**CSCE 5580: Computer Network**

**Project-1**

**Instructor:** Tao Wang

**Name:** Kishan Kumar Zalavadia

**EUID:** 11685261

**Date**: September 25, 2024

**Task-1:**

1. **Locate and install a wiretapping software tool such as Wireshark. It can eavesdrop on both wired and wireless networks. Make sure that you are downloading from the reliable source such as www.wireshark.org. Do not use third party websites since attackers may embed malware in it.**

**Ans**: Downloaded Wireshark on my MacBook from [www.wireshark.org](http://www.wireshark.org).

A screenshot of a phone

Description automatically generated

Figure 1

1. **(a) How many unique MAC addresses were on the network?**

**Ans**:12

* First, upload the file given in Wireshark.
* Navigate to Statistics -> Endpoints, as you can see in Figure 2.
* Under the ‘Ethernet’ tab, you can see all the unique MAC addresses as you can see in Figure 3.

A screenshot of a computer

Description automatically generated

Figure 2

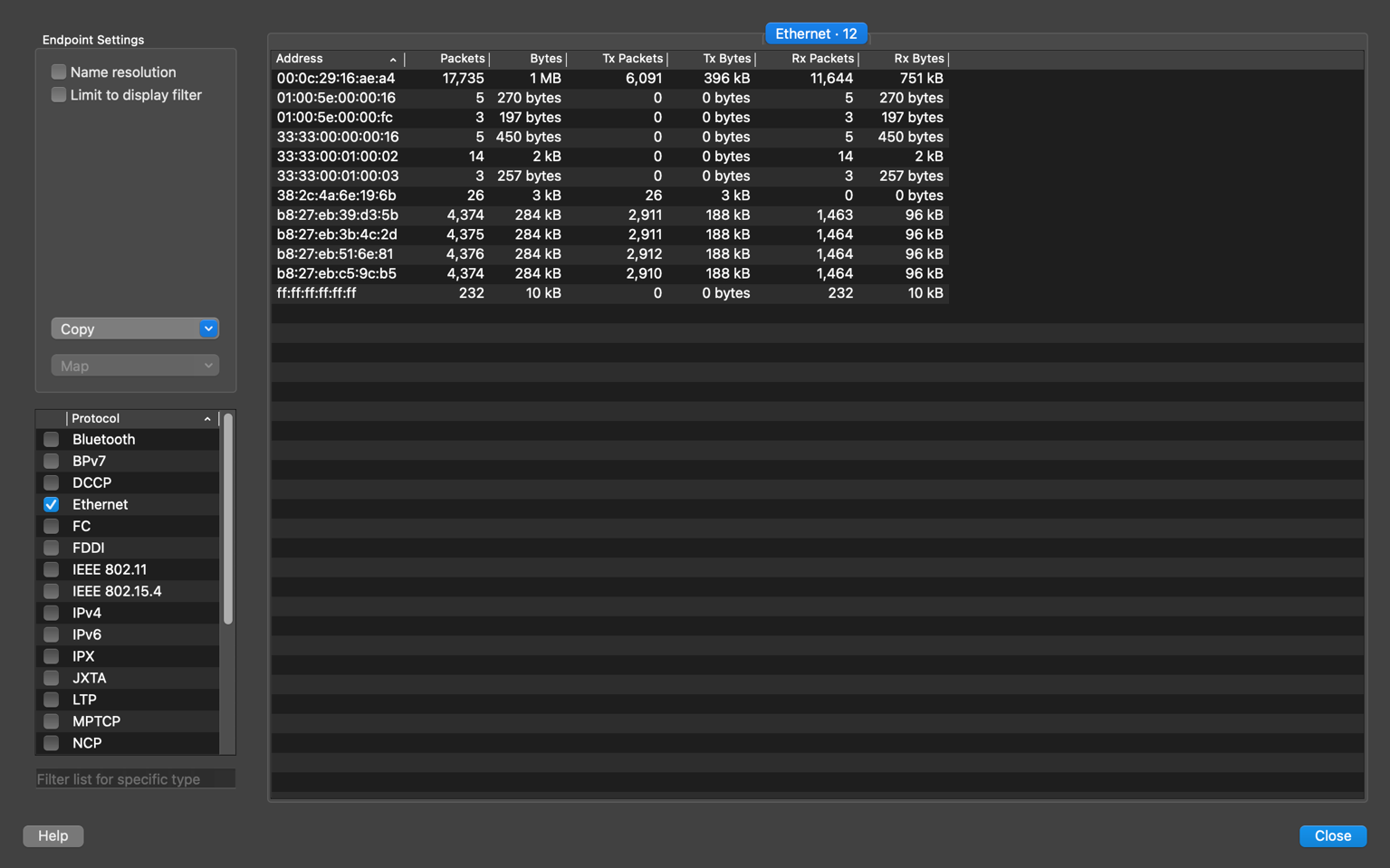


Figure 3

**(b) How many unique IP addresses were on the network (IPv4 and IPv6)?**

**Ans**:

* IPv4: 9
* IPv6: 5
* Similar to finding unique MAC addresses, first, upload the file.
* Then go to statistics -> Endpoints as you can see in Figure 2.
* By selecting IPv4 and IPv6 from the options on the left-hand side, you can see all the unique addresses associated with them, as you can see in Figure 4.



Figure 4

**(c) What were the two UDP protocols used?**

**Ans**:

* The two UDP protocols used are
  + Link-local Multicast Name Resolution
  + DHCPv6
* First, upload the given file to Wireshark.
* Navigate to Statistics-> Protocol Hierarchy, as you can see in Figure 5.
* In the list, you can see all the protocols used, as you can see in Figure 6.

A screenshot of a computer

Description automatically generated

Figure 5

A screenshot of a computer

Description automatically generated

Figure 6

**(d) Which Ethernet address was shared between an IPv4 and IPv6 address?**

**Ans**:

To find the ethernet address shared between IPv4 and IPv6 address, first, let us filter the search results with IPv4 by typing “ip” in the search bar. Figure 1.d.1 shows all the results related to IPv4.

