

# Networking

## Computer Lab Exercises

### Student Learner Outcomes (Objectives)

- 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 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.

### Scenario

You're hired by '*teh supa 13373 h4x0r*' team, and need to learn about their new network before starting your new job. The following lab will walk you through what to do in order to become more familiar with their network, and the internet as a whole.

### 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`
- `cd Networking`
- `sudo ./install.sh`

- Note: You'll need to enter the sudo password whenever prompted. For security reasons, you won't be able to see it as you type. Press enter when done.

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>

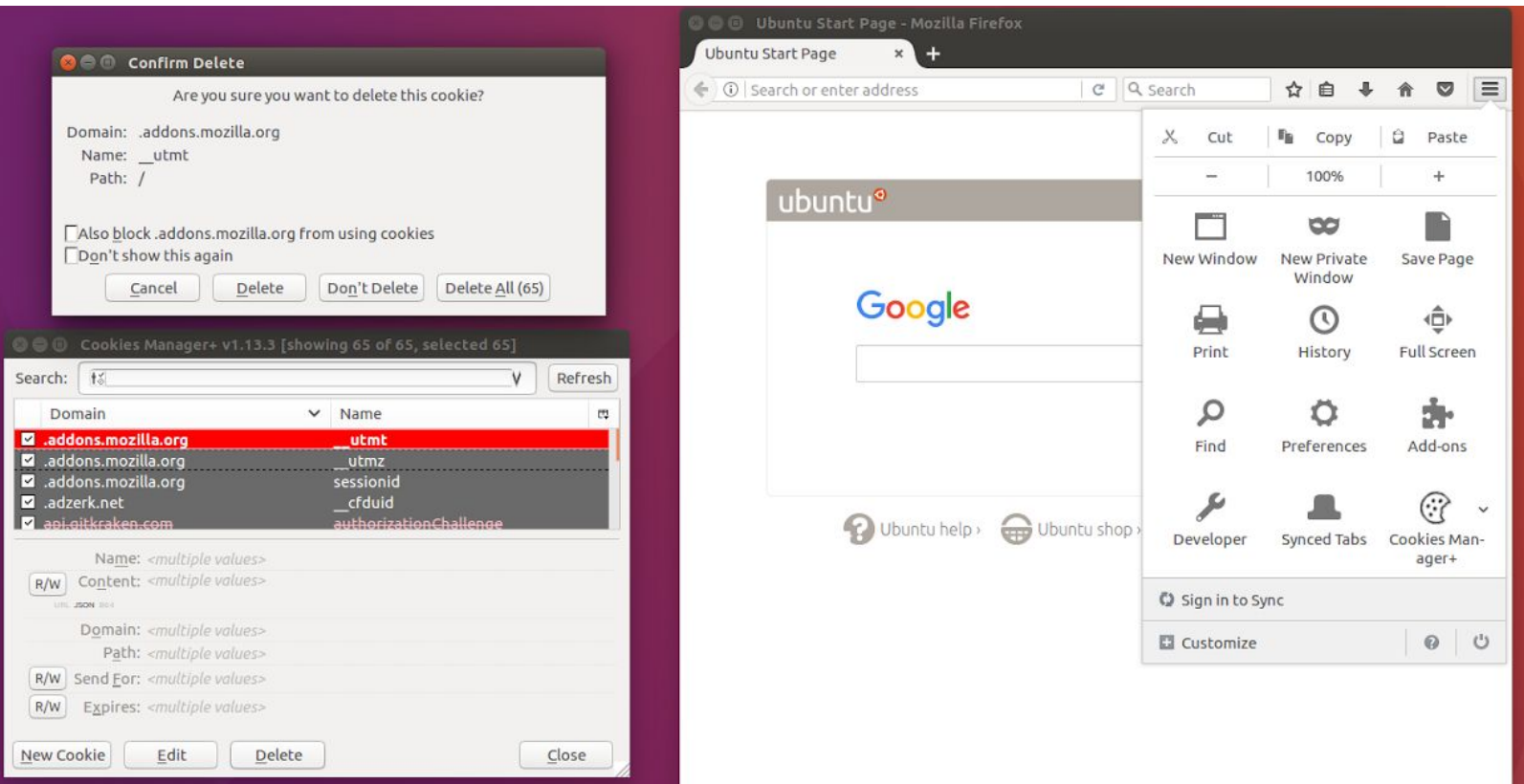
# Networking

## Computer Lab Exercises

- ifconfig
- iptables
- route
- ssh
- wget
- wireshark
- zenmap

### 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 'Ctrl+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. <https://www.facebook.com>
  - b. <https://www.google.com>
  - c. <https://www.imgur.com>
  - d. <https://www.reddit.com>

# Networking

## Computer Lab Exercises

### 9. Observe

- You're able to access the websites
- 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

- `sudo iptables -A OUTPUT -p tcp --destination-port 80 -j DROP`
- `sudo ip6tables -A OUTPUT -p tcp --destination-port 80 -j DROP`
  - Note: enter the user password when prompted for the sudo password
  - 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

- `https://www.facebook.com`
- `https://www.google.com`
- `http://www.imgur.com`
- `https://www.reddit.com`

