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.

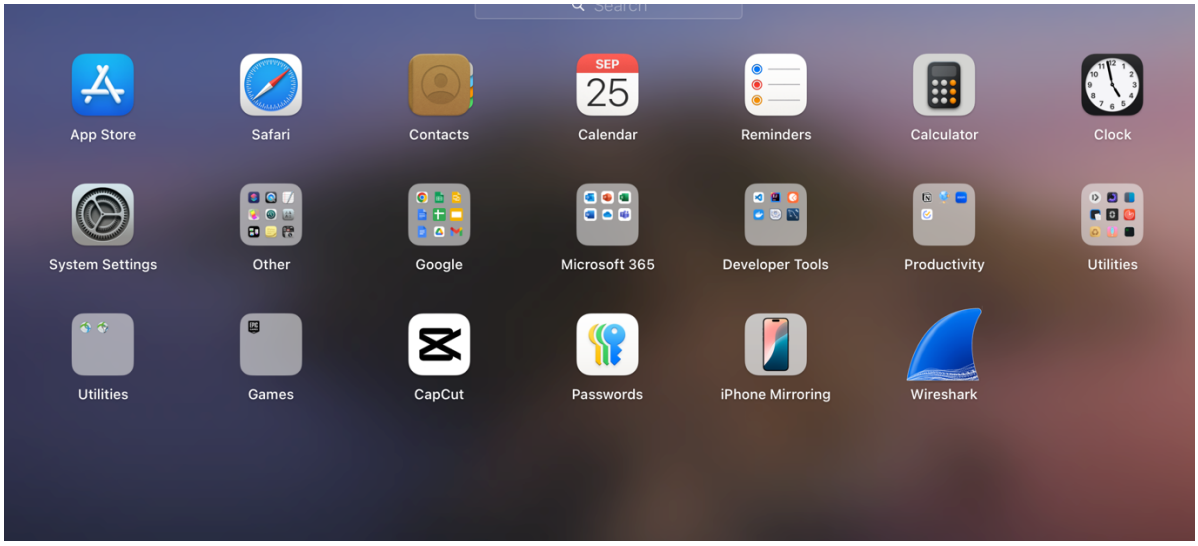


Figure 1

---

2. **(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.

