Lab 2 (Week 2) Wireshark and Tcpdump

CAN201

Dr. Wenjun Fan

Outline

- Wireshark
    - Packet sniffer
    - Getting Wireshark
    - Running Wireshark
    - Wireshark GUI
    - Taking Wireshark for a test run
- Tcpdump
- Hands-on Practice

Introduction

- One’s understanding of network protocols can often be greatly deepened by
    - “seeing protocols in action”.
    - “playing around with protocols”.
- Wireshark (Packet Sniffer) can help us in
    - observing the sequence of messages exchanged between two protocol entities.
    - delving down into the details of protocol operation.

Network testbed facilitating certain scenario can help us in

- causing protocols to perform certain actions.
- observing these actions and their consequences.

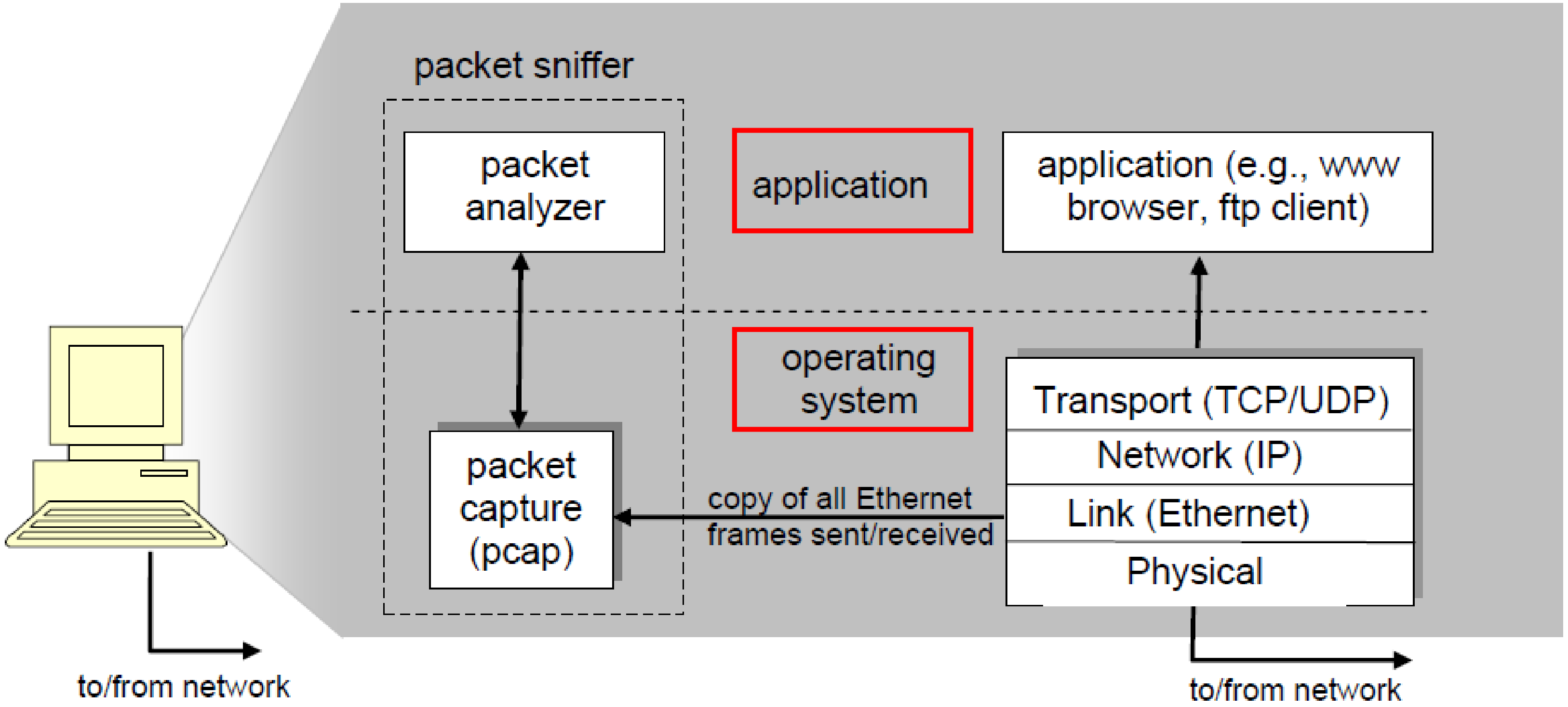
Packet Sniffer

- Packet sniffer: captures (“sniffs”) messages being sent/received from/by the sniffing target (e.g., your computer); also, it typically stores and displays the contents of the various protocol fields.
  - Wireshark
  - Tshark
  - Tcpdump
- Traffic control framework: control (or even manipulate) the original messages instead of a copy
  - NetfilterQueue
