Networking
Computer Lab Exercises

Student Learner Outcomes

- Understand how network traffic is routed using a GUI topographical representation
- How cookies are persistent when browsing websites
- How firewalls block traffic
- How Network Address Translation changes IP addresses
    - public vs private IP address
- Understand the security difference between telnet and ssh traffic
- How the Domain Name System resolves websites names to an IP address
- See http headers and tcp handshake network traffic
- Understand the security difference between http vs https
    - Extract files from tcp stream/session

Introduction

Students should now have a conceptual understanding of network traffic and packet structure, but seeing is believing. Students will use networking tools on a linux machine, Ubuntu 14.04. After completing the labs, they should be able to analyze and deconstruct basic network traffic and packet captures.

Setup

Each virtualized computer should already be pre-configured with the required programs and files. Press 'Ctl+Alt+t' to open a terminal and enter the following command

- `cd ~/Desktop/Networking; ./check.sh`

Looking at the command output, lines with a program should have a path. An example would be

- `ifconfig: /sbin/ifconfig /usr/share/man/man8/ifconfig.8.gz`

If a program's directory is blank, enter the following command to install them

- `sudo apt install git`
- `cd Desktop`
- `git clone https://github.com/adambutac/Gencyber-Networking Networking`
- `cd Networking`
- `./install.sh`

Also note that you may need to manually install the 'Cookies Manager+' add-on for Firefox, which can be found at the following url https://goo.gl/5KpYTo

This document should also be available on each computer in the 'Networking' folder on the 'Desktop' for ease of use when copying and pasting each terminal command.

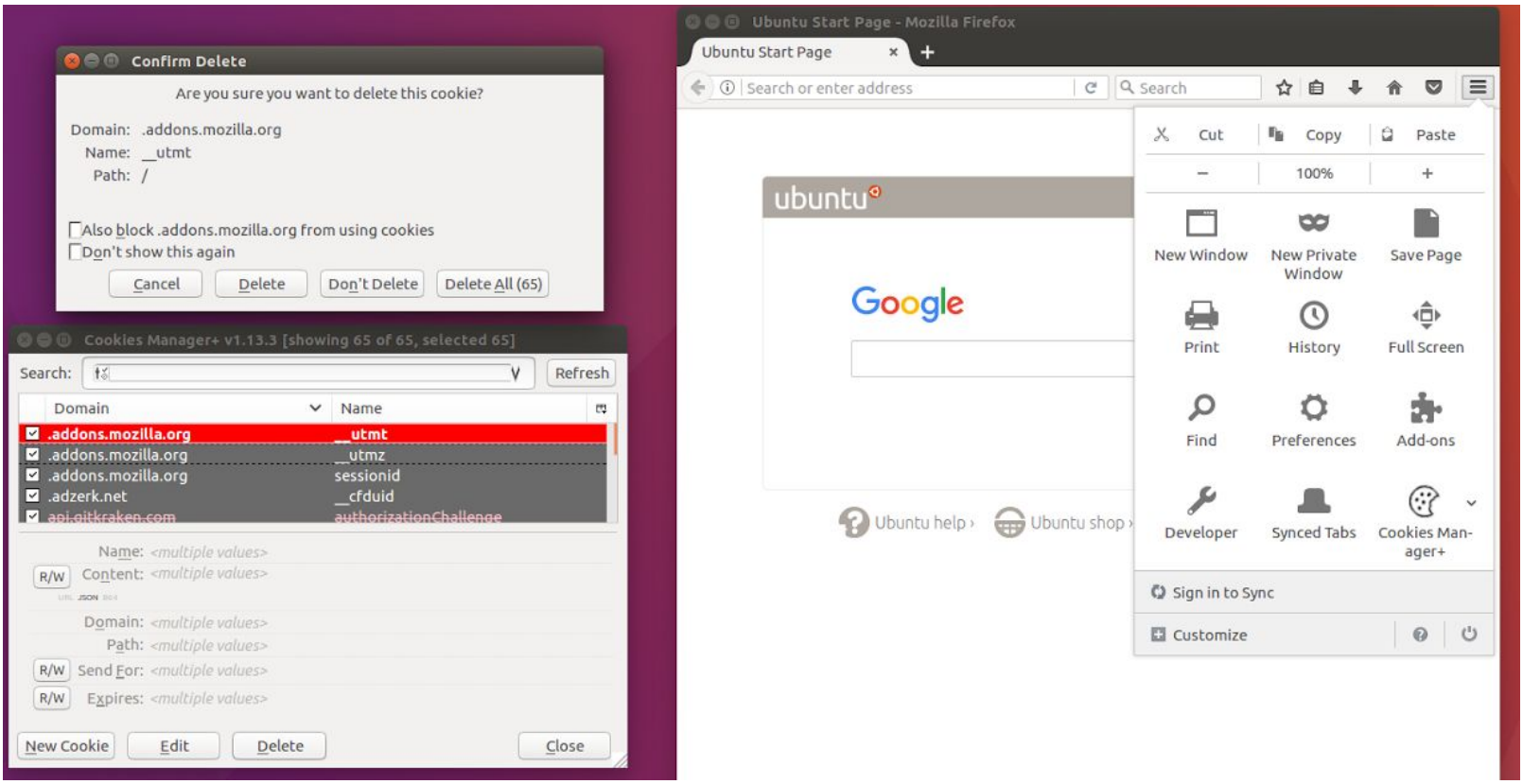
Programs

- Firefox
    - With 'Cookies Manager+' add-on https://goo.gl/5KpYTo
- ifconfig
- iptables
- route
- ssh
- wget
- wireshark
- zenmap