### 15. Observe

- You're able to access only some websites
  - Note: With the created firewall rules, you aren't able to access websites using HTTP (port 80)
  - Note: You're able to access websites using HTTPS (port 443)

16. In the terminal prompt, enter the following commands

- `sudo iptables -D OUTPUT -p tcp --destination-port 80 -j DROP`

# Networking

## Computer Lab Exercises

- b. `sudo iptables -D OUTPUT -p tcp --destination-port 80 -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
- 17. In Firefox, open a new tab and close all other tabs
- 18. Using Firefox, 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. **Observe**
  - a. You're able to access the websites
    - i. Note: With the firewall rules deleted, you're able to access all the 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 are kept 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
- 4. **Observe**
  - a. You're shown your 'private' IP address
    - i. Your IP address is the first decimal number in the first line
    - ii. Your 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. Your public IP address is not the same as your internal IP address, this is done by Network Address Translation (NAT)

# Networking

## Computer Lab Exercises

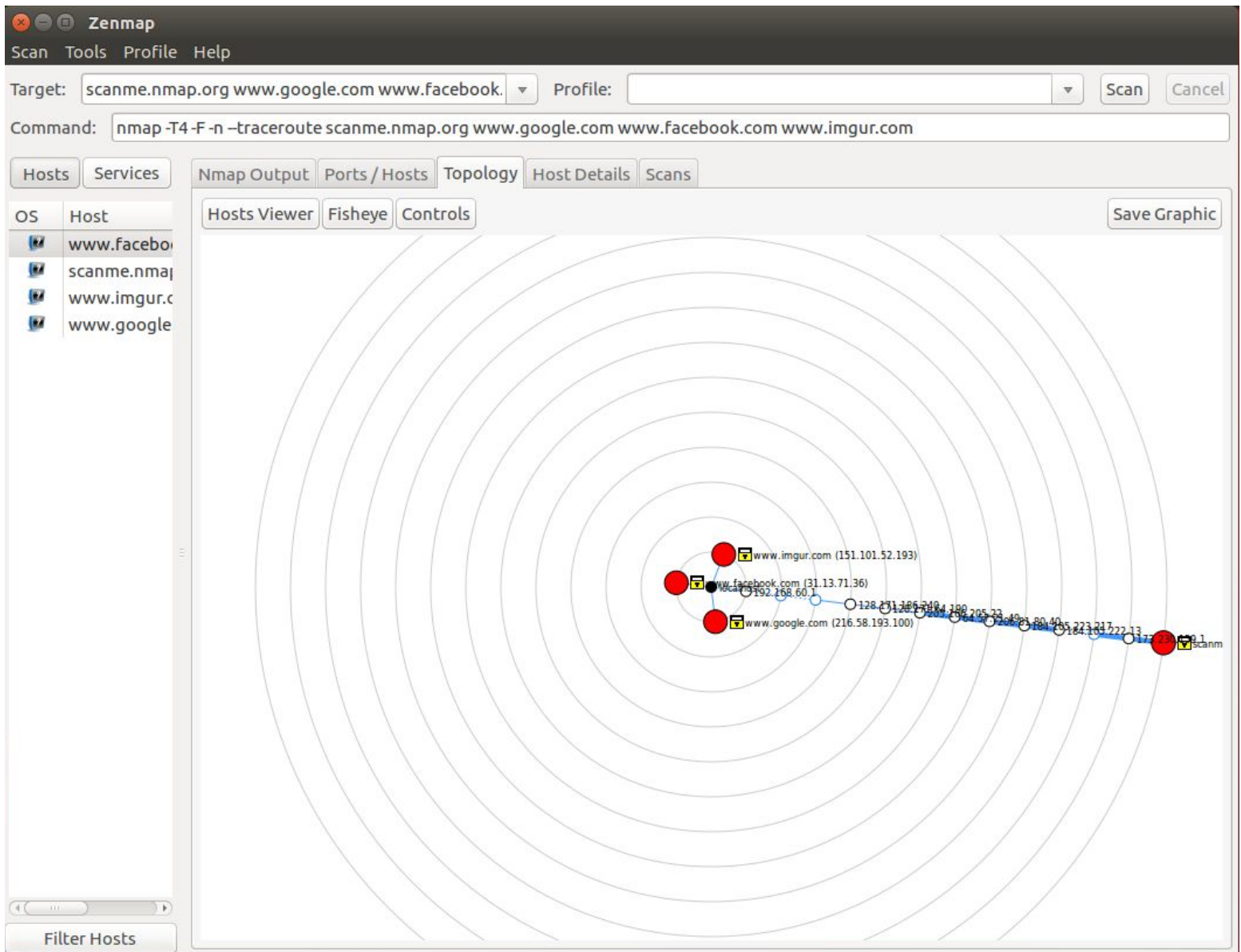
- d. Remember or write down both for reference later
- 5. In the terminal application, enter the following command
  - a. `sudo route -n | head -n 3`
    - i. Note: enter the user password when prompted for the sudo password
    - ii. Note: you won't be able to see the password as it's entered for security reasons
- 6. **Observe**
  - a. The first line shows the next 'hop' to send traffic to
  - b. A next hop is like your home router, which is connected to the wide internet
  - c. In short, it the next networking device you're connected to
  - d. 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' 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 saved from earlier
  - b. There are areas where packets are directed by a central device, this is a router, routing web traffic