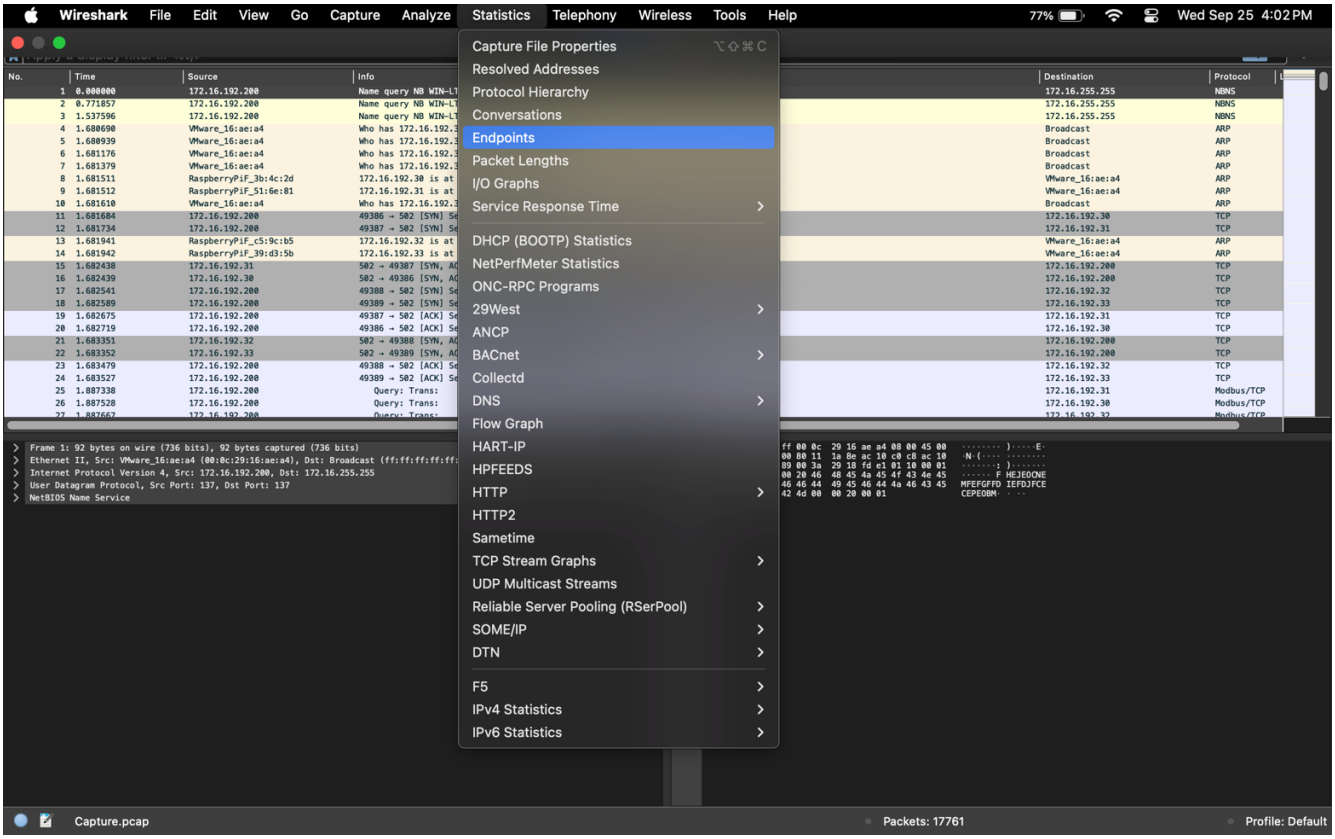


Figure 2

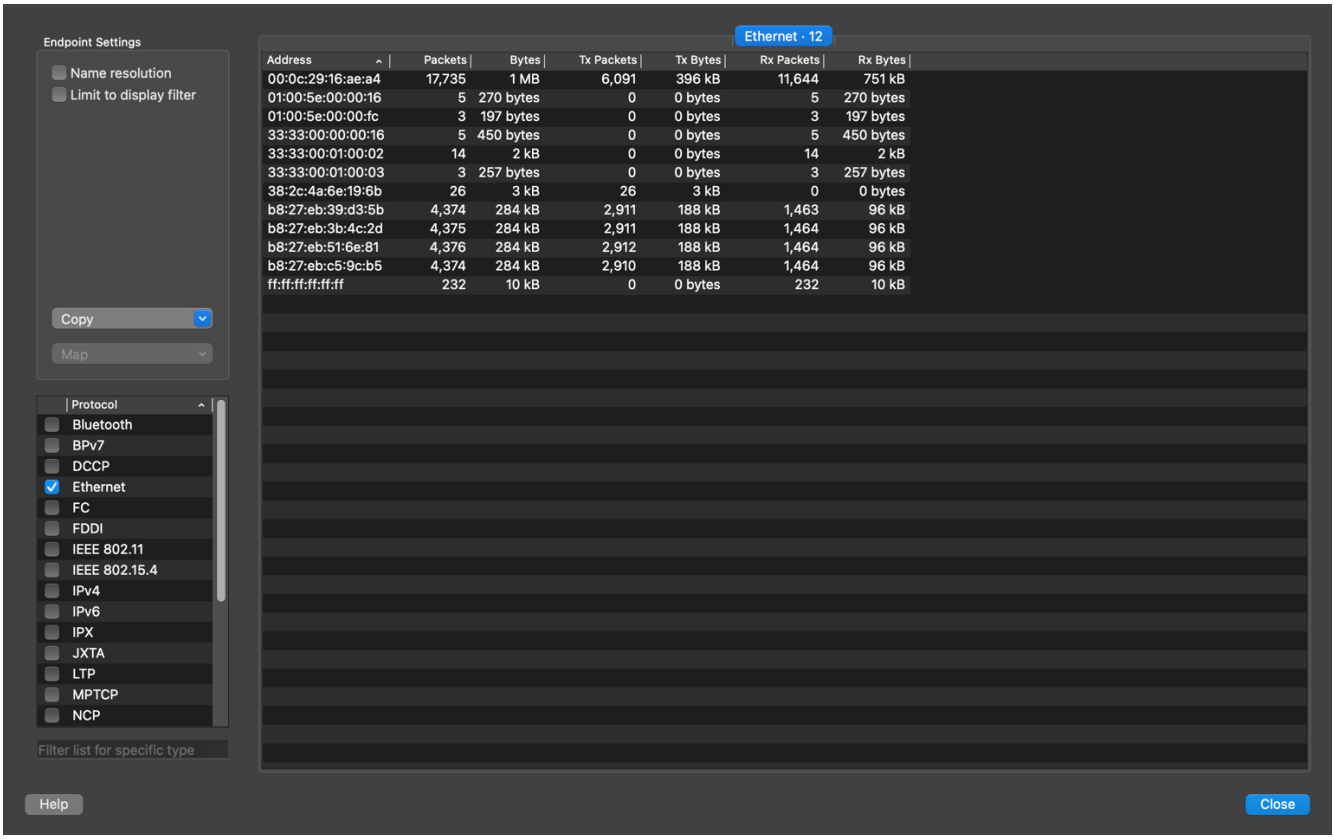


Figure 3

(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.

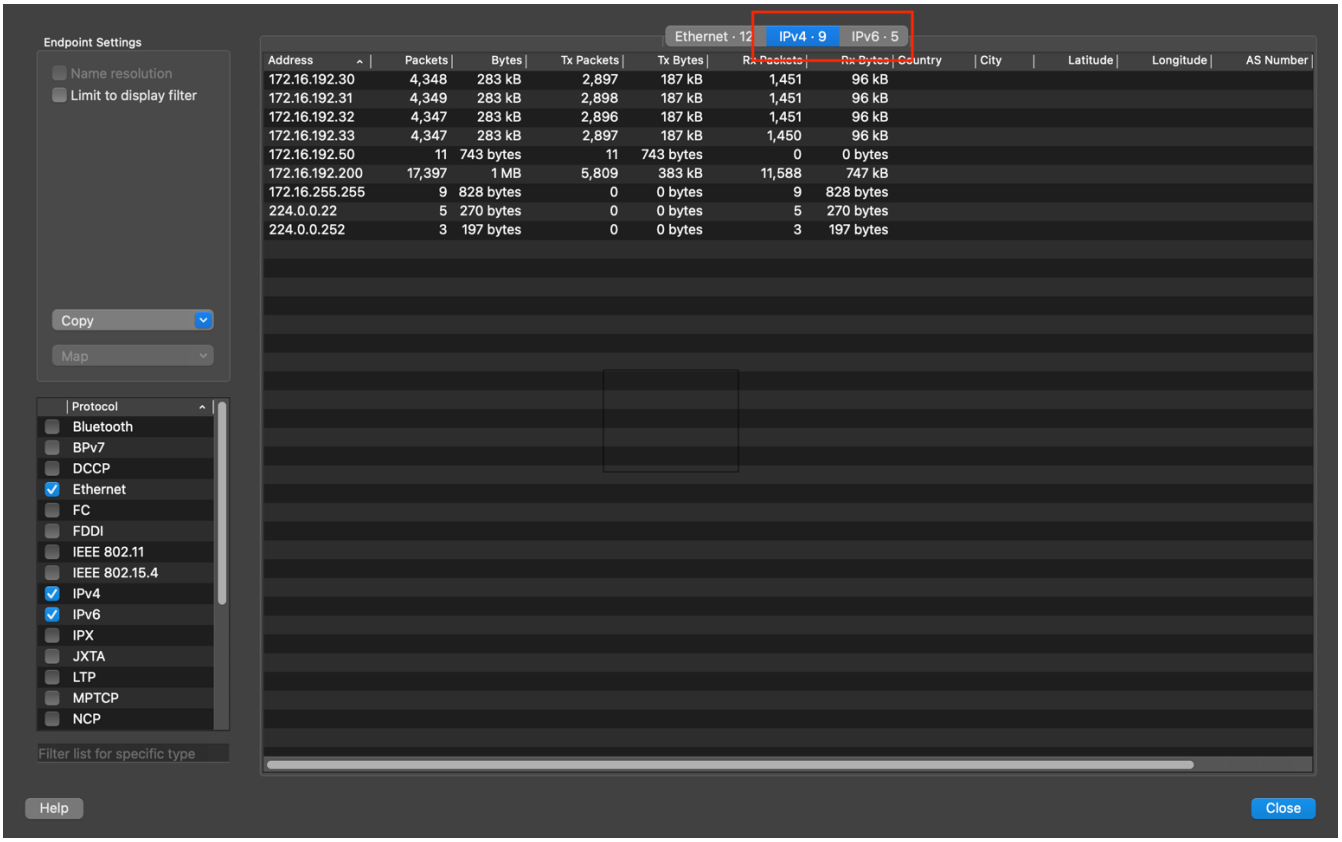


Figure 4

(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.

