2.3.5 - Exercises

1. Use Wireshark to capture the network activity of Netcat connecting to port 110

(POP3) and attempting a login.

2. Read and understand the output. Where is the session three-way handshake?

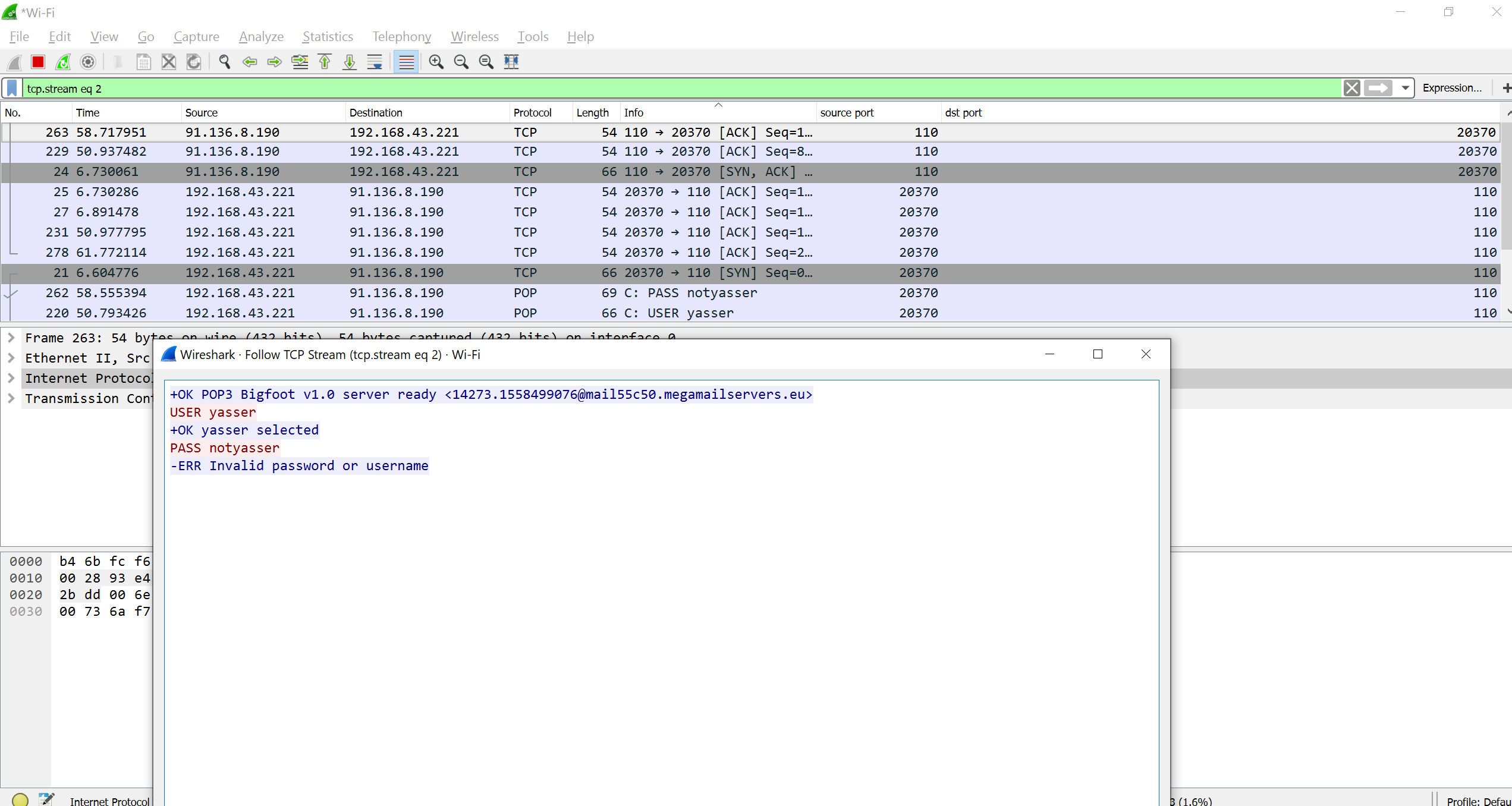
**First 3 packets, SYN, SYN-ACK, ACK**

Where is the session closed?

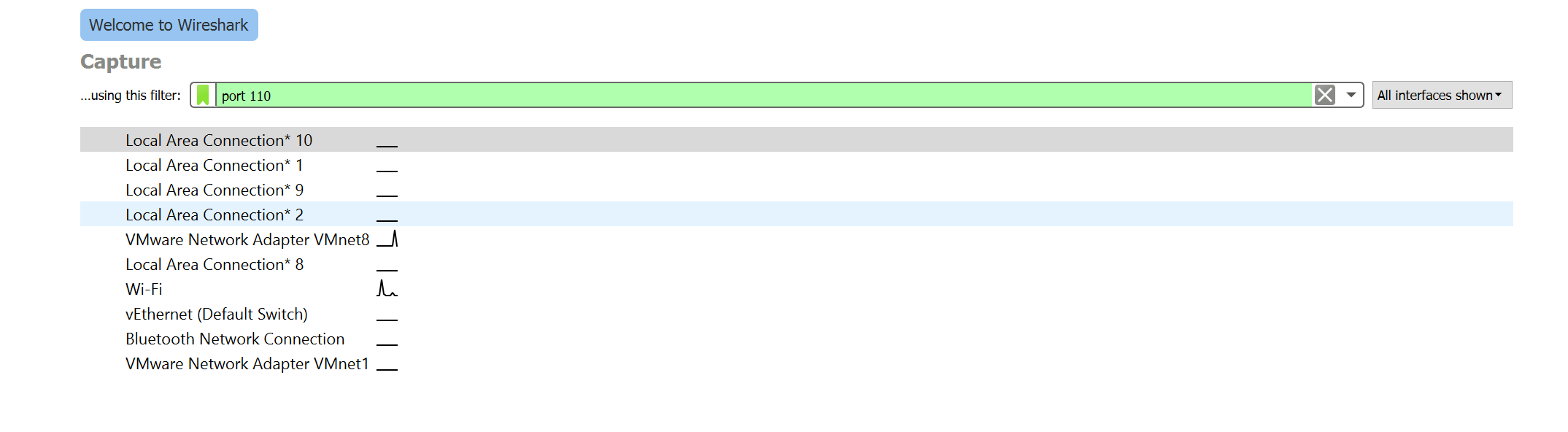
**when typing ( quit ), it sends FIN, ACK to end the connection**

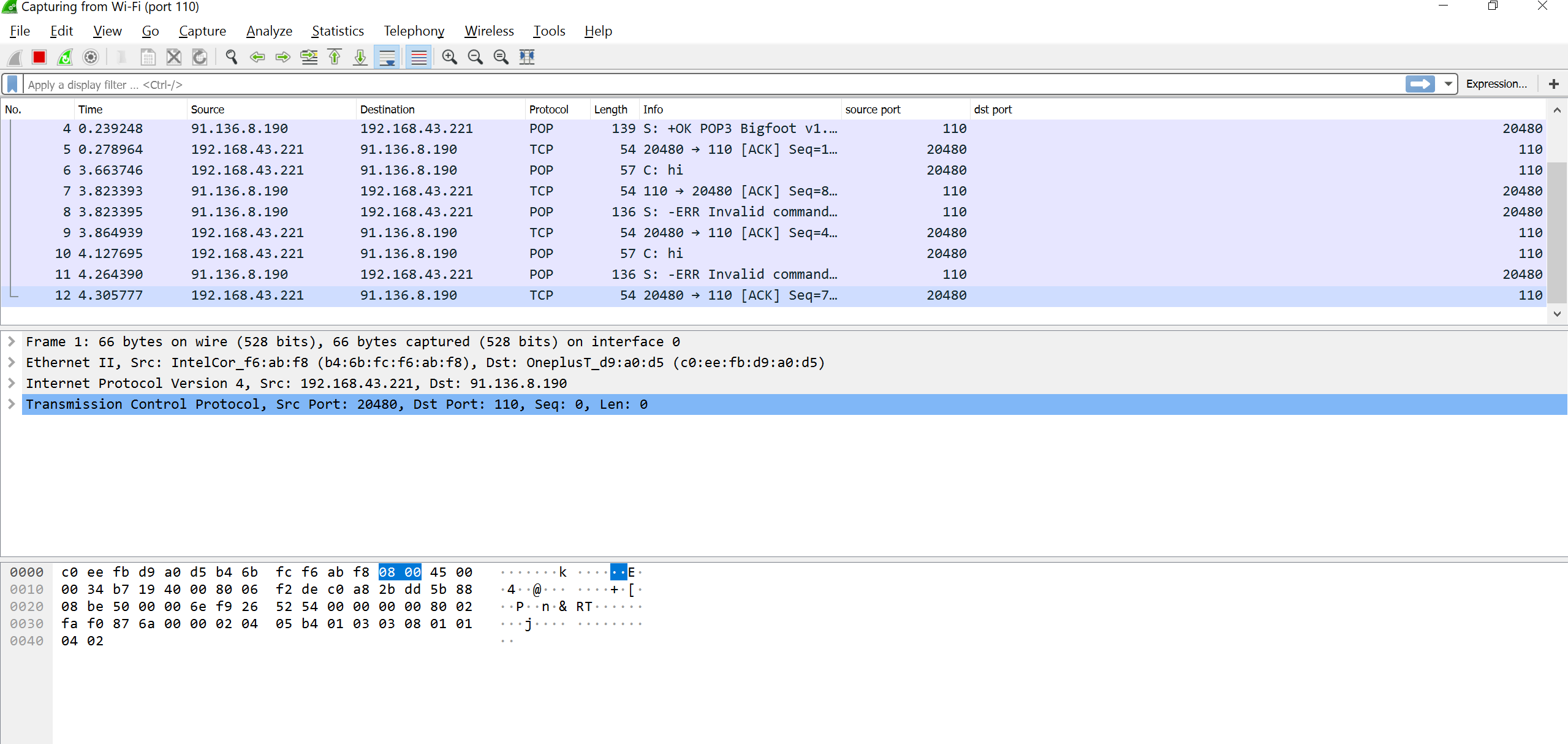
3. Follow the TCP stream to read the login attempt.

