PACKET CAPTURE TOOL :WIRESHARK

Rajib Paul and Young-June Choi

Department of Software and Computer Engineering
Ajou University

Contents

- Packet Capture and Analysis
- Install Wireshark
- Run Wireshark
- Analyze Wireshark

WireShark:

Packet Capture and Analysis

Network Packet Analysis

- Network Packet Analyzers
  - capture network packets first, then
  - display and analyze captured packet data as detailed as possible
- Usage
  - to troubleshoot network problems
    - usually by network administrators
  - to examine security problems
    - usually by network security engineers)
  - to debug protocol implementations
    - usually by protocol developers)
  - to learn network protocol internals
    - usually by students

Network Packet Analysis

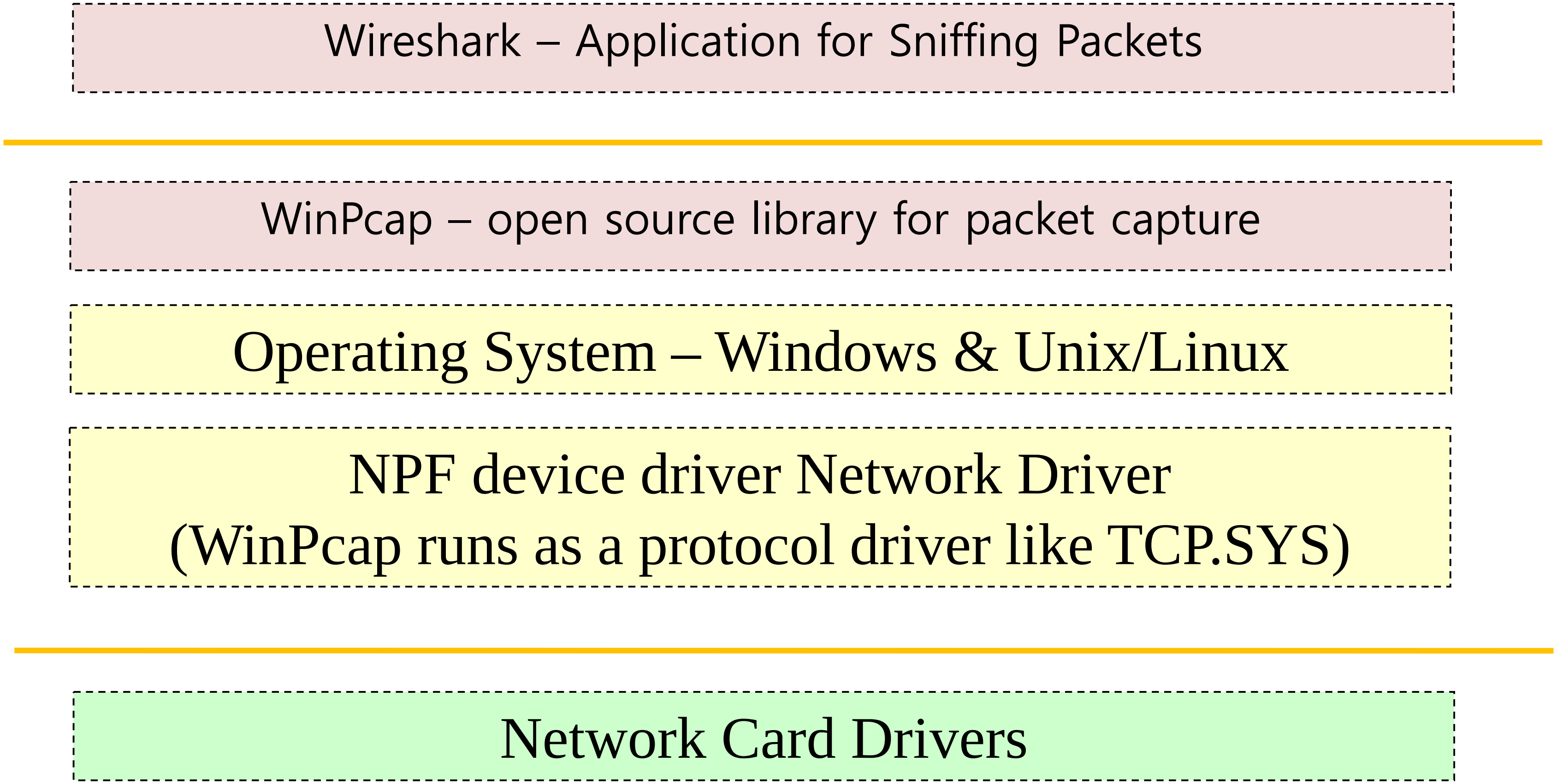
- Open Tools
  - WireShark (http://www.wireshark.org)
  - Analyzer (http://analyzer.polito.it)
  - and so many others

  - Wireshark is perhaps one of the best open source packet analyzers available today for **UNIX** and **Windows**.

