Lab I: Using Wireshark

Objectives

- To get the student familiar with Wireshark, the basic network protocol analyzer tool, and network equipment used in later activities for the course.
- To understand how data exchanged in computer networks is organized into layers.

Readings

- Go to `http://www.wireshark.org/docs/man-pages/wireshark-filter.html` and `http://www.wireshark.org/docs/dfref` and read about capture filters and display filters in Wireshark.
- Read the introduction part (pages 1–18) of the article *Understanding IP Addressing: Everything You Ever Wanted to Know*.

Equipment List

Equipment	Quantity
Linux host with one Ethernet card	3
Switch	1

Background

Since this is the first lab that you have to configure the PCs and network configuration in Linux, a brief introduction to necessary commands will be given.

Your Linux comes with graphical user interface, but in this lab (and most of other labs) you have to use console window (text mode). Most commands in Linux come with help. If you want to consult the command manual, use the command 'man'. For example, 'man ping' will show you how to use ping command. The content will be shown one page at a time. You can press space bar to scroll down or `Ctrl-b` to scroll up or 'q' to quit to the shell prompt.

Another useful shell feature is command/path completion to save typing time. You can type a partial command string and then press the Tab key. If the string is a unique prefix of a command, the shell will fill out the rest for you. For example, you can type

```
wir
```

followed by Tab. The shell will complete

```
wireshark
```

If multiple commands match your partial string `wir`, the shell will list those commands. This technique also applies to path completion, which will save your time in typing the whole pathname.

Another important command is `Ping`, a basic network utility for checking whether a target host is reachable or not. `Ping` sends an ICMP Echo Request message to the destination host, which then returns an ICMP Echo Reply message. For the list of options, issue `'man ping'`; or for brief parameter listing, try `'ping -h'`.

In Linux, Ethernet interfaces are named `eth0` (first port), `eth1`, and so on. You can use command

```
ifconfig
```

to display current network interface configuration.

You will also see interface `lo`. This is a loop back interface and will not be used in the lab. The equivalent `ifconfig` command in Windows is `ipconfig`.

Wireshark is a network protocol analyzer with a graphical user interface. Originally, its name was Ethereal but was changed to Wireshark many years ago due to some legal problem. However, the interfaces and functionalities of Wireshark have not changed much since the last version of Ethereal. Therefore, you can safely use most of the Ethereal tutorials in Wireshark. Using Wireshark, you can interactively capture and examine network traffic, view summaries, and get detailed information for each packet.

Saving files to a flash drive: You should explicitly eject a flash drive before removing it. Otherwise, files may not be properly copied; You would see the filenames but the file sizes are zero.

Procedures

Part I

Wireshark Basic

This part of the lab walks you through the steps of capturing and saving network traffic with Wireshark. The part is carried out on PC1.

1. Set up the network topology as shown in Fig. 1. Connect the cables to the interface `eth0` of the PCs.

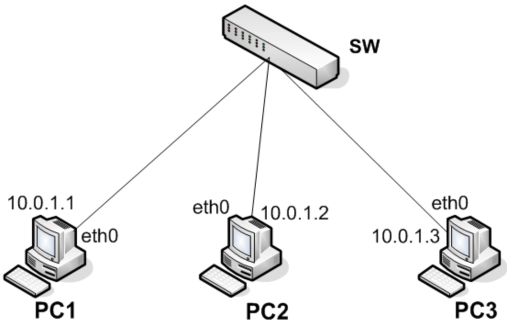


Figure 1: Network topology setup for Part I

2. Open Terminal in each Linux host to onfigure the interface `eth0` of each PC according to Fig. 1. For example, to configure the IP address of PC2, typing the following commands in the terminal window:

   ```
   ifconfig eth0 10.0.1.2 netmask 255.255.255.0 up
   ```

   or

   ```
   ifconfig eth0 10.0.1.2/24 up
   ```

3. At PC1, start Wireshark by typing the following command in the terminal window:

   ```
   wireshark &
   ```

   Or you can invoke the program from the menu *Applications* → *Internet* → *Wireshark*