4. Use the display filter to only see the port 110 traffic



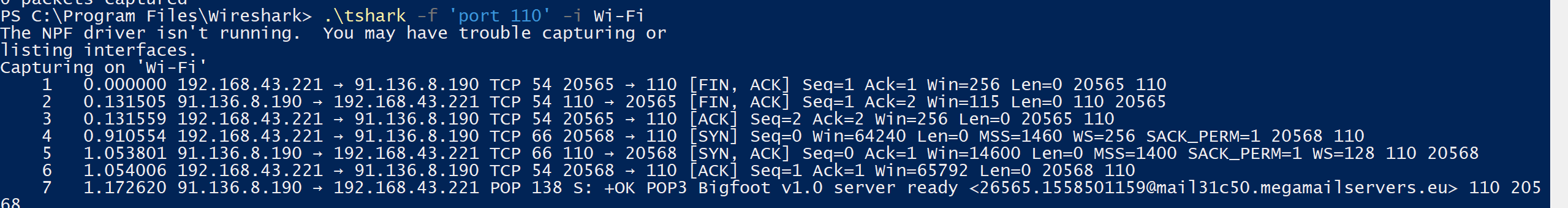
5. Re-run the capture, this time using the capture filter to only collect port 110





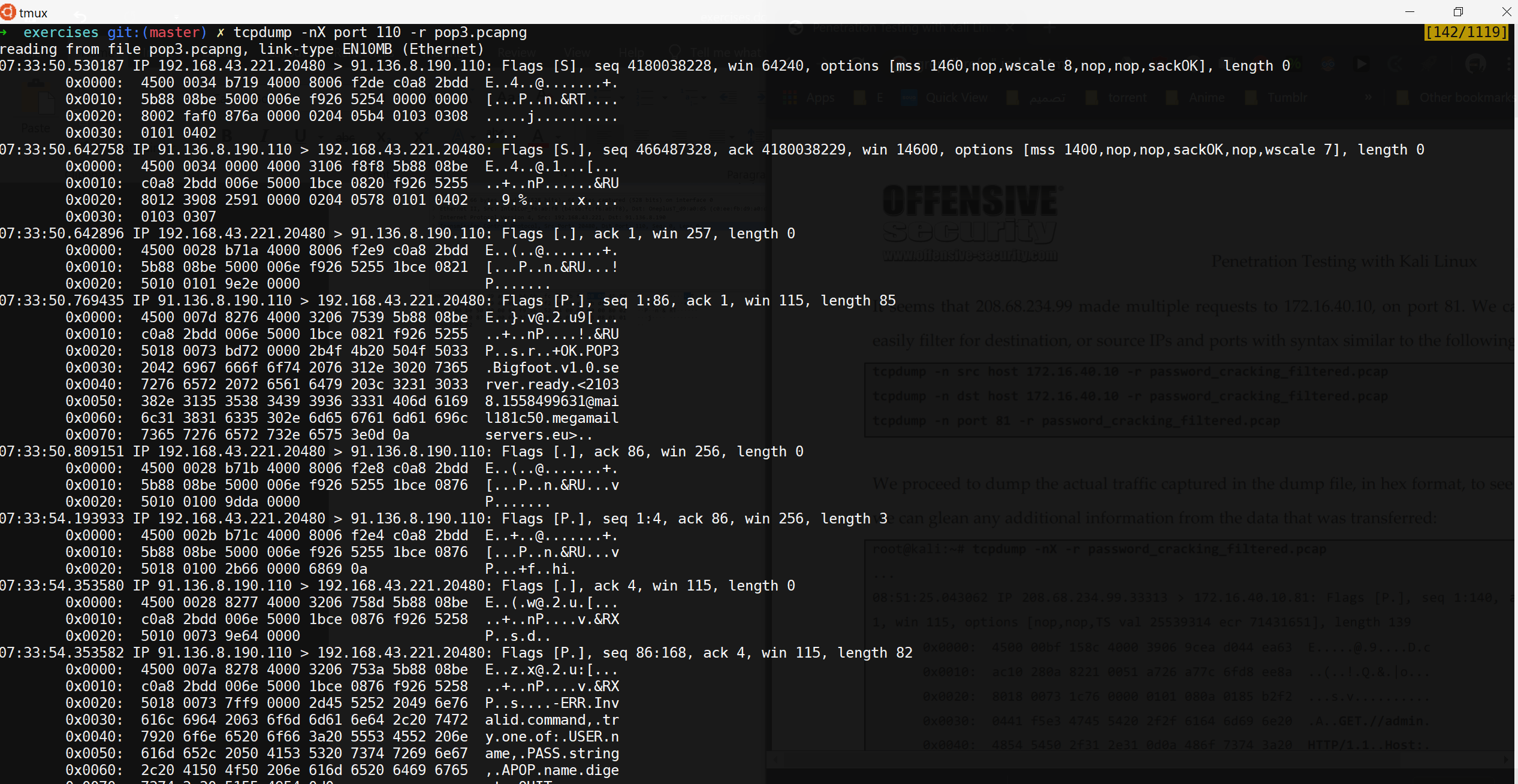
1. Use tcpdump to recreate the wireshark exercise of capturing traffic on port 110.

I don’t have tcpdump on Windows so I used tshark instead,



2. Use the -X flag to view the content of the packet. If data is truncated, investigate

how the -s flag might help



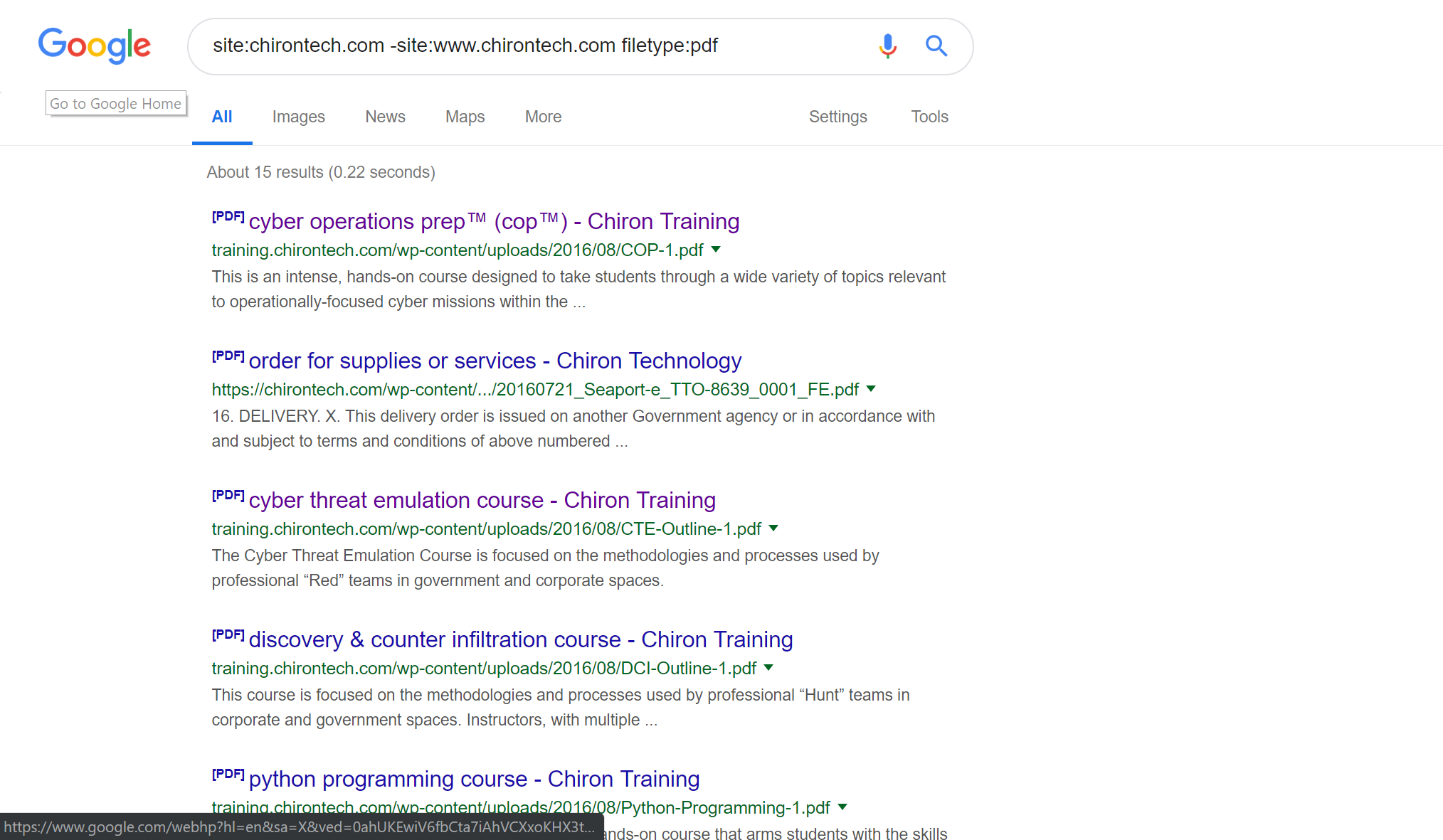
1. Choose an organization and use Google to gather as much information as