Networking
Computer Lab Exercises

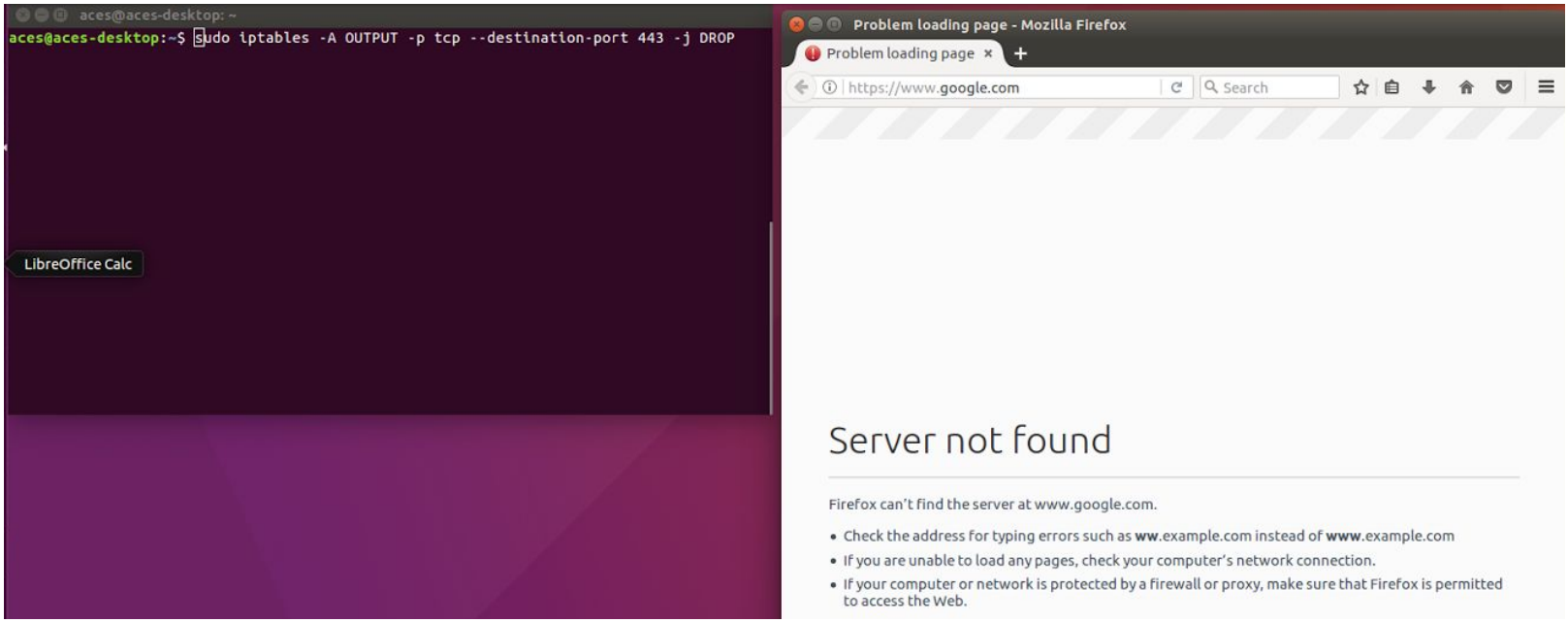
Section 1: Cookies and Firewalls

1. Click on the ‘Ubuntu’ logo in the top of the launcher on the left of side the desktop
2. In the search bar, type ‘Firefox’ and click the icon to launch it
3. Open the ‘Extras’ menu in the top right of Firefox
4. Click on the ‘Cookies Manager+’ icon
5. In the ‘Cookies Manager+’ window, selected a cookie in the main window and press ‘Ctl+A’ to select all the cookies
6. Click the ‘Delete’ button
7. In the following window, click ‘Delete All’
    a.



8. With the ‘Cookies Manager+’ window open, use Firefox to visit the following websites
    a. http://www.facebook.com
    b. http://www.google.com
    c. http://www.imgur.com
    d. http://www.reddit.com
9. **Observe**
    a. You’re able to access the websites
    b. As you visit each website, cookies are added and are persistent
10. Click on the ‘Ubuntu’ logo in the top of the launcher on the left of the desktop
11. In the search bar, type ‘Terminal’’ and click the icon to launch it
12. In the terminal prompt, enter the following commands

a. `sudo iptables -A OUTPUT -p tcp --destination-port 80 -j DROP`
b. `sudo iptables -A OUTPUT -p tcp --destination-port 443 -j DROP`
    i. Note: enter the user password when prompted for the sudo password
    ii. Note: you won't be able to see the password as it's entered for security reasons



13. In Firefox, open a new tab and close all other tabs
14. Using Firefox, visit the following websites
    a. http://www.facebook.com
    b. http://www.google.com
    c. http://www.imgur.com
    d. http://www.reddit.com
15. **Observe**
    a. You're able to access certain websites
        i. Note: With the created firewall rules, you aren't able to access websites using HTTP (port 80)
        ii. Note: You're able to access websites using HTTPS (port 443)
16. In the terminal prompt, enter the following commands
    a. `sudo iptables -D OUTPUT -p tcp --destination-port 80 -j DROP`
    b. `sudo iptables -D OUTPUT -p tcp --destination-port 443 -j DROP`
    c. Note: enter the user password when prompted for the sudo password
    d. Note: you won't be able to see the password as it's entered for security reasons
17. In Firefox, open a new tab and close all other tabs
18. Using Firefox, visit the following websites
    a. http://www.facebook.com

b. http://www.google.com
c. http://www.imgur.com
d. http://www.reddit.com

19. Observe

a. You're able to access the websites
    i. Note: With the firewall rules deleted, you able to access websites again

20. Close all open programs

21. Conclusion

a. Firewalls can prevent certain web traffic while allowing others based on predefined rules
b. Cookies store user information and keep it after you leave a website

Section 2: Routing, network address translation, and public vs private IP address

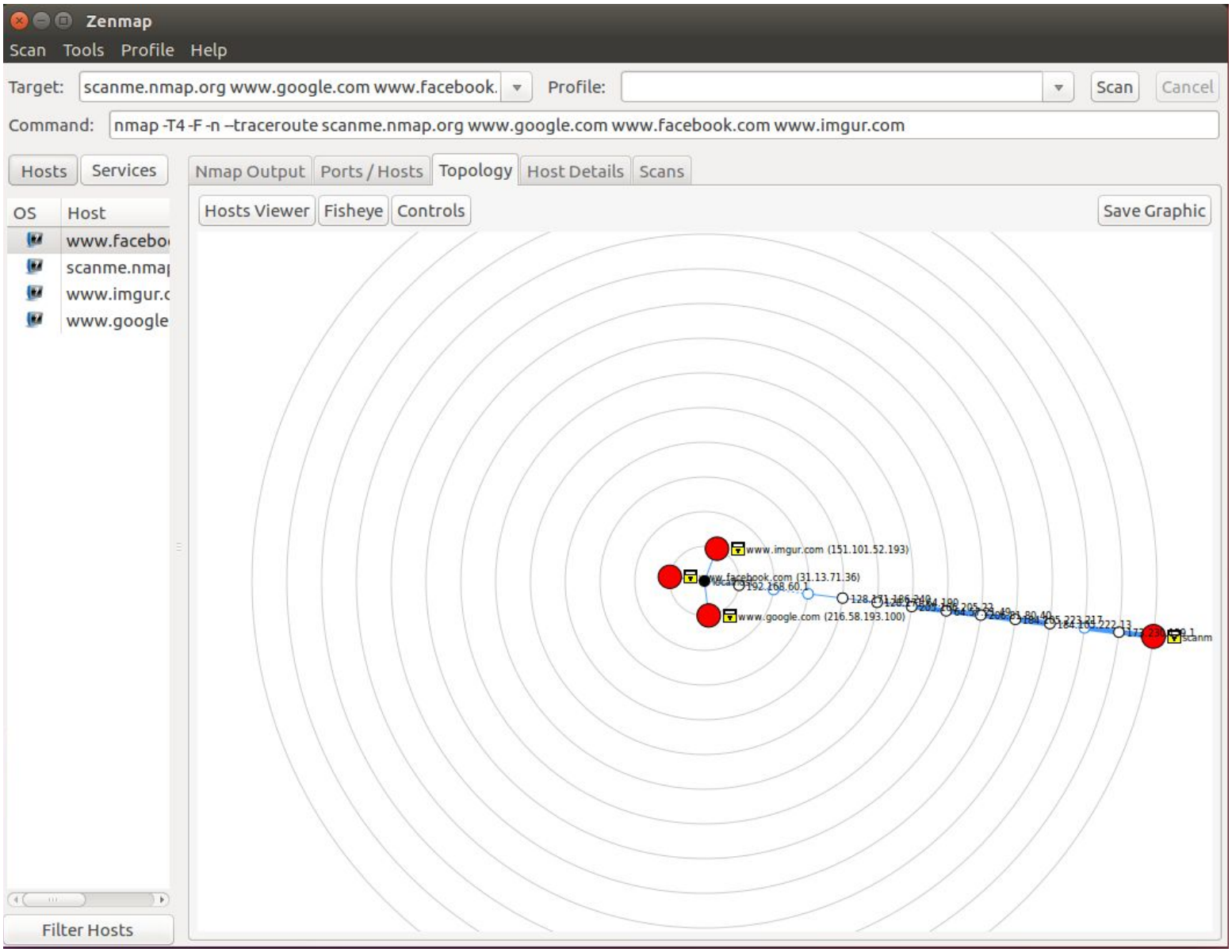
1. Click the 'Ubuntu' logo on the top of the launcher on the left side of the desktop.
2. In the search bar, type 'Terminal' and click the icon to launch it.
3. In the terminal application, enter the following command
    a. `echo private-ip; sudo ifconfig ens160 | grep -w inet; echo; echo "public-ip"; wget -qO- http://ipecho.net/plain; echo; echo`
        i. Note: enter the user password when prompted for the sudo password
        ii. Note: you won't be able to see the password as it's entered for security reasons
    b.

