CSCD58 Project Proposal – Packet Sniffer

Ahmed Halat [1006332951, halatahm]
Mohamed Halat [1006322962, halatmoh]
Armand Sarkezians [1006020574, sarkezi1]

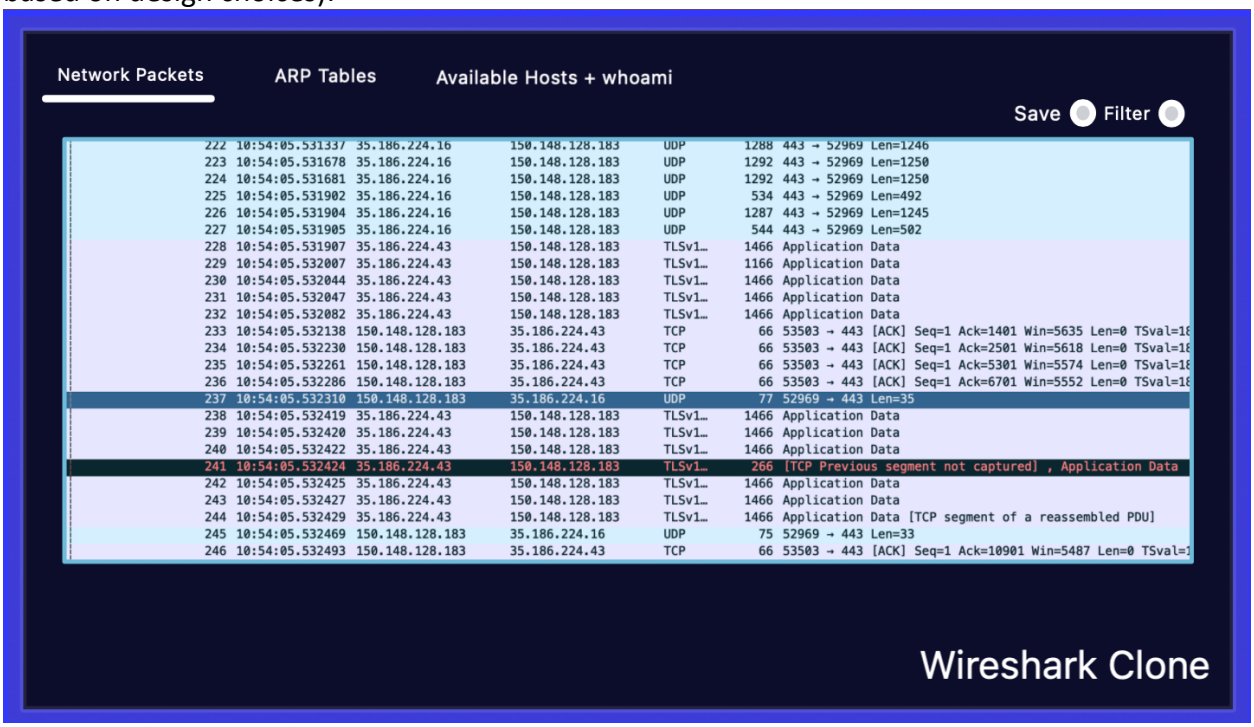
Description

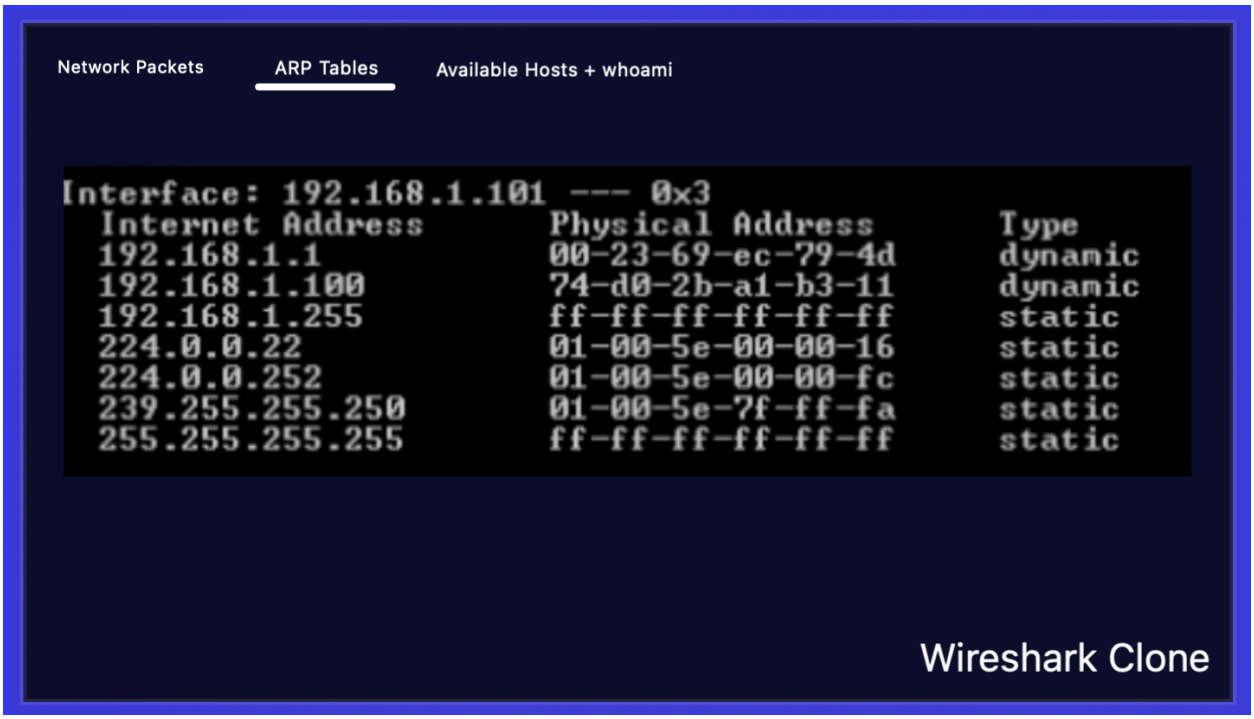
As our final project, we've decided to build a network packet sniffer, like Wireshark, with additional functionalities relating to the material covered in this course. These additional functionalities could include listing available hosts on the network with their whoami data, showing ARP tables for the network, and more.

