**Van Linh Ha 116.592.171**

**Lab 8: *Encryption – Data At-Rest & In-Flight* (2%)**

**Overview:**

In this lab we’ll looking at data At-Rest and In-flight. First, you’ll be logging into both unsecured and secured websites to generate unsecured and secured data transmission, which you will capture and analyze. Next, you’ll be creating a plain text file and an encrypted text file and analyze them using a disk forensic tool to see what they look like on disk.

**Objective:**

1. Capturing and analyzing:
   * Unsecured data traffic between a web-browser and a web-server.
   * Encrypted data traffic between a web-browser and a web-server.
   * Encrypted data traffic between a SSH client and a SSH-server.
2. Analyzing an:
   * Unencrypted text file using a forensic tool.
   * Encrypted file storing an unencrypted file using a forensic tool.

**The Lab Activities**

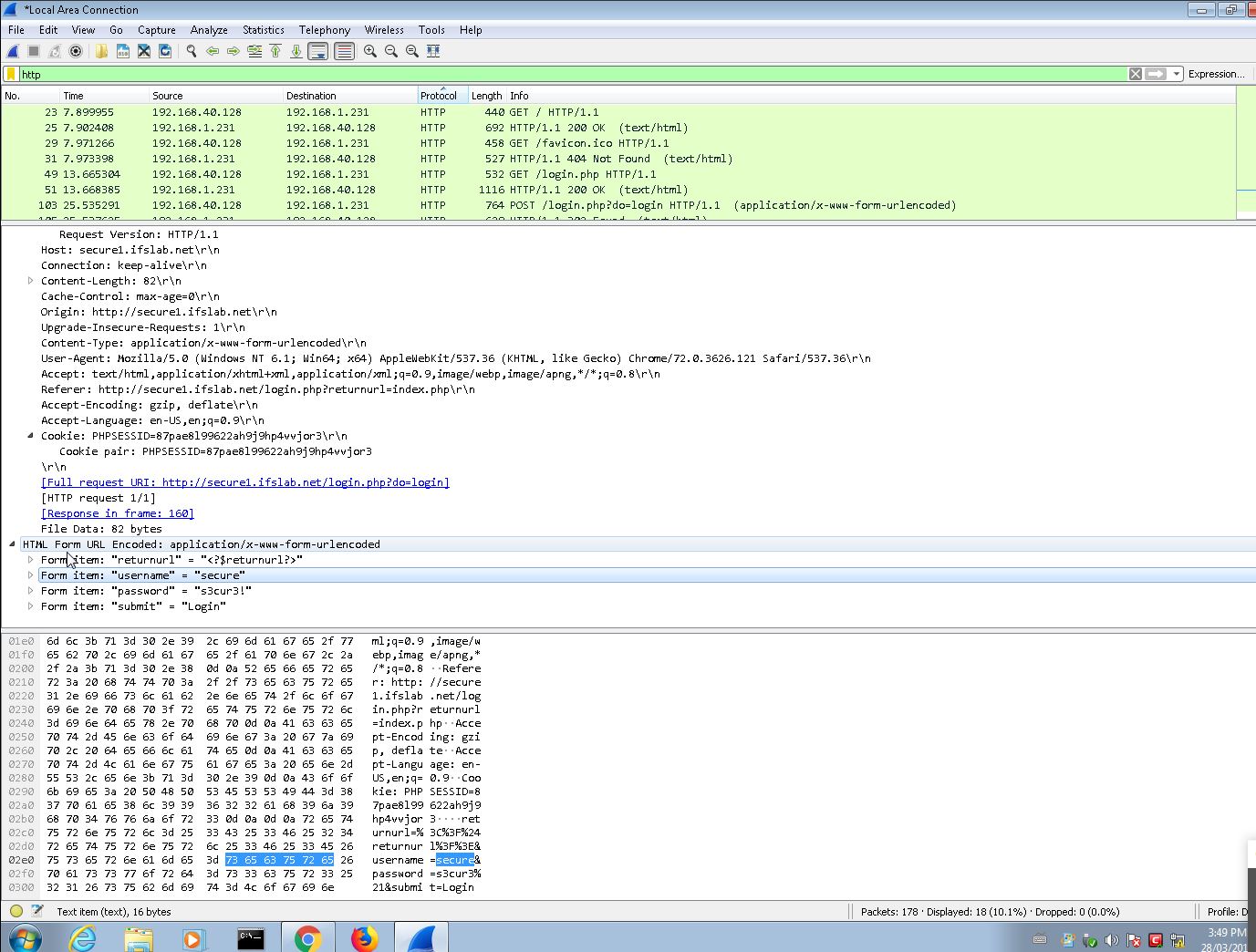
**NOTE**: The sections highlighted in:

