Project MITM/PCAP

## Learning Goals of this Project:

Students will get familiar with packet capture (PCAP) reading and some common man in the middle techniques. This is where a malicious user puts themselves in the middle of the conversation with another user or application and eavesdrops on all the traffic. Some papers which demonstrate this concept are the following:

* [Man-In-The-Middle Attack in Wireless and Computer Networking- A review](https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8344724)
* [Detection of man-in-the-middle attacks using physical layer wireless security techniques](https://dl.acm.org/doi/abs/10.1002/wcm.2527)
* [On the Feasibility of Large-Scale Infections of iOS Devices](https://wenke.gtisc.gatech.edu/papers/iworm.pdf)

Students will familiarize themselves with Layer 2 - 7 network traffic and how to analyze network traffic using Wireshark, a network protocol analyzer, and its libraries such as pyShark.

* For more details about Wireshark you can visit <https://www.wireshark.org>
* For details about pyShark and tshark you can visit <http://kiminewt.github.io/pyshark/>

Students will also familiarize themselves with application layer protocols such as HTTP and IRC.

* If you are not familiar with HTTP, we strongly recommend you learn about the protocol, methods, and requests. You can find a good introduction at [Mozilla's developer page](https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview) and [Sam Barros’ Medium page](https://medium.com/swlh/http-an-overview-of-web-development-4f6033efb9da)
* IRC was a very common protocol in the early 2000s. For its simplicity and efficiency it's still in use on multiple settings. Several Botnets use it for Command and Control (C&C) and hacking groups still rely on IRC to exchange information. You can read more and get familiar by reading [this Medium article](https://medium.com/the-complete-guide-for-irc-network-i-e-freenode/irc-introduction-and-its-main-ingredients-982cd3639a67).

Finally, this is a graduate course. So it is expected that students will research and understand how these network protocols work by reviewing their RFCs:

* RFC1459 (Internet Relay Chat Protocol): <https://datatracker.ietf.org/doc/html/rfc1459>
* RFC2616 (Hypertext Transfer Protocol): <https://datatracker.ietf.org/doc/html/rfc2616>

## The final deliverables:

A single json formatted file will be submitted to Gradescope. This file should be named ***project\_mitmpcap.json.*** A template can be found below **please See** [**Submission Details**](#4nmxs2gzqmyh) **for more information**

## 

## Important Reference Material :

* Read the RFCs provided.
* [Official Wireshark Guide](https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html)
* If you have no experience with networking or application layer protocols, we STRONGLY encourage you to research those topics. There are many great resources online like Google and YouTube.

### **Submission**

**Gradescope (autograded) - see** [**Submission Details**](#4nmxs2gzqmyh)

### 

### **Requirements**

Wireshark - <https://www.wireshark.org/download.html>

Python3 - [Download Python | Python.org](https://www.python.org/downloads/)

Ensure you have nslookup installed on your OS (DNSUtils) (it should come default on any Windows, MacOS or Linux environment)

### **Packet Capture**

The packet capture can be downloaded at: <https://cs6035.s3.amazonaws.com/mitm_packetcapture_spring_2023.pcap>

**BACKGROUND**

The Necrocryptors (TNC) is a hacking group known for multiple data leaks and has been active at underground forums selling personally-identifiable information (PII) and credit card data stolen from vulnerable websites.

Recently, TNC led a DDoS campaign against multiple targets in the United States, leading to a Federal Investigation by​​ the National Cyber Investigative Joint Task Force (NCIJTF). This investigation was coordinated by the FBI Cyber Crime division and after months of undercover investigation, NCIJTF was able to capture unencrypted communication between members of TNC. While NCIJTF did not disclose how this communication was captured, we can infer that either it came from an insider member of the organization or a sophisticated attack led by NCIJTF allowed this communication to be captured.

In this project, you are playing the role of Mark, an FBI agent from the Cyber Crime division.

You walk into the office, just back from a nice vacation in the Bahamas, and pour some coffee from the shared pot near your cubicle when you hear, "Mark! Great to see you are back! Come over to my desk right now, we need to talk."It's your boss, Bill. You think to yourself, *Geez! I just came back. This guy doesn't give me a break.*

You take your coffee to Bill’s office, close the door and listen as Bill starts.

"Mark, I have a task for you. We finally got our hands on some incriminating evidence against TNC. With this pile of evidence, the Attorney General is on my neck to bring those guys to justice. But we need some strong evidence of criminal activity that can't be disputed in court."

"Okay…" *My wife told me to take some extra days off, but no. I had to come back today…*

"I'm sending the packet your way,” Bill says, “You have one week to analyze the data and find clear evidence of criminal activity. The Attorney General sent us a list of things they are looking for. It's all on your desk."

"Sounds good, boss. It's great to be back."

You leave his desk, take a sip of coffee and go back to your computer. *No time to slowly get up to speed*, you think, *but that’s OK. I’m excited to help take TNC down.*

# Office Setup

Ok, vacation is over. Now it's time to configure your workspace and start the research.