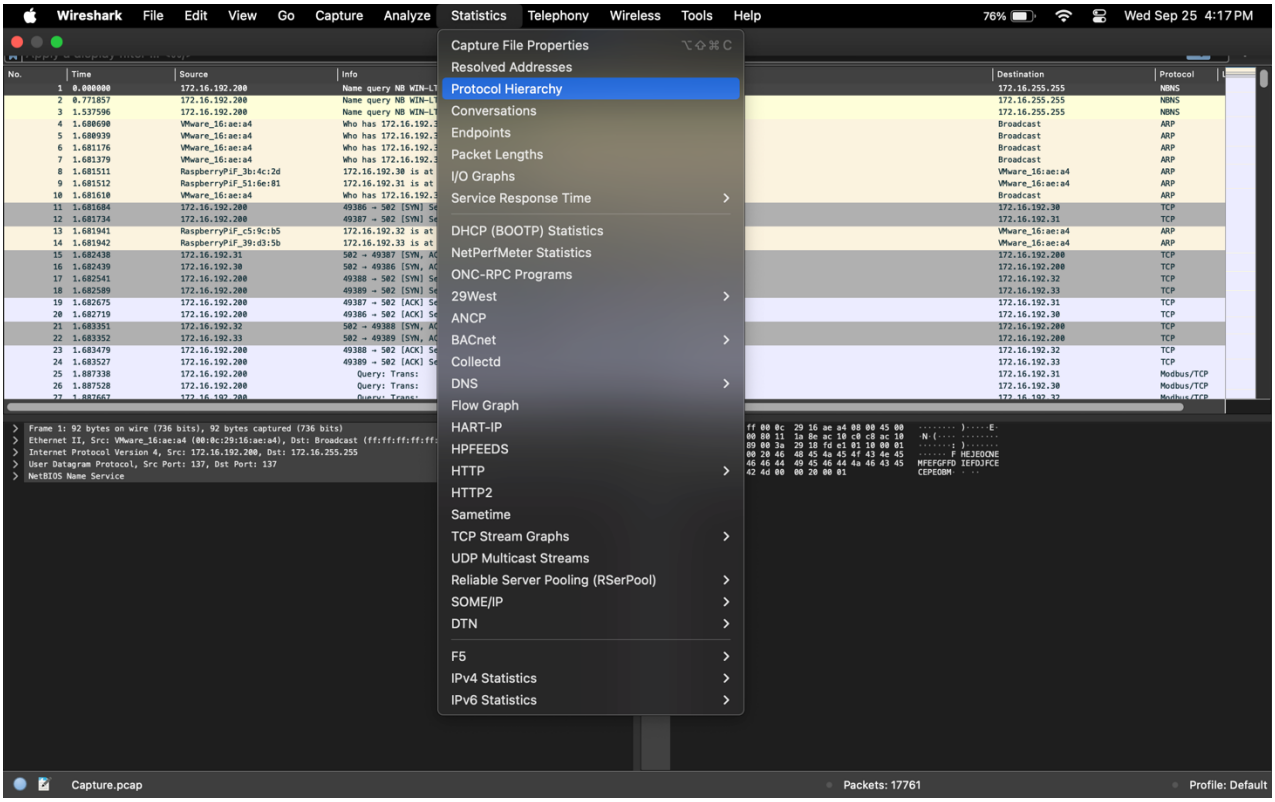


Figure 5

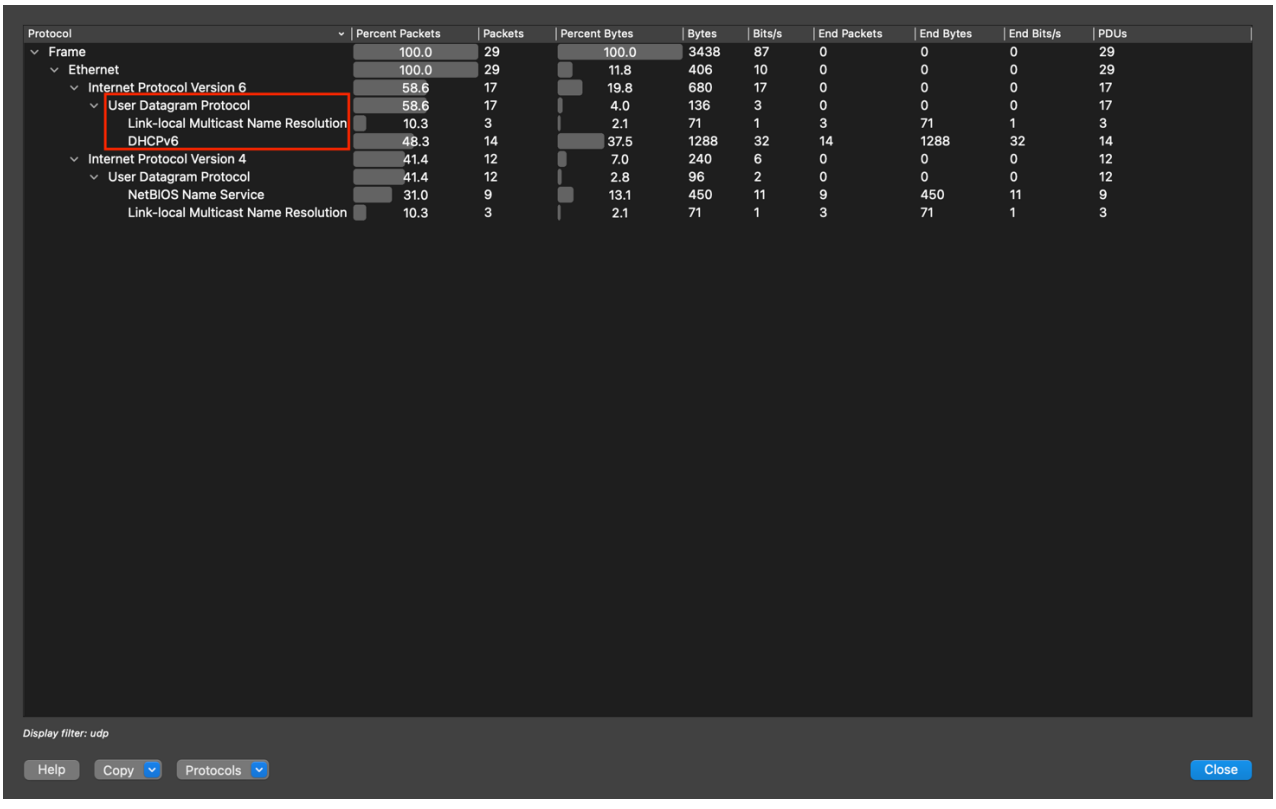


Figure 6

(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.