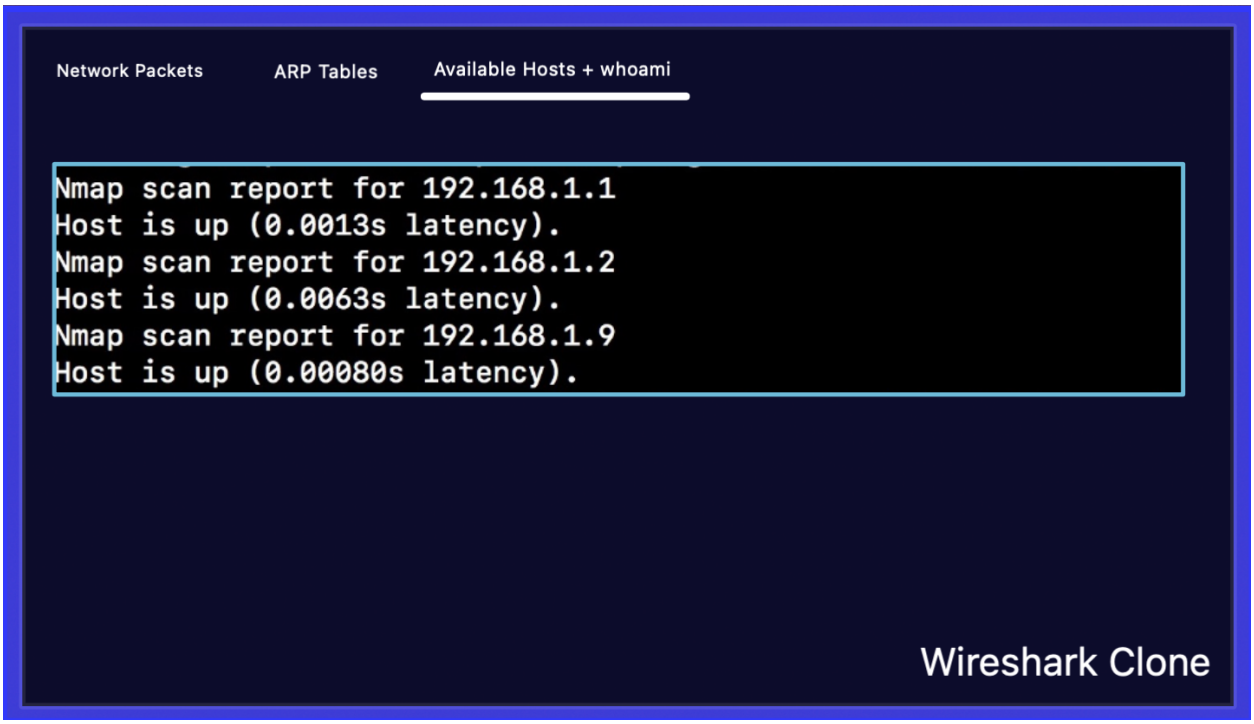
Our project would be divided into subpages, each with their own feature. The packet sniffing page would have listed data like Wireshark, including information like protocols, source, destination, payloads, and timestamps. The ARP table page would allow you to see your hosts' ARP table, whose information you can see in the available hosts + whoami page. This page would include as much information about each host that we can get our hands on.

Our packet sniffing implementation would also include some of the features that Wireshark offers, including but not limited to filtering based on protocol, selecting which interface to sniff on, and saving the network information in a file.

After selecting which interface to sniff on, our implementation would look somewhat like this (keep in mind this is something we sketched in 10 minutes, it may look very different based on design choices):







(The available hosts + whoami page is just Nmap only for the purposes of this proposal)

Rationale

The rationale behind this implementation is simple. We feel as though this project will allow us to apply a large amount of the knowledge we've gained throughout this semester. In

addition to this, it would be extremely cool to learn how an application like Wireshark works under the surface.

Goals and Targets

Some of our goals for this project include:

- Develop a packet sniffer
- Develop an ARP table reader
- Develop an information page regarding available hosts on the network along with all data we can gather on them
- Develop a nice-looking UI
- Allow users to save network traffic into files
- Allow users to filter through network traffic with different parameters

Relation to Computer Networks

The relation of this project to computer networks is vivid: Wireshark is a vital tool when it comes to detecting network traffic, and we want to create a similar tool. This project would allow us to dive deep into how network traffic is parsed by our computers, how we can access it as users and how to analyze it. It would remind and educate us more on the different protocols that exist in the networking world, and the meanings/data behind each one. While working on this project we would touch on ARP tables, a prevalent topic in Computer Networks. Depending on how many additional features we can implement, it may allow us to touch on more topics under the scope of Computer Networks.