You have two options to complete this assignment:

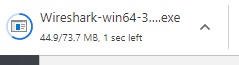
1. Install Wireshark into the VM; or
2. Create your own environment and install any tools needed.

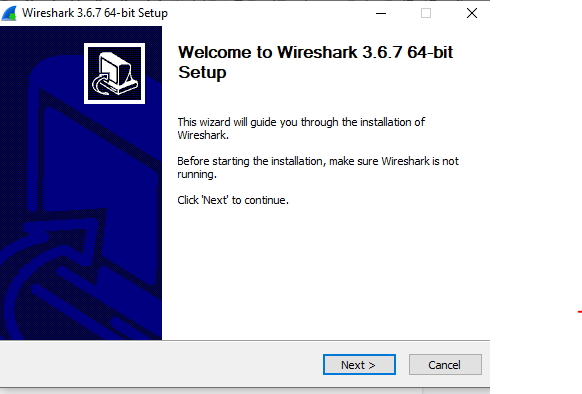
**This project does not require a lot of preparation. Just download wireshark, the provided PCAP file, and start analyzing.**

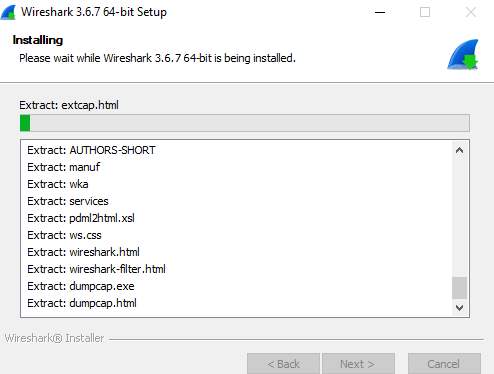
The next few pages will guide you on installing Wireshark on Windows, MacOS and Ubuntu setup.

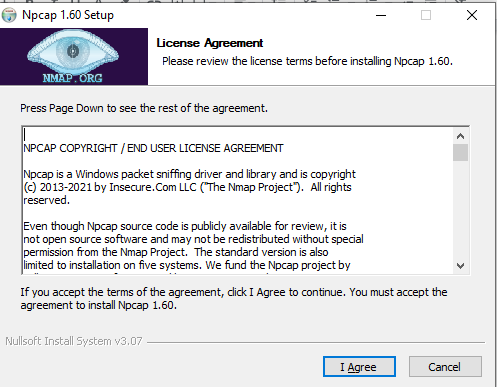
### **Installing Wireshark - Windows** To install Wireshark on Windows, please go to: <https://www.wireshark.org/download.html>. Once there, you will see a page like this:

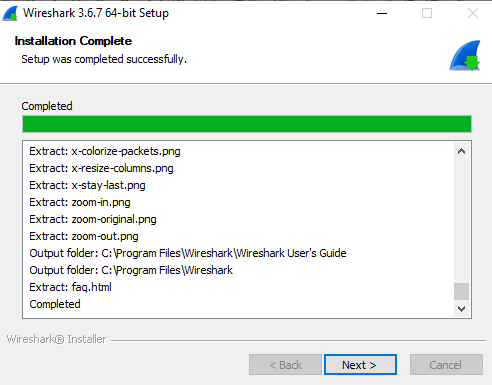
Click the correct Windows Installer (64-bit or 32-bit), depending on your OS.

Here is an example of what the 64 bit option looks like while it’s downloading in the Chrome browser. (It may look different in your browser.)   


After the file finishes downloading, execute it and you will see the following screen:  


Just click "Next >" on each page to install with default settings. Then you will see:   


A new installation window, for Npcap, will then come up. Please continue through this Npcap installation as well to proceed with the Wireshark installation.  


Once the Npcap installation is finished, the Wireshark installation should continue automatically. Once that installation is done, you will see the following:  


Click "Next" then "Finish."