- Most those tools are all based on
  - for windows OS, WinPcap (http://www.winpcap.org)
  - for linux OS, libpcap (http://www.tcpdump.org/)

Wireshark, OS, & WinPcap

- Stacks on Related Functions



Wireshark – Application for Sniffing Packets

WinPcap – open source library for packet capture

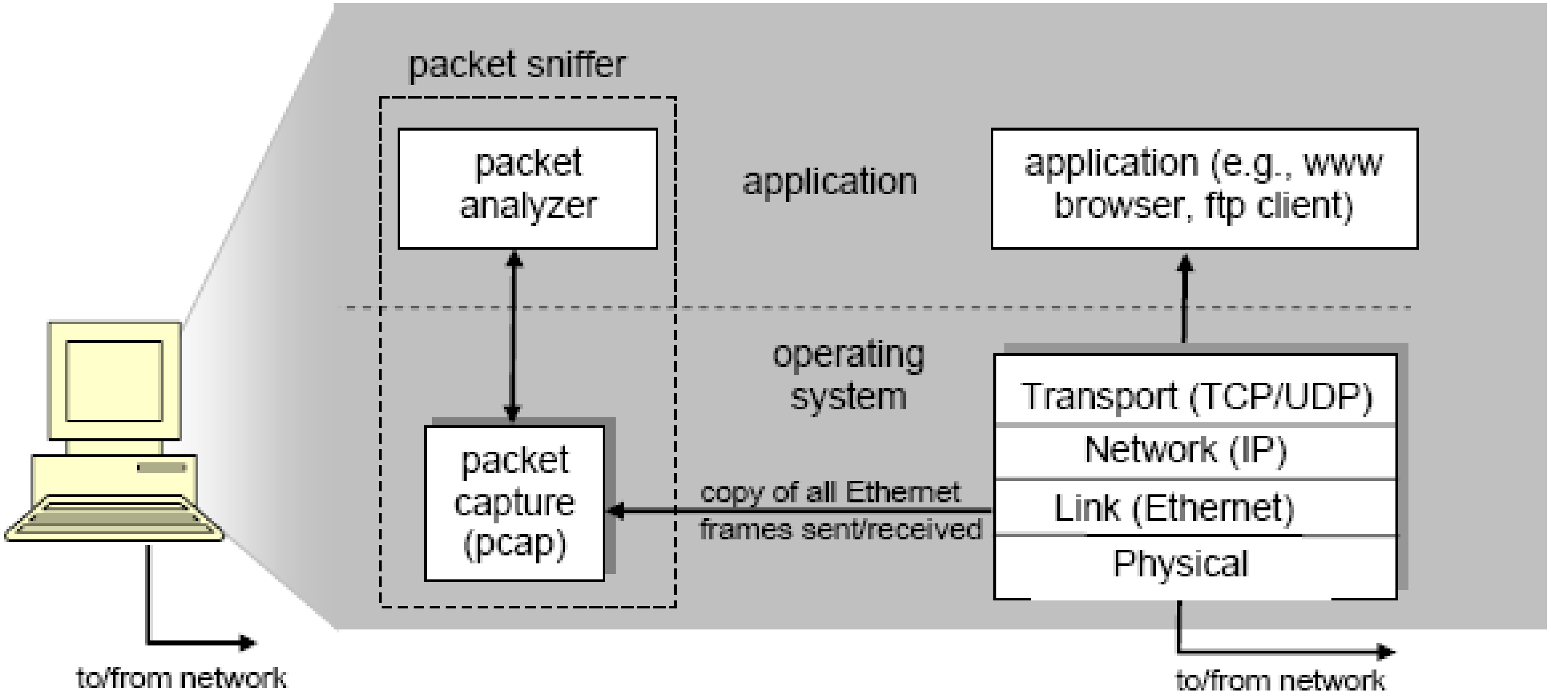
Operating System – Windows & Unix/Linux

NPF device driver Network Driver
(WinPcap runs as a protocol driver like TCP.SYS)