# Networking

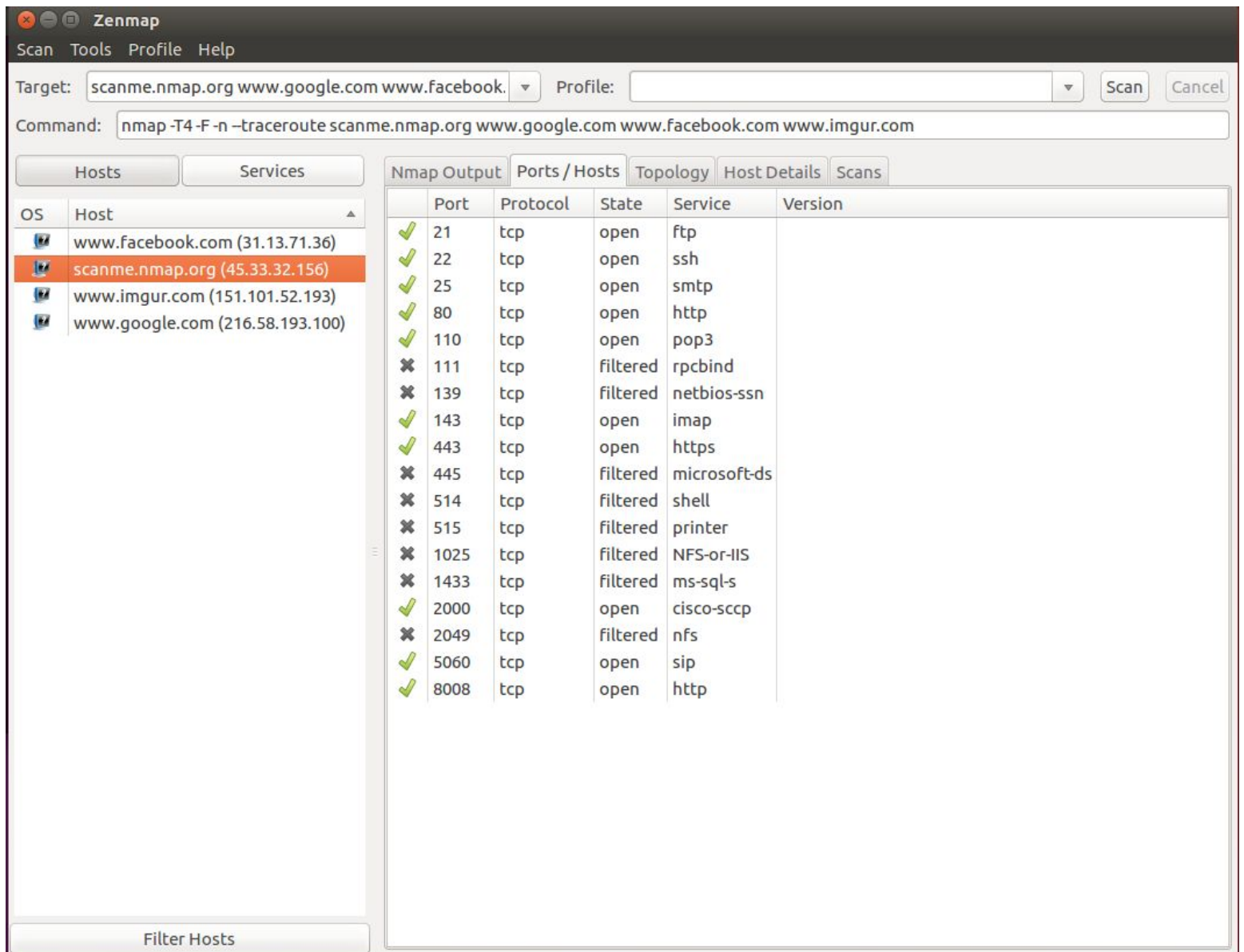
## Computer Lab Exercises



- 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 for each site
- 10. Observe**

# Networking

## Computer Lab Exercises



- How DNS resolves human readable websites to computer IP addresses in the 'Hosts' sidebar
  - Some sites have a lot of ports open, some don't
11. Close all open programs

### 12. Conclusion

- You can use GUI application, like zenmap, to better visualize a network's topology
- By visualizing a network, you're better able to understand and troubleshoot any issues