* green do not require IFS Lab or VM Workstation Pro & Windows 7
* yellow require VM Workstation Pro & Windows 7
* red require the IFS Lab

**In-flight**

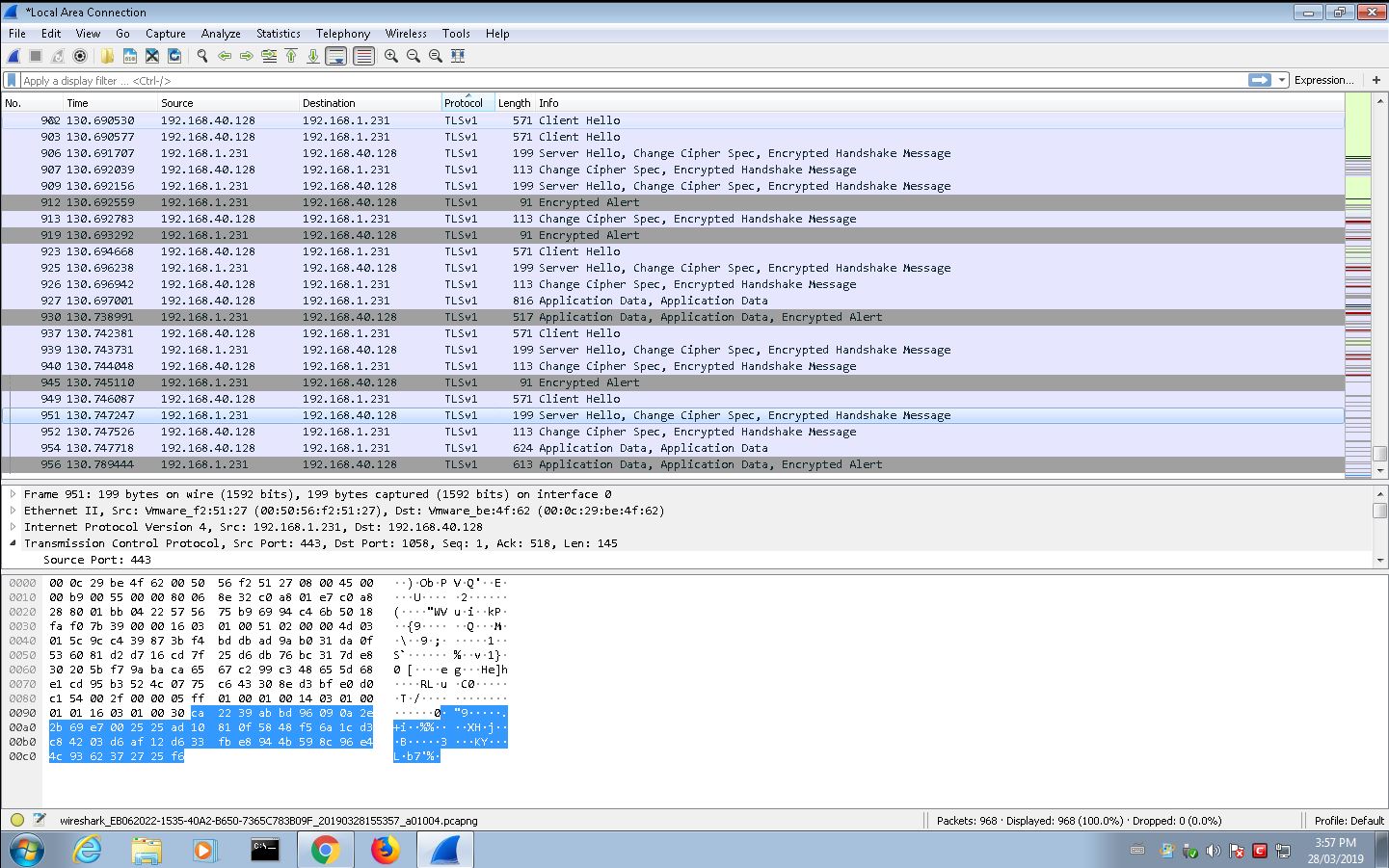
We will look at data ‘In Flight’. That is, looking at data being transmitted across a network. We’ll be seeing the difference between unsecured (plain text) and encryption data as it transferred from your browser to a webserver. Also, we will be looking at communication between the SSH client and an SSH server. To view this traffic you’ll be using a tool called *Wireshark* that was pre-installed on your VM.

