

Alex Shah  
EN.695.741.81.SP25 Information Assurance Analysis  
Mod 14 Lab  
May 5, 2025

## Part 1 Install Wireshark

On a Ubuntu 18.04 VM I installed Wireshark and opened the PCAP file, shown below with the Wireshark version 2.6.10 shown in the terminal window.

The screenshot shows the Wireshark interface on a Ubuntu 18.04 VM. The main window displays a list of network packets captured from the interface 0. The packets are filtered by the display filter 'ot\_pcap.pcapng'. The packet list shows various protocols including CIP, TCP, and UDP. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Common Industrial Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

In the bottom right corner, a terminal window is open, showing the command 'alex@alex-VirtualBox:~\$ wireshark --version' and the output 'Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1-ubuntu18.04.0)'. The terminal also displays the copyright information and the build details of the Wireshark version.

## Part 2 Analysis

**1.)** Using Wireshark to find the vendor for all hosts on the network; what kind of devices are 192.168.1.120, 192.168.1.213, & 192.168.1.34?

192.168.1.120 and 192.168.1.213 appear to be VMWare Virtual machines according to the MAC addresses. 192.168.1.34 appears to be a Dell device from the MAC address.

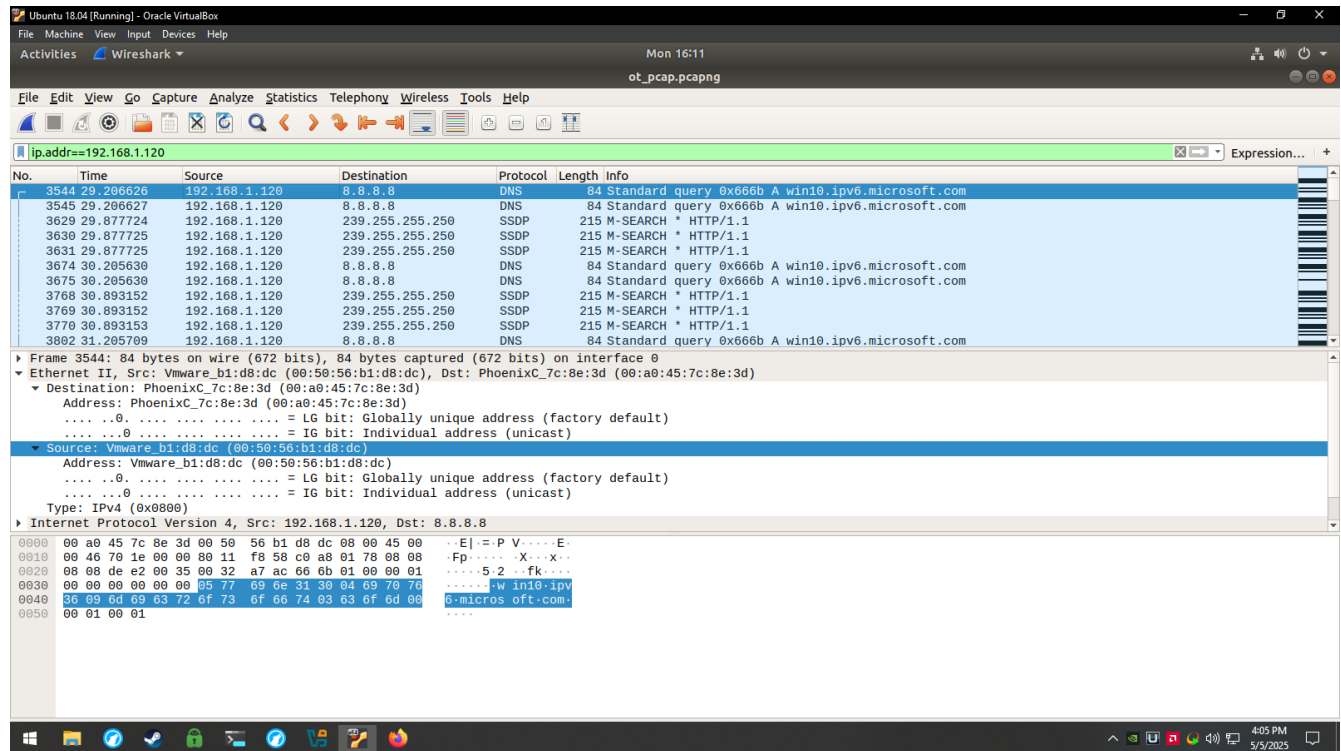


Figure 1: 192.168.1.120 Source Detail

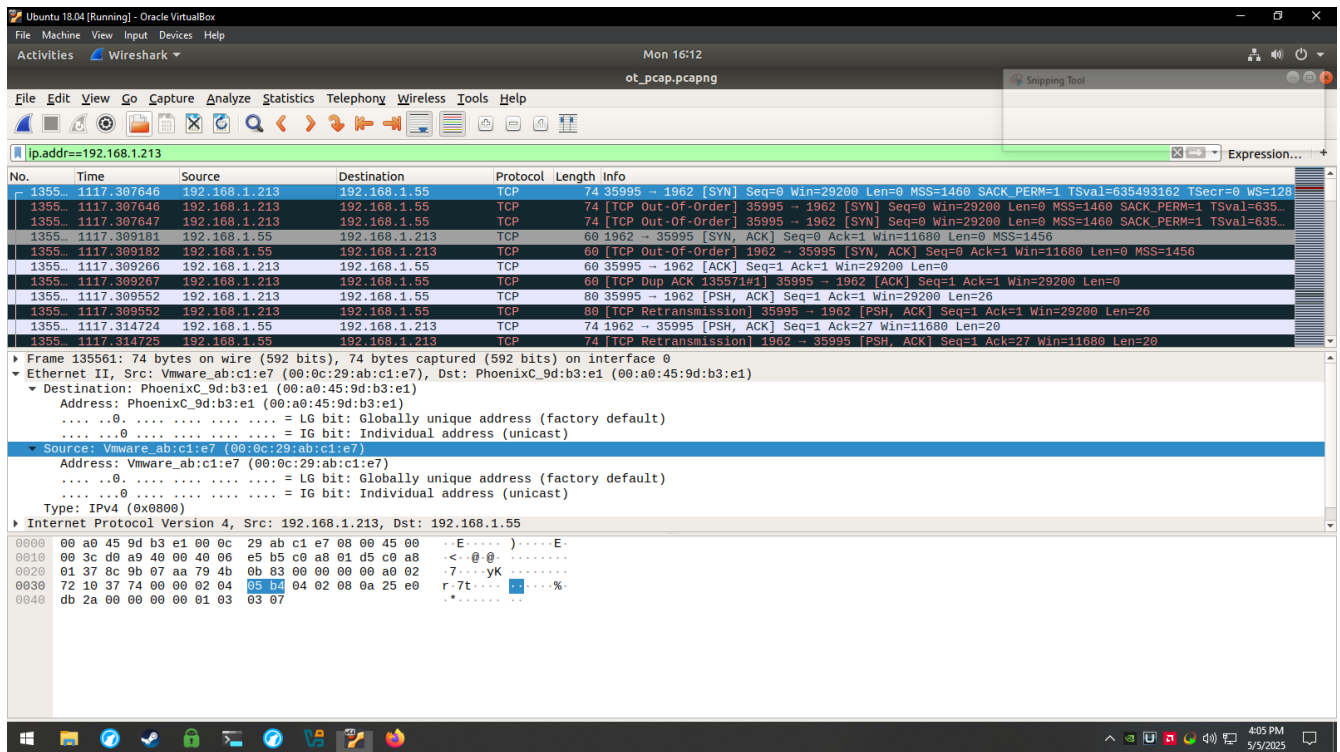


Figure 2: 192.168.1.213 Source Detail

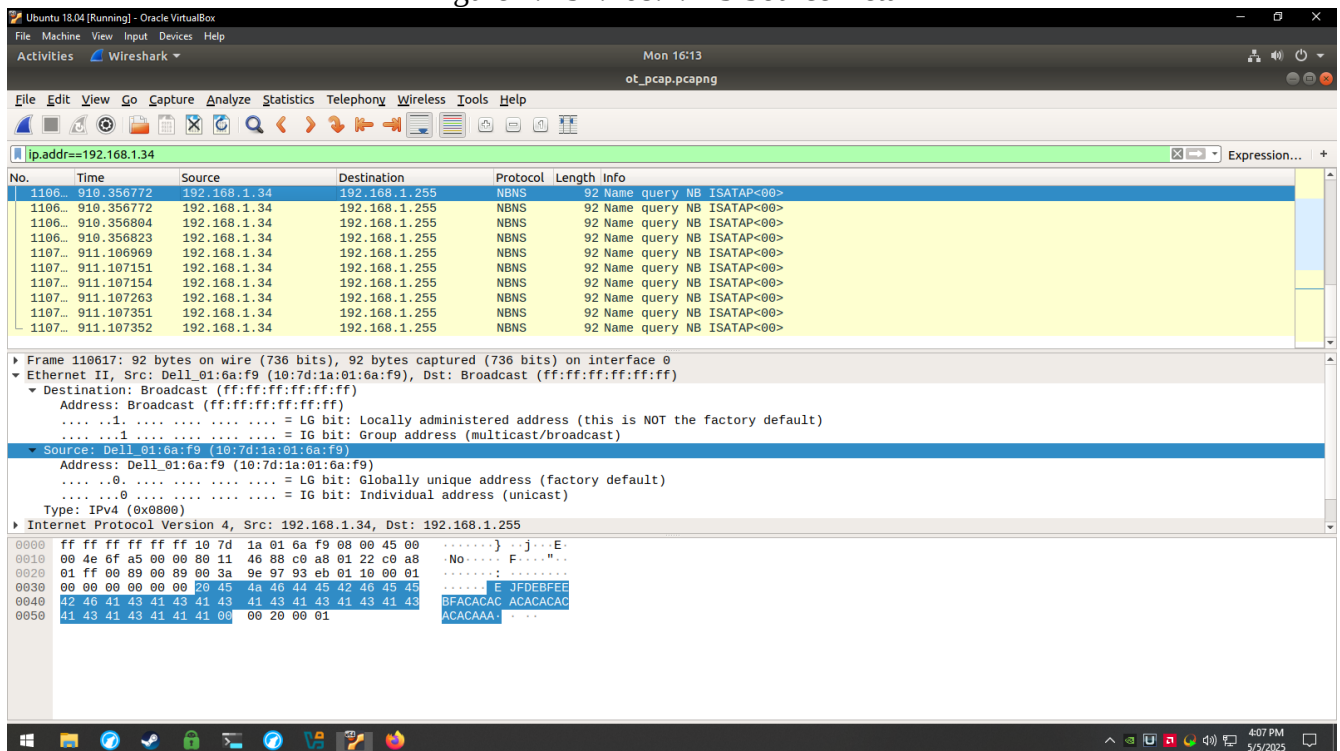


Figure 3: 192.168.1.34 Source Detail

**2.)** Use bro-cut to parse the conn.log file. Is there a host which initiates a high number of TCP connections?

Using bro-cut to show the host and destination IP and port and protocol, and filtering for TCP using grep, there are only 6 lines that use TCP. 4 of which are from 192.168.1.213 to another device on the network 192.168.1.55, one from 192.168.1.101 to another local device 192.168.1.10, and one from 192.168.1.122 to 192.168.1.10 as before. None of the hosts make a significant amount of connections but the number of packets between 192.168.101 and 192.168.1.122 communicating with 192.168.1.10 on port 44818 are higher than the rest.

```
alex@alex-VirtualBox:~$ cat '/home/alex/Downloads/lab14/conn.log' | bro-cut id.orig_h id.orig_p id.resp_h id.resp_p proto | grep tcp
192.168.1.213 35995 192.168.1.55 1962 tcp