4. **Observe**
    a. You're shown your 'private' IP address
        i. Your IP address is the first decimal number in the first line

   ii. You IP address is not ‘Bcast’ or ‘Mask’ or ‘127.0.0.1’
   b. You’re shown your ‘public’ IP address on the second line
   c. You public IP address is not the same as your internal IP address, this is done by Network Address Translation (NAT)
   d. Remember or write down both for reference later
5. In the terminal application, enter the following command
   a. `sudo route -n | head -n 3`
      i. Note: enter the user password when prompted for the sudo password
      ii. Note: you won’t be able to see the password as it’s entered for security reasons
6. **Observe**
   a. The first line shows your next ‘hop’ to send traffic to
   b. Remember or write down for reference later
7. Close all open programs
8. **Conclusion**
   a. You can see the difference between your public and private ip address
   b. You’re able to get basic networking information using ‘ifconfig’ and ‘route -n’ with the command line

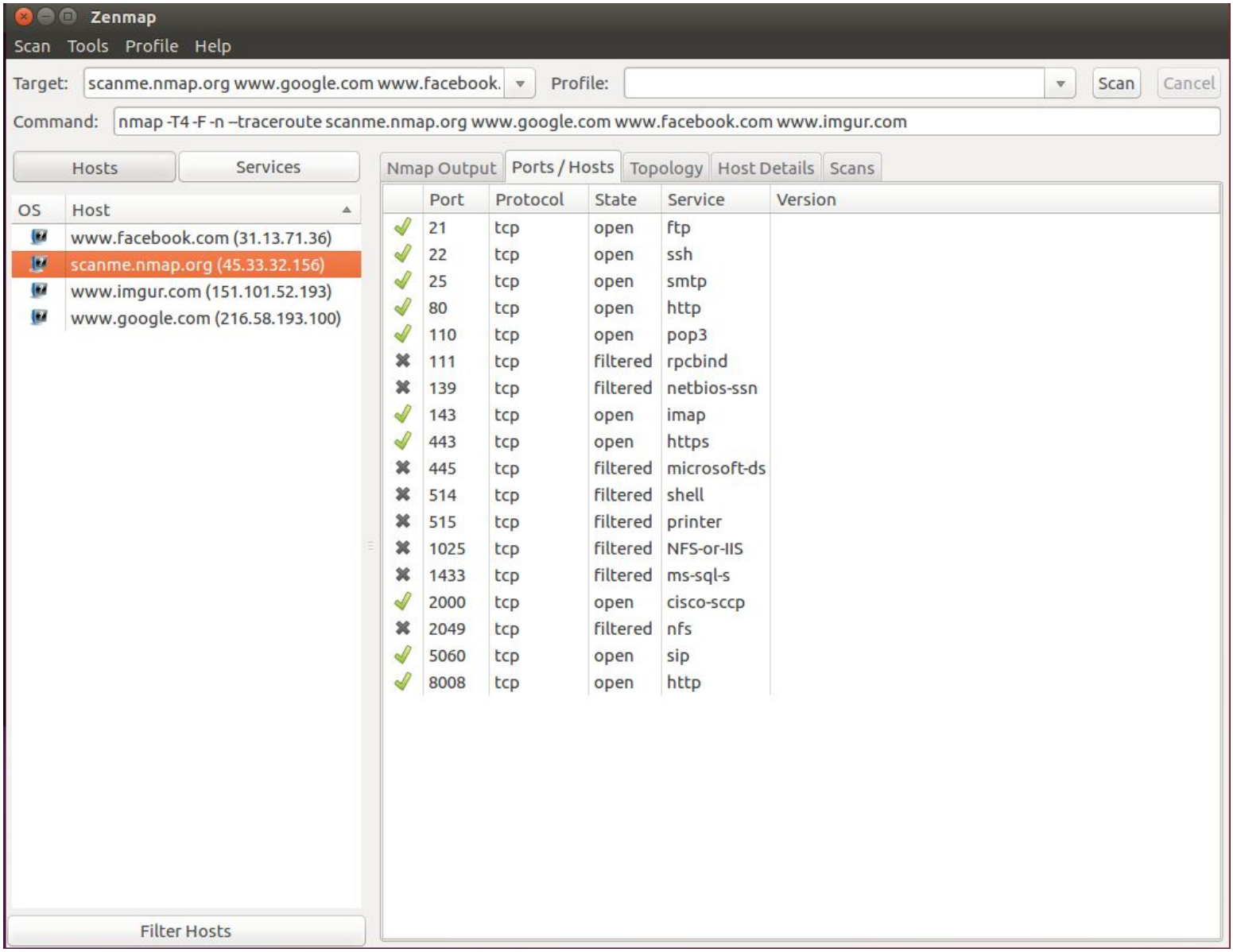
Section 3: Zenmap

1. Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.
2. In the search bar, type ‘Terminal’ and click the icon to launch it.
3. In the terminal application, enter the following command
   a. `sudo zenmap &`
      i. Note: enter the user password when prompted for the sudo password
      ii. Note: you won’t be able to see the password as it’s entered for security reasons
4. In the ‘Command Field’, enter the following
   a. `nmap -T4 -F -n --traceroute scanme.nmap.org www.google.com www.facebook.com www.imgur.com`
5. Click the ‘Scan’ button in the top right
6. In zenmap, click on the ‘Topology’ tab to see a graphical representation of every device between yours and the others
7. **Observe**
   a. The default gateway i.e. first hop, is closest to you, and should match what you save from earlier
   b. There are areas where packets are directed by a router from a central device



c. Some are closer or farther away from you

8. In zenmap, click on the 'Ports/Services' tab
9. Use the hosts list on the left to see what ports are open
10. **Observe**



a. How DNS resolves human readable websites to computer IP addresses
b. Some sites have a lot of ports open, some don't