**Part 1: Unsecured HTTP Communication**



**Part 2: Secured TLS/SSL Communication**

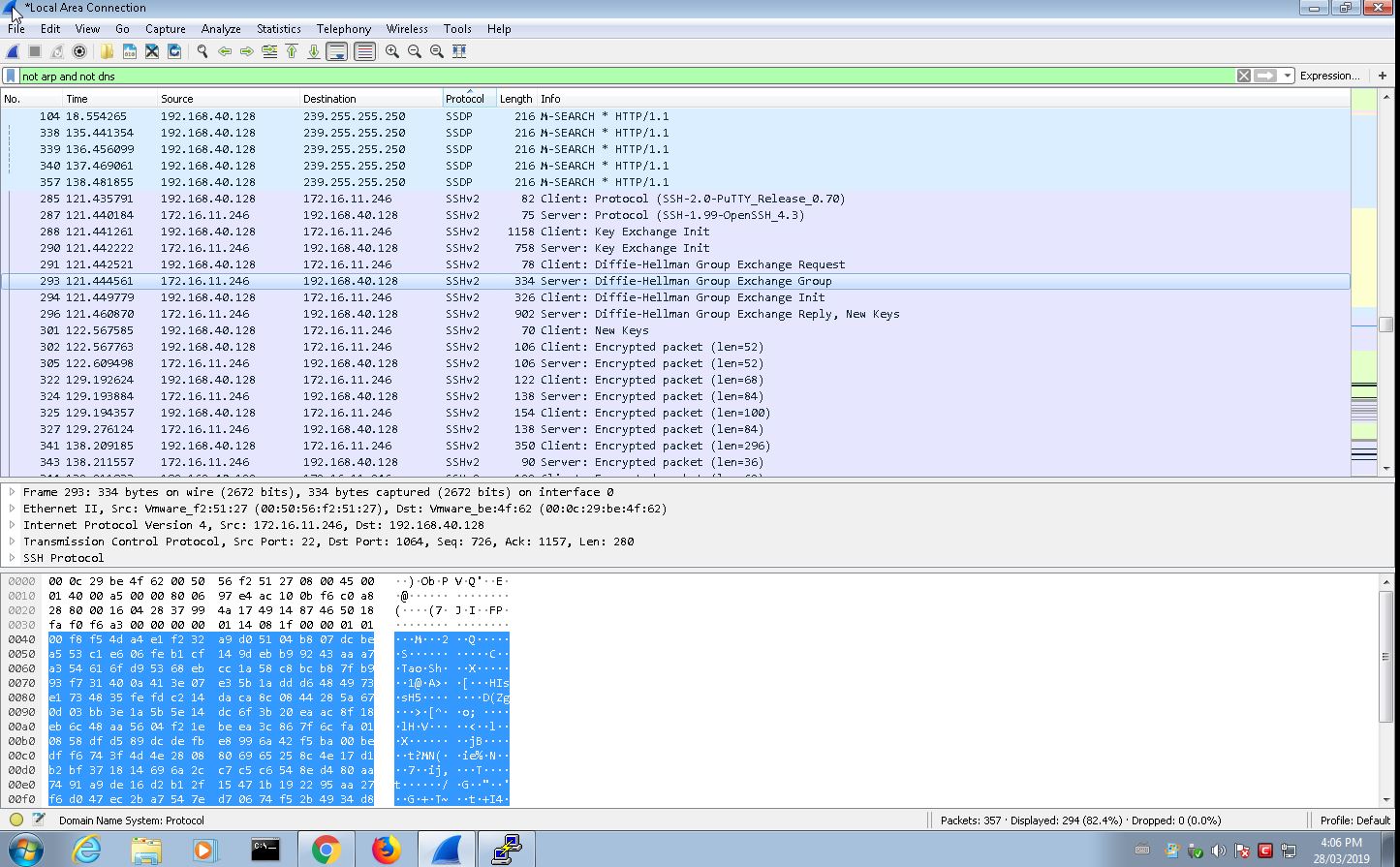
This is a repeat of the above, though you will be logging into a website that has security. Again, you’ll be using Wireshark to look at the TLS/SSL traffic between your browser and the website.