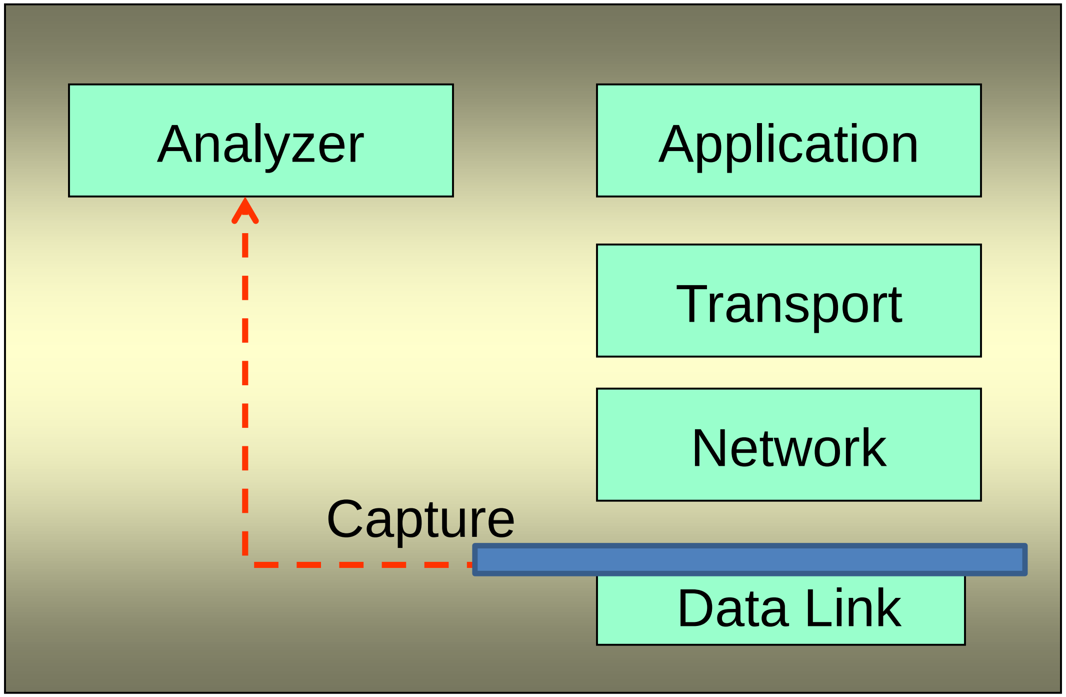
Network Card Drivers

Wireshark, OS, & WinPcap

- Basic Structure of Network Packet Analysis Operation



Remarks

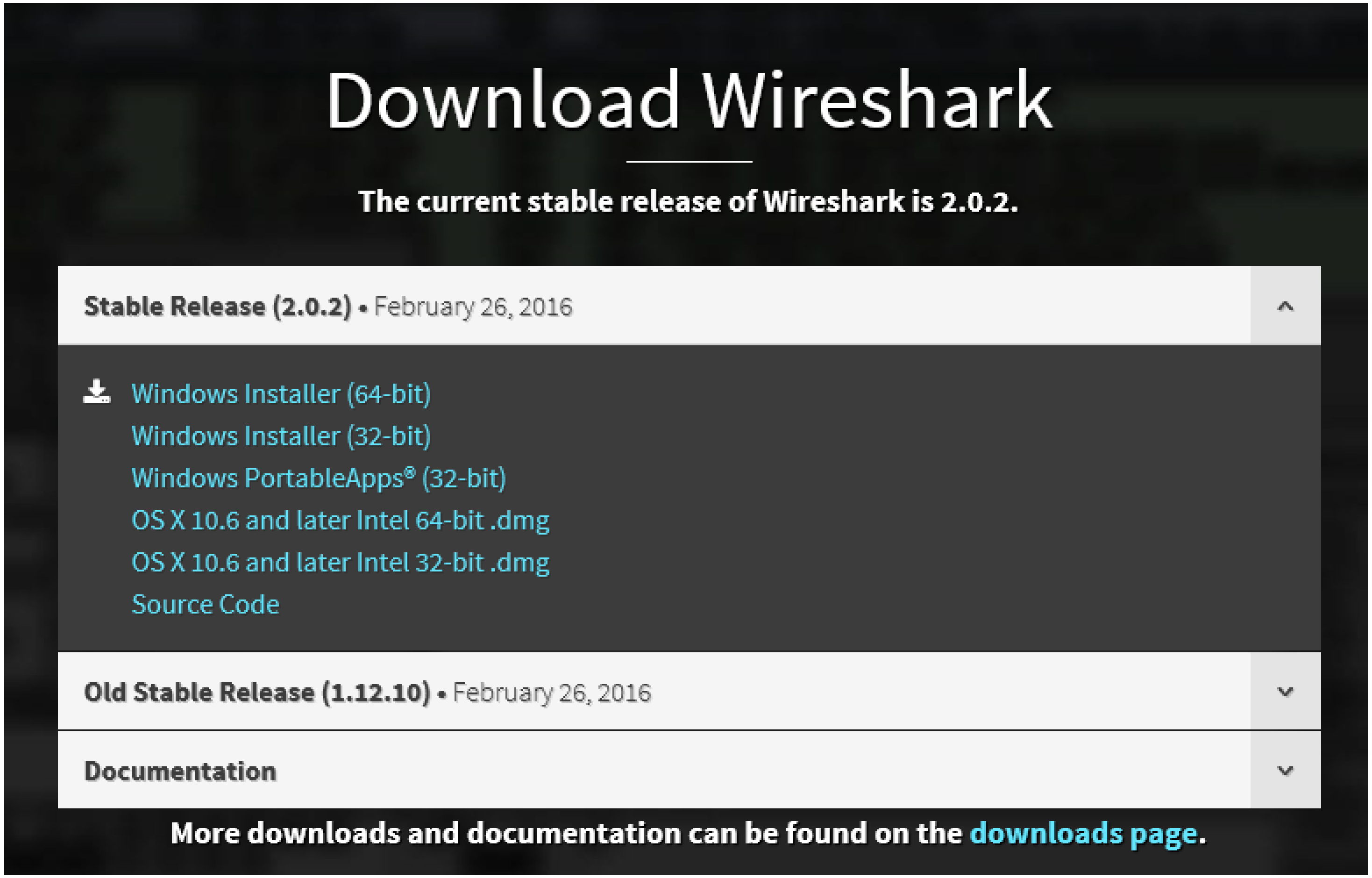

Analyzer
Application
Transport
Network
Capture
Data Link

WireShark:

Install Wireshark

Install WireShark

- visit at www.wireshark.org/#downlad



Download Wireshark

The current stable release of Wireshark is 2.0.2.