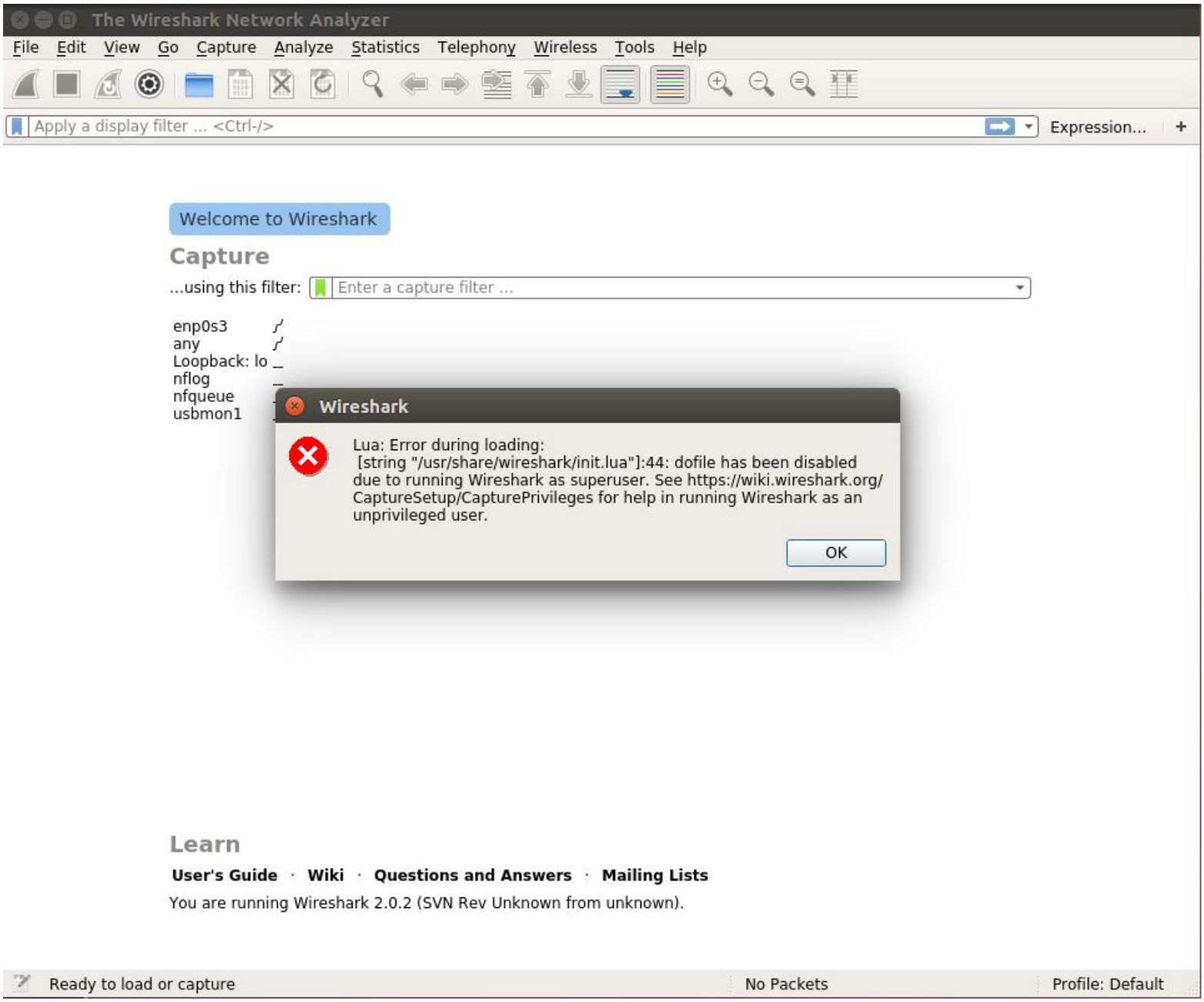
11. Close all open programs
12. **Conclusion**
    a. You're able to get basic networking information using 'ifconfig' and 'route -n' with the command line
    b. You can use GUI application, like zenmap, to better visualize a network's topology

Section 4: Wireshark

Part 1: Telnet versus Secure Shell

1. Click the 'Ubuntu' logo on the top of the launcher on the left side of the desktop.

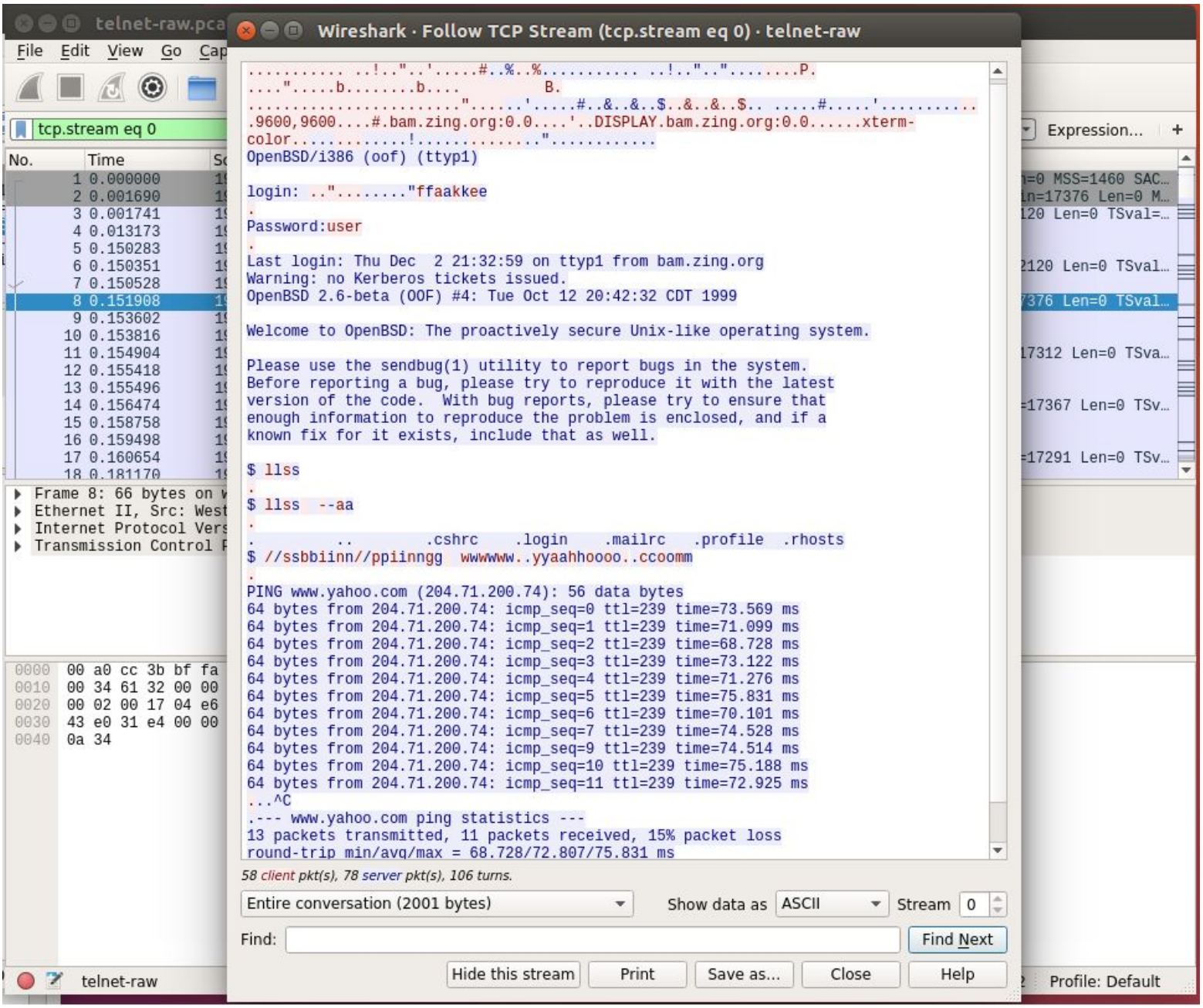
2. In the search bar, type ‘Terminal’ and click the icon to launch it.
3. In the terminal application, enter the following command
    a. `sudo wireshark &`
        i. Note: enter the user password when prompted for the sudo password
        ii. Note: you won’t be able to see the password as it’s entered for security reasons
4. An error message may appear, click ‘OK’ to close it