192.168.1.213 33063 192.168.1.55 41100 tcp
192.168.1.213 34311 192.168.1.55 41100 tcp
192.168.1.213 39903 192.168.1.55 41100 tcp
192.168.1.101 49224 192.168.1.10 44818 tcp
192.168.1.122 50901 192.168.1.10 44818 tcp
alex@alex-VirtualBox:~$ cat '/home/alex/Downloads/lab14/conn.log' | grep tcp
1515808844.280223 Cwxx6h3y32mdZjWHE7 192.168.1.213 35995 192.168.1.55 1962 tcp - 0.016877 62 214 RSTR - - 0 S
hAddFar 15 784 12 916 (empty)
1515808844.299258 C9WAjd4HnrGh8pPOLF 192.168.1.213 33063 192.168.1.55 41100 tcp - 0.106405 1335 546 SF - - 0 S
hAdadFF 58 5030 72 3980 (empty)
1515808845.737435 CwB35S2NPu7JP1qvXh 192.168.1.213 34311 192.168.1.55 41100 tcp - 0.084502 1335 546 SF - - 0 S
hAdadFF 58 5030 70 3900 (empty)
1515808844.398945 Cdjlqo16s3edoueNO 192.168.1.213 39903 192.168.1.55 41100 tcp - 1.427764 1327 526 SF - - 0 S
hAdadFF 60 5094 68 3780 (empty)
1515807726.972577 C6HGT6V6edAPjLU41 192.168.1.101 49224 192.168.1.10 44818 tcp - 1527.224618 20578378 7749000 OTH - - 0
Dada 43146 22304218 45499 9568960 (empty)
1515807726.986482 Cb7yXjsOVgN7hNAD08 192.168.1.122 50901 192.168.1.10 44818 tcp - 1527.196561 1471896 1688874 OTH - - 0 A
Dad 37662 2978376 37813 3201394 (empty)
alex@alex-VirtualBox:~$
```