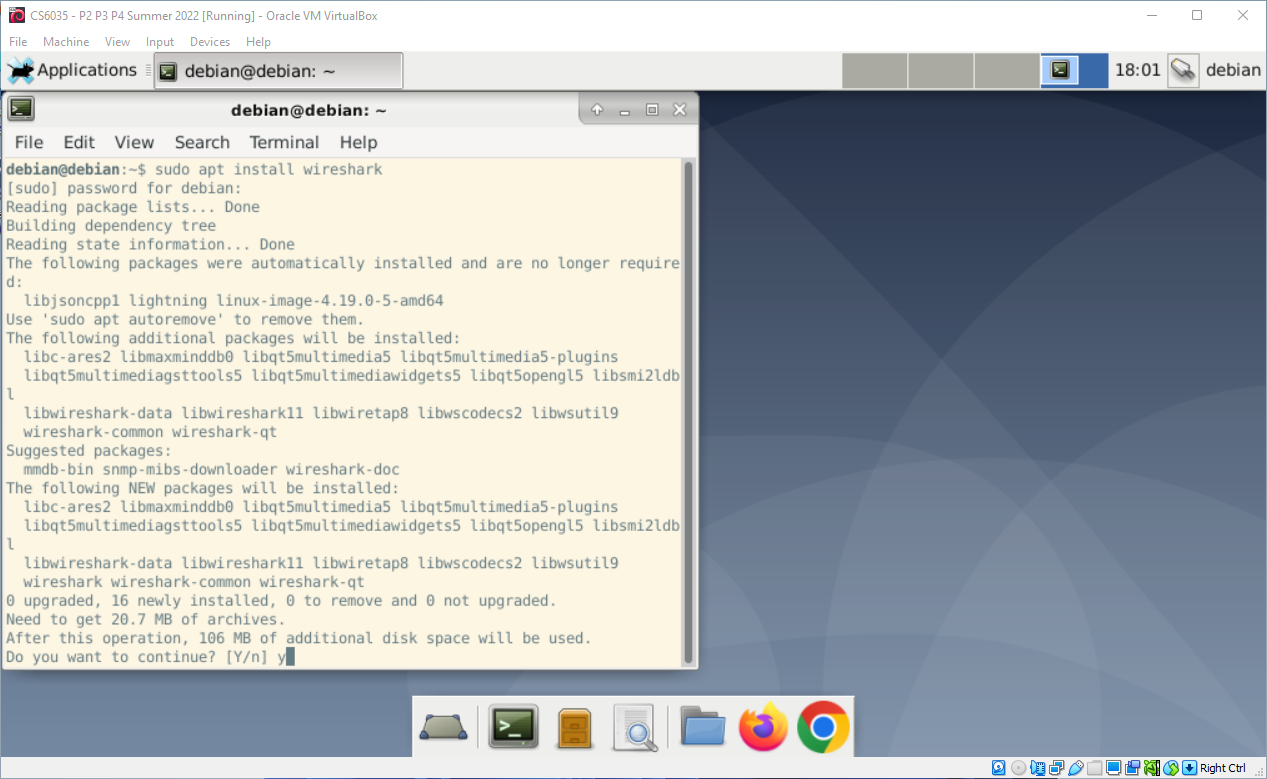
Congratulations! Wireshark is now installed on your computer!

### **Installing Wireshark - Ubuntu**

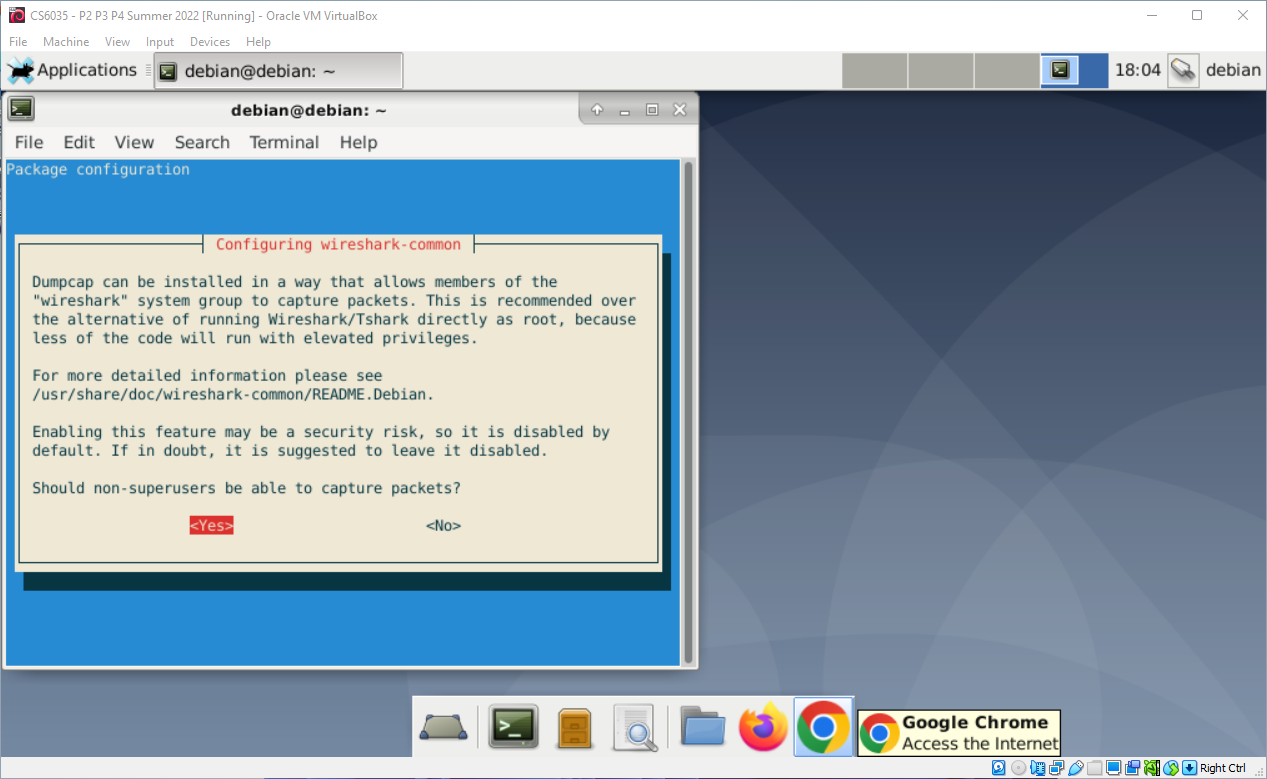
Inside your Linux box, Open Terminal Emulator and run the following command:

| sudo apt install wireshark |
| --- |

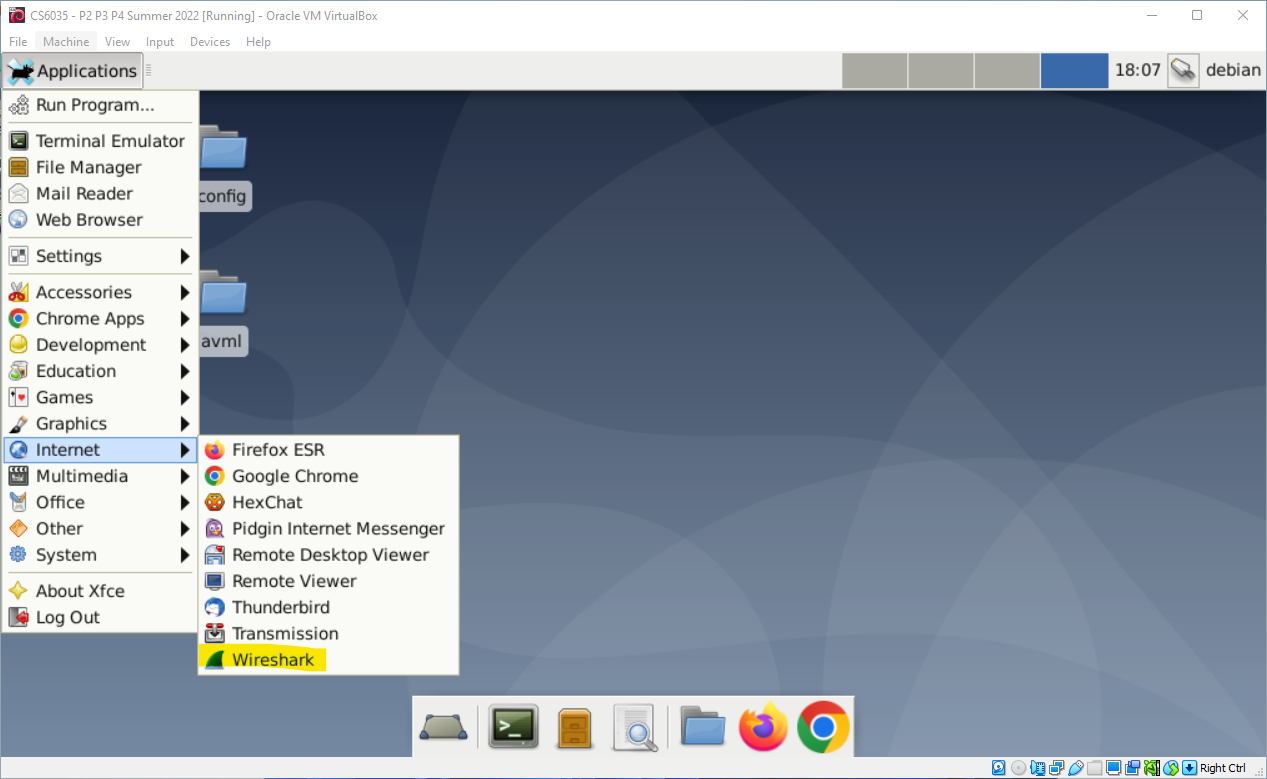
Type in the root password (debian) and "y" to download and install all required packages.



During the installation, if prompted, answer "Yes" for the question: “Should non-superusers be able to capture packets?”



Once the installation is complete, close the Terminal Emulator and locate Wireshark in Applications > Internet > Wireshark:



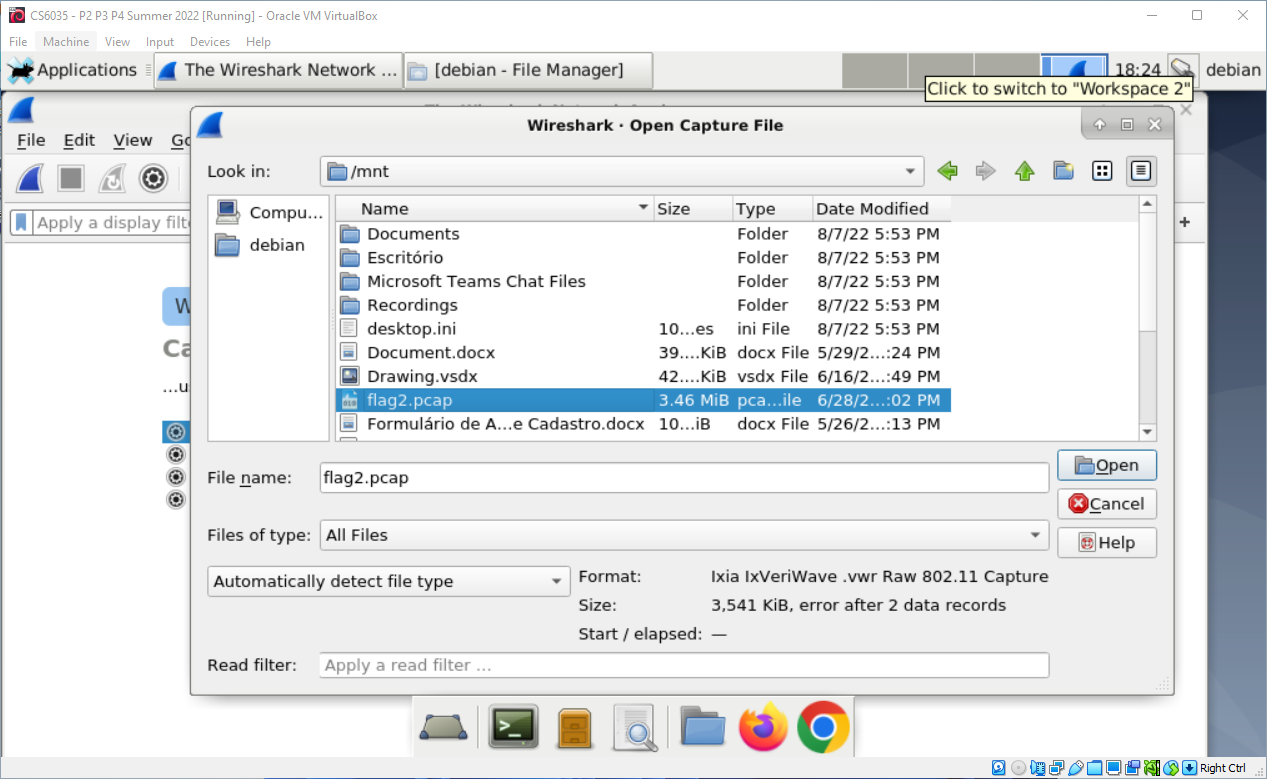
Congratulations! You are all set now!

### **Quick Intro to Wireshark**

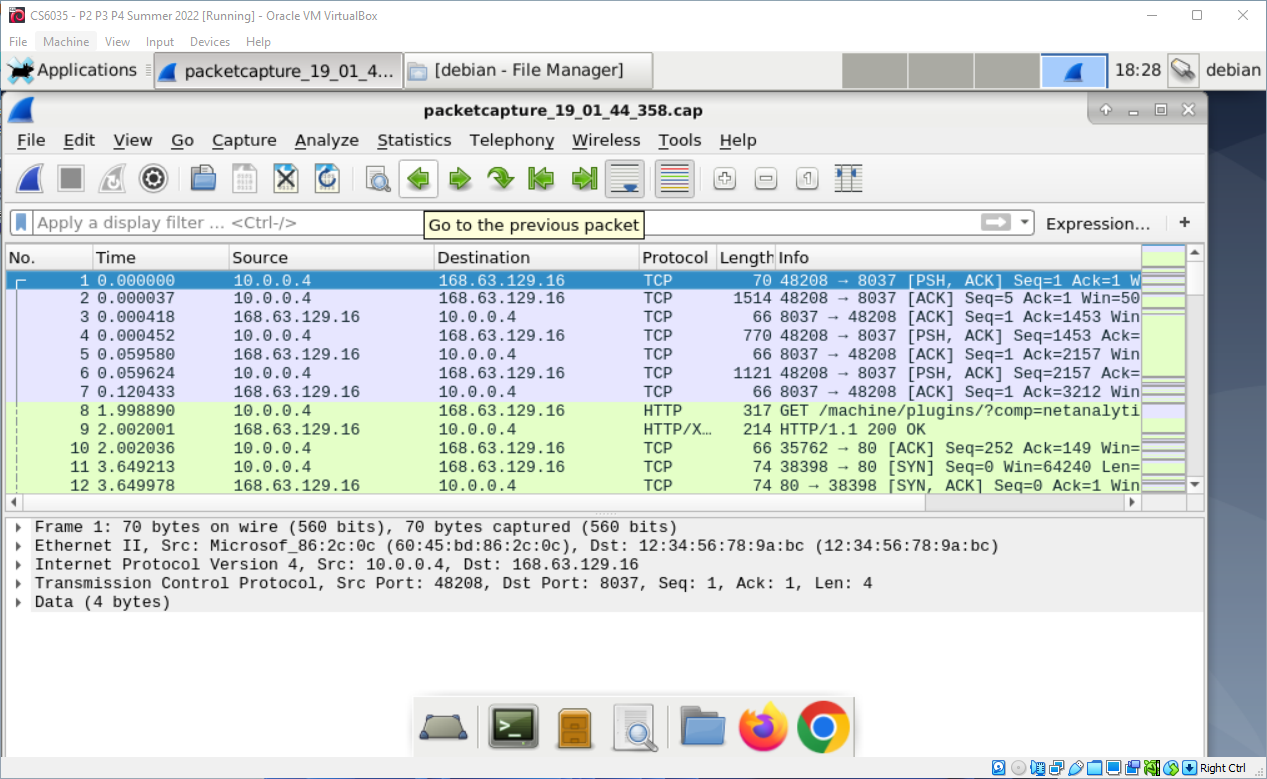
If you’re already familiar with Wireshark, you can skip this section. We will provide a quick introduction to Wireshark and basic functionalities.