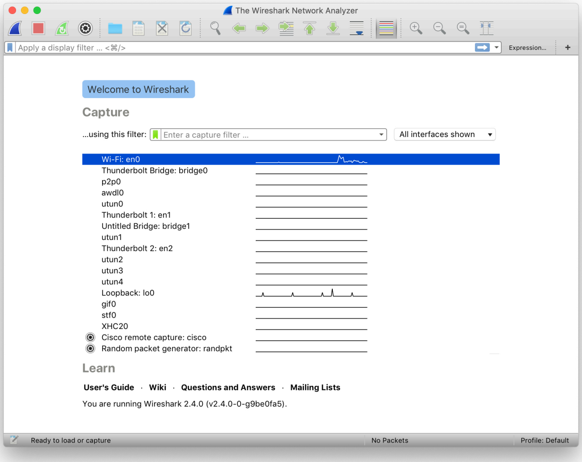
   The Wireshark main window is shown in Fig. 2. The one shown on your screen may look different depending on the OS.

4. Start traffic capture by double-clicking the interface name in the Start window. You should see a list of packets showing up in the capture window as shown in Fig. 3.

5. **Generating Ping traffic**: Open a separate Terminal window on PC1 and enter the commands

   ```
   ping -c 3 10.0.1.2
   ```

   ```
   ping -c 3 10.0.1.3
   ```


The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Expression...
+

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Wi-Fi: en0
Thunderbolt Bridge: bridge0
p2p0
awdl0
utun0
Thunderbolt 1: en1
Untitled Bridge: bridge1
utun1
Thunderbolt 2: en2
utun2
utun3
utun4
Loopback: lo0
gif0
stf0
XHC20
Cisco remote capture: cisco
Random packet generator: randpkt

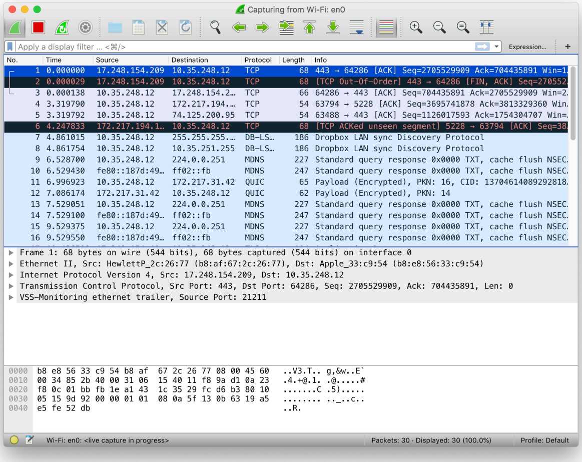
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.4.0 (v2.4.0-0-g9be0fa5).