Figure 4: Bro-cut showing TCP connections

**3.)** Use Wireshark to examine the most “talkative” host’s traffic. Does this look like Nmap scanning  
Note: "Talkative" means- the most packets or traffic/sessions seen

The host 192.168.1.10 has the largest number of packets in Wireshark’s endpoints view. It communicated many CIP and ACK packets with 192.168.101 and 192.168.122 with the destination port being 44818. This seems to show legitimate “Common Industrial Protocol” traffic on the known port for CIP 44818.

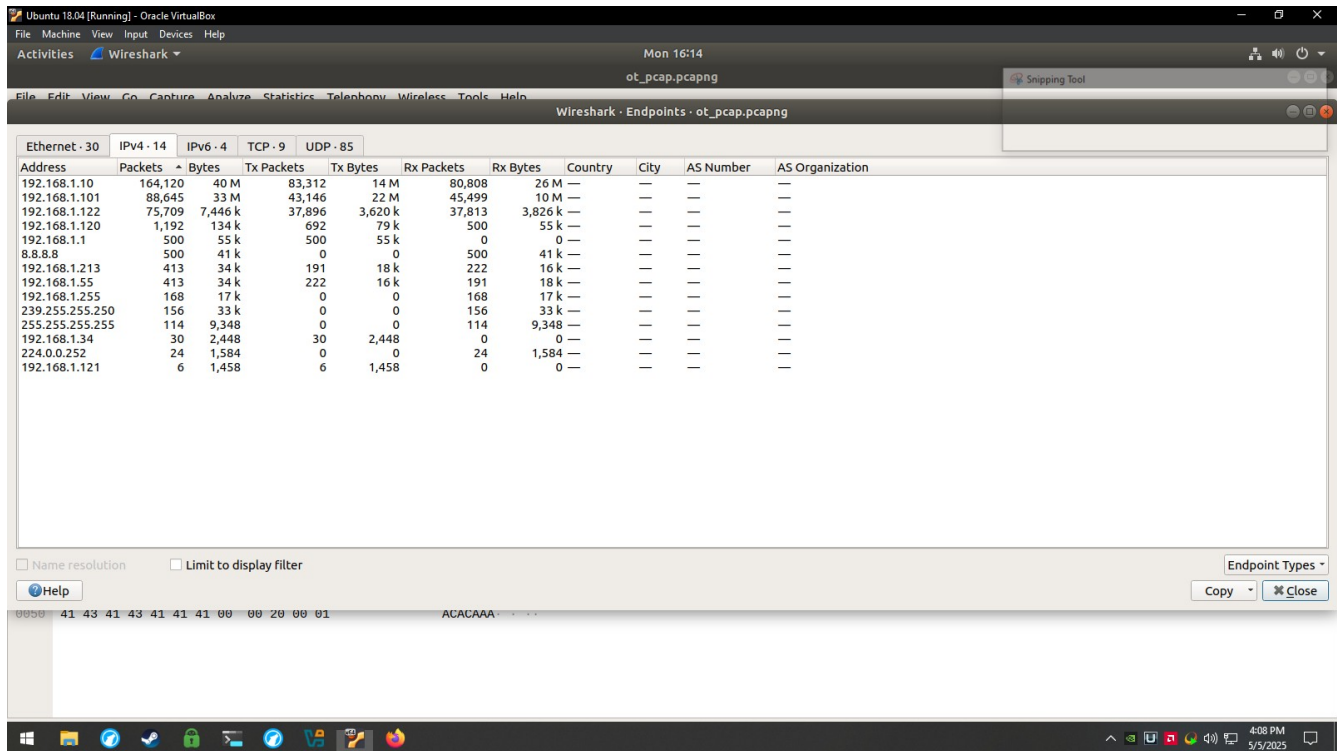


Figure 5: 192.168.1.10 has the most packets

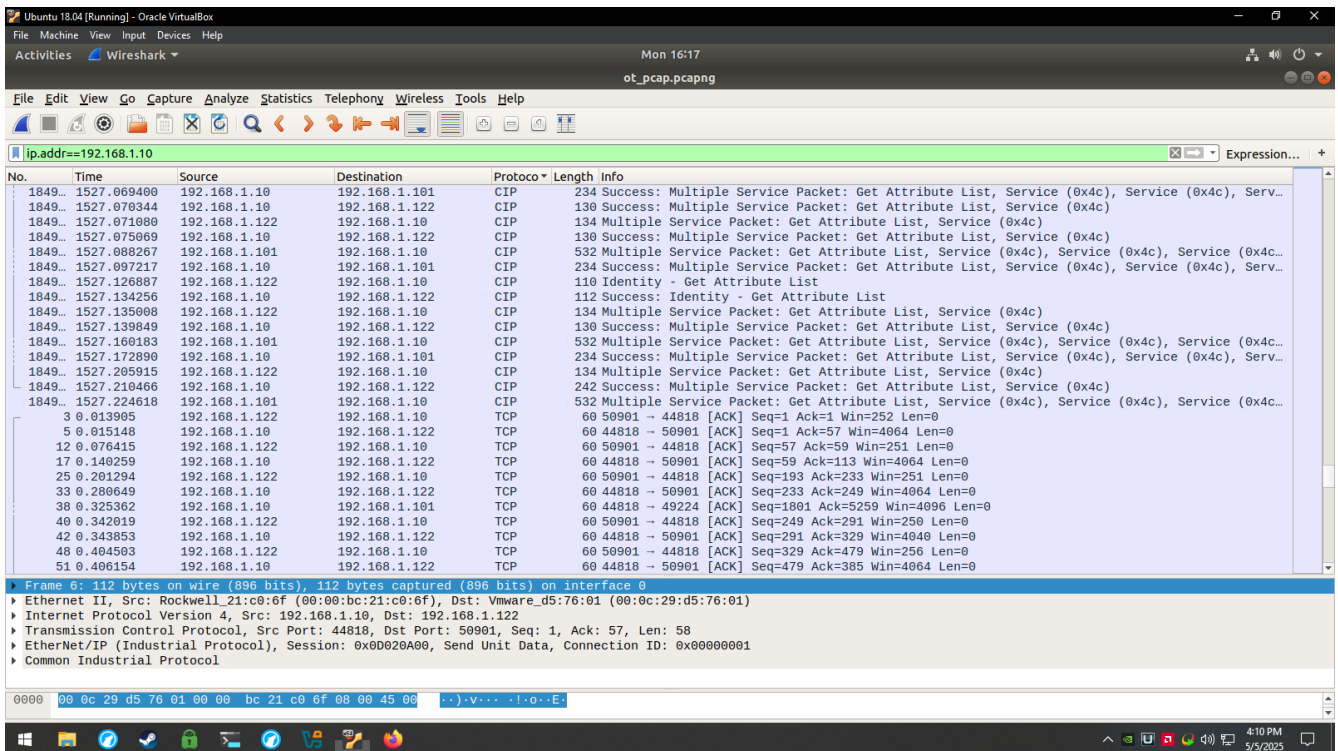


Figure 6: CIP and ACK traffic to and from 192.168.1.10



4.) Each entry in the conn.log file has a “proto” field. Use grep and bro-cut to count the number of ICMP connections. Is there evidence of ping sweeping?