Stable Release (2.0.2) • February 26, 2016

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- OS X 10.6 and later Intel 64-bit .dmg
- OS X 10.6 and later Intel 32-bit .dmg
- Source Code

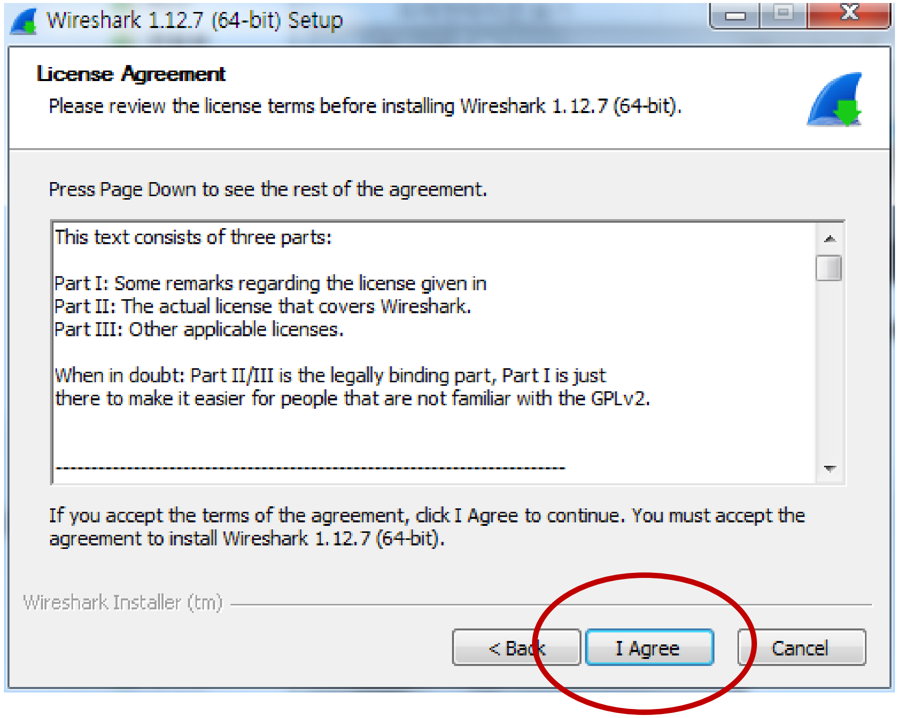
Old Stable Release (1.12.10) • February 26, 2016

Documentation

More downloads and documentation can be found on the downloads page.

Install WireShark

- install wireshark



Wireshark 1.12.7 (64-bit) Setup

License Agreement

Please review the license terms before installing Wireshark 1.12.7 (64-bit).

Press Page Down to see the rest of the agreement.

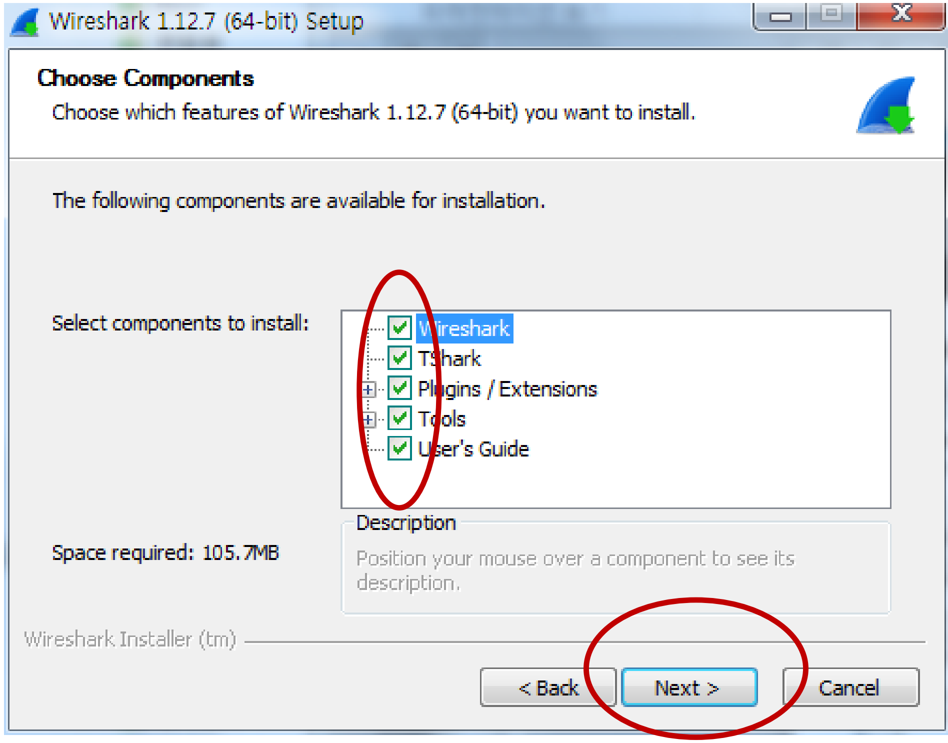
This text consists of three parts:

Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.

When in doubt: Part II/III is the legally binding part, Part I is just there to make it easier for people that are not familiar with the GPLv2.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 1.12.7 (64-bit).

Wireshark Installer (tm)



Wireshark 1.12.7 (64-bit) Setup

Choose Components

Choose which features of Wireshark 1.12.7 (64-bit) you want to install.

The following components are available for installation.