5. In the top left of wireshark, select 'File' then 'Open'

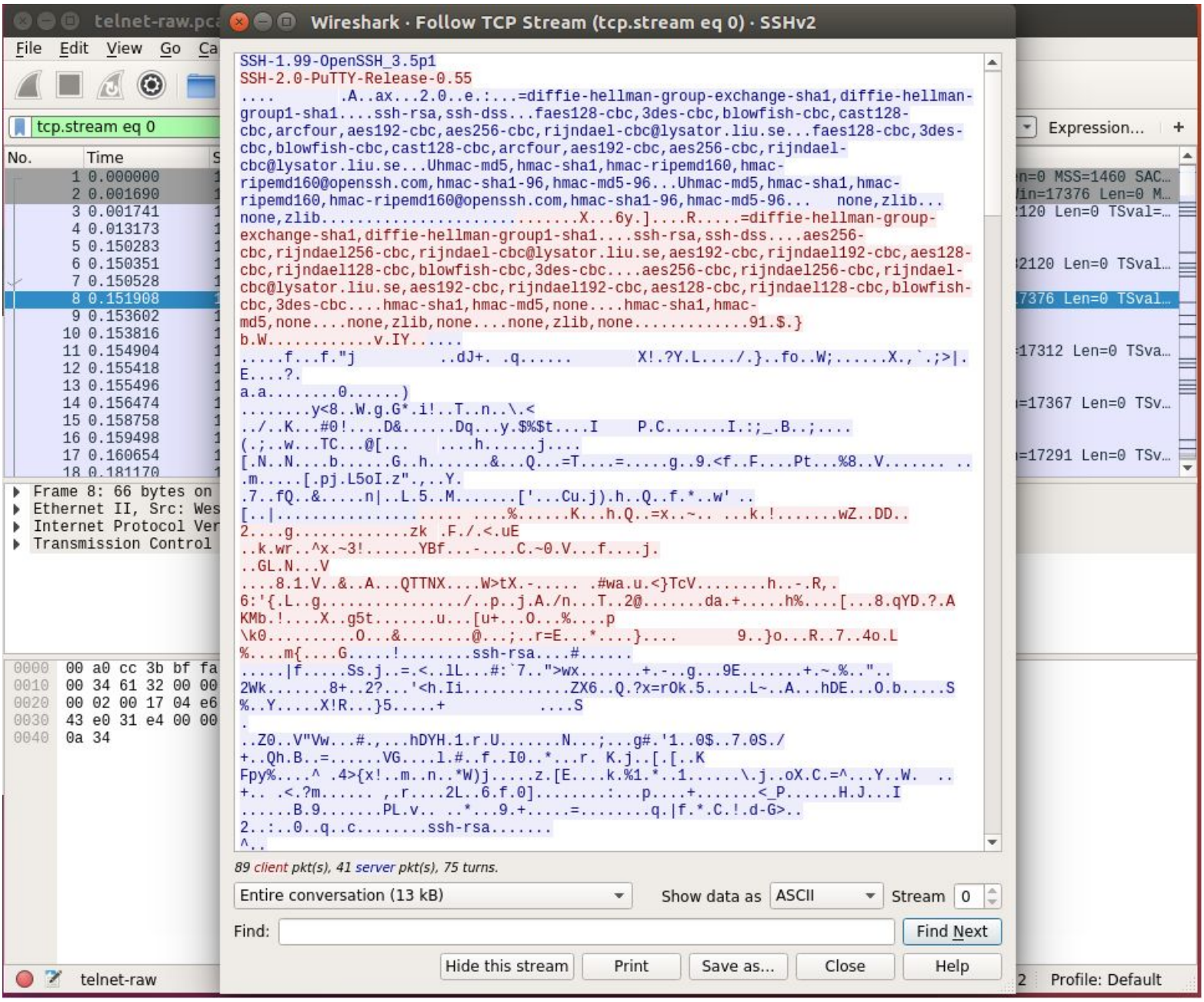
6. In the file explorer menu, navigate to the Desktop, open the ‘Networking Folder’ then 'pcap' folder and select the ‘telnet.pcap’ file, and click ‘Open’
7. In main packet list frame of wireshark, right click on any packet to open the options sub-menu
8. In the sub menu, hover over the ‘Follow’ option, and select ‘TCP Stream’
9. **Observe**
    a. The window shows the raw packet network data
    b. At the beginning, in the top, you can clearly see the username and password being entered
    c. This is bad security practice