There is only one entry that has ICMP in conn.log where presumably the router at 192.168.1.1 communicates with 192.168.1.120. In wireshark the traffic looks to be multiple failed attempts to query or resolve subdomains on google.com like “clients2.google.com”

```
alex@alex-VirtualBox:~/Downloads/lab14$ cat '/home/alex/Downloads/lab14/conn.log' | grep icmp
1515807759.176461 CAD4A13Juk80L06Yue 192.168.1.1 3 192.168.1.120 1 icmp - 1486.814020 34740 0 0TH - - 0 -
500 48740 0 0 (empty)
```

Figure 6: bro-cut showing ICMP lines

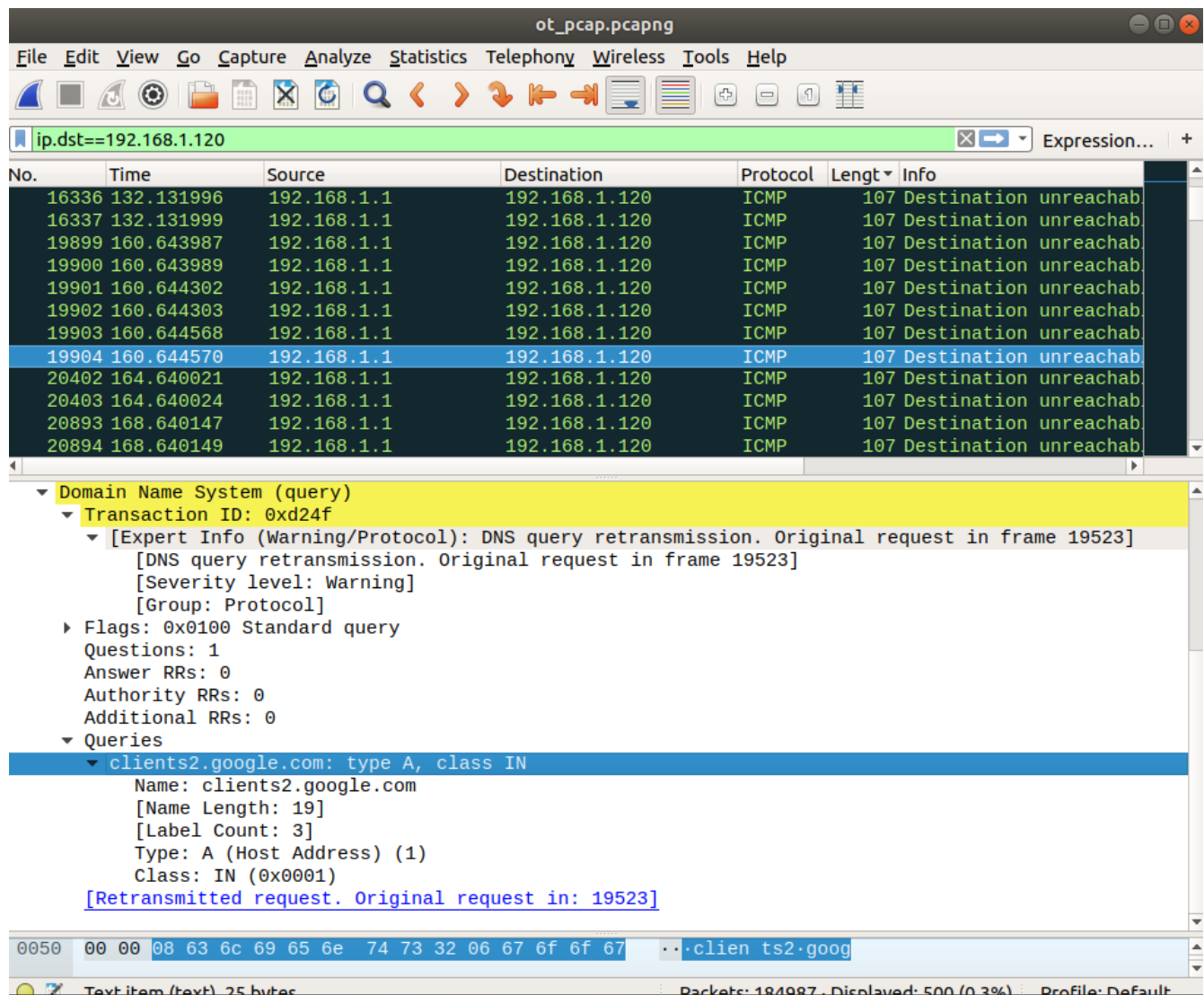


Figure 7: ICMP packets to 192.168.1.120 in wireshark

**5.)** Each conn.log entry has a field “id.resp\_p” which indicates the destination port. Use bro-cut to summarize the connections between hosts in terms of port number. Google any suspicious port numbers you find. Is there evidence of exploitation?

See appendix for a full list of IP/ports

There are several destination ports listed in conn.log, totaling 11. Port 44818 we saw as CIP traffic common for ICS systems. Port 53 is DNS traffic that seems to go to Google’s public DNS. Port 547 is commonly used for DHCPv6 addressing, which should be legitimate traffic. Port 1900 seems to be legitimate traffic to a multicast IP address, which is commonly used for SSDP Simple Service Discovery protocol but it could be used for scanning. Ports 137 and 138 seem to be for Windows NetBIOS which could be legitimate traffic or scanning for vulnerable Windows services. Port 5355 seems to be name discovery for host or MAC address, which could be used for scanning or legitimate traffic. But port 1, 1947, 1962, and 41100, seem to be unusual ports, with port 1 being uncommonly use, and the rest being non standard or product related that could be legitimate depending on the vendor and products on the network, or ephemeral ports that could be used in an attempt to scan the network.

```
alex@alex-VirtualBox:~/Downloads/lab14$ cat '/home/alex/Downloads/lab14/conn.log' | bro-cut id.resp_p | sort | uniq
1
137
138
1900
1947
1962
41100
44818
53
5355
547
```