- Network scanner: scan the target (system or network) via sending probing packets
  - Nmap

Tools’ Links

- Wirshark: https://www.wireshark.org/
- Tshark: https://www.wireshark.org/docs/man-pages/tshark.html
- Tcpdump: https://www.tcpdump.org/
- NetfilterQueue: https://pypi.org/project/NetfilterQueue/
- Nmap: https://nmap.org/

Packet Sniffer Structure



Wireshark

Wireshark is a free network protocol analyzer and so an ideal packet analyzer for our labs:

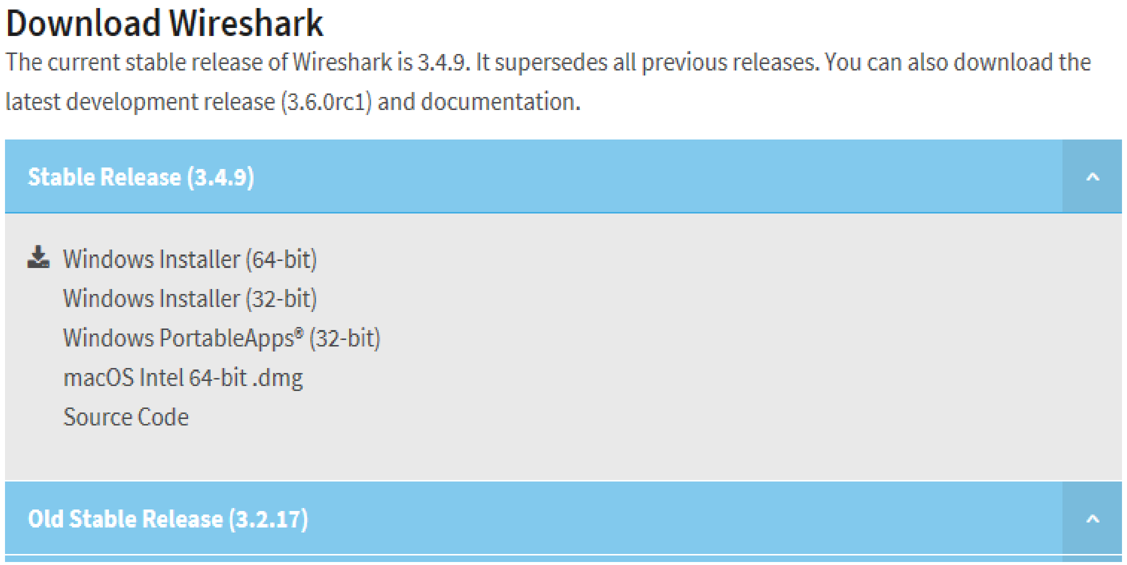
- runs on Windows, Mac, and Linux/Unix computers.
- includes the capability to analyze hundreds of protocols
- has a well-designed user interface
- operates in computers using Ethernet, serial (PPP and SLIP), 802.11 wireless LANs, and many other link-layer technologies.
- it is stable, has a large user base and well-documented support:
  - User guide (http://www.wireshark.org/docs/wsug_html_chunked/)
  - Man pages (http://www.wireshark.org/docs/man-pages/)
  - Detailed FAQ (http://www.wireshark.org/faq.html)

Getting Wireshark

Download and install the Wireshark software:

- Go to (http://www.wireshark.org/download.html) and download and install the Wireshark binary for your computer.