Networking
Computer Lab Exercises

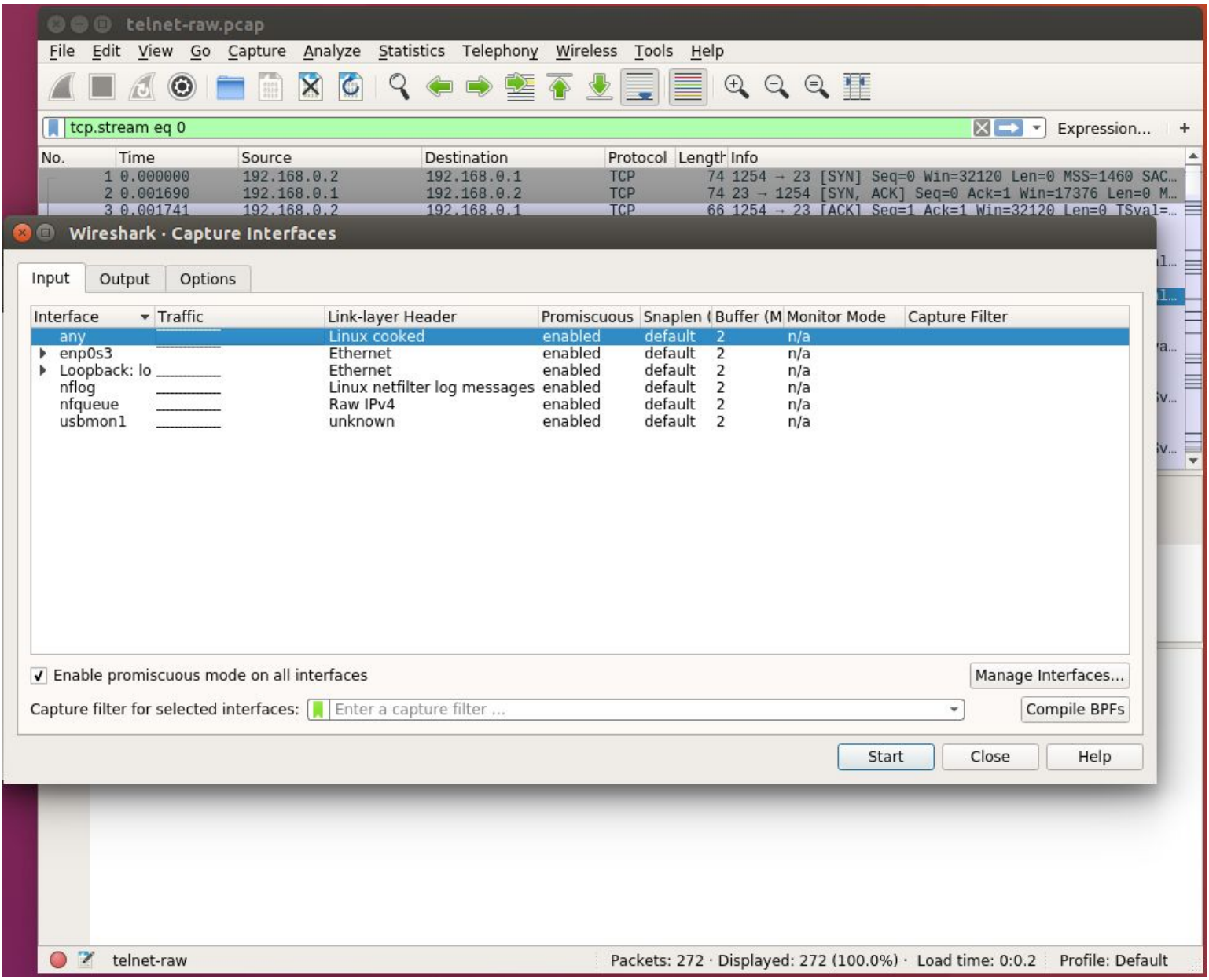


10. Close the ‘Follow TCP Stream’ windows
11. In the top left of wireshark, select 'File' then 'Open'
12. In the file explorer menu, navigate to the Desktop, open the ‘Networking Folder’ then 'pcap' folder, and select the ‘ssh.pcap’ file, and click ‘Open’
13. In main packet list frame of wireshark, right click on any packet to open the options sub-menu
14. In the sub menu, hover over the ‘Follow’ option, and select ‘TCP Stream’
15. **Observe**
    a. The window shows the raw packet network data
    b. At the beginning, in the top, you can see some data, but the rest is gibberish

c. This is good security practice



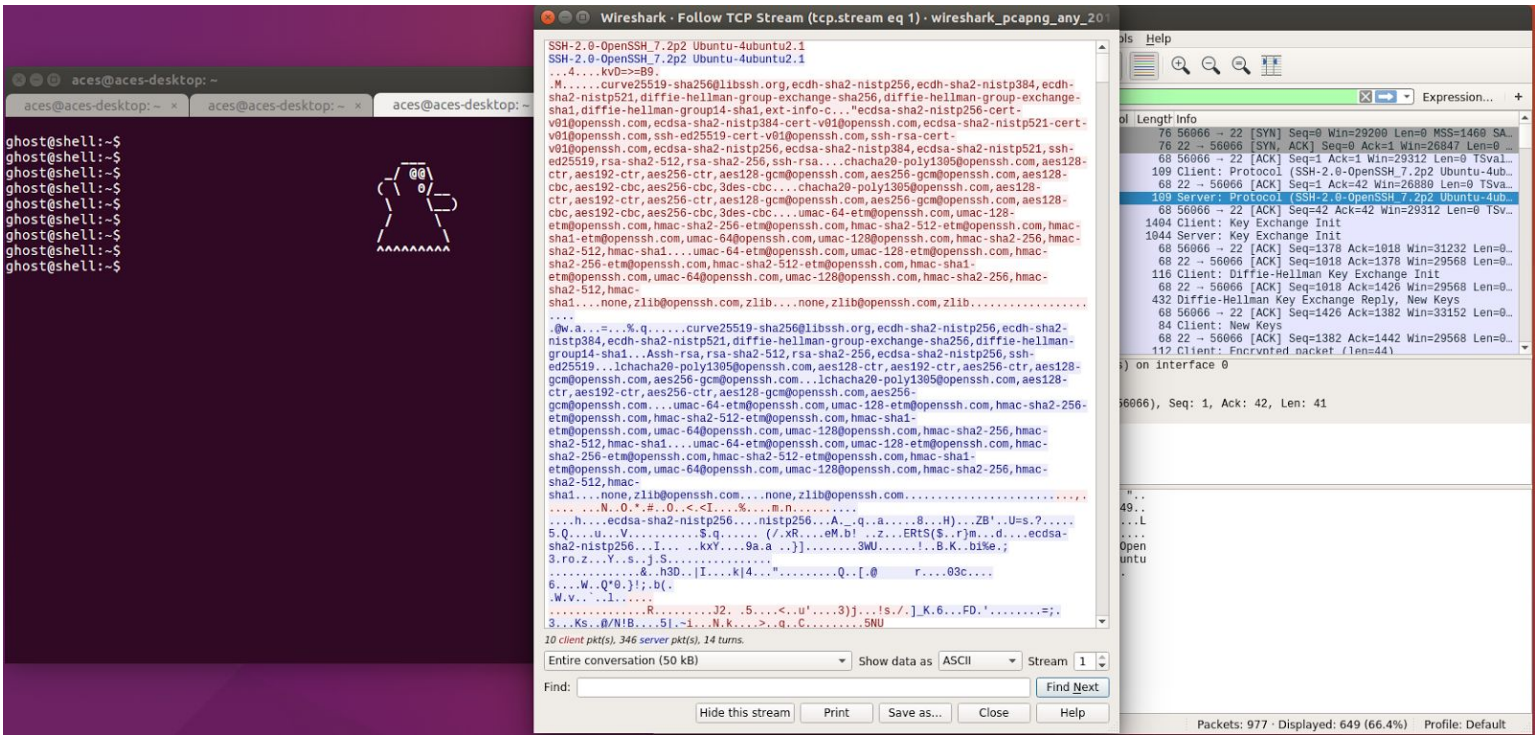
16. Close the ‘Follow TCP Stream’ window
17. In the top of wireshark, click on the ‘Capture’ submenu and select ‘Options’
18. In the ‘Capture Interfaces’ window, select ‘any’ and click ‘Start’ in the bottom right



