INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment IV

Harassment at Nitroba University

2017/2018

{danielporto, nuno.m.santos}@tecnico.ulisboa.pt

Introduction

In this guide, you need to solve a case, which is entitled "Harassment at Nitroba University". This exercise will help you gain hands-on experience on network forensics and requires the examination of a network trace. The trace file can be obtained from the zip file `csf-lab4-artifacts.zip`, available in the course website. To analyze these artifacts, we recommend you to use the Kali Linux distribution.

Context

You are a security administrator at the prestigious (and fictional) Nitroba State University. Nitroba's IT department received an email from Lily Tuckrige, a teacher in the Chemistry Department. Tuckrige has been receiving harassing emails and she suspects that they are being sent by a student in her class Chemistry 109 (CHEM109), which she is teaching this summer. The email was received at Tuckridge's personal email account, `lilytuckrige@yahoo.com`. She took a screenshot of the web browser and sent it in (see Figure 1). She wants to know who is doing it.

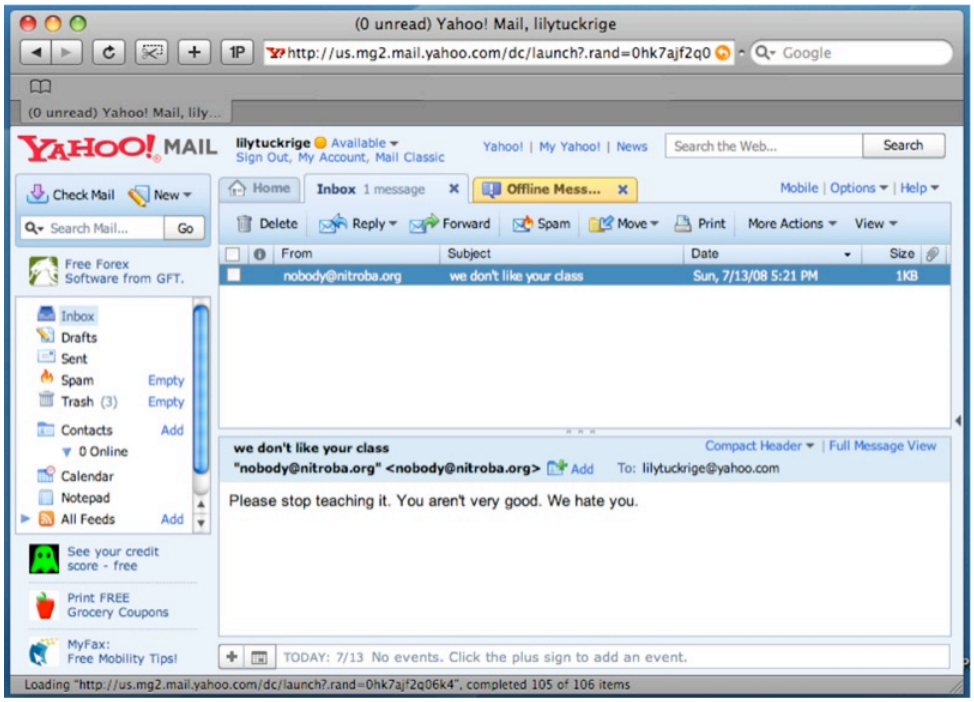

Figure 1: Screenshot of Tuckrige's web browser.

The system administrator who received the complaint wrote back to Tuckridge that Nitroba needed the full headers of the email message. Tuckridge responded by clicking the "Full message headers" button in Yahoo Mail and sent in another screenshot, this one with mail headers. Figure 2 shows the screenshot. The mail header shows that the mail message originated from the IP address 140.247.62.34, which is a Nitroba student dorm room:

```
$ host 140.247.62.34
34.62.247.140.in-addr.arpa domain name pointer G24.student.nitroba.org
```

Three women share the dorm room: Alice, Barbara, and Candice. Nitroba provides a 10mbps Ethernet connection in every dorm room but not Wi-Fi access, so Barbara's boyfriend Kenny installed a Wi-Fi router in the room. There is no password on the Wi-Fi.

Because several email messages appear to come from the IP address, after obtaining proper legal approval, Nitroba decides to place a network sniffer on the ethernet port. This new network setup is represented in Figure 3. All of the packets are logged. On Monday 7/21 Tuckridge received another

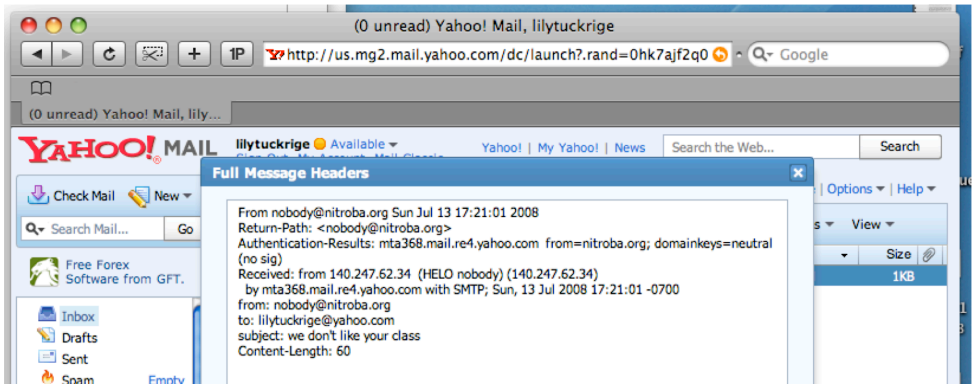

Figure 2: Second screenshot of Tuckrige's web browser revealing the email header.