- For Ubuntu (Linux), look at this:
  - https://cloudcone.com/docs/article/how-to-install-wireshark-on-ubuntu-18-04-lts/

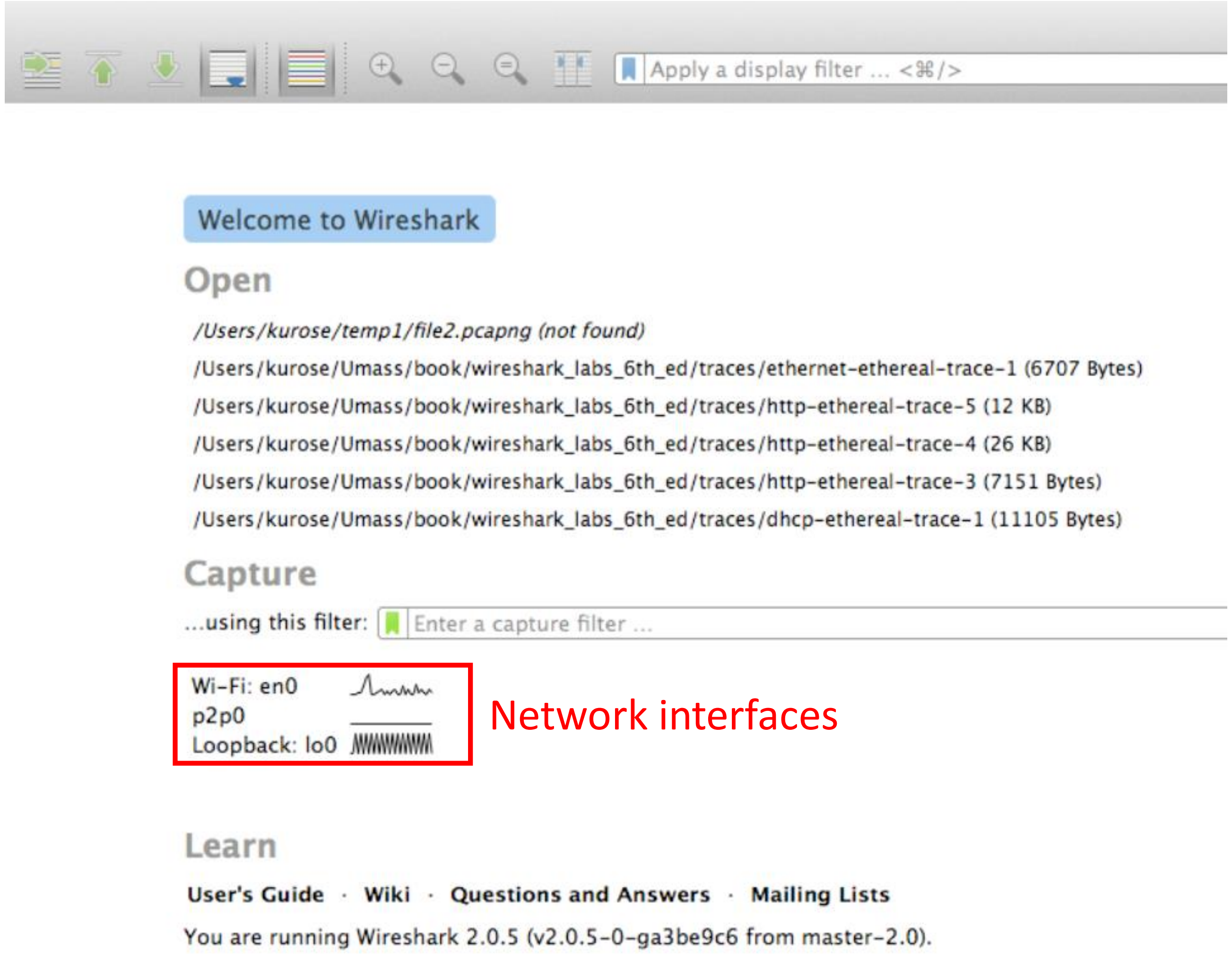


Download Wireshark

The current stable release of Wireshark is 3.4.9. It supersedes all previous releases. You can also download the latest development release (3.6.0rc1) and documentation.

Stable Release (3.4.9)
Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
macOS Intel 64-bit .dmg
Source Code
Old Stable Release (3.2.17)

Running Wireshark



Welcome to Wireshark

Open

/Users/kurose/temp1/file2.pcapng (not found)

/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/ethernet-ethereal-trace-1 (6707 Bytes)

/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/http-ethereal-trace-5 (12 KB)

/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/http-ethereal-trace-4 (26 KB)

/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/http-ethereal-trace-3 (7151 Bytes)

/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/dhcp-ethereal-trace-1 (11105 Bytes)