possible about it

**ChironTech**

2. Use the Google filetype search operator and look for interesting documents from

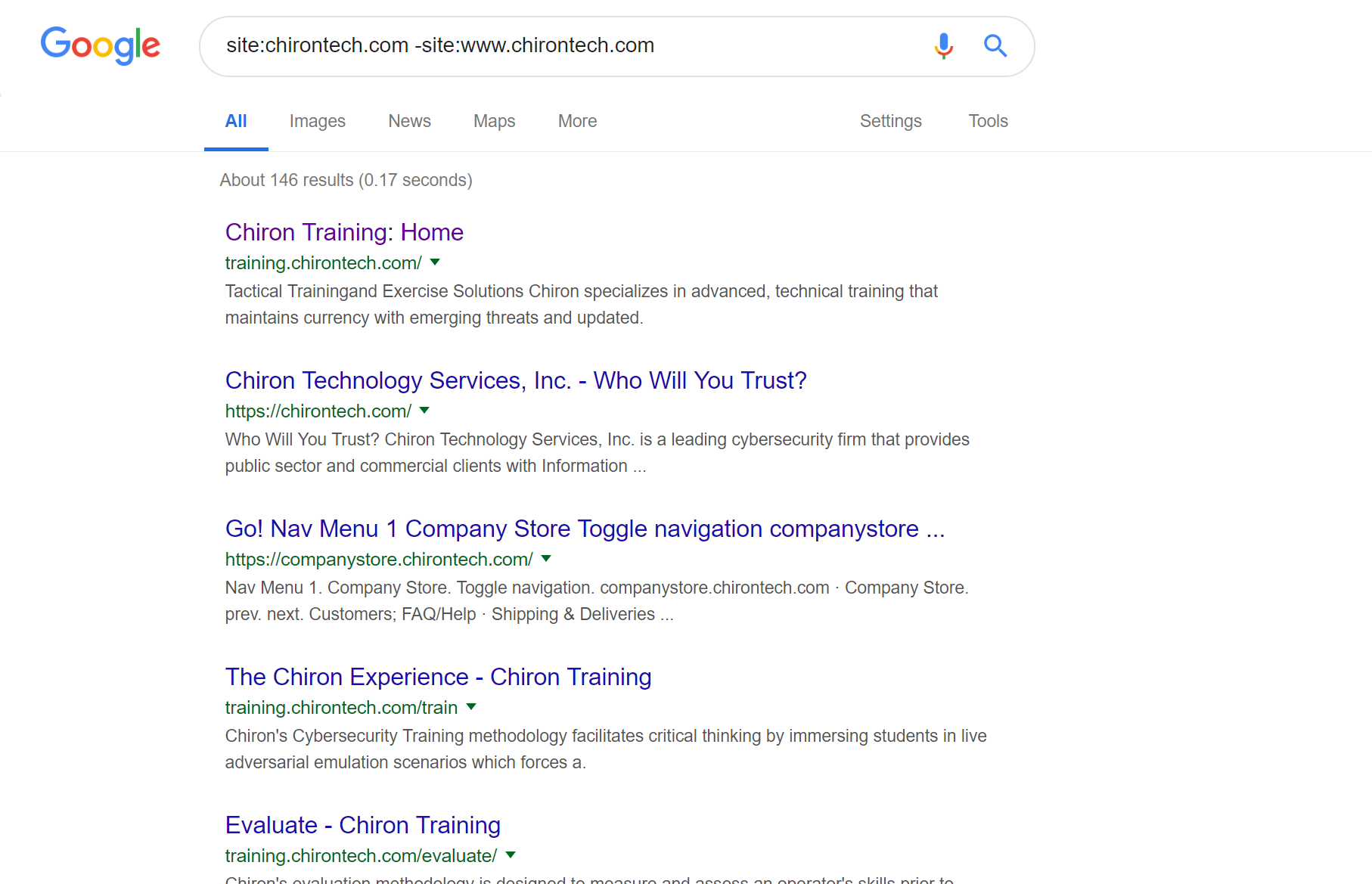
the target organization



3. Re-do the exercise on your company’s domain. Can you find any data leakage

you were not aware of?

**Nothing was found 😊**



3.2.1 - Exercise

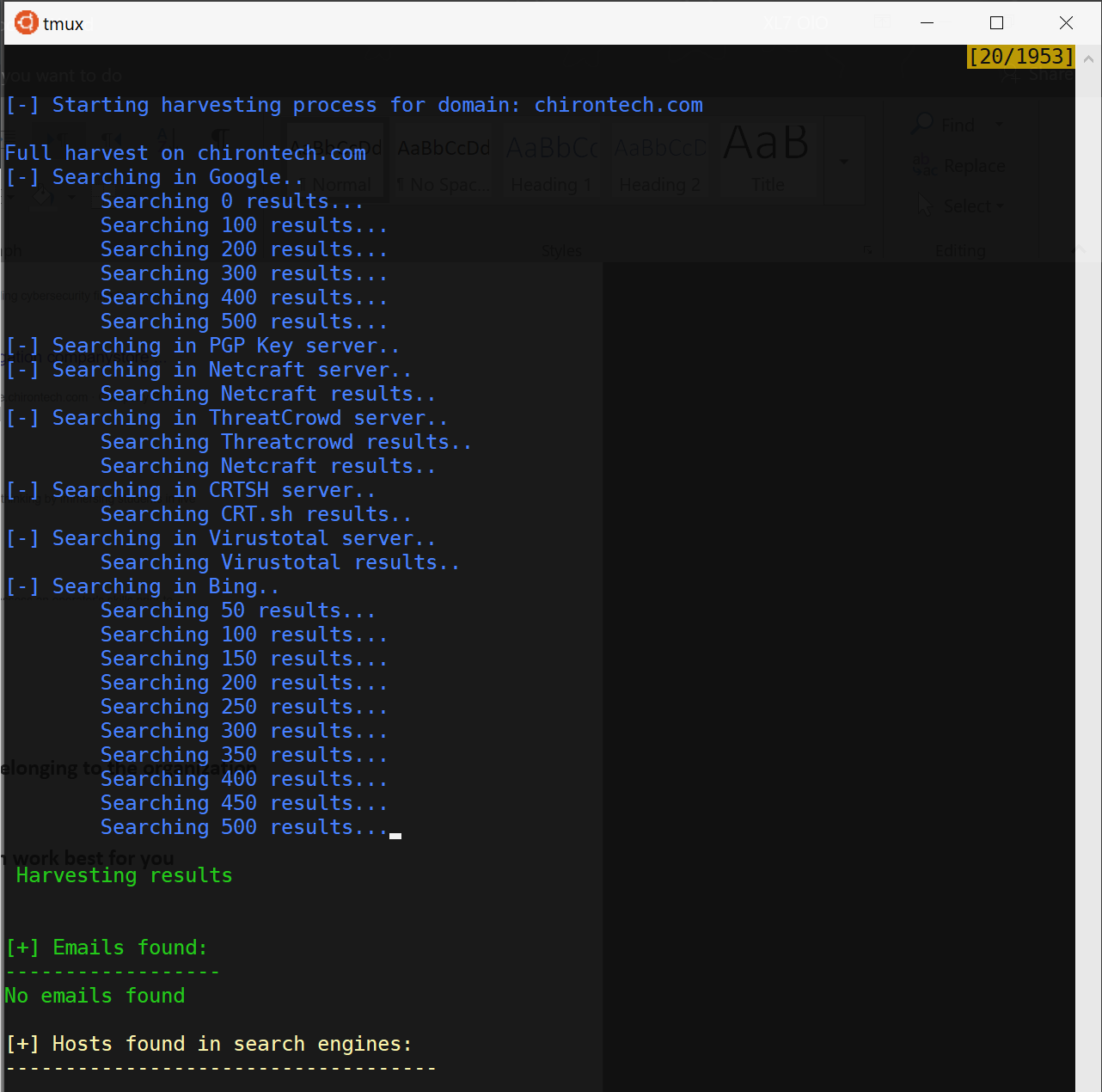
1. Use theharvester to enumerate email addresses belonging to the organization