Figure 8: Destination port numbers found in conn.log

# Appendix

Ports part 1:

```
alex@alex-VirtualBox:~/Downloads/lab14$ cat '/home/alex/Downloads/lab14/conn.log' | bro-cut id.orig_h id.orig_p id.resp_h id.resp_p | sort | uniq
192.168.1.101 49224 192.168.1.10 44818
192.168.1.120 137 192.168.1.255 137
192.168.1.120 138 192.168.1.255 138
192.168.1.120 49399 8.8.8.8 53
192.168.1.120 50155 8.8.8.8 53
192.168.1.120 50247 8.8.8.8 53
192.168.1.120 50248 239.255.255.250 1900
192.168.1.120 50612 8.8.8.8 53
192.168.1.120 50883 8.8.8.8 53
192.168.1.120 51041 8.8.8.8 53
192.168.1.120 51042 239.255.255.250 1900
192.168.1.120 51644 8.8.8.8 53
192.168.1.120 53100 8.8.8.8 53
192.168.1.120 53108 8.8.8.8 53
192.168.1.120 53157 8.8.8.8 53
192.168.1.120 53158 239.255.255.250 1900
192.168.1.120 53164 8.8.8.8 53
192.168.1.120 53171 8.8.8.8 53
192.168.1.120 53424 8.8.8.8 53
192.168.1.120 53525 8.8.8.8 53
192.168.1.120 53526 239.255.255.250 1900
192.168.1.120 53539 8.8.8.8 53
192.168.1.120 53702 8.8.8.8 53
192.168.1.120 54447 8.8.8.8 53
192.168.1.120 54530 8.8.8.8 53
192.168.1.120 54531 239.255.255.250 1900
192.168.1.120 54979 8.8.8.8 53
192.168.1.120 55104 8.8.8.8 53
192.168.1.120 55105 239.255.255.250 1900
192.168.1.120 55248 8.8.8.8 53
192.168.1.120 55481 8.8.8.8 53
192.168.1.120 55628 8.8.8.8 53
192.168.1.120 55629 239.255.255.250 1900
192.168.1.120 55880 8.8.8.8 53
192.168.1.120 56549 8.8.8.8 53
192.168.1.120 56951 8.8.8.8 53
192.168.1.120 57016 224.0.0.252 5355
192.168.1.120 57058 8.8.8.8 53
192.168.1.120 57059 239.255.255.250 1900
192.168.1.120 57120 8.8.8.8 53
192.168.1.120 57182 8.8.8.8 53
192.168.1.120 57183 239.255.255.250 1900
192.168.1.120 57436 8.8.8.8 53
192.168.1.120 57437 239.255.255.250 1900
192.168.1.120 57494 8.8.8.8 53
192.168.1.120 58000 8.8.8.8 53
192.168.1.120 58597 8.8.8.8 53
192.168.1.120 58618 8.8.8.8 53
192.168.1.120 58682 8.8.8.8 53
192.168.1.120 59274 8.8.8.8 53
192.168.1.120 59275 239.255.255.250 1900
192.168.1.120 59379 8.8.8.8 53
192.168.1.120 59654 8.8.8.8 53
192.168.1.120 60909 8.8.8.8 53
192.168.1.120 61244 8.8.8.8 53
192.168.1.120 61625 8.8.8.8 53
```