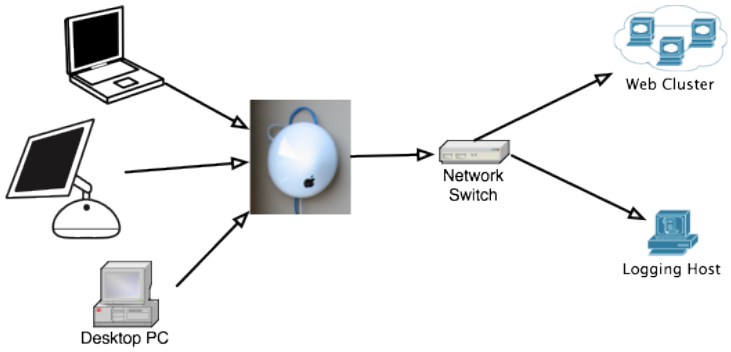

Figure 3: Nitroba's network comprising a packet sniffer (the logging host).

harassing email. But this time instead of receiving it directly, the perpetrator sent it through a web-based service called "willselfdestruct.com". The website briefly shows the message to Tuckridge, and then the website reports that the "Message Has Been Destroyed". This scenario takes place in Summer 2008.

You have been given the screenshots, the packets that were collected from the Ethernet tap, and the Chemistry 109 list. The screenshots are depicted in the Appendix. The hash values for *nitroba.pcap*, i.e., the file containing the collected network traces are:

Algorithm	**Value**
MD5	`9981827f11968773ff815e39f5458ec8`
SHA1	`65656392412add15f93f8585197a8998aaeb50a1`
SHA256	`2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb`

The Chemistry 109 class list comprises the following individuals:

Teacher	Lily Tuckrige
Students	Amy Smith, Burt Greedom, Tuck Gorge, Ava Book, Johnny Coach, Jeremy Ledvkin, Nancy Colburne, Tamara Perkins, Esther Pringle, Asar Misrad, Jenny Kant

Assignment: Your mission is to determine if one of the students in the class was responsible for the harassing email and to provide clear, definite evidence to support your conclusion.

Deliverables

Write a forensic report that describes your findings. The deadline for this work is December 15^{th}. Until then, you must upload to Fenix a compressed zip file containing two deliverables:

- **Digital Forensic Report**: A document in which you present your main findings according to what was requested in each exercise. You must identify all recovered evidence artifacts, if any, and explain how you obtained them. We suggest that you use the basic template that can be downloaded from the course website for this specific assignment.
- **Evidence Artifacts:** All evidence artifacts recovered during the forensic analysis. Please make sure that the respective file names and MD5 values are indicated in the report.

Good luck!

Appendix: Screenshots of self-destruct message

The screenshots below reflect the sequence of events that took place in the presented scenario: notification of incoming email message on the web browser (Figure 4), the content of that message (Figure 5), the harassing message on "willselfdestruct.com" (Figure 6), and the destruction of the message (Figure 7).

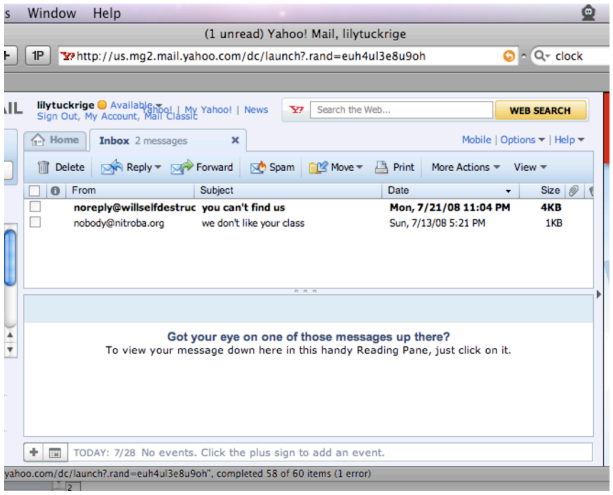

Figure 4: Incoming email message on the web browser.

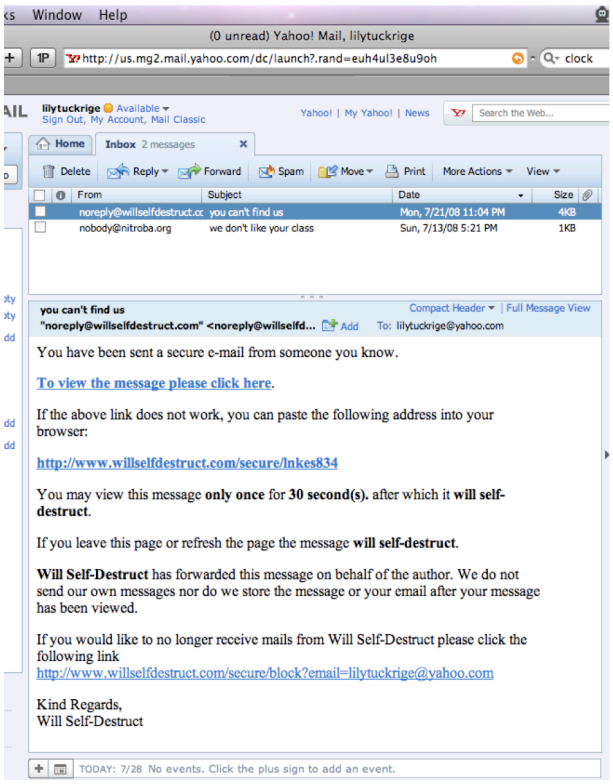

Figure 5: The content of the email message pointing to "willselfdestruct.com".

Figure 6: The original message on "willselfdestruct.com".

Figure 7: Message being destroyed on "willselfdestruct.com".