19. In the ‘Display Filter’ field, enter the following
    a. `tcp.port == 22`
20. Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.
21. In the search bar, type ‘Terminal’ and click the icon to launch it.
22. In the terminal application, enter the following command
    a. `ssh ghost@theshell.xyz`
        i. Note: You’ll be asked if you’re sure you want to connect in the terminal, answer ‘yes’

Networking
Computer Lab Exercises

23. In main packet list frame of wireshark, right click on any packet to open the options sub-menu
24. In the sub menu, hover over the ‘Follow’ option, and select ‘TCP Stream’
25. Observe
    a. The window shows the raw packet network data
    b. The previous command connected to a remote server
    c. At the beginning, in the top, you can see some data, but the rest is gibberish
    d. This is good security practice

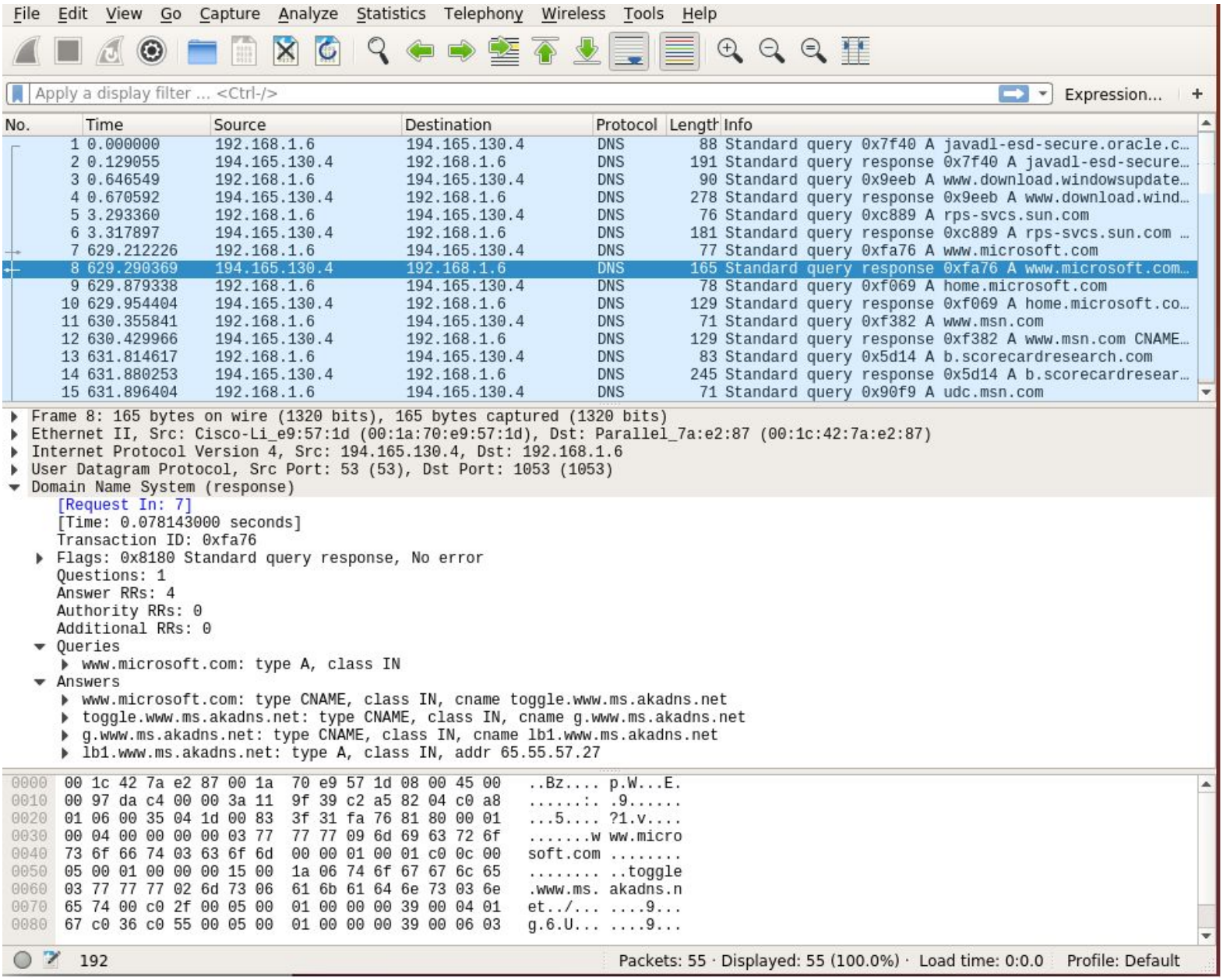


26. Close all open programs

Part 2: Domain Name System

1. Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.
2. In the search bar, type ‘Terminal’ and click the icon to launch it.
3. In the terminal application, enter the following command
    a. `sudo wireshark &`
        i. Note: enter the user password when prompted for the sudo password
        ii. Note: you won’t be able to see the password as it’s entered for security reasons
4. An error message may appear, click ‘OK’ to close it
5. In the top left of wireshark, select 'File' then 'Open'
6. In the file explorer menu, navigate to the Desktop, open the ‘Networking Folder’ then 'pcap' folder, and select the ‘fucker get the 192 dns cap from pcapr’ file, and click ‘Open’
7. In the ‘Display Filter’ field, enter the following
    a. `udp.stream eq 1`

8. In main packet list frame of wireshark, select the first packet, Number 16
9. In packet information frame of wireshark, expand the ‘Domain Name System’ field, then the ‘Queries’ field
10. **Observe**
    a. The information in the ‘Queries’ section shows what website the computer was trying to find
11. In main packet list frame of wireshark, select an answer packet, Number 19
12. In packet information frame of wireshark, expand the ‘Domain Name System’ field, then the Answers’ field
13. **Observe**
    a. The information in the ‘Answers’ section shows the IP address of the website that was asked for



14. In the top of wireshark, click on the ‘Capture’ submenu and select ‘Options’
15. In the ‘Capture Interfaces’ window, select ‘any’ and click ‘Start’ in the bottom right
16. In the ‘Display Filter’ field, enter the following
    a. `udp.port == 22`
17. Click on the ‘Ubuntu’ logo in the top of the launcher on the left of side the desktop
18. In the search bar, type ‘Firefox’ and click the icon to launch it
19. Using Firefox to visit the following websites
    a. https://www.dankafmemes.gov
    b. https://www.facebook.com
    c. https://www.google.com
    d. https://www.imgur.com
    e. https://www.reddit.com
20. In wireshark, observe the ‘Queries’ and ‘Answers’ field of the packets
21. **Observe**
    a. This is actual network traffic showing how website names are turned into IP addresses
    b. Only addresses that exist are answered, while those that aren’t are ignored
22. Close all open programs