## Section 4: Wireshark

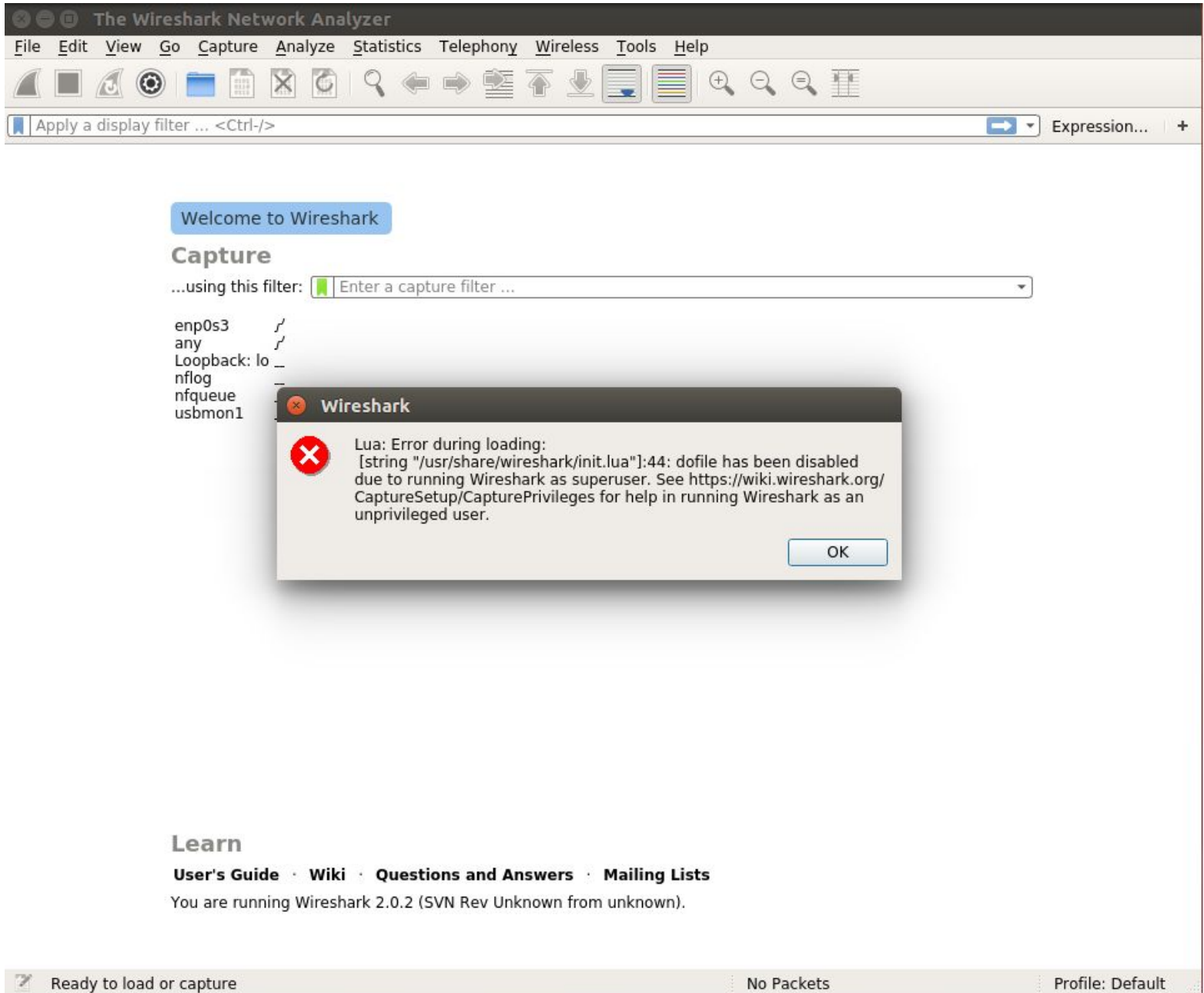
### Part 1: Telnet versus Secure Shell



# Networking

## Computer Lab Exercises

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



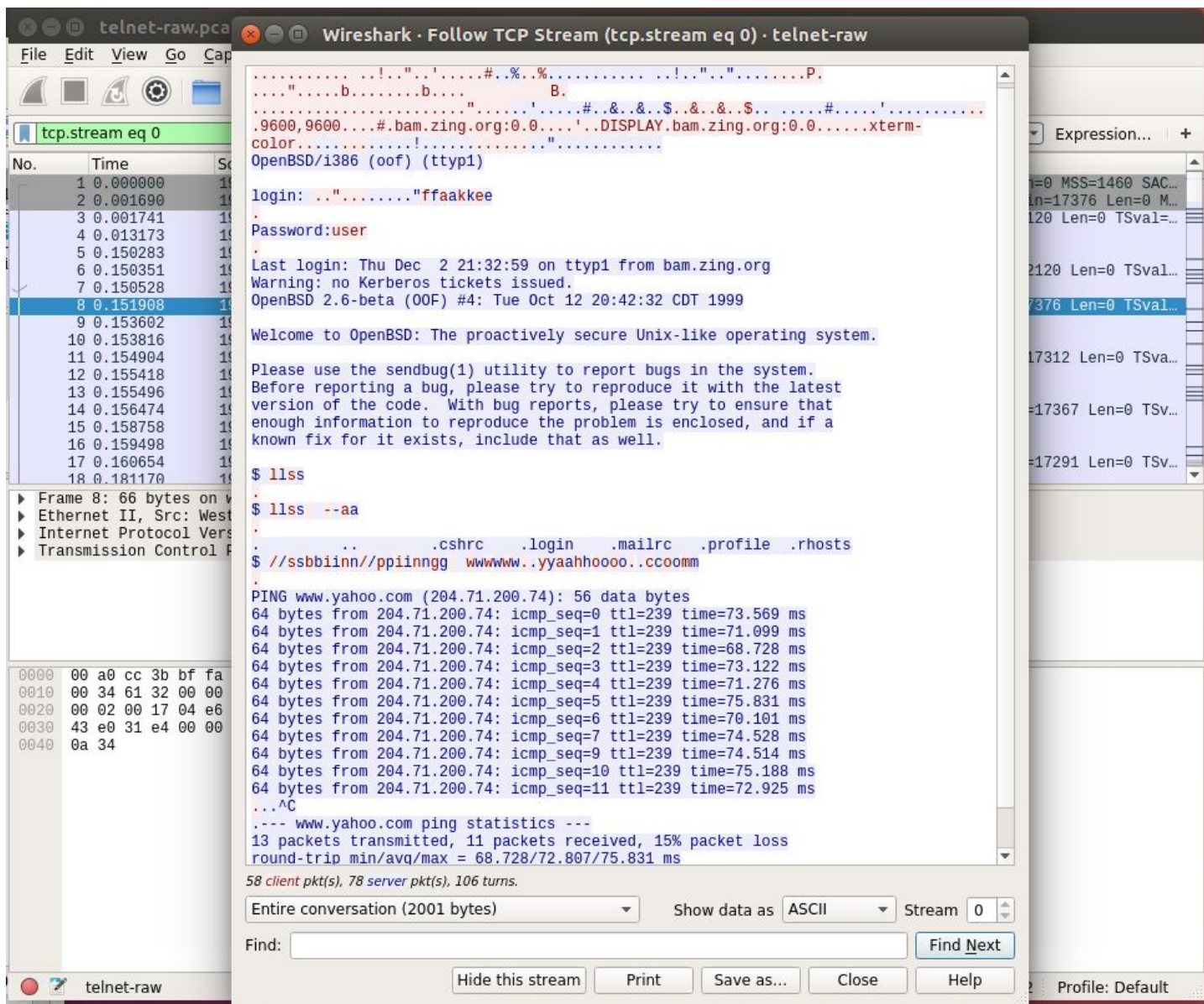
5. In the top left of wireshark, select 'File' then 'Open'