## Ports part 2:

```
192.168.1.120 55105 239.255.255.250 1900
192.168.1.120 55248 8.8.8.8 53
192.168.1.120 55481 8.8.8.8 53
192.168.1.120 55628 8.8.8.8 53
192.168.1.120 55629 239.255.255.250 1900
192.168.1.120 55880 8.8.8.8 53
192.168.1.120 56549 8.8.8.8 53
192.168.1.120 56951 8.8.8.8 53
192.168.1.120 57016 224.0.0.252 5355
192.168.1.120 57058 8.8.8.8 53
192.168.1.120 57059 239.255.255.250 1900
192.168.1.120 57120 8.8.8.8 53
192.168.1.120 57182 8.8.8.8 53
192.168.1.120 57183 239.255.255.250 1900
192.168.1.120 57436 8.8.8.8 53
192.168.1.120 57437 239.255.255.250 1900
192.168.1.120 57494 8.8.8.8 53
192.168.1.120 58000 8.8.8.8 53
192.168.1.120 58597 8.8.8.8 53
192.168.1.120 58618 8.8.8.8 53
192.168.1.120 58682 8.8.8.8 53
192.168.1.120 59274 8.8.8.8 53
192.168.1.120 59275 239.255.255.250 1900
192.168.1.120 59379 8.8.8.8 53
192.168.1.120 59654 8.8.8.8 53
192.168.1.120 60909 8.8.8.8 53
192.168.1.120 61244 8.8.8.8 53
192.168.1.120 61625 8.8.8.8 53
192.168.1.120 61626 239.255.255.250 1900
192.168.1.120 62379 8.8.8.8 53
192.168.1.120 62566 8.8.8.8 53
192.168.1.120 62598 8.8.8.8 53
192.168.1.120 62666 8.8.8.8 53
192.168.1.120 63080 8.8.8.8 53
192.168.1.120 63172 8.8.8.8 53
192.168.1.120 63279 8.8.8.8 53
192.168.1.120 63280 239.255.255.250 1900
192.168.1.120 63381 8.8.8.8 53
192.168.1.120 63541 224.0.0.252 5355
192.168.1.120 64530 8.8.8.8 53
192.168.1.121 138 192.168.1.255 138
192.168.1.122 138 192.168.1.255 138
192.168.1.122 50901 192.168.1.10 44818
192.168.1.122 63993 192.168.1.255 1947
192.168.1.122 63993 255.255.255.255 1947
192.168.1.1 3 192.168.1.120 1
192.168.1.213 33063 192.168.1.55 41100
192.168.1.213 34311 192.168.1.55 41100
192.168.1.213 35995 192.168.1.55 1962
192.168.1.213 39903 192.168.1.55 41100
192.168.1.34 137 192.168.1.255 137
192.168.1.34 50426 224.0.0.252 5355
192.168.1.34 55068 224.0.0.252 5355
fe80::2d5a:70f8:9de5:b43c 57016 ff02::1:3 5355
fe80::2d5a:70f8:9de5:b43c 63541 ff02::1:3 5355
fe80::8d70:c288:7871:b57e 546 ff02::1:2 547
alex@alex-VirtualBox:~/Downloads/Lab14$
```