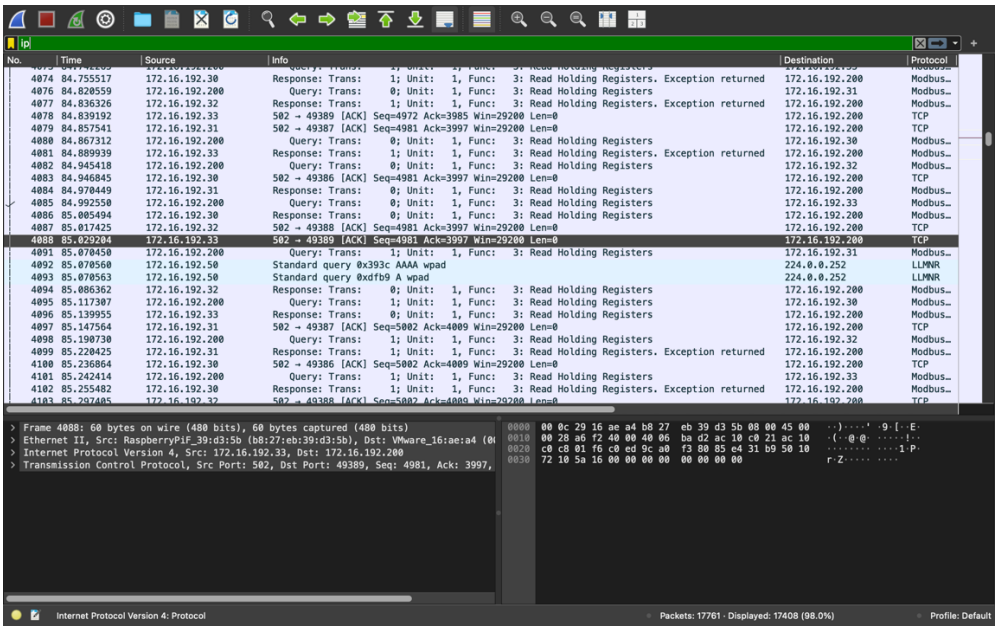


Figure 1.d.1

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

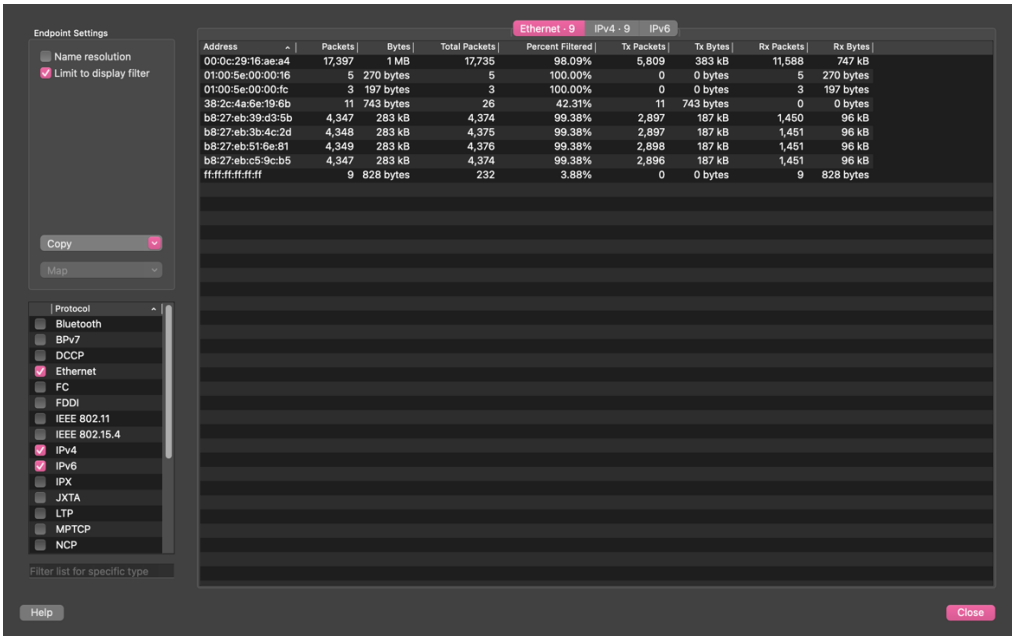


Figure 1.d.2

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.