# Networking

## Computer Lab Exercises

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
10. Close the 'Follow TCP Stream' window
11. In the top left of wireshark, select 'File' then 'Open'



# Networking

## Computer Lab Exercises

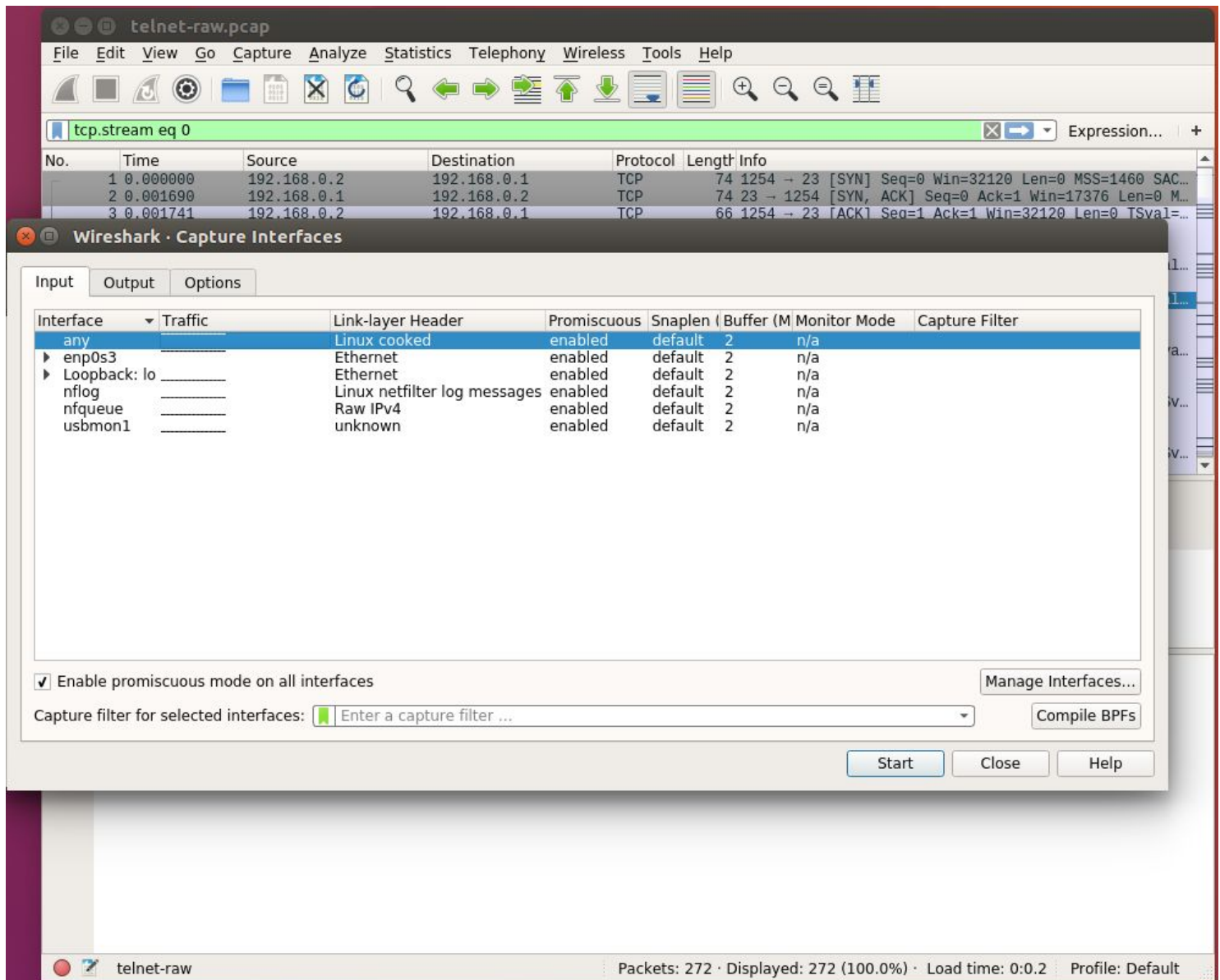
12. In the file explorer menu, navigate to the Desktop, open the 'Networking' folder, then 'pcap' folder, and select the 'ssh.pcap' file, and click 'Open'
13. In main packet list frame of wireshark, right click on any packet to open the options sub-menu
14. In the sub menu, hover over the 'Follow' option, 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 illegible
  - 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

