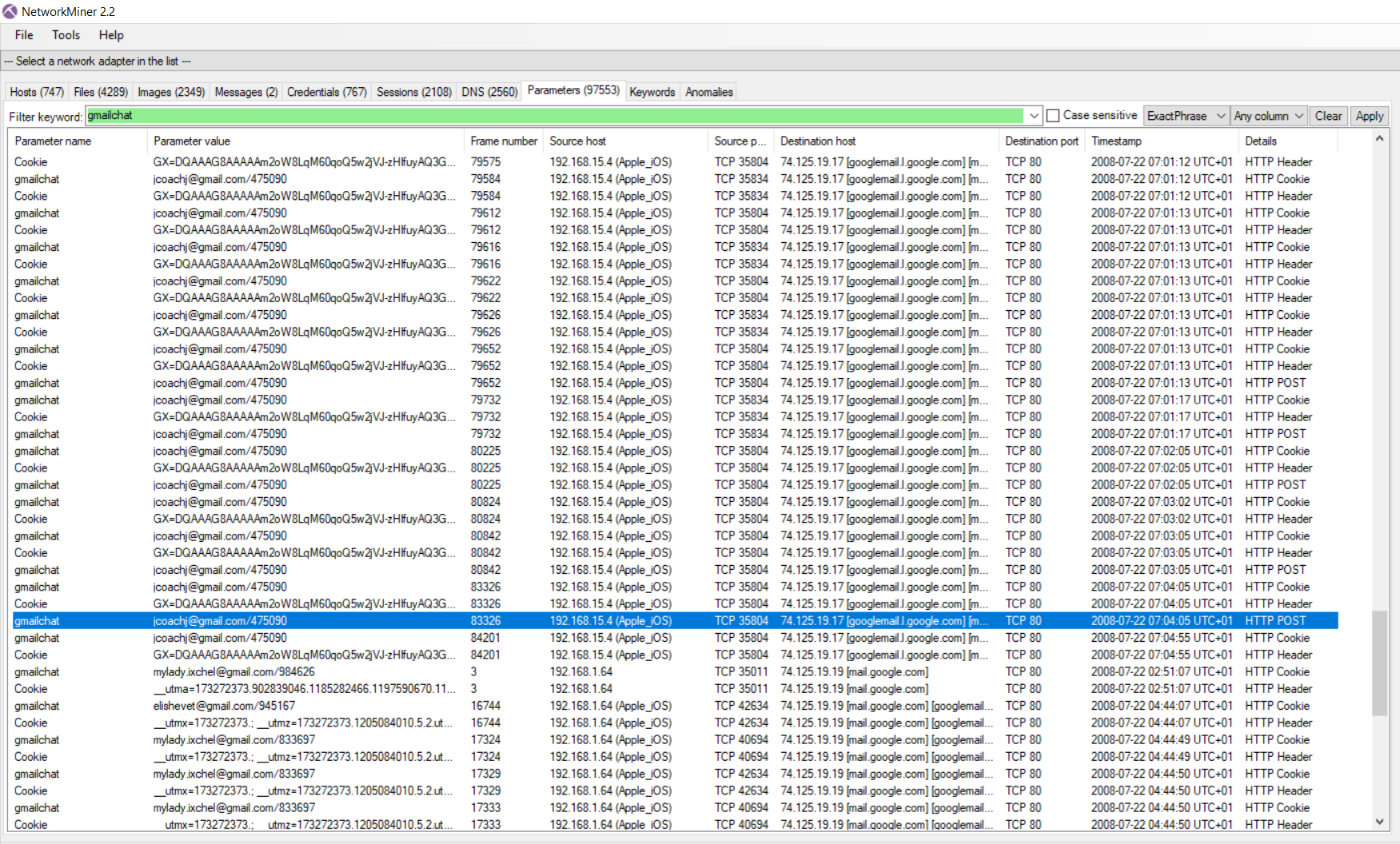
We started to look for information about social media websites and ways to extract usernames from said sites’ packets. We tried to look at *Facebook*, *Yahoo* and *Amazon* packets, before we actually found some useful information regarding G*mail*. Apparently, there is a cookie parameter used by *Gmail,* called *gmailchat*, that is allowed to be sent across an unencrypted ‘HTTP’ session that displays the email of the user. With this information we went over to the ‘Parameters’ tab in the **NetworkMiner** tool and searched for the keyword *gmailchat*:

Figure 8 - Results of the search on NetworkMiner

As can be seen in the screenshot, someone with the IP address 192.168.15.4 used *gmail* with the email ‘jcoachj@gmail.com’, just seconds before and after the *willselfdestruct* and the *sendanonymousemail.net* emails were sent (the timestamp of the *sendanonymousemail.net* email is 2008-07-22 07:02:57 UTC+1, as can be seen in Figure 2).

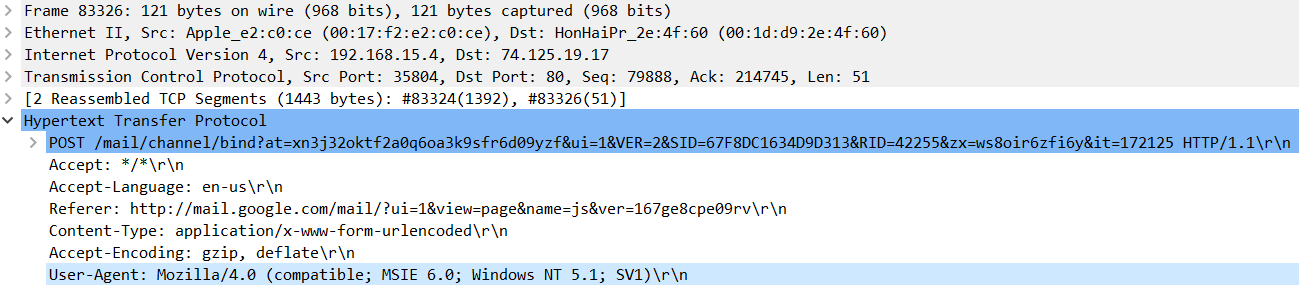
If we go to **Wireshark** and search these packets we find that they have the same fingerprint as the packets that sent the harassing emails:

Figure 9 - One of the packets that contained the gmailchat cookie

This means that the same device was used to access *gmail* and sending the harassing emails!

# Analysis results

After having found all this evidence, the person who used *gmail* with the account ‘jcoachj@gmail.com’ at that time was most likely the culprit of this crime. However, there is no way to be absolutely sure unless there is visual evidence. Maybe the person that accessed *gmail* left his computer unattended for just 30 seconds and that was enough for the culprit to send the emails. This is unlikely, since there is 2 different messages in an interval of 2 minutes, but still possible. And what if the culprit stole the username and password and logged into *gmail* to frame the legitimate owner of that email address. It’s just no possible to be completely sure of who the author of the harassing emails is.

Since we never found out the true owner of the ‘jcoachj@gmail.com’, despite the name implying it belongs to Johnny Coach, a student of Lily Tuckrige and a student of the Chemistry 109 class, this may be something to be investigated further, in collaboration with the Nitroba University.

# Conclusions

As was said before, it’s not possible to find clear and definite evidence of who sent the harassing emails without having visual evidence by the reasons stated in the previous sections.

15th December 2017, Instituto Superior Técnico

Luís Aguiar - 80950

Jorge Pereira - 81428

Filipe Azevedo - 82468