Ready to load or capture　No Packets　Profile: Default

Figure 2: Wireshark Start window



```
No.  Time      Source           Destination     Protocol Length Info
  1 0.000000  17.248.154.209   10.35.248.12    TCP        68 443 → 64286 [ACK] Seq=2705529909 Ack=704435891 Win=1…
  2 0.000029  17.248.154.209   10.35.248.12    TCP        68 [TCP Out-Of-Order] 443 → 64286 [FIN, ACK] Seq=270552…
  3 0.000138  10.35.248.12     17.248.154.2…   TCP        66 64286 → 443 [ACK] Seq=704435891 Ack=2705529909 Win=2…
  4 3.319790  10.35.248.12     172.217.194.…   TCP        54 63794 → 5228 [ACK] Seq=3695741878 Ack=3813329360 Win…
  5 3.319792  10.35.248.12     74.125.200.95   TCP        54 63488 → 443 [ACK] Seq=1126017593 Ack=1754304707 Win=…
  6 4.247833  172.217.194.1…   10.35.248.12    TCP        68 [TCP ACKed unseen segment] 5228 → 63794 [ACK] Seq=38…
  7 4.861015  10.35.248.12     255.255.255.…   DB-LS…    186 Dropbox LAN sync Discovery Protocol
  8 4.861754  10.35.248.12     10.35.251.255   DB-LS…    186 Dropbox LAN sync Discovery Protocol
  9 6.528700  10.35.248.12     224.0.0.251     MDNS      227 Standard query response 0x0000 TXT, cache flush NSEC…
 10 6.529430  fe80::187d:49…   ff02::fb        MDNS      247 Standard query response 0x0000 TXT, cache flush NSEC…
 11 6.996923  10.35.248.12     172.217.31.42   QUIC       65 Payload (Encrypted), PKN: 16, CID: 13704614089292818…
 12 7.086174  172.217.31.42    10.35.248.12    QUIC       62 Payload (Encrypted), PKN: 14
 13 7.529051  10.35.248.12     224.0.0.251     MDNS      227 Standard query response 0x0000 TXT, cache flush NSEC…
 14 7.529100  fe80::187d:49…   ff02::fb        MDNS      247 Standard query response 0x0000 TXT, cache flush NSEC…
 15 9.529375  10.35.248.12     224.0.0.251     MDNS      227 Standard query response 0x0000 TXT, cache flush NSEC…
 16 9.529550  fe80::187d:49…   ff02::fb        MDNS      247 Standard query response 0x0000 TXT, cache flush NSEC…

▶ Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
▶ Ethernet II, Src: HewlettP_2c:26:77 (b8:af:67:2c:26:77), Dst: Apple_33:c9:54 (b8:e8:56:33:c9:54)
▶ Internet Protocol Version 4, Src: 17.248.154.209, Dst: 10.35.248.12
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 64286, Seq: 2705529909, Ack: 704435891, Len: 0
▶ VSS-Monitoring ethernet trailer, Source Port: 21211

0000  b8 e8 56 33 c9 54 b8 af  67 2c 26 77 08 00 45 60   ..V3.T.. g,&w..E`
0010  00 34 85 2b 40 00 31 06  15 40 11 f8 9a d1 0a 23   .4.+@.1. .@.....#
0020  f8 0c 01 bb fb 1e a1 43  1c 35 29 fc d6 b3 80 10   .......C .5).....
0030  05 15 9d 92 00 00 01 01  08 0a 5f 13 0b 63 19 a5   ........ .._..c..
0040  e5 fe 52 db                                        ..R.
```

Wi-Fi: en0: <live capture in progress>　Packets: 30 · Displayed: 30 (100.0%)　Profile: Default

Figure 3: Wireshark caption option window

which will send (ping) three packets to PC2 and PC3. You should see some output messages on the screen.

6. **Generating Telnet traffic**: Continue at PC1 terminal, enter the command

    ```
    telnet 10.0.1.2
    ```

    This command establishes a remote terminal session to PC2. Enter the username

    `root`

    with the password

    `networklab`

    when the login prompt shows up. Then, type `exit` to end the session.

7. **Stopping traffic capture**: Click the Red square icon in the capture window (the 2nd one in the taskbar).

8. **Setting display filters**: In the Wireshark capture window on PC1, set the display filter in the box below the taskbar to

```
ip.addr == 10.0.1.3
```

Now the capture window will display only packets to or from PC3.

If you want to display packets of both PC2 and PC3, use

```
ip.addr == 10.0.1.2 or ip.addr == 10.0.1.3
```

Go to *Help* → *Manual pages* → *Wireshark filter* for more filter patterns.

Lab Questions

I.1 Enter `icmp` in the Wireshark display filter and select one frame in the capture window to answer the following questions:

(a) What is the total frame size?

(b) How many protocol layers the frame has? How many protocols the frame has? How do you know?

(c) For each protocol, what is the header size and payload size in bytes? Which protocol has the highest and lowest percentages of overhead?

(d) How many layers contain the address information in the header? How are they different?

I.2 Enter `tcp` in the Wireshark display filter and select one frame in the capture window to answer the following questions:

(a) What is the total frame size?

(b) How many protocol layers the frame has? How many protocols the frame has?

(c) For each protocol, what is the header size and payload size in bytes? Which protocol has the highest and lowest percentages of overhead?