A screenshot of a computer

Description automatically generated

Figure 1.d.1

Now, get to statistics 🡪 Endpoint and note down all the ethernet addresses as shown in Figure 1.d.2.

A screenshot of a computer

Description automatically generated

Figure 1.d.2

Now, let us filter the search results with IPv6 by typing “ipv6” in the search bar. Figure 1.d.3 shows all the results related to IPv6.

A screenshot of a computer

Description automatically generated

Figure 1.d.3

Now, get to statistics 🡪 Endpoint and note all the ethernet addresses as shown in Figure 1.d.4.

A screenshot of a computer

Description automatically generated

Figure 1.d.4

As you can compare the result, the ethernet address which is common is the one that is shared between IPv4 and IPv6.

There are two addresses shared, which are **00:0c:29:16:ae:a4** and **38:2c:4a:6e:19:6b**.

**(e) It seems that there is a Human-Machine Interface (HMI) server that interacts with**

**multiple devices in the network through Modbus. What is the IP address of the**

**server?**

**Ans**: The IP address of the server is "**172.16.192.200**“

A screenshot of a computer

Description automatically generated

Figure 9

* To see all the addresses related to Modbus, type “modbus” in the search bar.
* Then you can see all the details related to only ‘modbus,’ as you can see in Figure 9.
* To see all the unique addresses related to modbus, go to statistics->Endpooints, as you can see in Figure 10.

A screenshot of a computer

Description automatically generated

Figure 10

* There are 5 IP addresses related to the Modbus, but the high usage IP address which has the most number of packets is "**172.16.192.200**“.

**Explanation -2:**

First, go to statistics🡪 Conversations to see all the conversations.

A screenshot of a computer

Description automatically generated

Figure 11

**A screenshot of a computer

Description automatically generated**

Figure 12

As you can see in Figure 11, a high number of packets have been sent from IP address 172.16.192.200. That means this can be the server.

So, therefore, "**172.16.192.200**“ is the IP address of the server.