Capture

…using this filter: Enter a capture filter …

Wi-Fi: en0
p2p0
Loopback: lo0

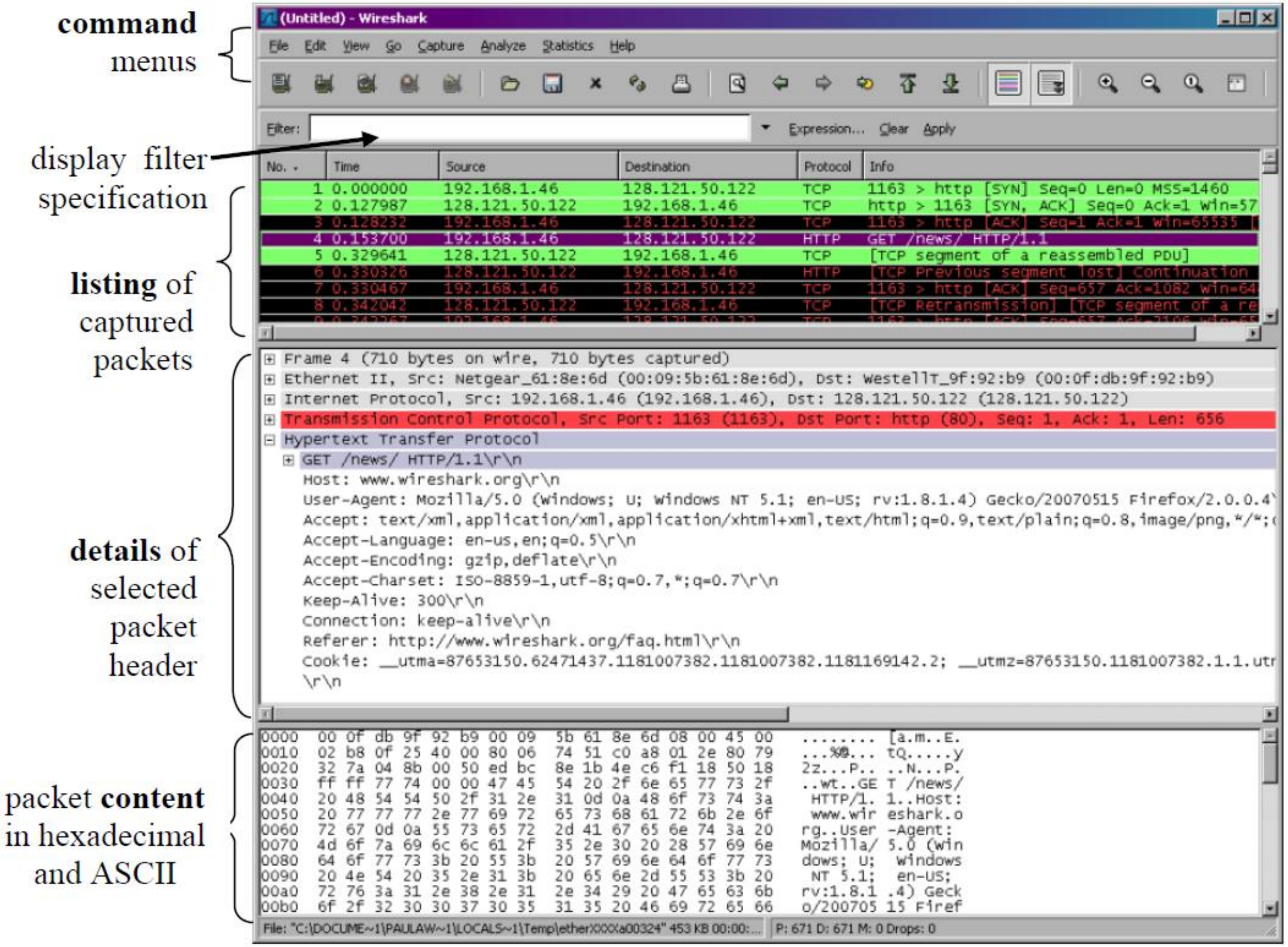
Network interfaces

Learn

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

You are running Wireshark 2.0.5 (v2.0.5-0-ga3be9c6 from master-2.0).

Wireshark Graphical User Interface


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

command menus

display filter specification

listing of captured packets

details of selected packet header

packet **content** in hexadecimal and ASCII

```
No. -  Time      Source          Destination     Protocol Info
     1 0.000000  192.168.1.46    128.121.50.122  TCP      1163 > http [SYN] Seq=0 Len=0 MSS=1460
     2 0.127987  128.121.50.122  192.168.1.46    TCP      http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
     3 0.128232  192.168.1.46    128.121.50.122  TCP      1163 > http [ACK] Seq=1 Ack=1 Win=65535 [
     4 0.153700  192.168.1.46    128.121.50.122  HTTP     GET /news/ HTTP/1.1
     5 0.329641  128.121.50.122  192.168.1.46    TCP      [TCP segment of a reassembled PDU]
     6 0.330326  128.121.50.122  192.168.1.46    HTTP     [TCP Previous segment lost] Continuation
     7 0.330467  192.168.1.46    128.121.50.122  TCP      1163 > http [ACK] Seq=657 Ack=1082 Win=64
     8 0.342042  128.121.50.122  192.168.1.46    TCP      [TCP Retransmission] [TCP segment of a re
     9 0.342267  192.168.1.46    128.121.50.122  TCP      1163 > http [ACK] Seq=657 Ack=2106 Win=65
```

```