The screenshot shows the Wireshark interface with the 'Follow TCP Stream' window open for an SSHv2 connection. The packet list on the left shows several packets, with packet 8 selected. The main pane displays the raw packet data in ASCII, which is mostly illegible due to encryption. The bottom pane shows the packet details for the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The status bar at the bottom indicates '89 client pkt(s), 41 server pkt(s), 75 turns'.



# Networking

## Computer Lab Exercises



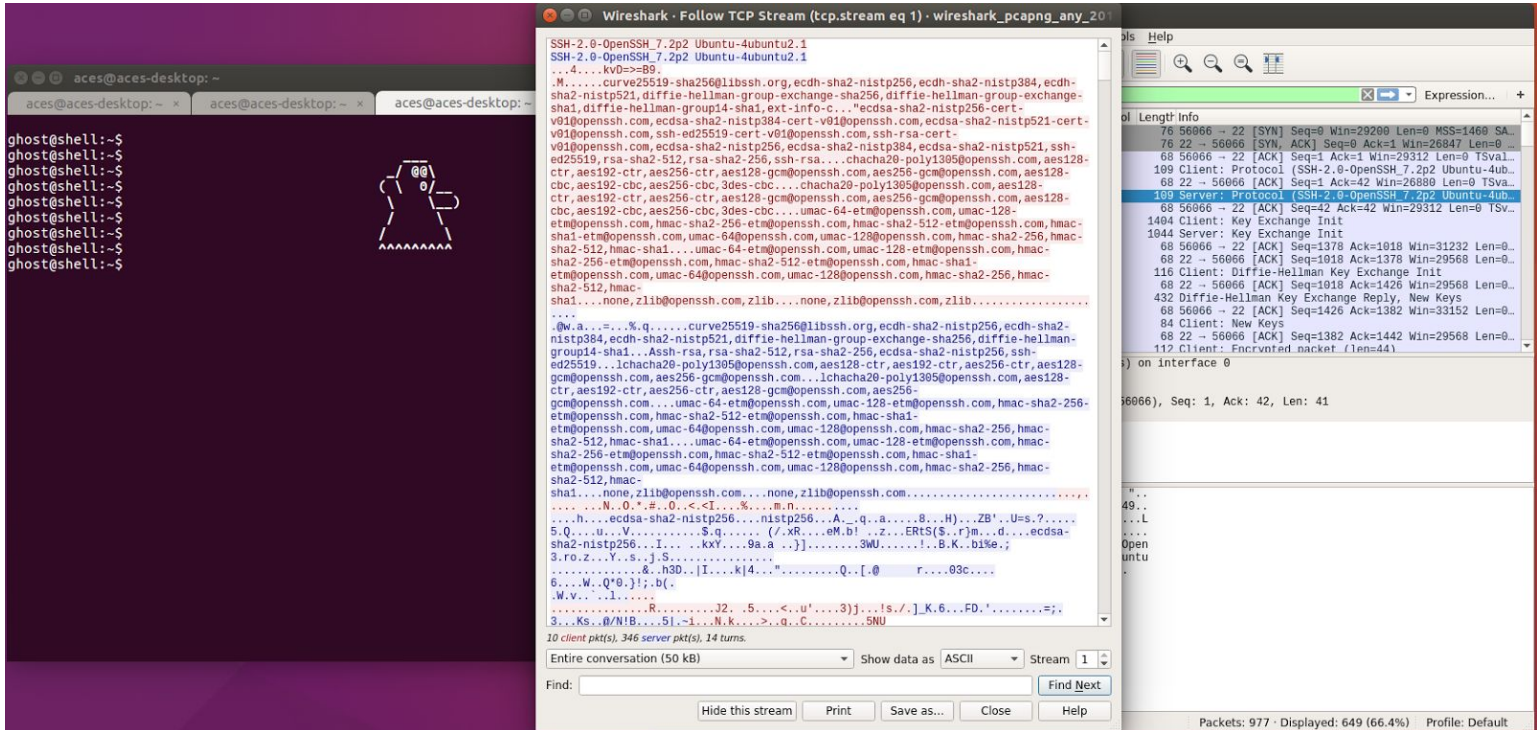
19. In the 'Display Filter' field, enter the following
  - a. `tcp.port == 22`
20. Click the 'Ubuntu' logo on the top of the launcher on the left side of the desktop.
21. In the search bar, type 'Terminal' and click the icon to launch it.
22. In the terminal application, enter the following command
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