Select components to install:

☑ Wireshark
☑ TShark
☑ Plugins / Extensions
☑ Tools
☑ User's Guide

Space required: 105.7MB

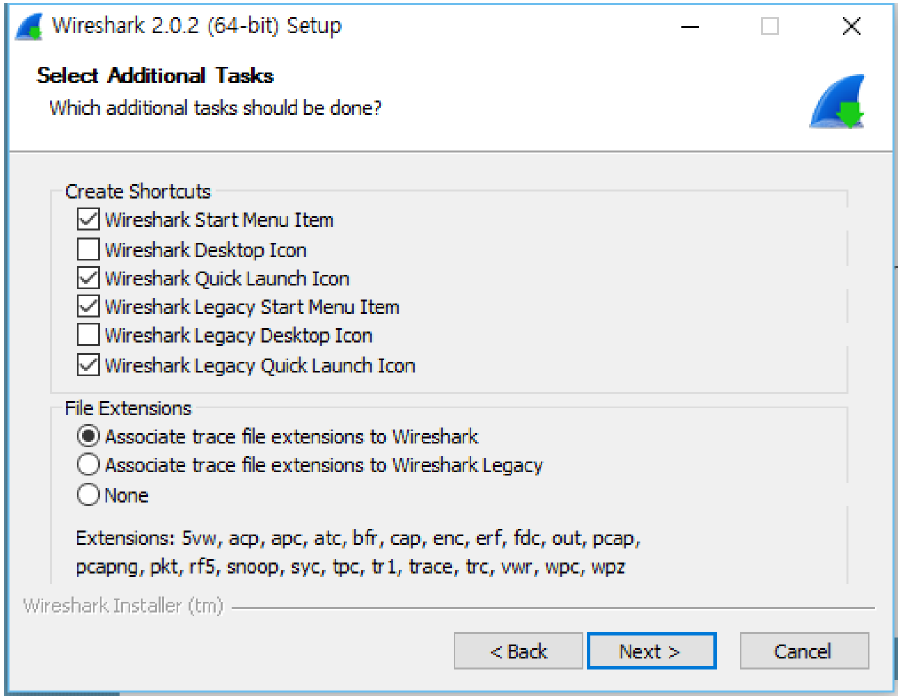
Description

Position your mouse over a component to see its description.

Wireshark Installer (tm)

Install WireShark

- install wireshark



Wireshark 2.0.2 (64-bit) Setup

Select Additional Tasks

Which additional tasks should be done?

Create Shortcuts

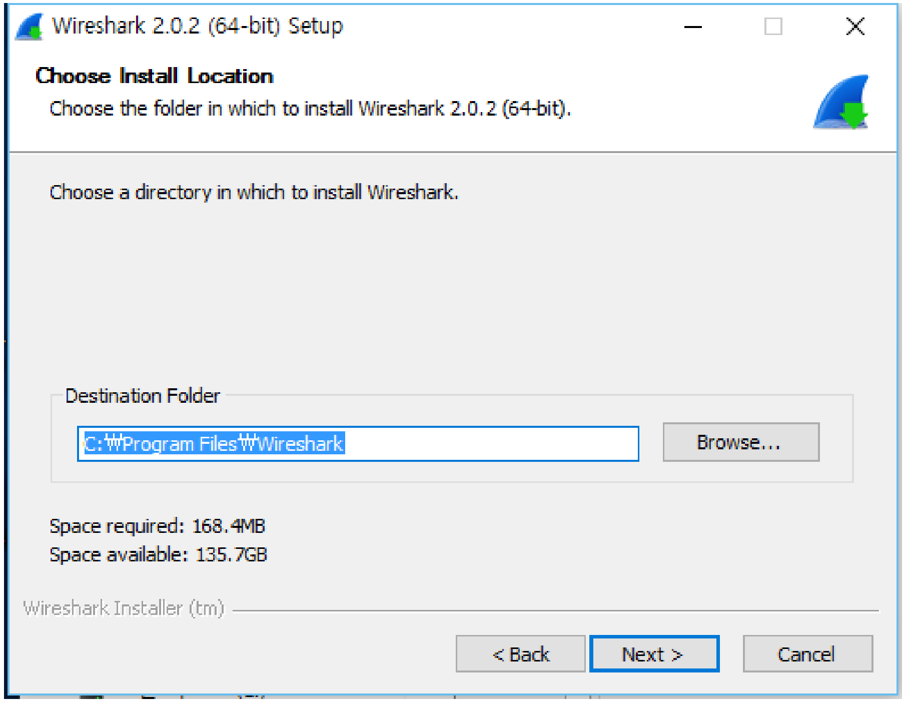
☑ Wireshark Start Menu Item
□ Wireshark Desktop Icon
☑ Wireshark Quick Launch Icon
☑ Wireshark Legacy Start Menu Item
□ Wireshark Legacy Desktop Icon
☑ Wireshark Legacy Quick Launch Icon

File Extensions

● Associate trace file extensions to Wireshark
○ Associate trace file extensions to Wireshark Legacy
○ None

Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, out, pcap, pcapng, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz

Wireshark Installer (tm)



Wireshark 2.0.2 (64-bit) Setup

Choose Install Location

Choose the folder in which to install Wireshark 2.0.2 (64-bit).

Choose a directory in which to install Wireshark.