⊞ Frame 4 (710 bytes on wire, 710 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
⊞ Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
⊟ Hypertext Transfer Protocol
  ⊞ GET /news/ HTTP/1.1\r\n
     Host: www.wireshark.org\r\n
     User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
     Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
     Accept-Language: en-us,en;q=0.5\r\n
     Accept-Encoding: gzip,deflate\r\n
     Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
     Keep-Alive: 300\r\n
     Connection: keep-alive\r\n
     Referer: http://www.wireshark.org/faq.html\r\n
     Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utr
     \r\n
```

```
0000  00 0f db 9f 92 b9 00 09  5b 61 8e 6d 08 00 45 00   ........ [a.m..E.
0010  02 b8 0f 25 40 00 80 06  74 51 c0 a8 01 2e 80 79   ...%@... tQ.....y
0020  32 7a 04 8b 00 50 ed bc  8e 1b 4e c6 f1 18 50 18   2z...P.. ..N...P.
0030  ff ff 77 74 00 00 47 45  54 20 2f 6e 65 77 73 2f   ..wt..GE T /news/
0040  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0050  20 77 77 77 2e 77 69 72  65 73 68 61 72 6b 2e 6f    www.wir eshark.o
0060  72 67 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   rg..User -Agent:
0070  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0080  64 6f 77 73 3b 20 55 3b  20 57 69 6e 64 6f 77 73   dows; U;  Windows
0090  20 4e 54 20 35 2e 31 3b  20 65 6e 2d 55 53 3b 20    NT 5.1;  en-US;
00a0  72 76 3a 31 2e 38 2e 31  2e 34 29 20 47 65 63 6b   rv:1.8.1 .4) Geck
00b0  6f 2f 32 30 30 37 30 35  31 35 20 46 69 72 65 66   o/200705 15 Firef
```