you chose in the previous exercises

2. Experiment with different data sources (-b). Which work best for you

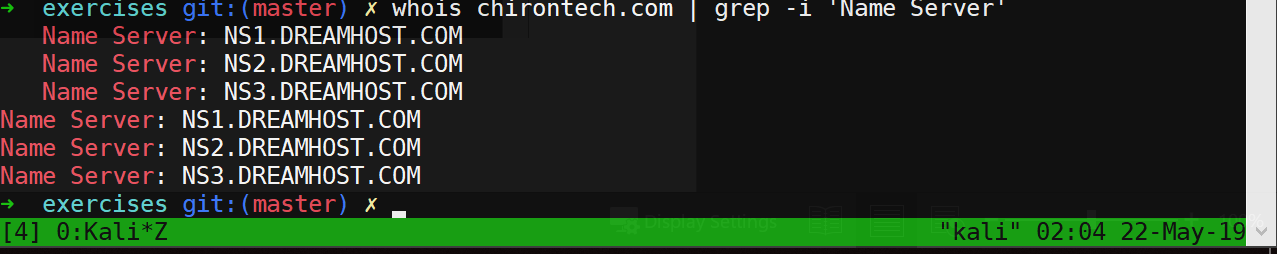
**Tried with the all flag, but no email was found !!**

**Anyway google is very effective and usually it yields the best results for me**

****

3.3.3 - Exercise

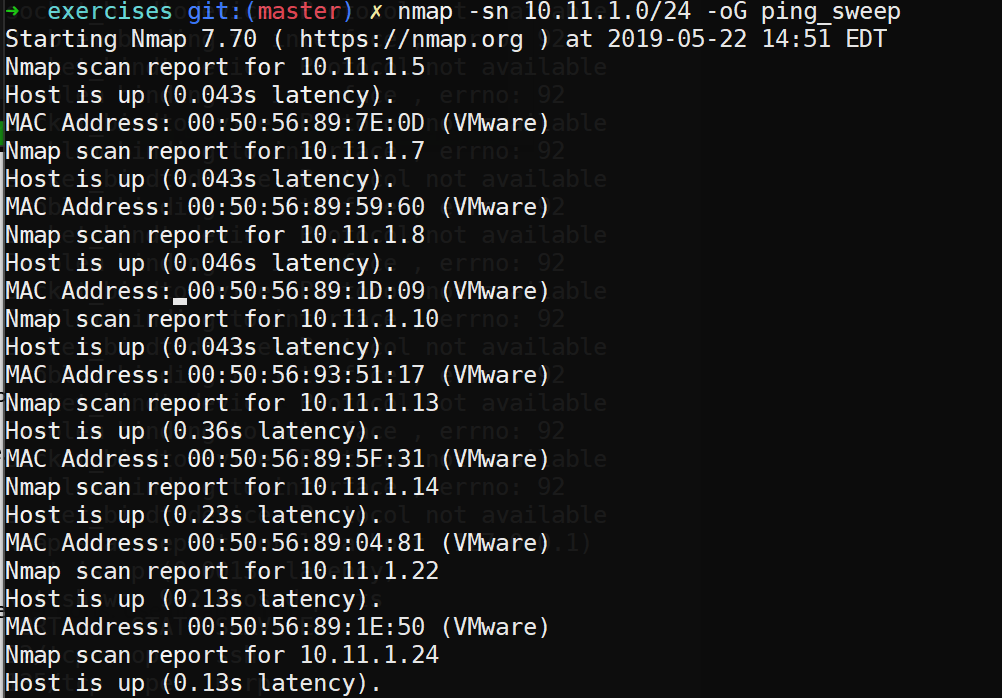
1. Use the whois tool in Kali to identify the name servers of your target organization