Destination Folder

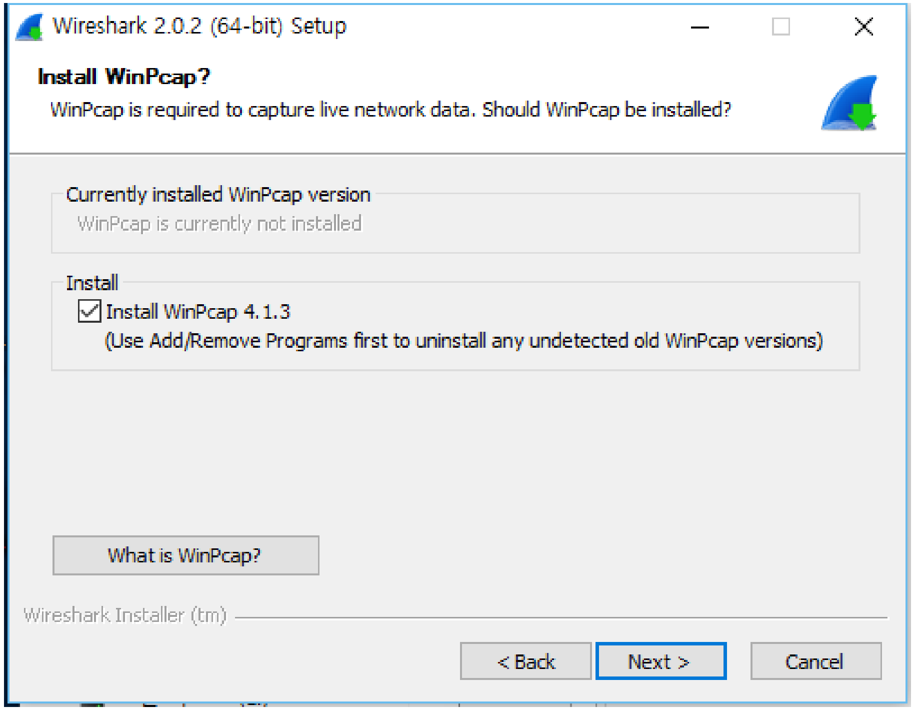
C:₩Program Files₩Wireshark

Space required: 168.4MB
Space available: 135.7GB

Wireshark Installer (tm)

Install WireShark

- install winpcap



Wireshark 2.0.2 (64-bit) Setup

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

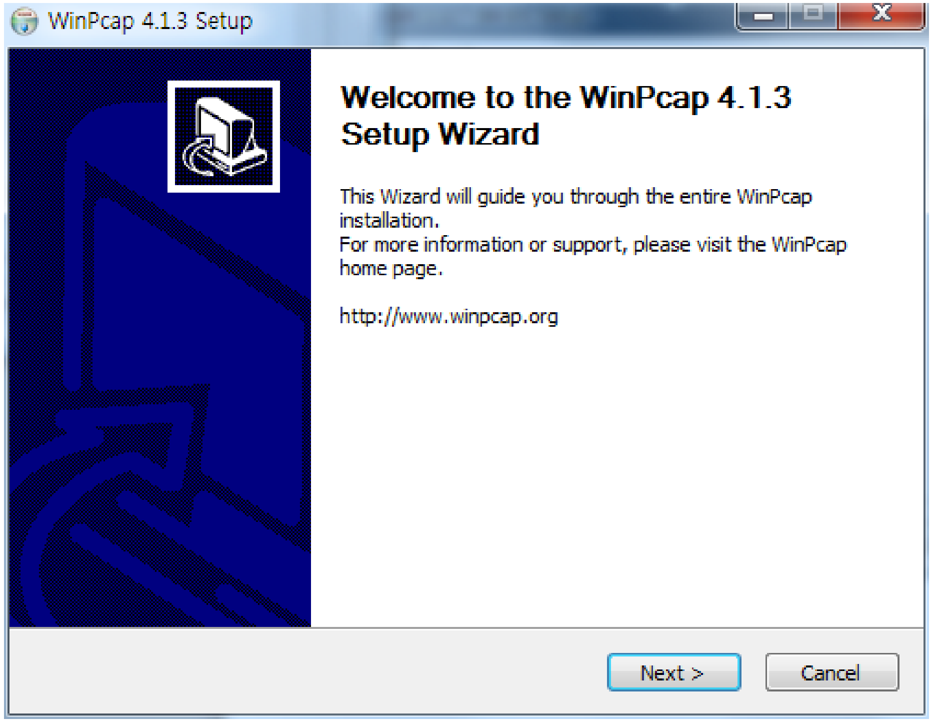
Currently installed WinPcap version

WinPcap is currently not installed

Install

☑ Install WinPcap 4.1.3

(Use Add/Remove Programs first to uninstall any undetected old WinPcap versions)