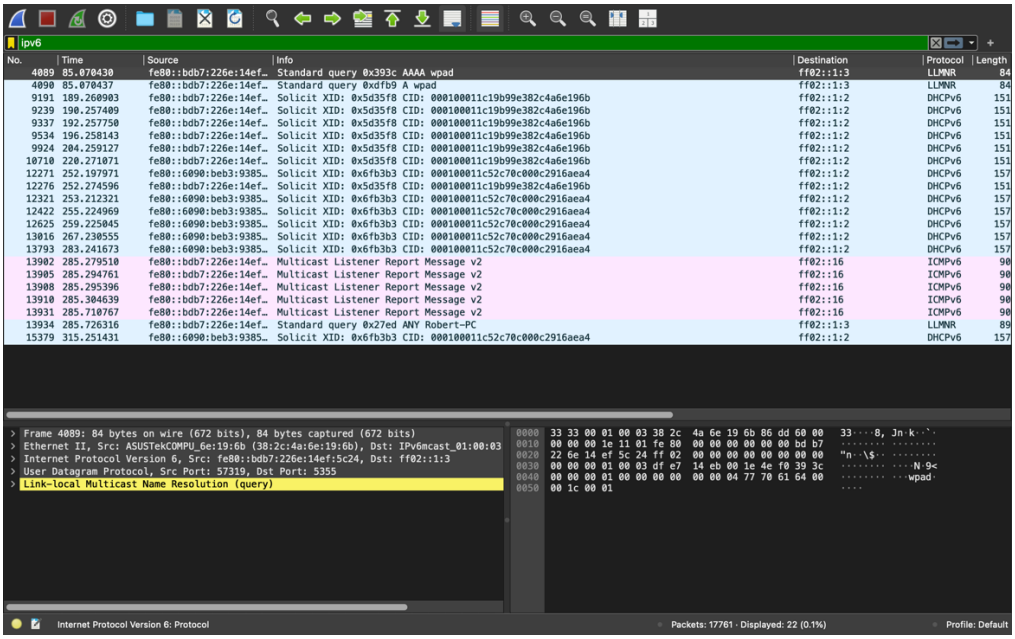


Figure 1.d.3

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

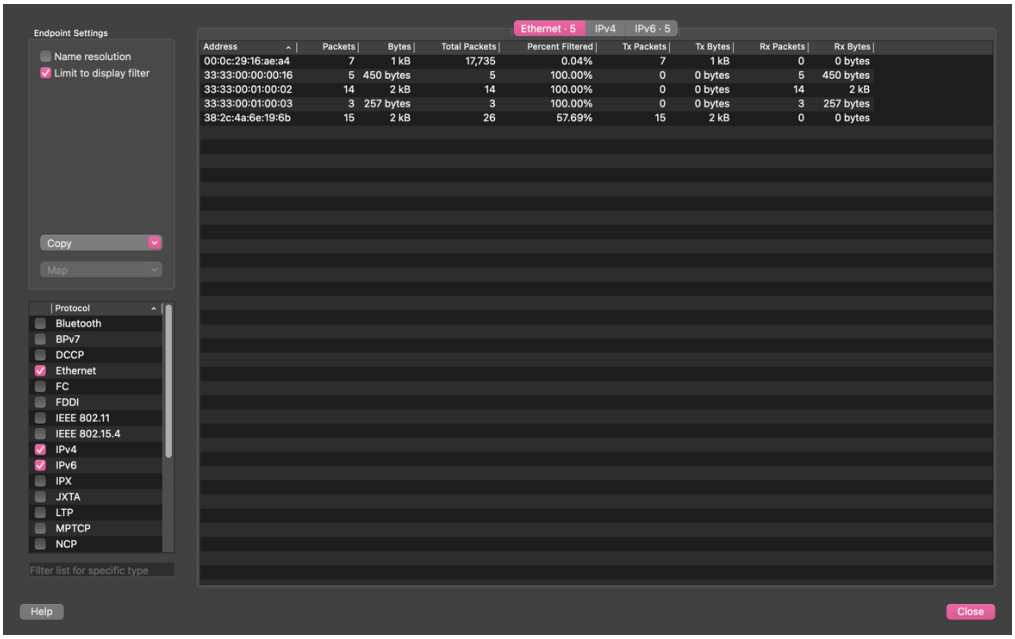


Figure 1.d.4

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**"

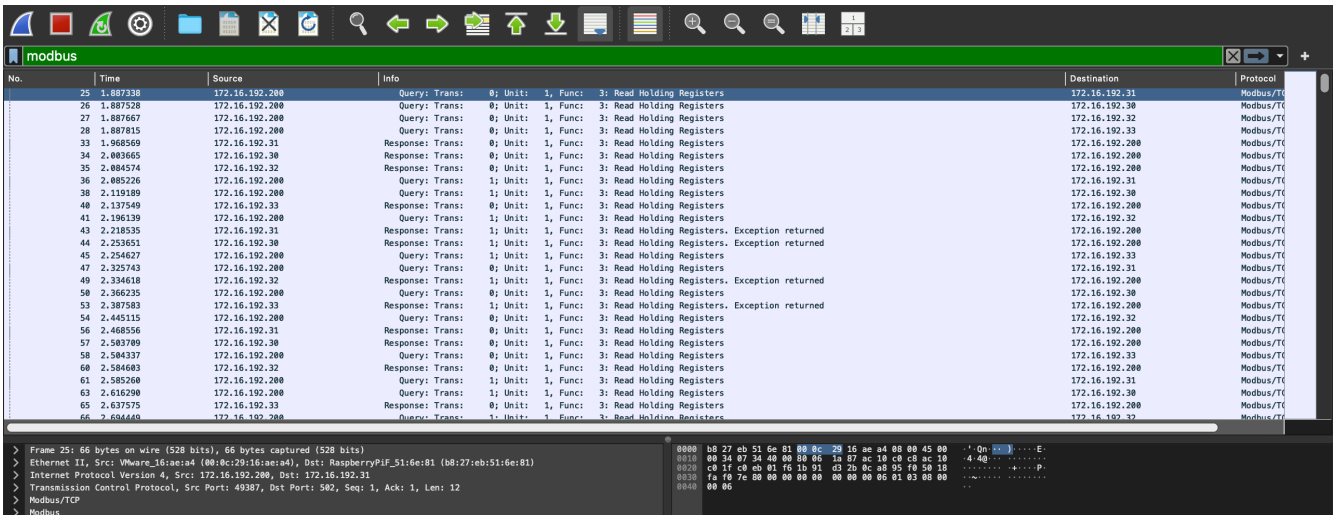


Figure 9

- 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.

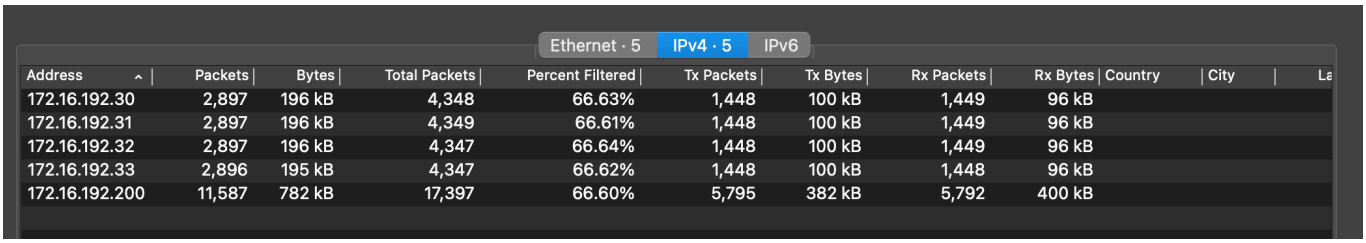


Figure 10

- 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.