**Task-2:**

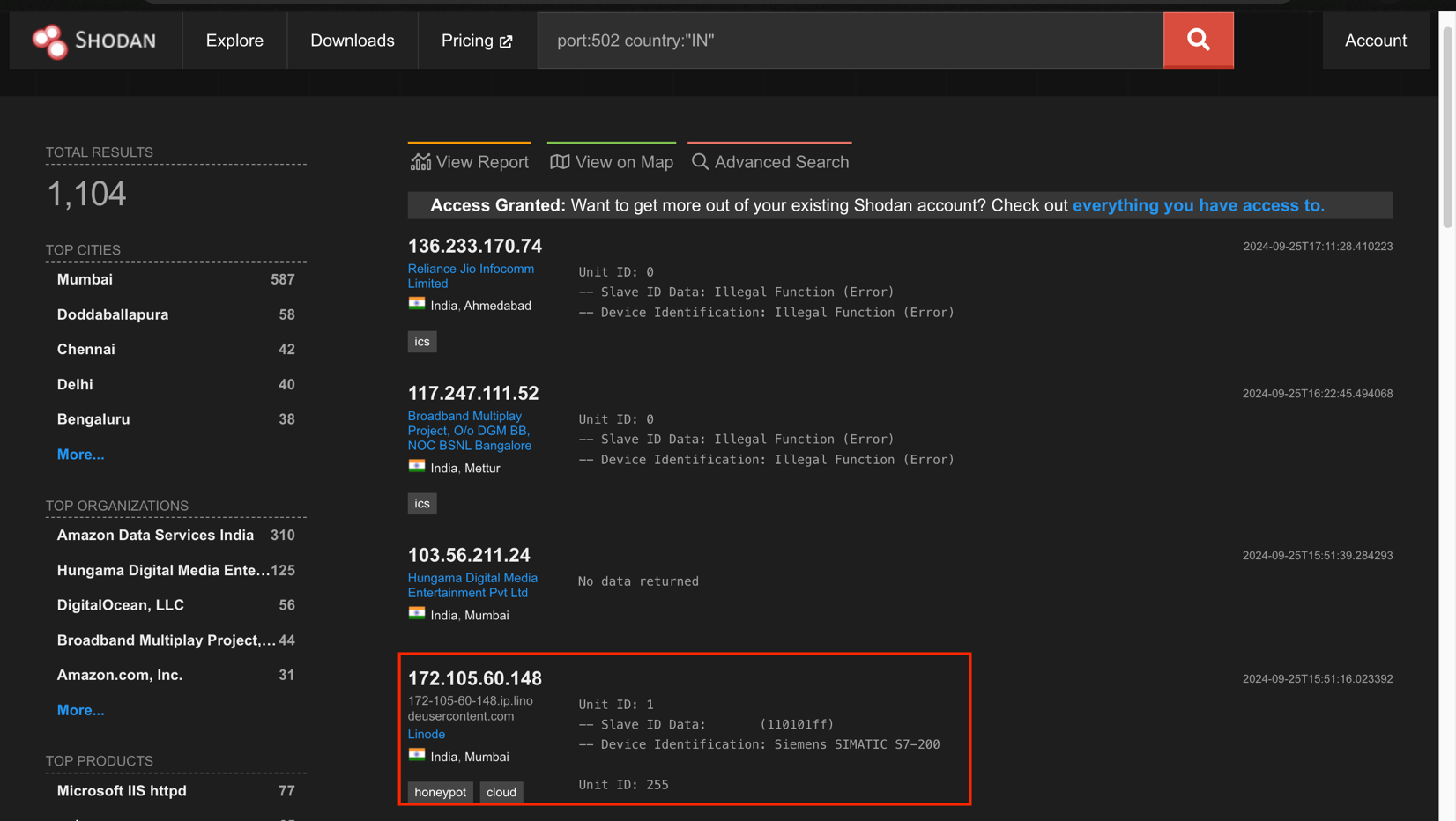
****

Figure 11

**A screenshot of a computer

Description automatically generated**

Figure 12

**A screenshot of a computer

Description automatically generated**

Figure 13

**Device/IP address returned by Shodan that does not show “error” or illegal:** 172.105.60.148

**Device Identification:** siemens simatic s7-200

**A screenshot of a computer

Description automatically generated**

Figure 14

**About the device:** <https://www.cisa.gov/news-events/ics-advisories/icsa-24-261-01>

**Vulnerability Overview**

**Uncontrolled Resource Consumption:**

If a device is vulnerable to this, it will not handle the TCP packets which are in incorrect structure. Using this vulnerability, an unauthenticated attacker can cause a denial of service condition. This device does not manage how it uses its limited resources. Because of that, someone can use more resources than what they want, which will lead to a position where there are no further resources left, eventually causing the product to stop working.

Some limited resources are storage, CPU power, and memory. The attacker can use all the resources, leading to a denial of service where authenticated and authorized users cannot use the service.

Because of the denial of service, the device speed can decrease, or the device can crash.

To avoid these types of attacks, where the resource is exhausted, there should be some mechanisms implemented that will limit the use of resources by unauthorized users. Caching database outputs can be used to minimize resource usage. The system should identify the attackers and block offenders.