WinPcap 4.1.3 Setup

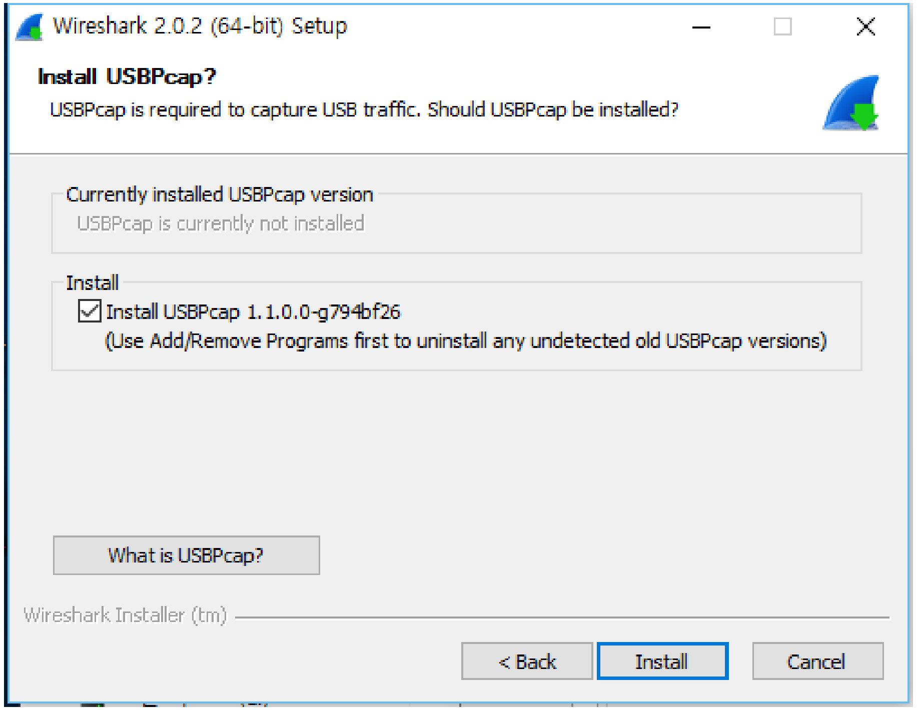
Welcome to the WinPcap 4.1.3 Setup Wizard

This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org

Install WireShark

- install winpcap



Wireshark 2.0.2 (64-bit) Setup

Install USBPcap?

USBPcap is required to capture USB traffic. Should USBPcap be installed?

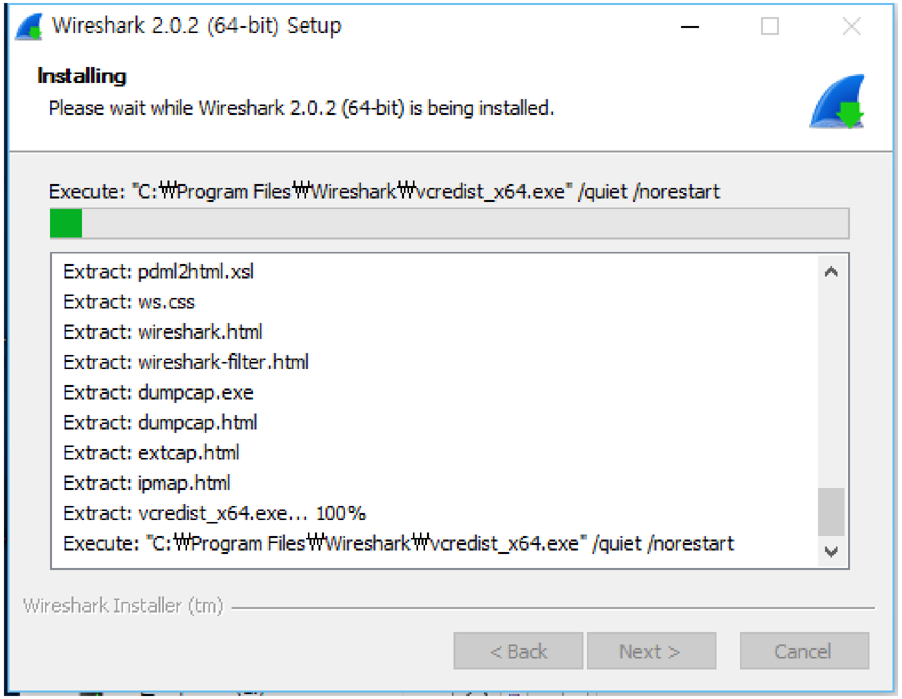
Currently installed USBPcap version

USBPcap is currently not installed

Install

☑ Install USBPcap 1.1.0.0-g794bf26

(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)



Wireshark 2.0.2 (64-bit) Setup

Installing

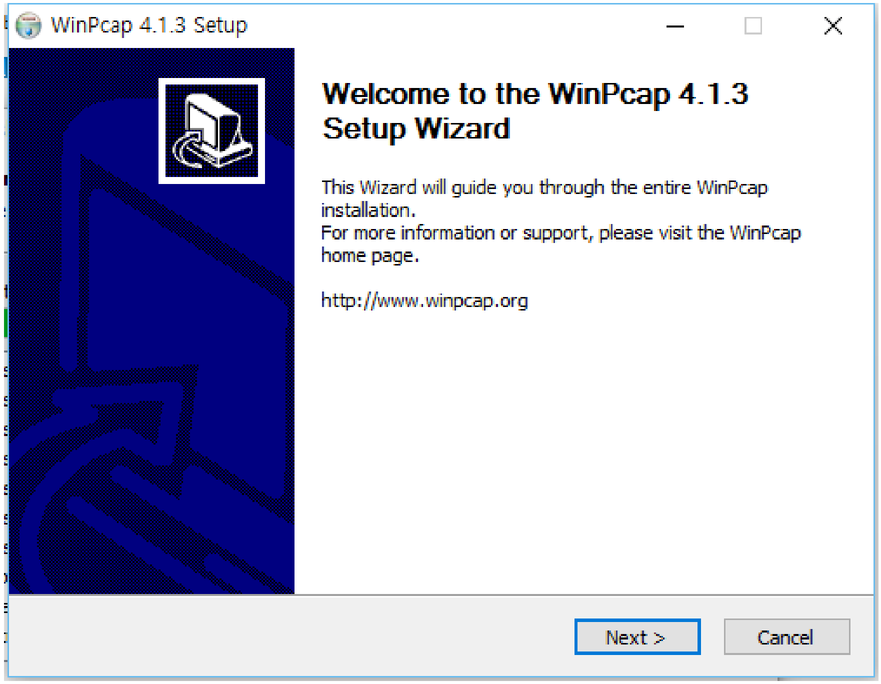
Please wait while Wireshark 2.0.2 (64-bit) is being installed.