# Networking

## Computer Lab Exercises

### 25. Observe

- The window shows the raw packet network data
- The previous command connected to a remote server
- At the beginning, in the top, you can see some data, but the rest is gibberish
- This is good security practice



### 26. Close all open programs

## Part 2: Domain Name System

- Click the 'Ubuntu' logo on the top of the launcher on the left side of the desktop.
- In the search bar, type 'Terminal' and click the icon to launch it.
- In the terminal application, enter the following command
  - `sudo wireshark`
    - Note: enter the user password when prompted for the sudo password
    - Note: you won't be able to see the password as it's entered for security reasons
- An error message may appear, click 'OK' to close it
- In the top left of wireshark, select 'File' then 'Open'
- In the file explorer menu, navigate to the Desktop, open the 'Networking' folder, then 'pcap' folder, and select the 'dns.pcap' file, and click 'Open'
- In the 'Display Filter' field, enter the following
  - `udp.stream eq 1`
- In main packet list frame of wireshark, select the first packet, Number 16
- In packet information frame of wireshark, expand the 'Domain Name System' field, then the 'Queries' field
- Observe**

# Networking

## Computer Lab Exercises

- 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 and after
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 after 'addr'

The image shows the Wireshark network traffic analysis interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list table displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.6	194.165.130.4	DNS	88	Standard query 0x7f40 A javadl-esd-secure.oracle.c...
2	0.129055	194.165.130.4	192.168.1.6	DNS	191	Standard query response 0x7f40 A javadl-esd-secure...
3	0.646549	192.168.1.6	194.165.130.4	DNS	90	Standard query 0x9eeb A www.download.windowsupdate...
4	0.670592	194.165.130.4	192.168.1.6	DNS	278	Standard query response 0x9eeb A www.download.wind...
5	3.293360	192.168.1.6	194.165.130.4	DNS	76	Standard query 0xc889 A rps-svcs.sun.com
6	3.317897	194.165.130.4	192.168.1.6	DNS	181	Standard query response 0xc889 A rps-svcs.sun.com ...
7	629.212226	192.168.1.6	194.165.130.4	DNS	77	Standard query 0xfa76 A www.microsoft.com
8	629.290369	194.165.130.4	192.168.1.6	DNS	165	Standard query response 0xfa76 A www.microsoft.com...
9	629.879338	192.168.1.6	194.165.130.4	DNS	78	Standard query 0xf069 A home.microsoft.com
10	629.954404	194.165.130.4	192.168.1.6	DNS	129	Standard query response 0xf069 A home.microsoft.co...
11	630.355841	192.168.1.6	194.165.130.4	DNS	71	Standard query 0xf382 A www.msn.com
12	630.429966	194.165.130.4	192.168.1.6	DNS	129	Standard query response 0xf382 A www.msn.com CNAME...
13	631.814617	192.168.1.6	194.165.130.4	DNS	83	Standard query 0x5d14 A b.scorecardresearch.com
14	631.880253	194.165.130.4	192.168.1.6	DNS	245	Standard query response 0x5d14 A b.scorecardresear...
15	631.896404	192.168.1.6	194.165.130.4	DNS	71	Standard query 0x90f9 A udc.msn.com

The packet details pane for packet 8 shows the following information:

- Frame 8: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
- Ethernet II, Src: Cisco-Li\_e9:57:1d (00:1a:70:e9:57:1d), Dst: Parallel\_7a:e2:87 (00:1c:42:7a:e2:87)
- Internet Protocol Version 4, Src: 194.165.130.4, Dst: 192.168.1.6
- User Datagram Protocol, Src Port: 53 (53), Dst Port: 1053 (1053)
- Domain Name System (response)
  - [Request In: 7]
  - [Time: 0.078143000 seconds]
  - Transaction ID: 0xfa76
  - Flags: 0x8180 Standard query response, No error
  - Questions: 1
  - Answer RRs: 4
  - Authority RRs: 0
  - Additional RRs: 0
- Queries
  - www.microsoft.com: type A, class IN
- Answers
  - www.microsoft.com: type CNAME, class IN, cname toggle.www.ms.akadns.net
  - toggle.www.ms.akadns.net: type CNAME, class IN, cname g.www.ms.akadns.net
  - g.www.ms.akadns.net: type CNAME, class IN, cname lb1.www.ms.akadns.net
  - lb1.www.ms.akadns.net: type A, class IN, addr 65.55.57.27