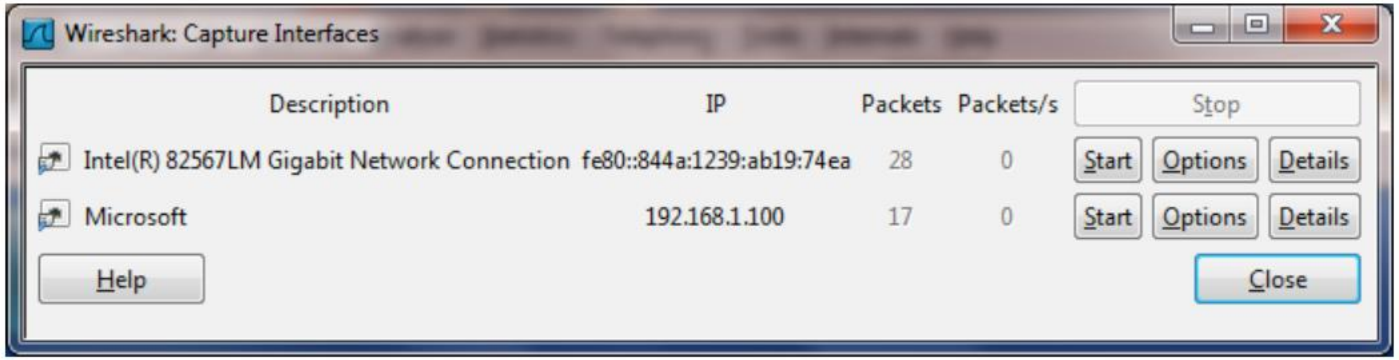
File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa00324" 453 KB 00:00:... P: 671 D: 671 M: 0 Drops: 0

Taking Wireshark for a Test Run (1/4)

1. Start up your favourite web browser, which will display your selected homepage.
2. Start up the Wireshark software. You will initially see a window. Wireshark has not yet begun capturing packets.
3. To begin packet capture, select the Capture pull down menu and select *Interfaces*. This will cause the “Wireshark: Capture Interfaces” window to be displayed.
   - ❖ Notice that if you are running Wireshark on Windows OS, you should “run as administrator”, otherwise you may encounter “no interfaces found” error.

Taking Wireshark for a Test Run (2/4)

4. You’ll see a list of the interfaces on your computer and a count of the packets that have been observed on that interface so far. Click on *Start* for the interface on which you want to begin packet capture.

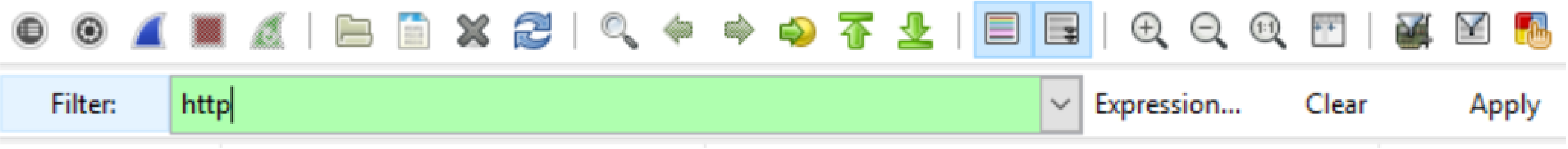


Description	IP	Packets	Packets/s
Intel(R) 82567LM Gigabit Network Connection	fe80::844a:1239:ab19:74ea	28	0
Microsoft	192.168.1.100	17	0