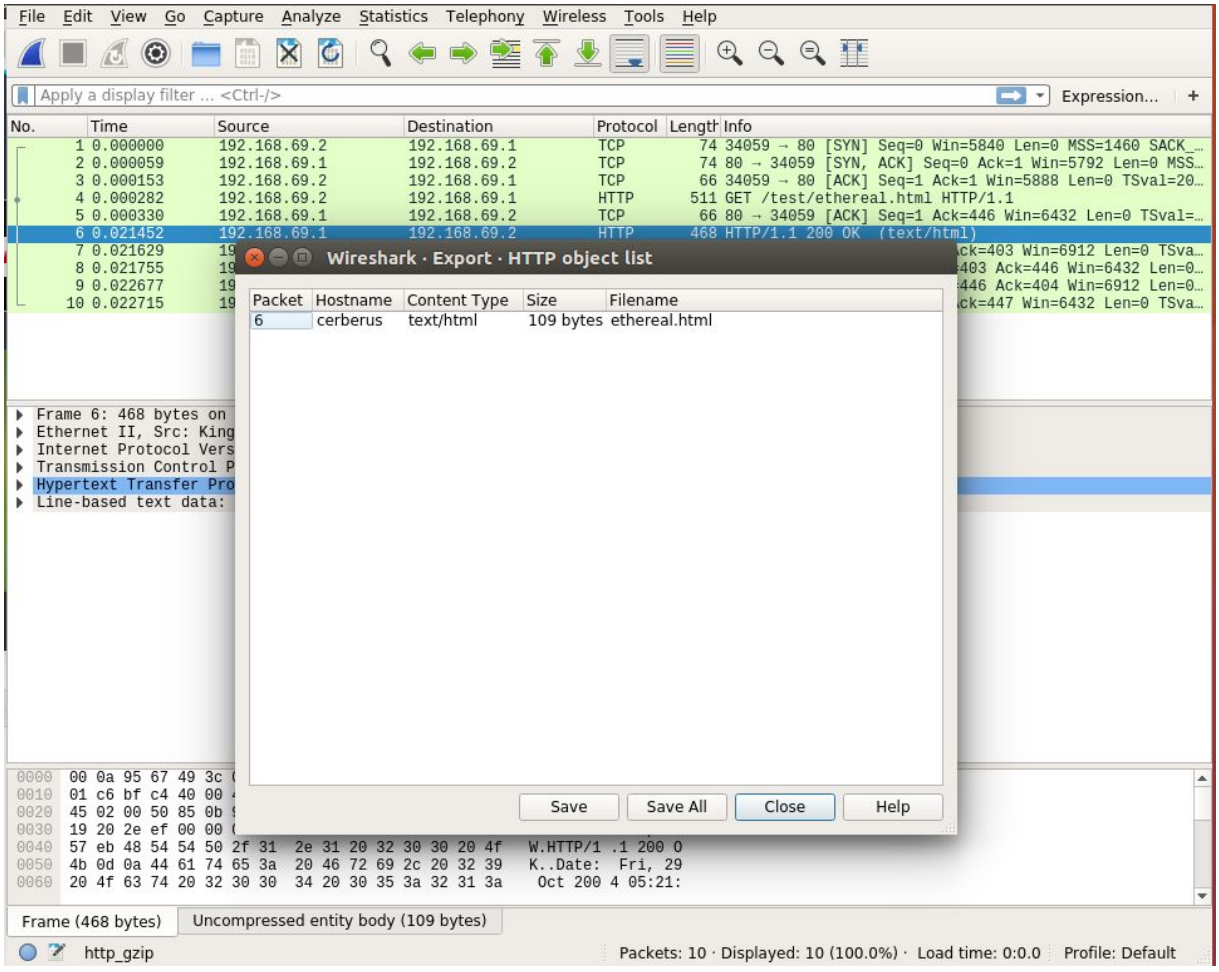
Part 3: TCP Handshake

1. Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.
2. In the search bar, type ‘Terminal’ and click the icon to launch it.
3. In the terminal application, enter the following command
    a. `sudo wireshark &`
        i. Note: enter the user password when prompted for the sudo password
        ii. Note: you won’t be able to see the password as it’s entered for security reasons
4. An error message may appear, click ‘OK’ to close it
5. In the top left of wireshark, select 'File' then 'Open'
6. In the file explorer menu, navigate to the Desktop, open the ‘Networking Folder’ then 'pcap' folder, and select the ‘tcp-handshake.pcap’ file, and click ‘Open’
7. In main packet list frame of wireshark, select the first packet, Number 1
8. In packet information frame of wireshark, expand the ‘Transmission Control Protocol’ field
9. Go through the three packets while looking at the ‘Flags’ field
10. Observe
    a. You can see the SYN, SYN/ACK, and ACK handshake of TCP
11. In the top of wireshark, click on the ‘Capture’ submenu and select ‘Options’
12. In the ‘Capture Interfaces’ window, select ‘any’ and click ‘Start’ in the bottom right
13. In the ‘Display Filter’ field, enter the following
    a. `udp.port == 443`
14. Click on the ‘Ubuntu’ logo in the top of the launcher on the left of side the desktop
15. In the search bar, type ‘Firefox’ and click the icon to launch it
16. Using Firefox to visit the following websites
    a. http://www.facebook.com
    b. http://www.google.com

   c. http://www.imgur.com
   d. http://www.reddit.com
17. In packet information frame of wireshark, expand the ‘Transmission Control Protocol’ field
18. Go through the three packets while looking at the ‘Flags’ field
19. **Observe**
   a. You can see the SYN, SYN/ACK, ACK handshake of TCP
   b. You can also see ‘Malformed Packets’ that show how TCP verified packet data integrity

Part 5: HTTP versus HTTPS

1. Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.
2. In the search bar, type ‘Terminal’ and click the icon to launch it.
3. In the terminal application, enter the following command
   a. `sudo wireshark &`
      i. Note: enter the user password when prompted for the sudo password
      ii. Note: you won’t be able to see the password as it’s entered for security reasons
4. An error message may appear, click ‘OK’ to close it
5. In the top left of wireshark, select 'File' then 'Open'
6. In the file explorer menu, navigate to the Desktop, open the ‘Networking Folder’ then 'pcap' folder, and select the ‘http.pcap’ file, and click ‘Open’
7. In the top left of wireshark, select 'File' then, ‘Export Objects’, then ‘HTTP’
8. In the file explorer menu, make sure you’re in the ‘Networking’ folder on the desktop before clicking ‘Save All’



9. Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.
10. In the search bar, type ‘Files’ and click the icon to launch it
11. Navigate to the ‘Networking’ in the ‘Desktop’ folder
12. Right click on ‘etheral.html’ and select ‘Open with Firefox’
13. **Observe**
    a. Using wireshark, we were able to look at a web page that was sent over the network
    b. Pictures and videos on websites are also able to be extracted from network traffic
    c. This is bad security practice
14. In the top of wireshark, click on the ‘Capture’ submenu and select ‘Options’
15. In the ‘Capture Interfaces’ window, select ‘any’ and click ‘Start’ in the bottom right
16. Click on the ‘Ubuntu’ logo in the top of the launcher on the left of side the desktop
17. In the search bar, type ‘Firefox’ and click the icon to launch it
18. Using Firefox to visit the following websites
    a. https://www.facebook.com
    b. https://www.google.com
    c. https://www.imgur.com
    d. https://www.reddit.com
19. In the top left of wireshark, select 'File' then, ‘Export Objects’, then ‘HTTP’
20. **Observe**
    a. Since the network traffic is secured with HTTPS, you aren’t able to extract the webpage, pictures, or videos
    b. This is good security practice
21. Close all open programs