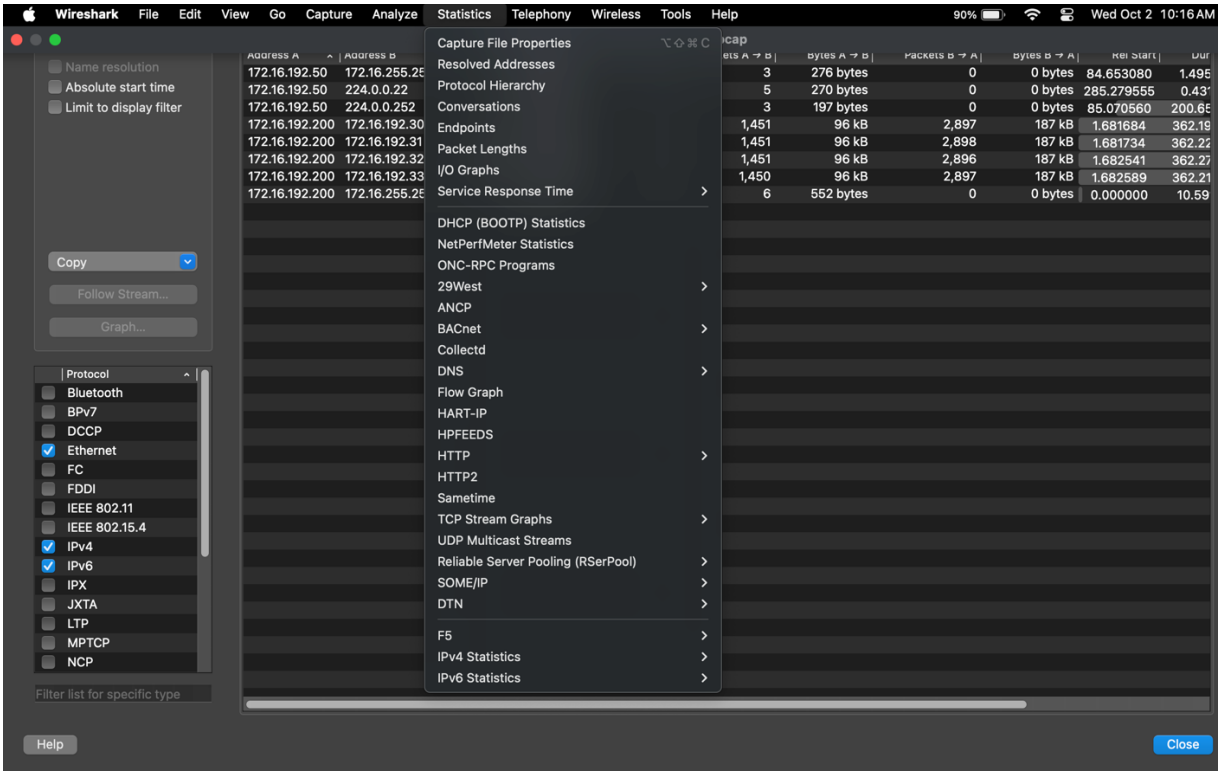
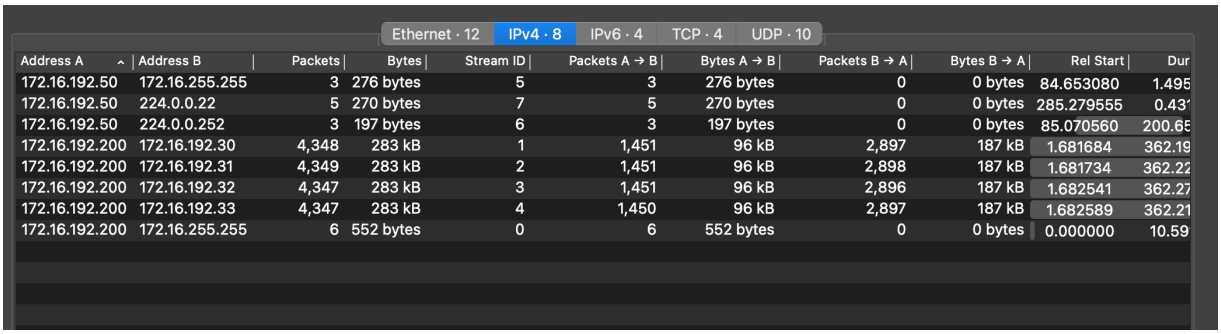


Figure 11



Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Dur
172.16.192.50	172.16.255.255	3	276 bytes	5	3	276 bytes	0	0 bytes	84.653080	1.495
172.16.192.50	224.0.0.22	5	270 bytes	7	5	270 bytes	0	0 bytes	285.279555	0.43
172.16.192.50	224.0.0.252	3	197 bytes	6	3	197 bytes	0	0 bytes	85.070560	200.6
172.16.192.200	172.16.192.30	4,348	283 kB	1	1,451	96 kB	2,897	187 kB	1.681684	362.19
172.16.192.200	172.16.192.31	4,349	283 kB	2	1,451	96 kB	2,898	187 kB	1.681734	362.22
172.16.192.200	172.16.192.32	4,347	283 kB	3	1,451	96 kB	2,896	187 kB	1.682541	362.27
172.16.192.200	172.16.192.33	4,347	283 kB	4	1,450	96 kB	2,897	187 kB	1.682589	362.21
172.16.192.200	172.16.255.255	6	552 bytes	0	6	552 bytes	0	0 bytes	0.000000	10.59

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:

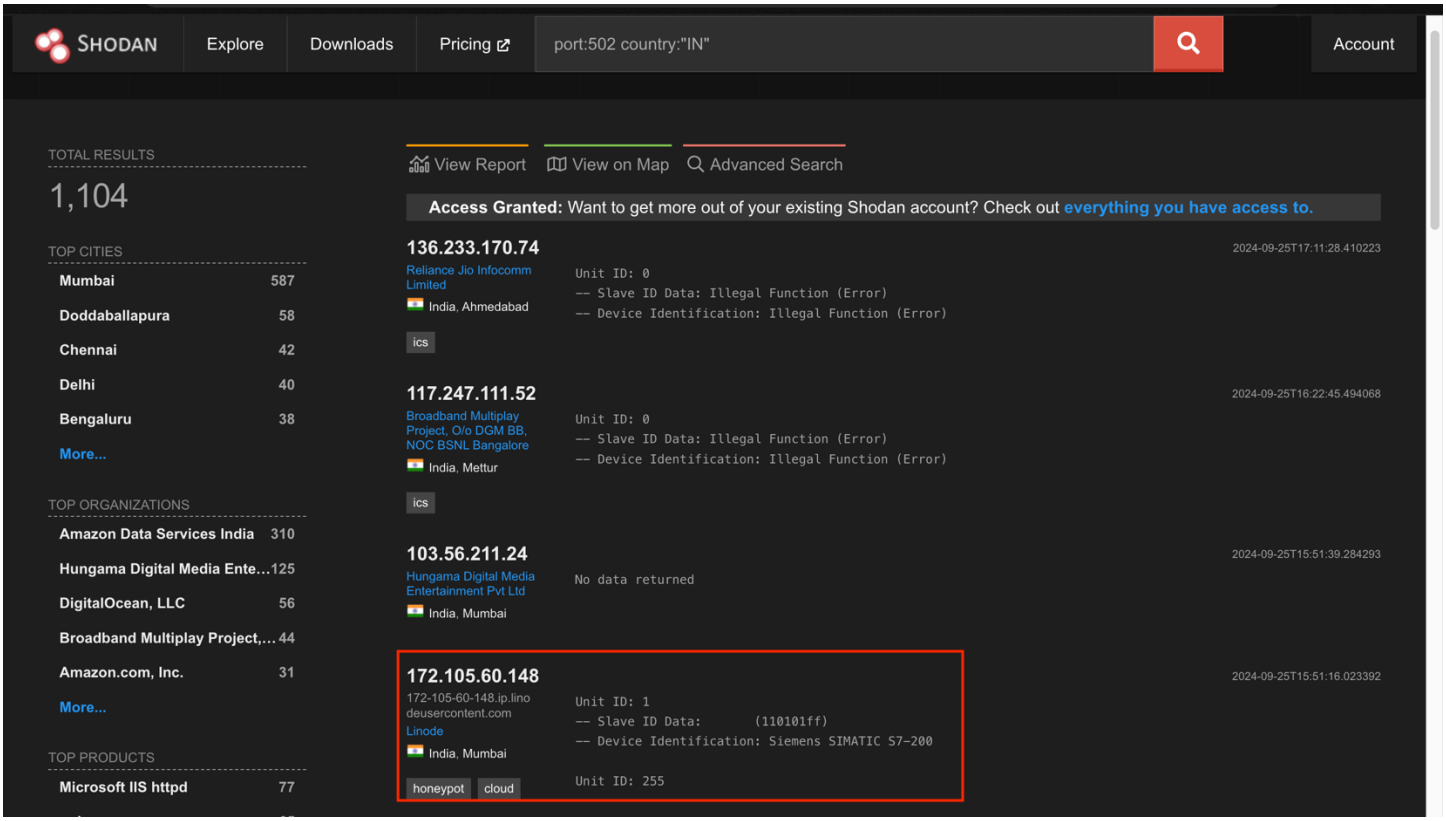


Figure 11

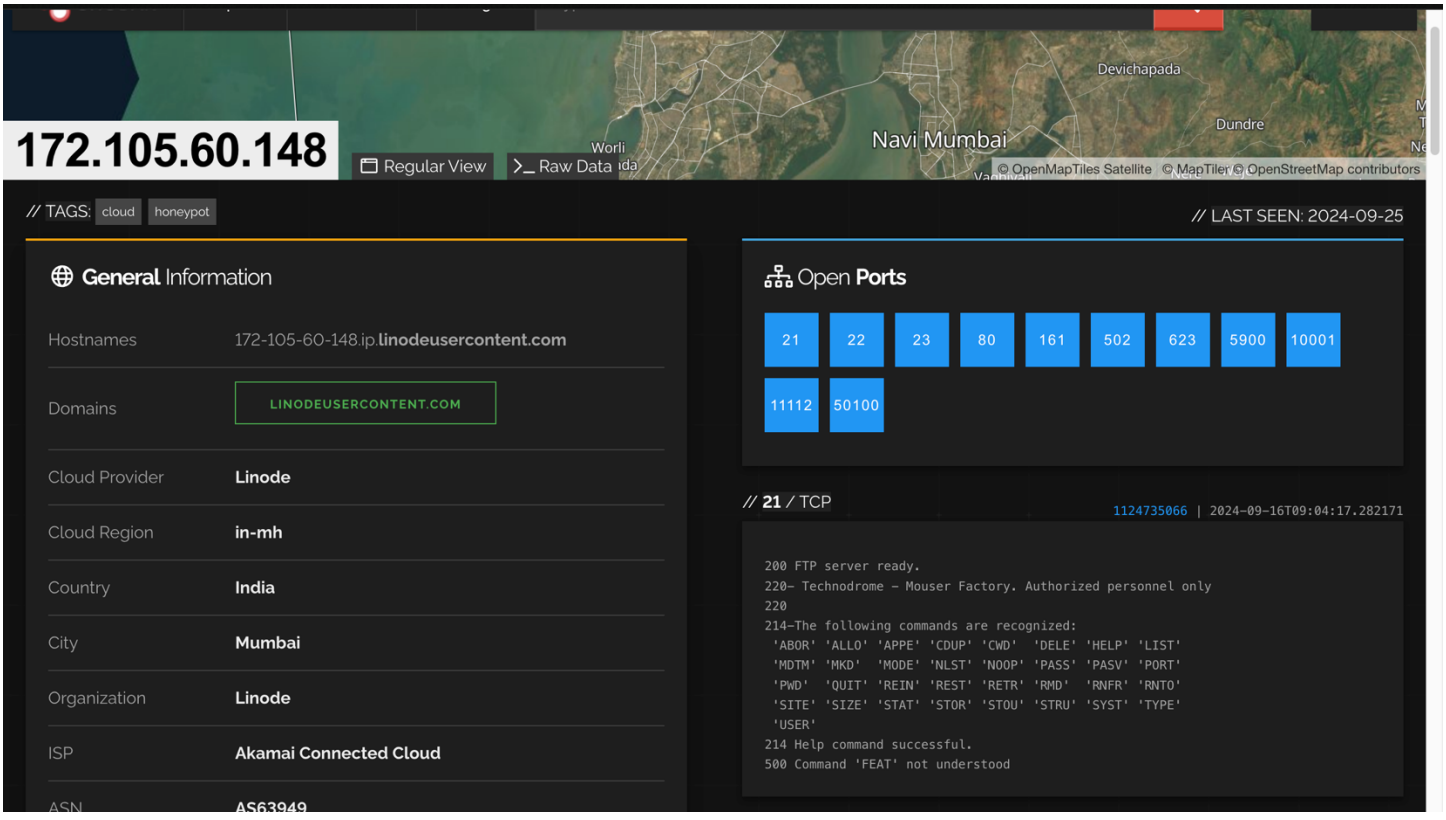


Figure 12

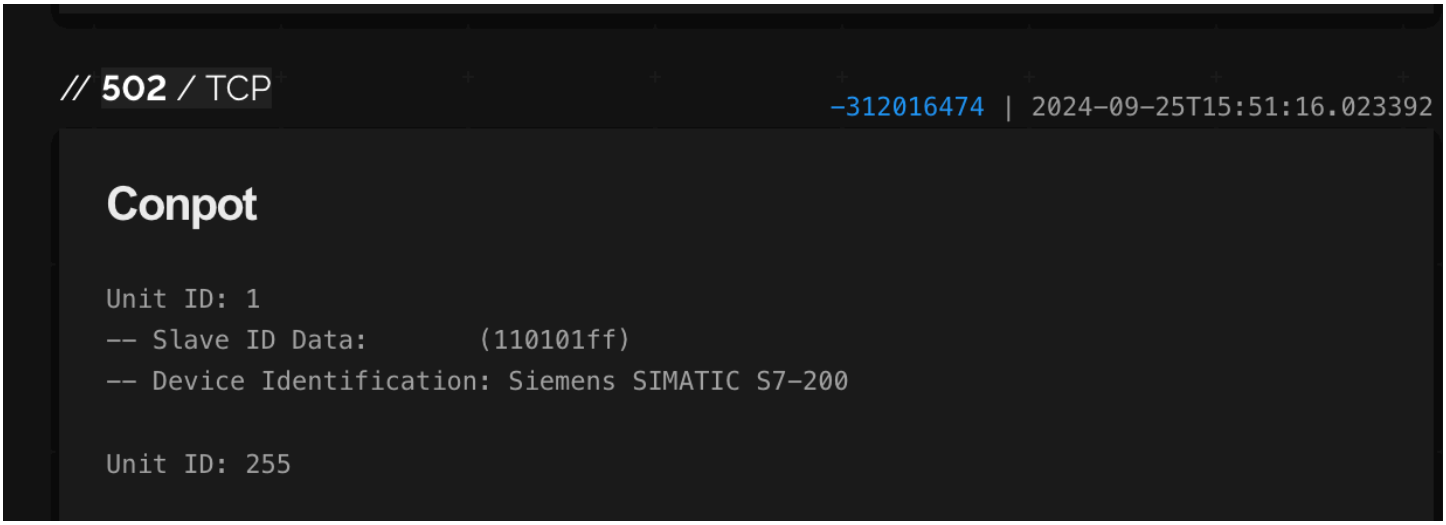


Figure 13