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 1c 42 7a e2 87 00 1a 70 e9 57 1d 08 00 45 00 ..Bz.... p.W...E.
0010 00 97 da c4 00 00 3a 11 9f 39 c2 a5 82 04 c0 a8 .....: .9.....
0020 01 06 00 35 04 1d 00 83 3f 31 fa 76 81 80 00 01 ...5.... ?1.v....
0030 00 04 00 00 00 00 03 77 77 77 09 6d 69 63 72 6f .....w ww.micro
0040 73 6f 66 74 03 63 6f 6d 00 00 01 00 01 c0 0c 00 soft.com .....
0050 05 00 01 00 00 00 15 00 1a 06 74 6f 67 67 6c 65 ..... ..toggle
0060 03 77 77 77 02 6d 73 06 61 6b 61 64 6e 73 03 6e .www.ms. akadns.n
0070 65 74 00 c0 2f 00 05 00 01 00 00 00 39 00 04 01 et.../... ..9...
0080 67 c0 36 c0 55 00 05 00 01 00 00 00 39 00 06 03 g.6.U... ..9...
```

The status bar at the bottom indicates: 192, Packets: 55 · Displayed: 55 (100.0%) · Load time: 0:0:0 · Profile: Default

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

# Networking

## Computer Lab Exercises

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. <https://www.facebook.com>
  - b. <https://www.google.com>
  - c. <https://www.imgur.com>
  - d. <https://www.reddit.com>



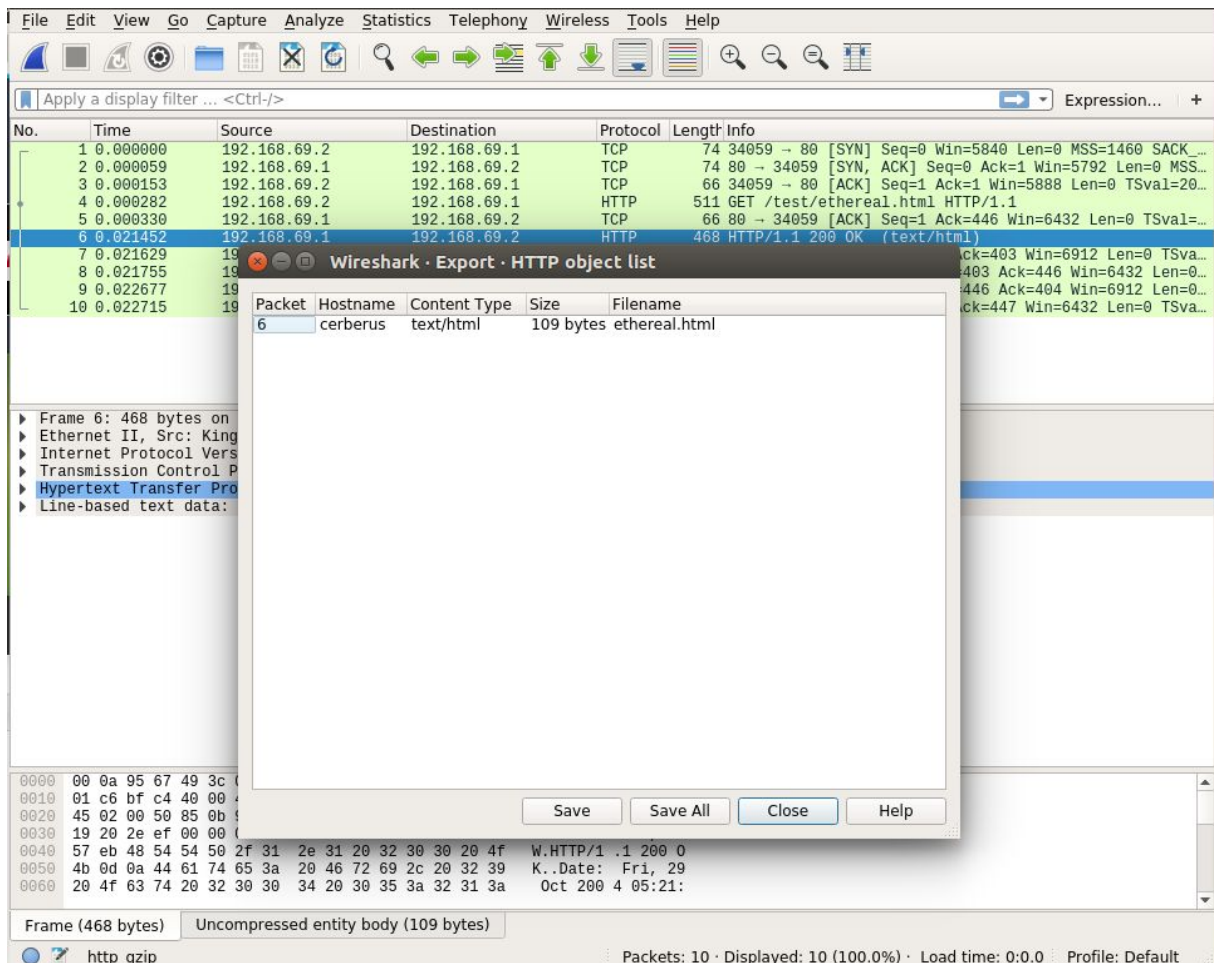
# Networking

## Computer Lab Exercises

17. In the 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 verifies packet data integrity
20. Close all open programs

### 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'





# Networking

## Computer Lab Exercises

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' folder in the 'Desktop' folder
12. Right click on 'ethereal.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. 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>
  17. In the top left of wireshark, select 'File' then, 'Export Objects', then 'HTTP'

### 18. 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
19. Close all open programs

### 20. Conclusion

- a. Using wireshark you're able to see network traffic as it's sent over a computer network
- b. Using wireshark, you're able to see unsecure (in the clear, plain text) information, which is bad
- c. You're also able to see how encryption prevents network information from being eavesdropped on bad hackerz