5. By selecting Capture pulldown menu and selecting Stop, you can stop packet capture. But don’t stop packet capture yet. Let’s capture some interesting packets first - using a web browser to generate HTTP protocol based network traffic.

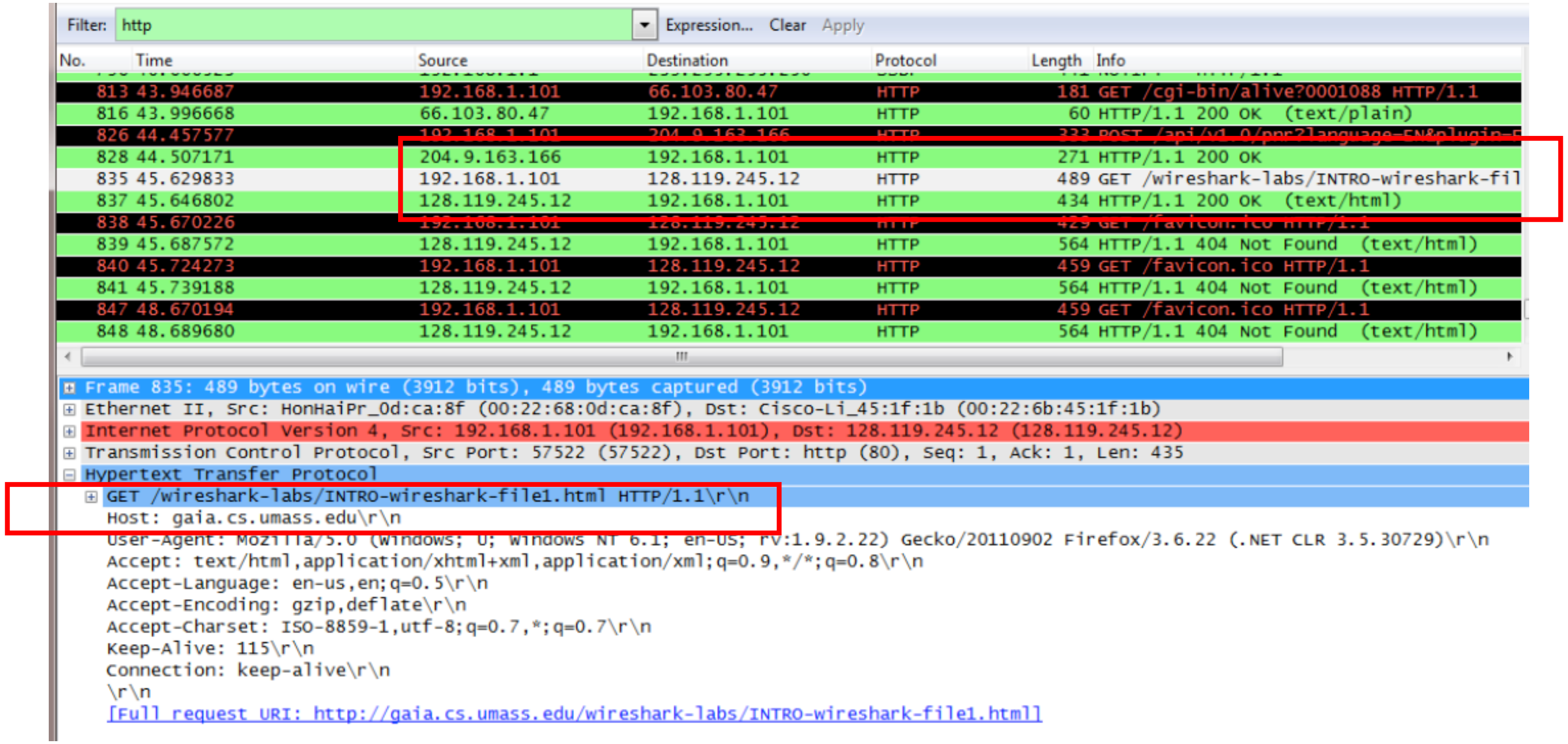
Taking Wireshark for a Test Run (3/4)