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

Device Identification: siemens simatic s7-200

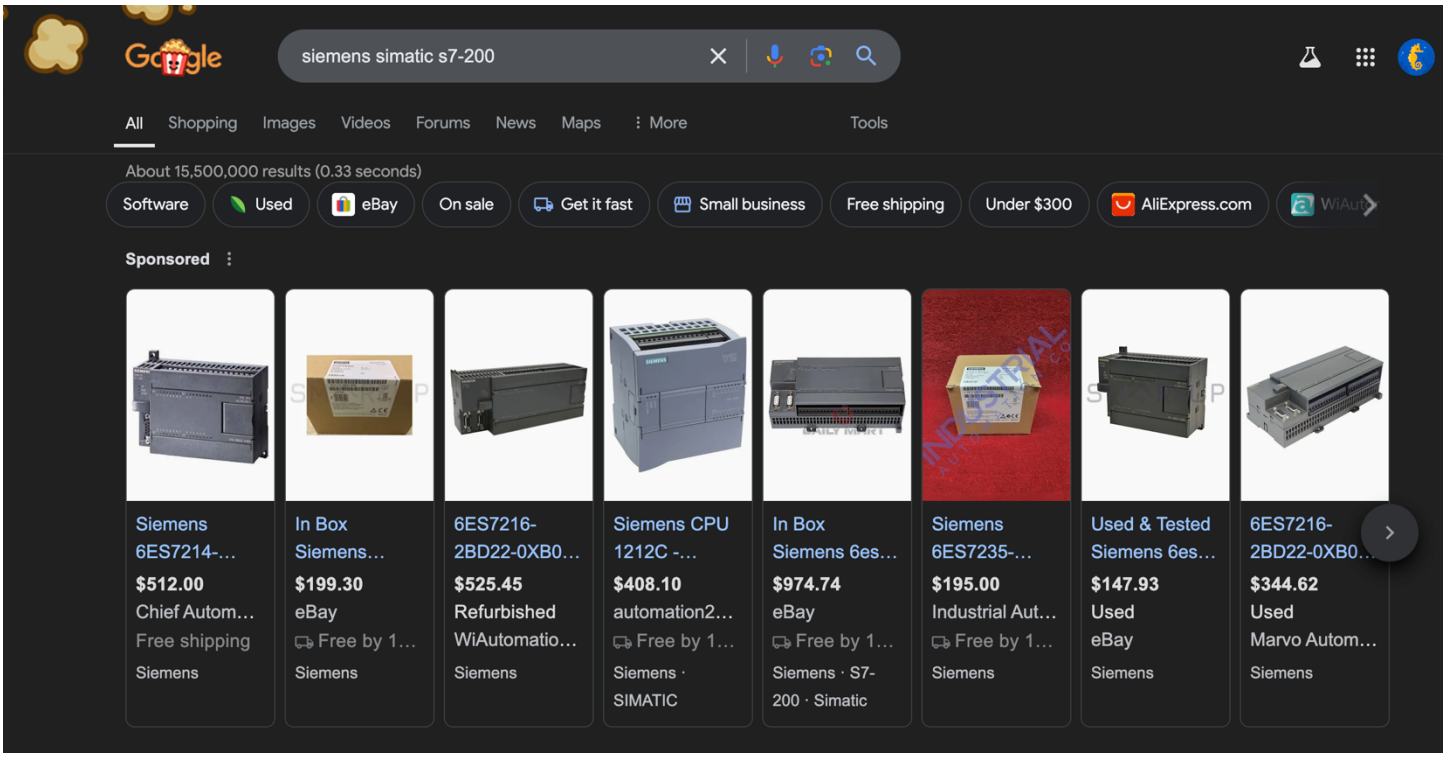


Figure 14

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.