When you open Wireshark, you will be asked how you want to set up the packet capture. In our case, we will open a previously recorded PCAP file that contains all captured network traffic.

To open an existing file, go to “File > Open.” Locate the downloaded PCAP file and click “Open”:



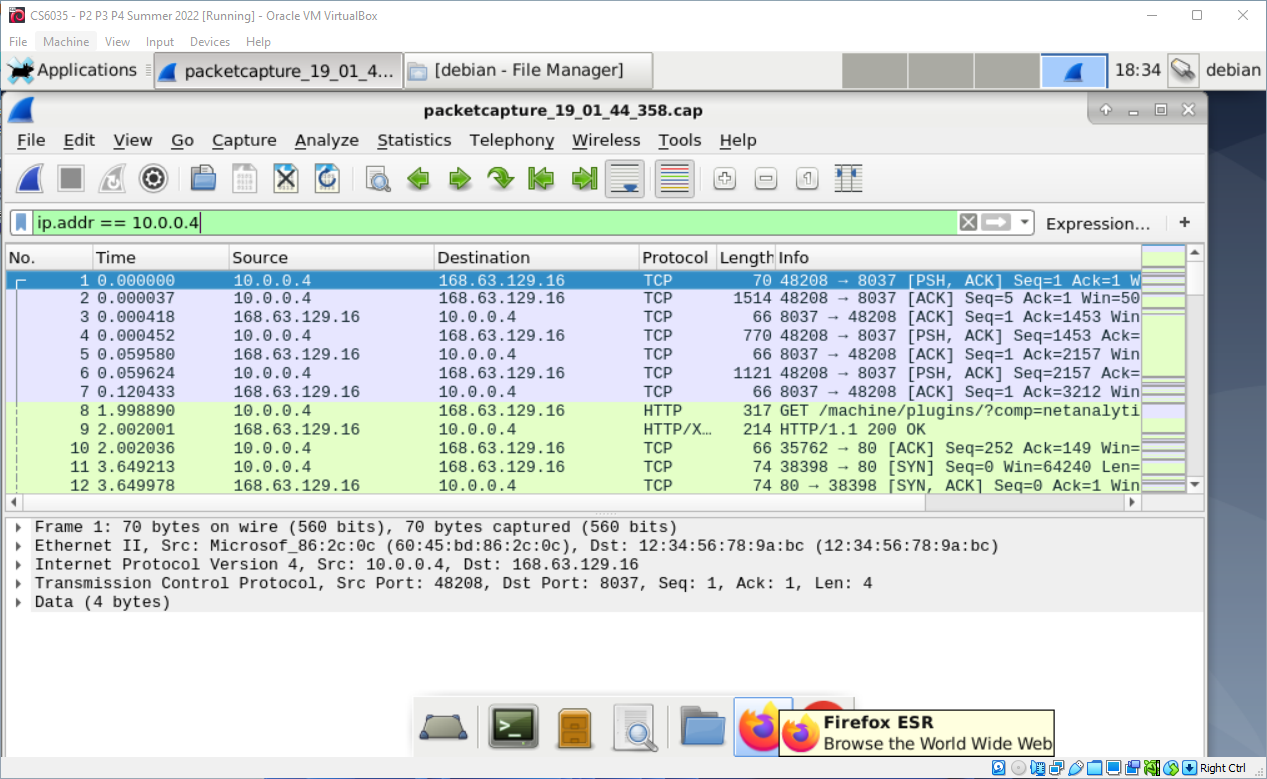
You can use the filter bar to filter for a specific IP address, protocol or payload inside the packet. Use the “Expression” button to show all available filters:



To make your life easier, here are some basic filters to serve as a starting point:

Filter all packets with IP address 10.0.0.4:

| ip.addr==10.0.0.4 |
| --- |



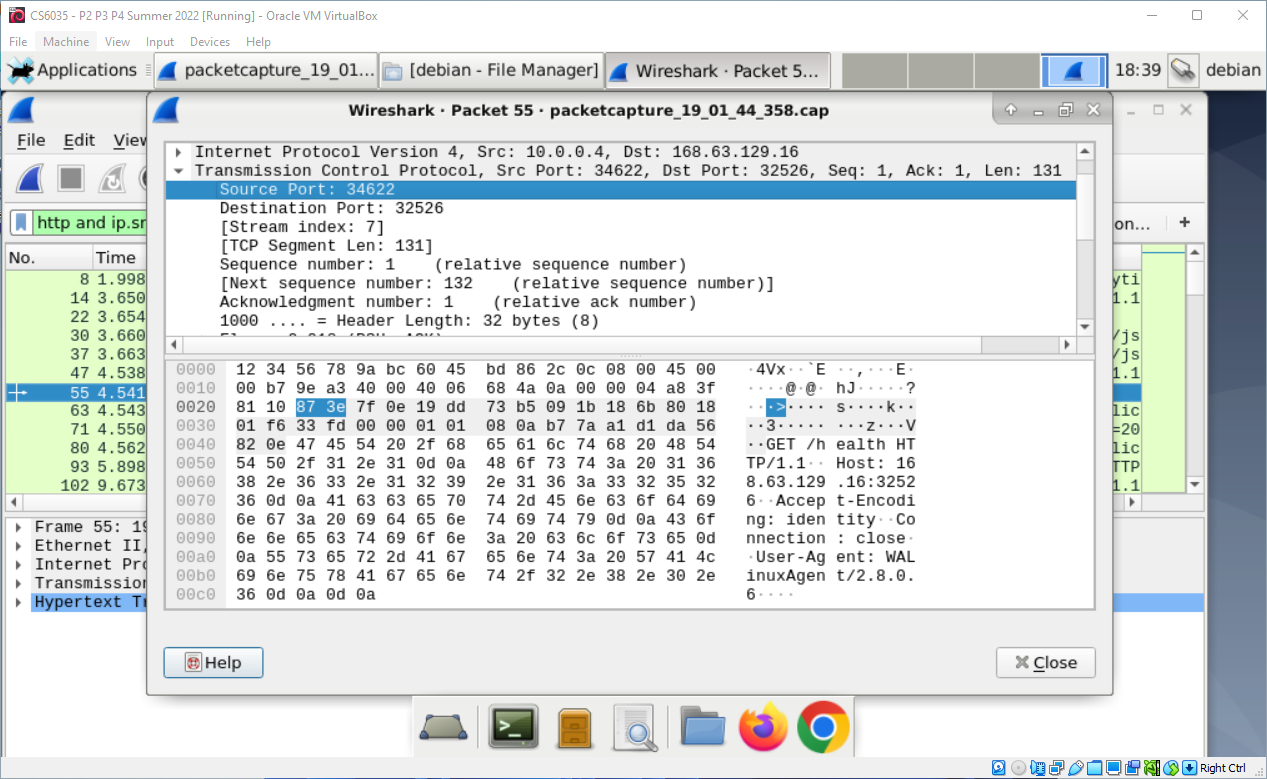
Filter all packets with source IP 10.0.0.4:

| ip.src== (10.0.0.4) |
| --- |

Filter all http packets and destination IP 200.210.70.4:

| http and ip.dst==200.210.70.4 |
| --- |

Double-clicking on any packet will take you to the packet screen. There, you can see the actual packet and payload on the bottom of the screen and expand/collapse the protocol layers on the top of the screen.



Now you know the basics, I **strongly** recommend you review the Wireshark Guide at <https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html> and the DisplayFilters section at <https://wiki.wireshark.org/DisplayFilters>.

There are numerous videos on YouTube explaining basic Wireshark functionality. I recommend this one from Anson Alex: <https://www.youtube.com/watch?v=TkCSr30UojM>

### **Python**

For this project, you will also need the Python interpreter which can be found here: [Python download page](https://www.python.org/downloads/)  
For a guided walkthrough using VScode, please refer to the following document: [Python tutorial](https://code.visualstudio.com/docs/python/python-tutorial)

Good luck!

# Task 1 (12 points):

*Your first task is to figure out where the hackers are spending their time and gather some evidence for the Attorney General. This will also give you a good overview of Wireshark filters.*

The Attorney General needs some evidence of The Necrocryptors’ associates and where the group meets. For this, you need to gather the following information:

* **Task 1.1: What is the server address used by the hackers to communicate?** *E.g.: irc.someplace.net (2 points)*
* **Task 1.2: What is the nickname of the malicious actors involved in this conversation ? Add the names in the order they appear in the conversation** For the autograder, use the following format: *firstactor,secondactor,thirdactor (2 points)*
* **Task 1.3: What channel do they use to communicate?** Hint: *Channel names always start with #, so include # in your answer (2 points)*
* **Task 1.4: What is the hash used by the malicious actor to validate its identity?** *(6 points)*

# Task 2 (29 points):

*Your second task will require you to recover a payload from the conversation. There are multiple ways to do this. You can use Wireshark, pyShark or any other library available.*

As part of the evidence gathering, the Attorney General needs concrete evidence of malicious intent. For Task 2, you will need to review the conversation between members of TNC and gather incriminating data from this conversation.