6. While Wireshark is running, enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and have that page displayed in your browser.
7. After your browser has displayed the INTRO-wireshark-file1.html page (it is a simple one line of congratulations), stop Wireshark packet capture by selecting stop in the Wireshark capture window.
8. Type in "http" (without the quotes, and in lower case) into the display filter specification window at the top of the main Wireshark window. Then select *Apply* (to the right of where you entered "http").


Filter: http

Taking Wireshark for a Test Run (4/4)

9. Find and select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window.



No.	Time	Source	Destination	Protocol	Length	Info
813	43.946687	192.168.1.101	66.103.80.47	HTTP	181	GET /cgi-bin/alive?0001088 HTTP/1.1
816	43.996668	66.103.80.47	192.168.1.101	HTTP	60	HTTP/1.1 200 OK (text/plain)
826	44.457577	192.168.1.101	204.9.163.166	HTTP	333	POST /api/v1.0/pnr?language=EN&plugin=F
828	44.507171	204.9.163.166	192.168.1.101	HTTP	271	HTTP/1.1 200 OK
835	45.629833	192.168.1.101	128.119.245.12	HTTP	489	GET /wireshark-labs/INTRO-wireshark-fil
837	45.646802	128.119.245.12	192.168.1.101	HTTP	434	HTTP/1.1 200 OK (text/html)
838	45.670226	192.168.1.101	128.119.245.12	HTTP	429	GET /favicon.ico HTTP/1.1
839	45.687572	128.119.245.12	192.168.1.101	HTTP	564	HTTP/1.1 404 Not Found (text/html)
840	45.724273	192.168.1.101	128.119.245.12	HTTP	459	GET /favicon.ico HTTP/1.1
841	45.739188	128.119.245.12	192.168.1.101	HTTP	564	HTTP/1.1 404 Not Found (text/html)
847	48.670194	192.168.1.101	128.119.245.12	HTTP	459	GET /favicon.ico HTTP/1.1
848	48.689680	128.119.245.12	192.168.1.101	HTTP	564	HTTP/1.1 404 Not Found (text/html)

```
⊞ Frame 835: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
⊞ Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
⊞ Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 57522 (57522), Dst Port: http (80), Seq: 1, Ack: 1, Len: 435
⊟ Hypertext Transfer Protocol
  ⊞ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.22) Gecko/20110902 Firefox/3.6.22 (.NET CLR 3.5.30729)\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

Tcpdump

Refer to https://opensource.com/article/18/10/introduction-tcpdump

Command-line:

```
tcpdump -i enp0s3 -w data.pcap
```

Hands-on Practice

Based on last week’s two VMs, i.e., VM1 and VM2, do the following steps:

1. Run Tcpdump on VM2 for listening on the network interface and save the captured traffic into data.pcap file.
2. Use VM1 to ping VM2, no more than 10 ICMP packets (using ‘Ctrl + C’ to stop ‘ping’ command).
3. On VM2, use ‘Ctrl + C’ to stop ‘tcpdump’ command, and then use Wireshark to open the data.pcap file and display the captured ICMP packets.
4. In the display window of Wireshark, select and highlight one entry/line to indicate one of the captured ICMP ping packets.
5. Show the result to TA to manifest your understanding.

- Office hour (appointment required):

Monday: 12:00 – 13:00

Tuesday: 12:00 – 13:00