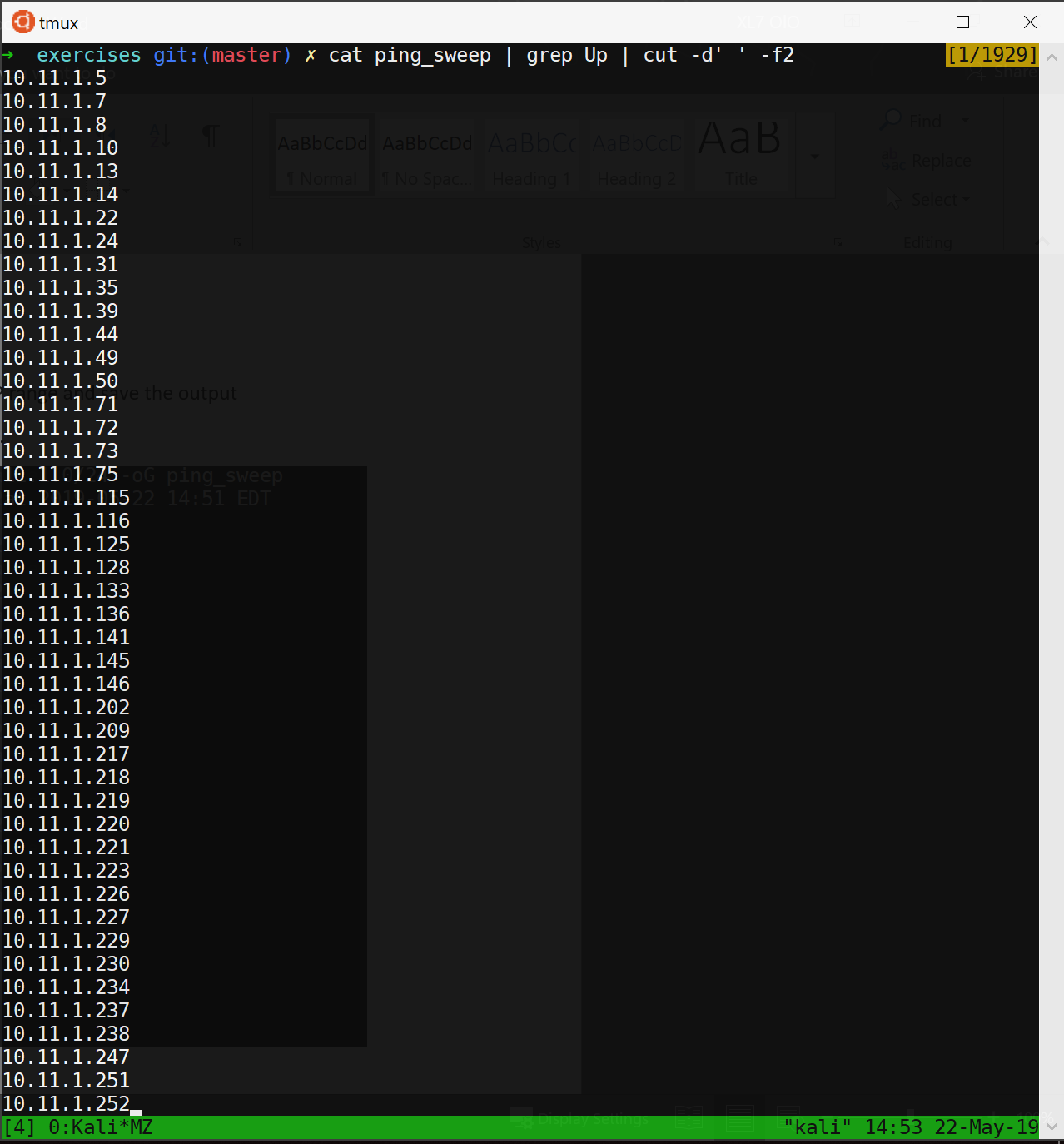
****

4.2.8 - Exercises

1. Use nmap to conduct a ping sweep of your target IP range and save the output

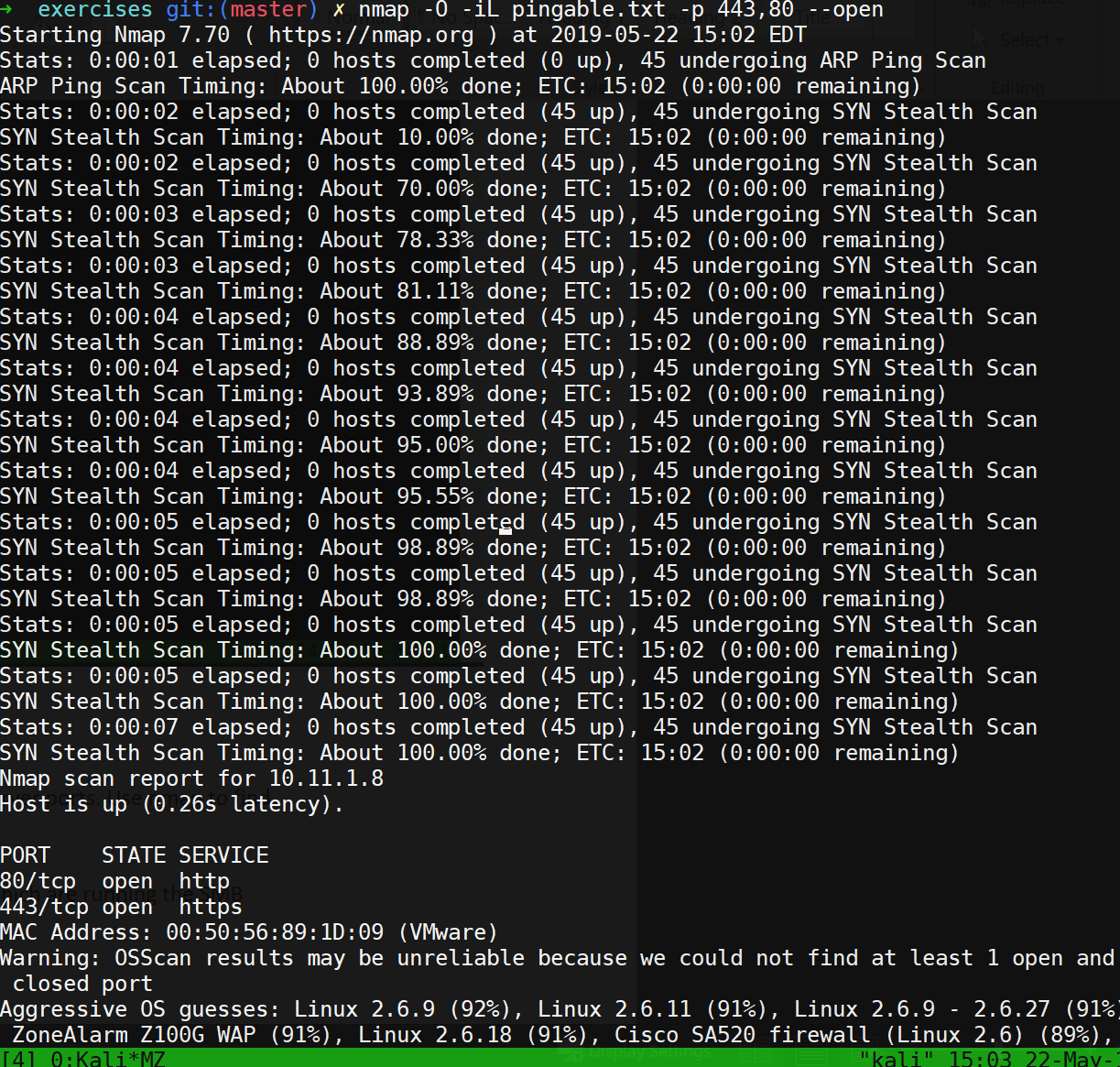
to a file, so that you can grep for hosts that are online.





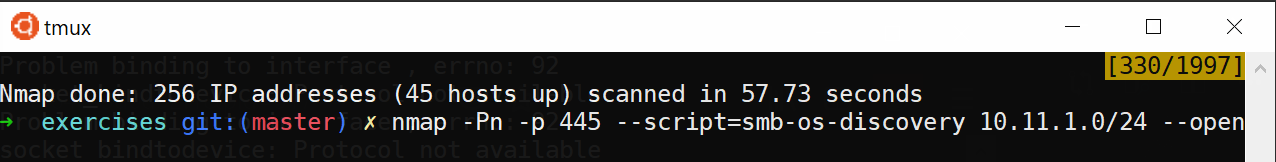
2. Scan the IPs you found in exercise 1 for open webserver ports. Use nmap to find

the web server and operating system versions.



3. Use the NSE scripts to scan the servers in the labs which are running the SMB

service.



4. Explore the various command line options that nmap offers while scanning an

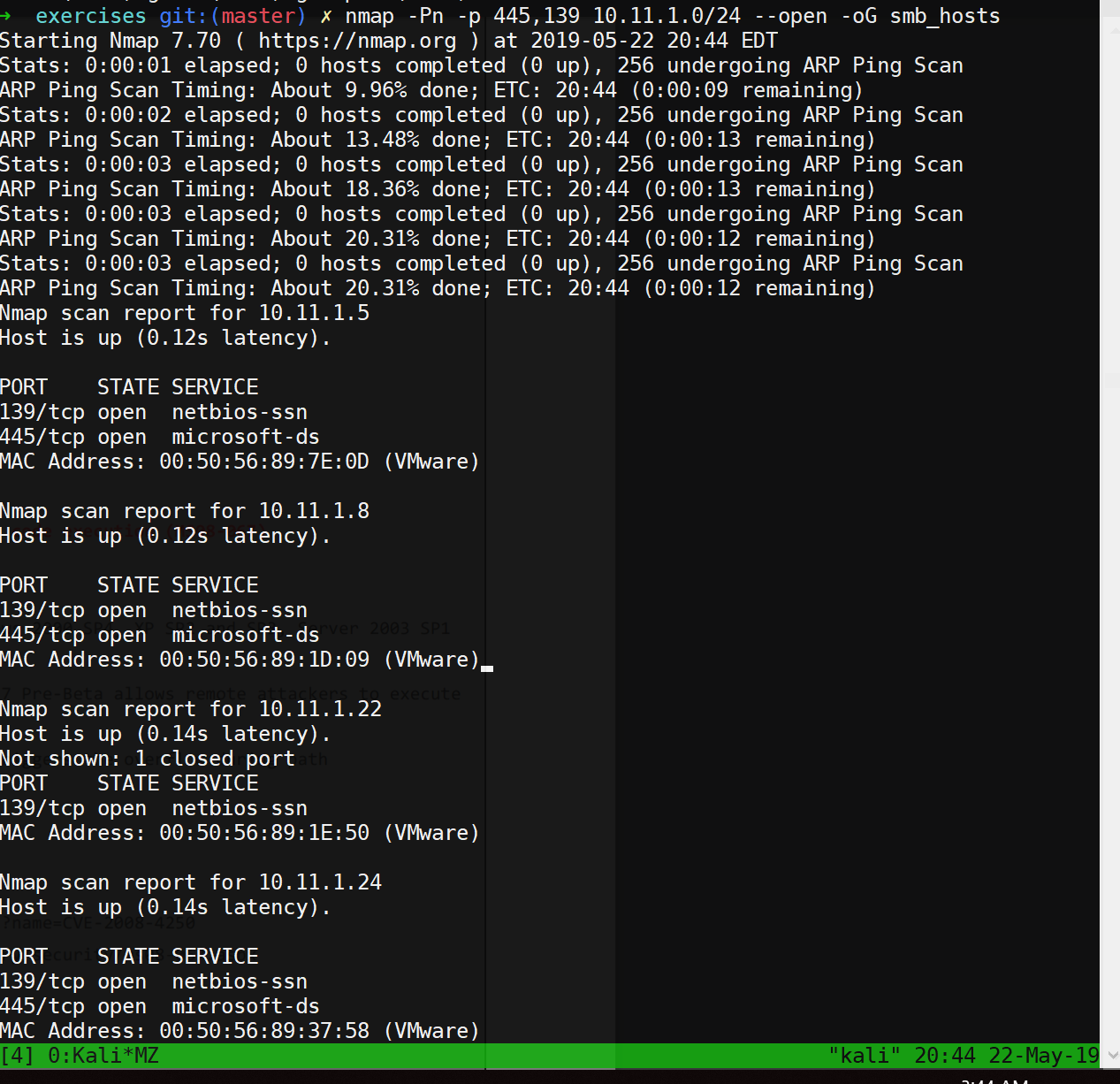
online host you discovered within your target IP range. Monitor the bandwidth

usage changes for the different options. Weigh the use of collecting as much

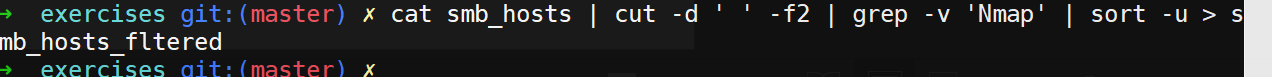
information as possible against the resources it takes to gather it.