* **Task 2.1: One of the hackers transfers a file to another hacker, after confirming their identity. What is the name of the file?** *(Including extension)**(6 points)*
* **Task 2.2: It seems that the file transferred is encrypted. What encryption method or algorithm was used to encrypt the file?** *(Just the 3-letter name)**(4 points)*
* **Task 2.3: If you decrypt and run the file, you'll get a unique hash based on your GTID. What is the hash generated?** *(19 points)*

# Task 3 (26 points):

The Attorney General lets you know that they think there is a web server in here that is phishy and is spitting out long numbers and letters. The Necrocryptors hacking group is known to play tricks with these values. The Attorney General needs the following information to track the folks operating the website:

* **Task 3.1: The site domain name** *(Record just the site’s domain name and the top-level-domain (TLD) name, with the period. E.G: host-name.tld)**(2 points)*
* **Task 3.2: The public IP address** *(2 points)*
* **Task 3.3: The primary nameserver for this TLD** *(You may need to look outside the pcap for this information. Think about tools that will give you the nameserver data for a specific domain) (6 points)*
* **Task 3.4: The hash provided by entering your Georgia Tech ID in the field** *(i.e. 902042) (NOTE: The website is real and safe to access) (16 points)*

# Task 4 (33 points):

The Attorney General is impressed by you but says they believe the group is also using another server to host a malicious file. It appears that one of the hackers recently accessed this server and downloaded a file from it. As a last minute request, the Attorney General is asking you to investigate what this file is, and where it is hosted.

* **Task 4.1: What is the IP address for the server in question?** *(2 points)*
* **Task 4.2: What is the username used to log in the server?** *(4 points)*
* **Task 4.3: What is the password used to log in the server?** *(4 points)*
* **Task 4.4: One file is downloaded from the server, what is the file name?** *(3 points)*
* **Task 4.5: What is the programming language used to create this file?** *(The hackers are using a common encoding format to hide the real contents)**(5 points)*
* **Task 4.6 If you run this file you'll get a Combined hash. What is the unique hash for your GTID (i.e*****902042*) ?** *(15 points)*

Suddenly, your phone rings. It's Bill. He says the Attorney General is on line one and they want a status update from you in court tomorrow. Bill says they need you to provide all your findings in, as they phrased it, “This thing called a JSON format.”

## Submission Details:

These are the instructions for how the Attorney General needs you to submit your findings.

**File submission instructions:**

This project needs to be submitted via gradescope. Navigate to the course in Canvas and click ‘Gradescope’. On the gradescope website, click ‘Project MITM and submit there. (For this project there's no limit to how many times you use Gradescope.)

Name your submission file: ***project\_mitm.json***. In addition, ensure you replace the placeholders with the flags you retrieve from each relevant task.

*Note: You can use Notepad++/TextEdit or Vim to create and edit this file.* ***IMPORTANT****: Do not use LibreOffice, Word, or any similar document editor. Your submission must be in proper JSON format with no special characters in order to pass the autograder; these document editors are likely to introduce special characters that will make your submission fail the autograder.*

Here is an example of the provided JSON file:

| {  "task1.1": "<copy flag 1 here>",  "task1.2": "<copy flag 2 here>",  "task1.3": "<copy flag 3 here>",  "task1.4": "<copy flag 4 here>",  "task2.1": "<copy flag 5 here>",  "task2.2": "<copy flag 6 here>",  "task2.3": "<copy flag 7 here>",  "task3.1": "<copy flag 8 here>",  "task3.2": "<copy flag 9 here>",  "task3.3": "<copy flag 10 here>",  "task3.4": "<copy flag 11 here>",  "task4.1": "<copy flag 12 here>",  "task4.2": "<copy flag 13 here>",  "task4.3": "<copy flag 14 here>",  "task4.4": "<copy flag 15 here>",  "task4.5": "<copy flag 16 here>",  "task4.6": "<copy flag 17 here>" } |
| --- |

And here is an example of how your submitted file should look:   
(Note: this is an example; none of these values are correct.)

| {  "task1.1": "something.something.something",  "task1.2": "BigBird,CookieMonster,OscarTheGrouch",  "task1.3": "#WOW",  "task1.4": "a12342342bcde393202013434",  "task2.1": "somefile.extension",  "task2.2": "something",  "task2.3": "a123242342342342342934234",  "task3.1": "<something.something",  "task3.2": "192.168.1.10",  "task3.3": "ns-something-something.something.something",  "task3.4": "abcdef1234567890953453434",  "task4.1": "192.168.8.7",  "task4.2": "something",  "task4.3": "something",  "task4.4": "something",  "task4.5": "something",  "task4.6": "12123123129413249121249aa" } |
| --- |