**Part 3: Secured SSH Communication**

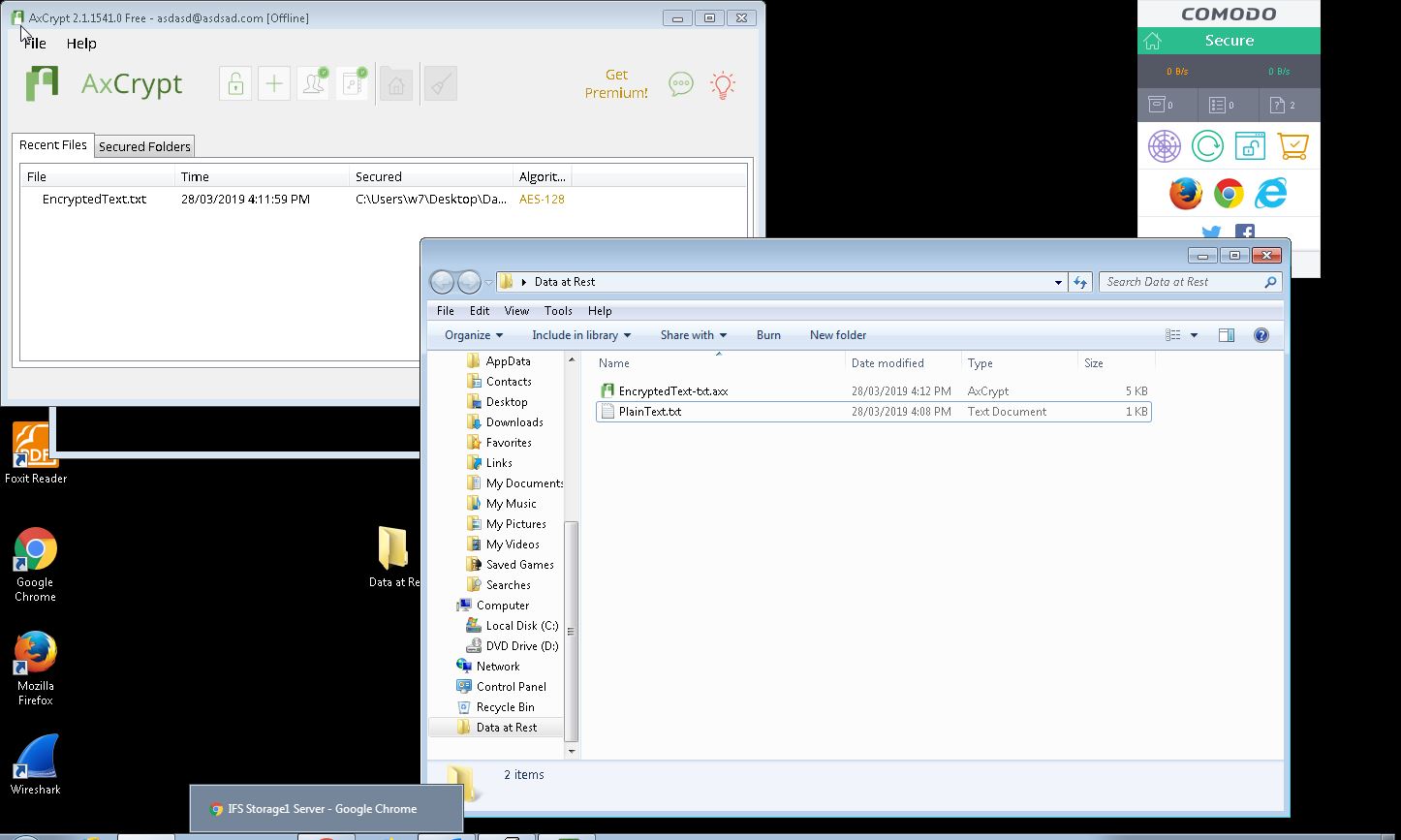
This is a repeat of the above, though you will be using the *PuTTY* Secure Shell (SSH) client to connect to an SSH server. Again, you’ll be using Wireshark to look at the traffic between your SSH client and the server.

1. Save the file as <<MySenecaUsername>>\_SecuredSSHCommunication.jpeg and insert it into your report under the heading “**Secured SSH Communication**”.



**At Rest**

In this section we’ll be looking at data ‘at rest’. That is, looking at data sitting on storage media. We’ll be literally seeing the difference between unsecured data (plain text) and encrypted data as it resides at rest.



**Part 5: Secured Text**

Now that we have the files created, we can now look at the files using a forensics tool called *Autopsy*. This tool is used later in IFS Program for the forensics course.

1. You ‘ll notice you can easily see the contents of your text file.