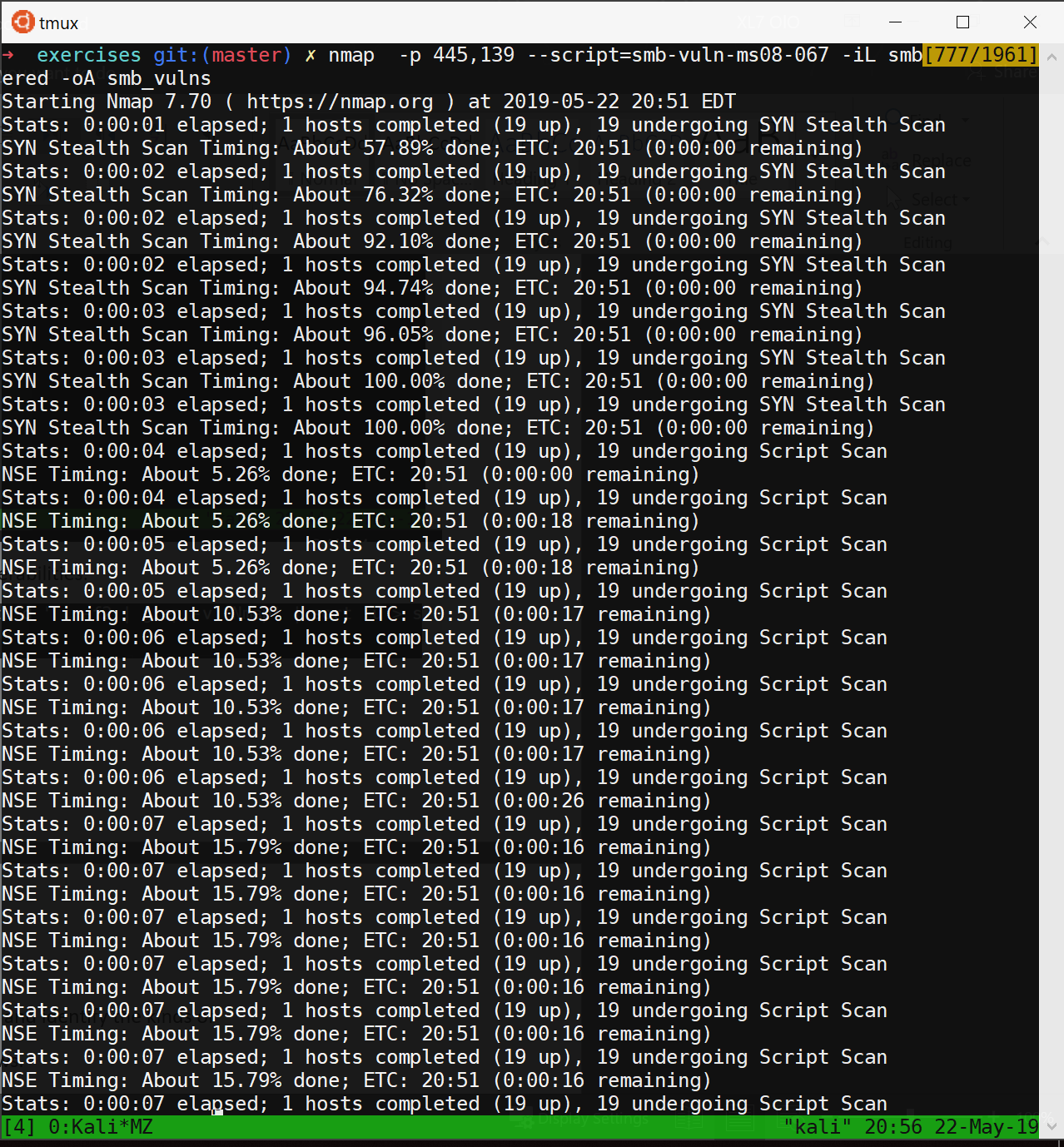
4.3.4 - Exercises

1. Use Nmap to make a list of which SMB servers in the lab are running Windows.



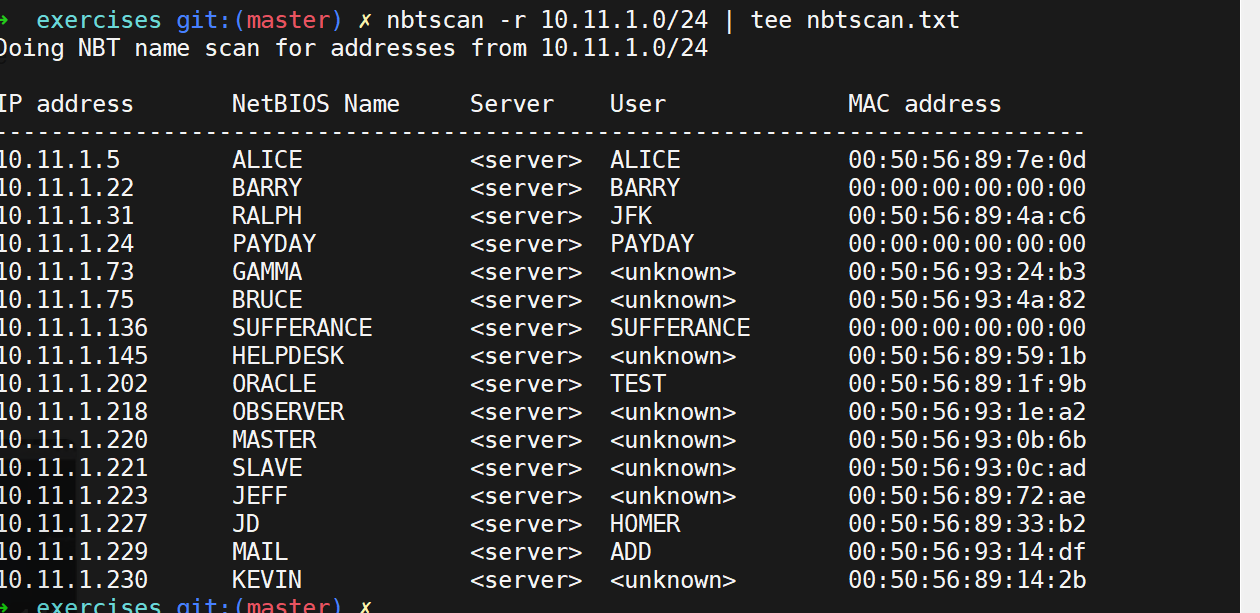
2. Use NSE scripts to scan these systems for SMB vulnerabilities.





3. Use nbtscan and enum4linux against these systems and identify the kinds of

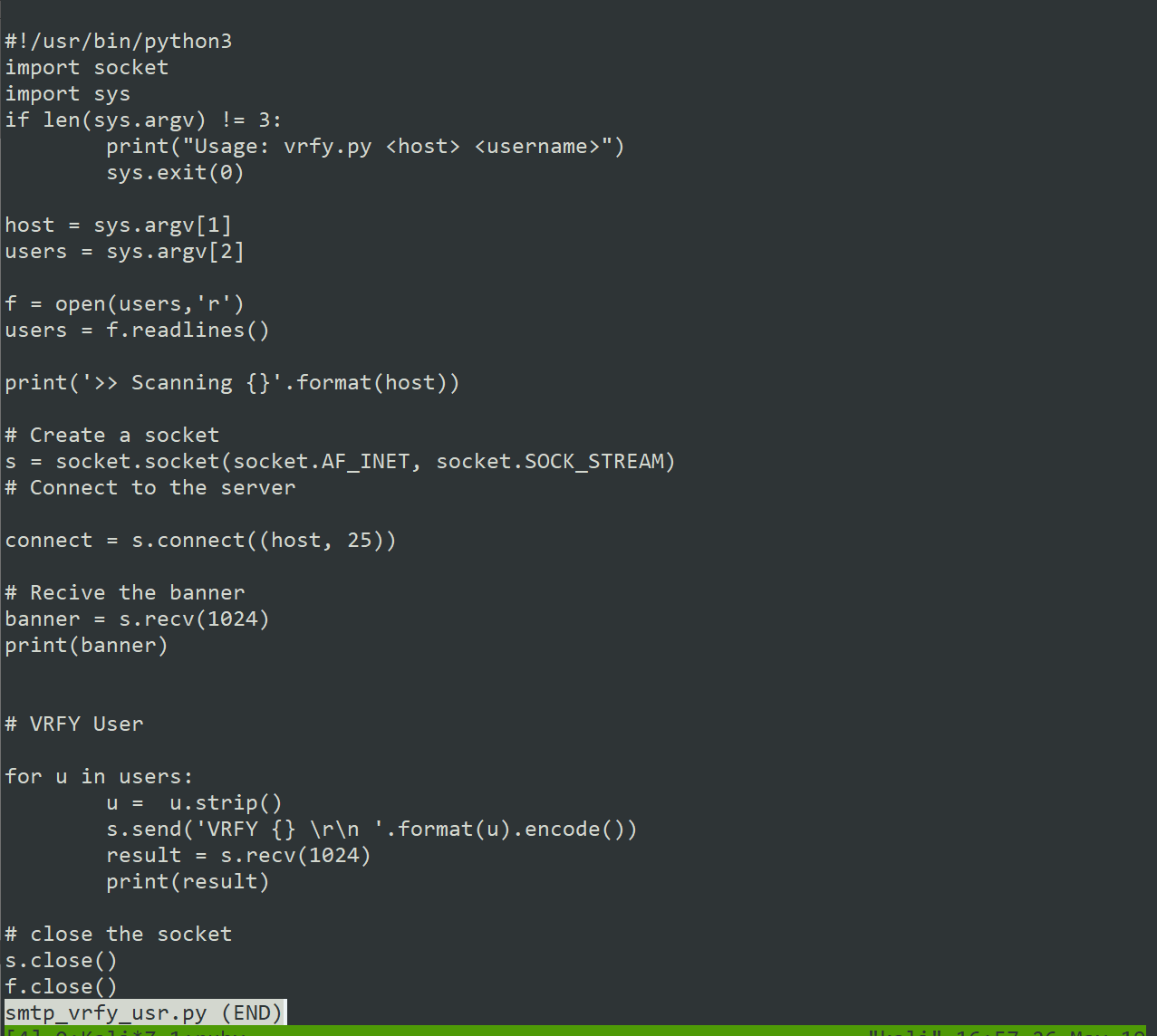
data you can obtain from different versions of Windows.

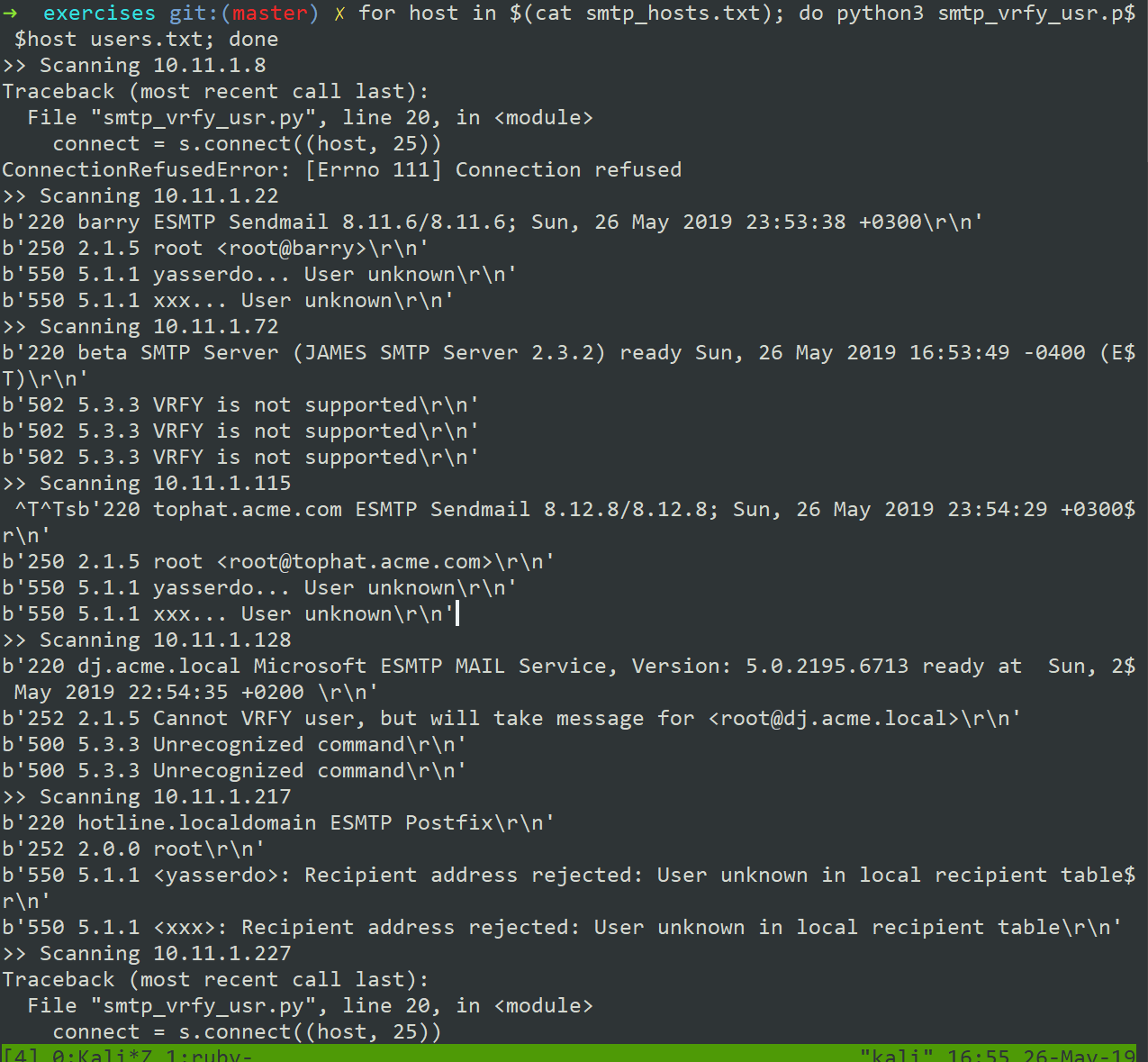




4.4.1 - Exercise 1. Search your target network range, and see if you can identify any systems that respond to the SMTP VRFY command

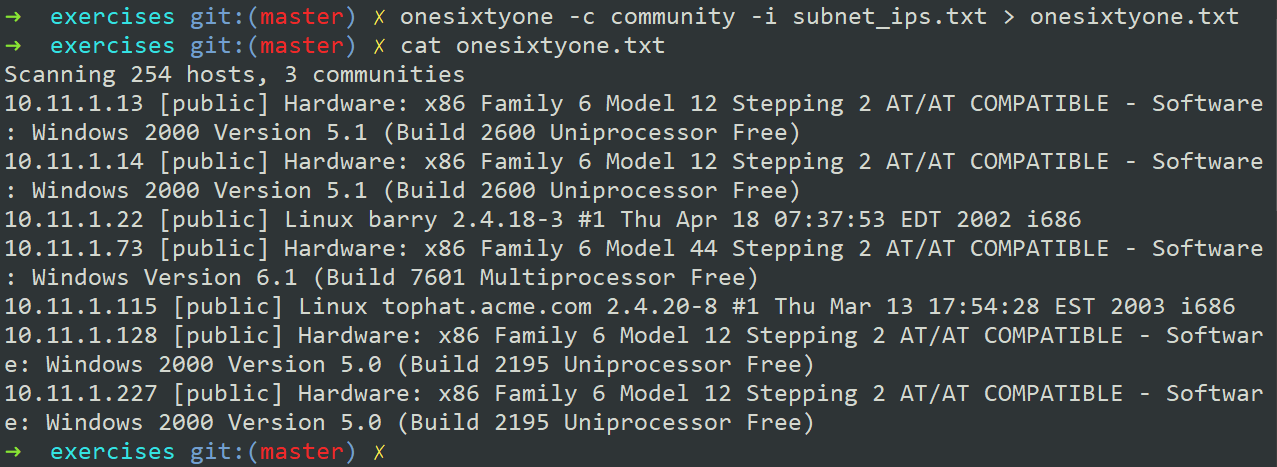
**I wrote this script to enumerate smtp users via a file input.**





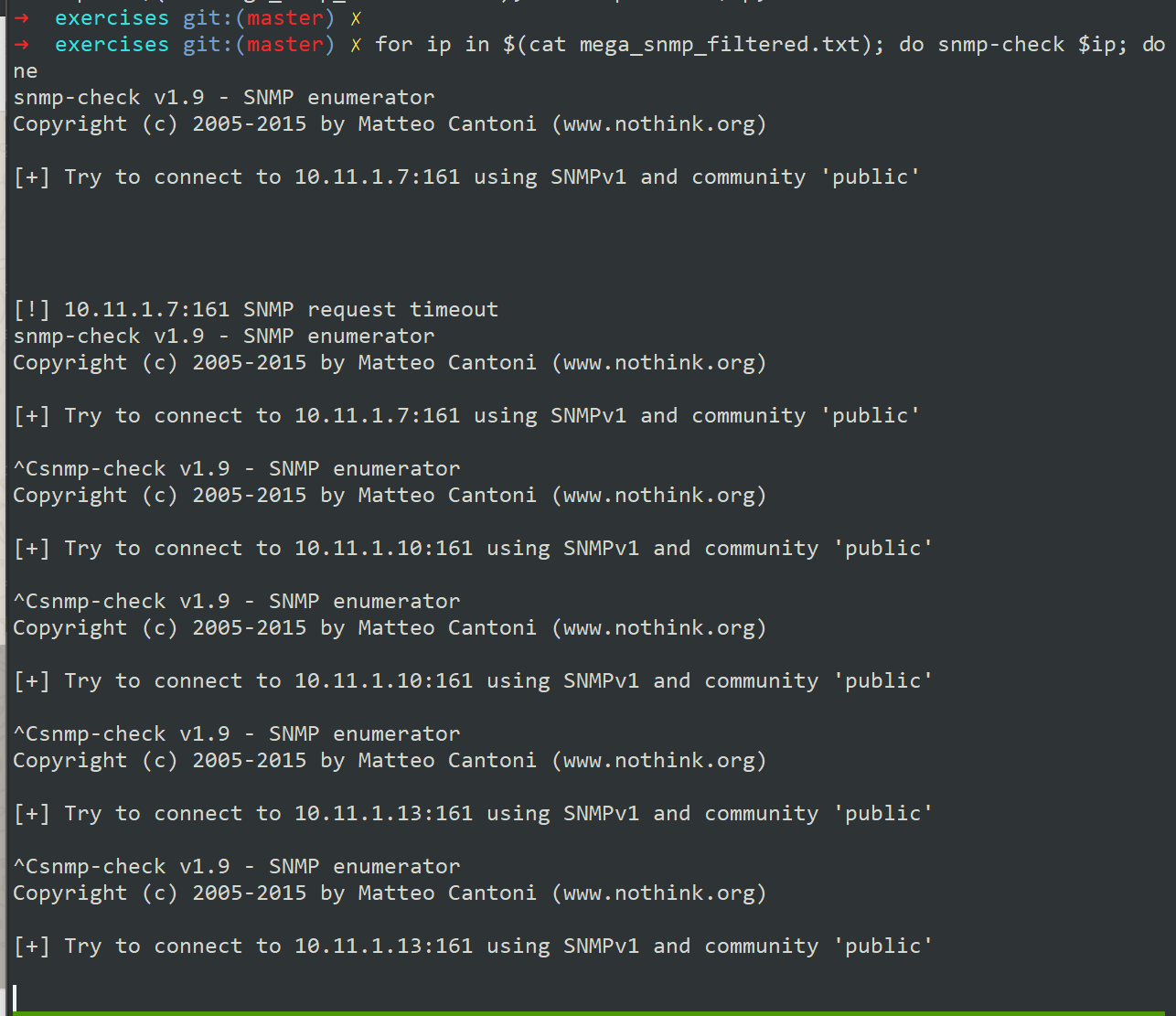
4.5.4 - Exercises

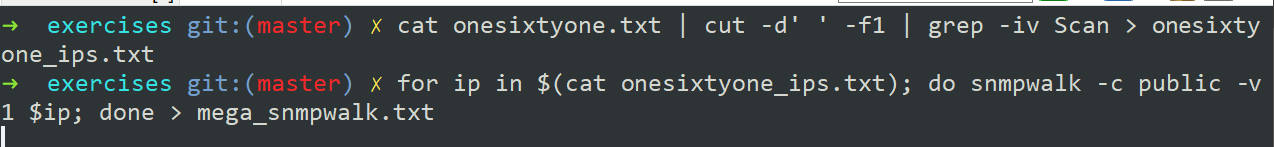
1. Scan your target network with onesixtyone. Identify any SNMP servers.



2. Use snmpwalk and snmp-check to gather information about the discovered

targets.



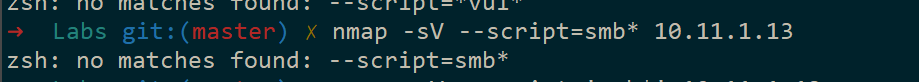


5.2.2 - Exercises

1. Use nmap scripts and OpenVAS to conduct targeted scans (against single hosts)

against systems in your target network.

**Using Nmap with smb\* scripts**



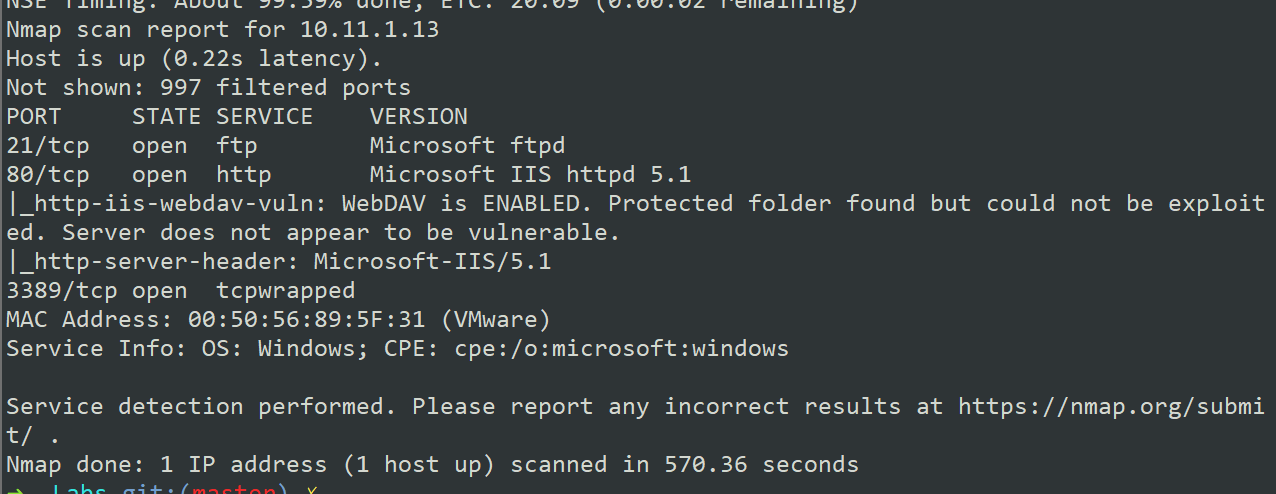
OpenVAS

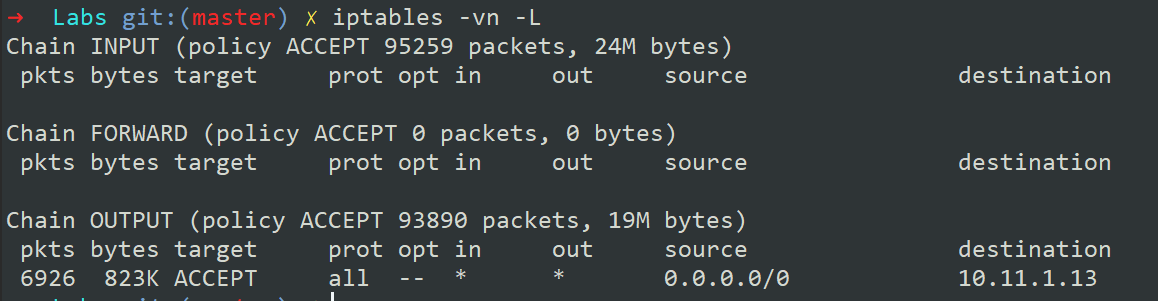


2. Account for the traffic using iptables. How many resources does scanning a

single host require, in terms of network bandwidth, and time?

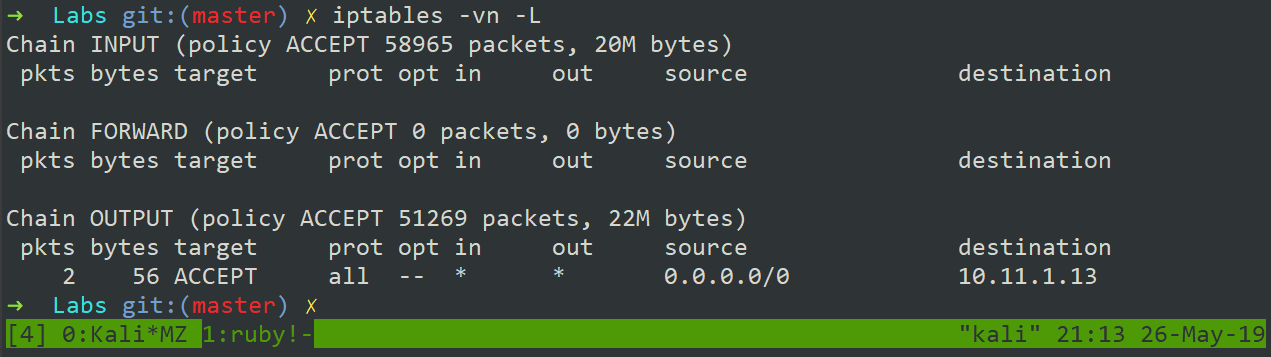
**Nmap:**

****



**OpenVAS**





3. Consider the sort of vulnerabilities a scanner will identify. What are the

limitations of the tool? Why

**They don’t identify human vulnerabilities, such as misconfiguration, they are useful but they don’t replace the human mind.**