Execute: "C:₩Program Files₩Wireshark₩vcredist_x64.exe" /quiet /norestart

```
Extract: pdml2html.xsl
Extract: ws.css
Extract: wireshark.html
Extract: wireshark-filter.html
Extract: dumpcap.exe
Extract: dumpcap.html
Extract: extcap.html
Extract: ipmap.html
Extract: vcredist_x64.exe... 100%
Execute: "C:₩Program Files₩Wireshark₩vcredist_x64.exe" /quiet /norestart
```

Install WireShark

- install winpcap



WinPcap 4.1.3 Setup

Welcome to the WinPcap 4.1.3 Setup Wizard

This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

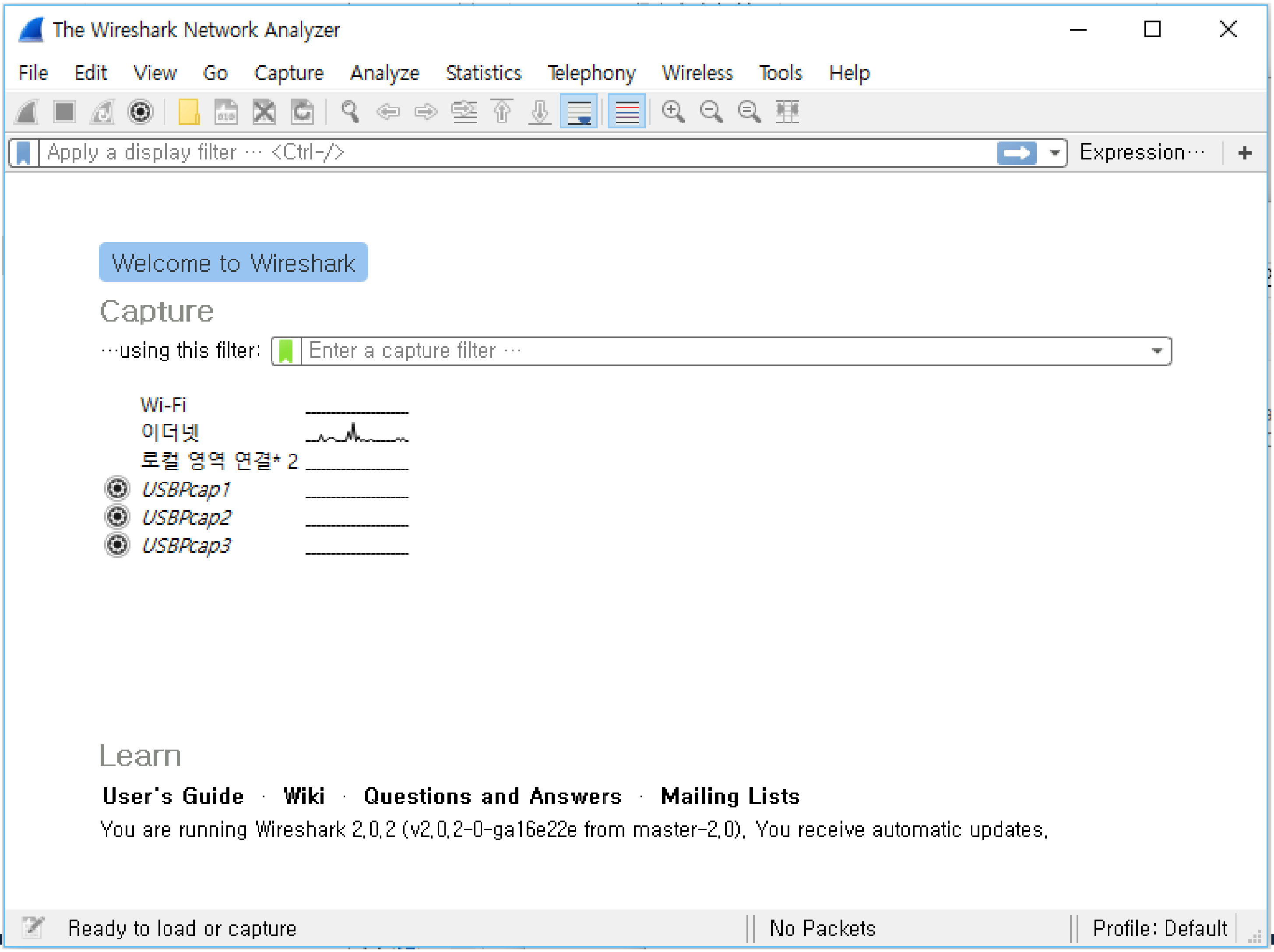
http://www.winpcap.org

WireShark:

Run Wireshark

Run WireShark

- Wireshark Start Screen



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

Apply a display filter … <Ctrl-/>

Welcome to Wireshark

Capture

…using this filter: Enter a capture filter …

Wi-Fi
이더넷
로컬 영역 연결* 2
USBPcap1
USBPcap2
USBPcap3

Learn

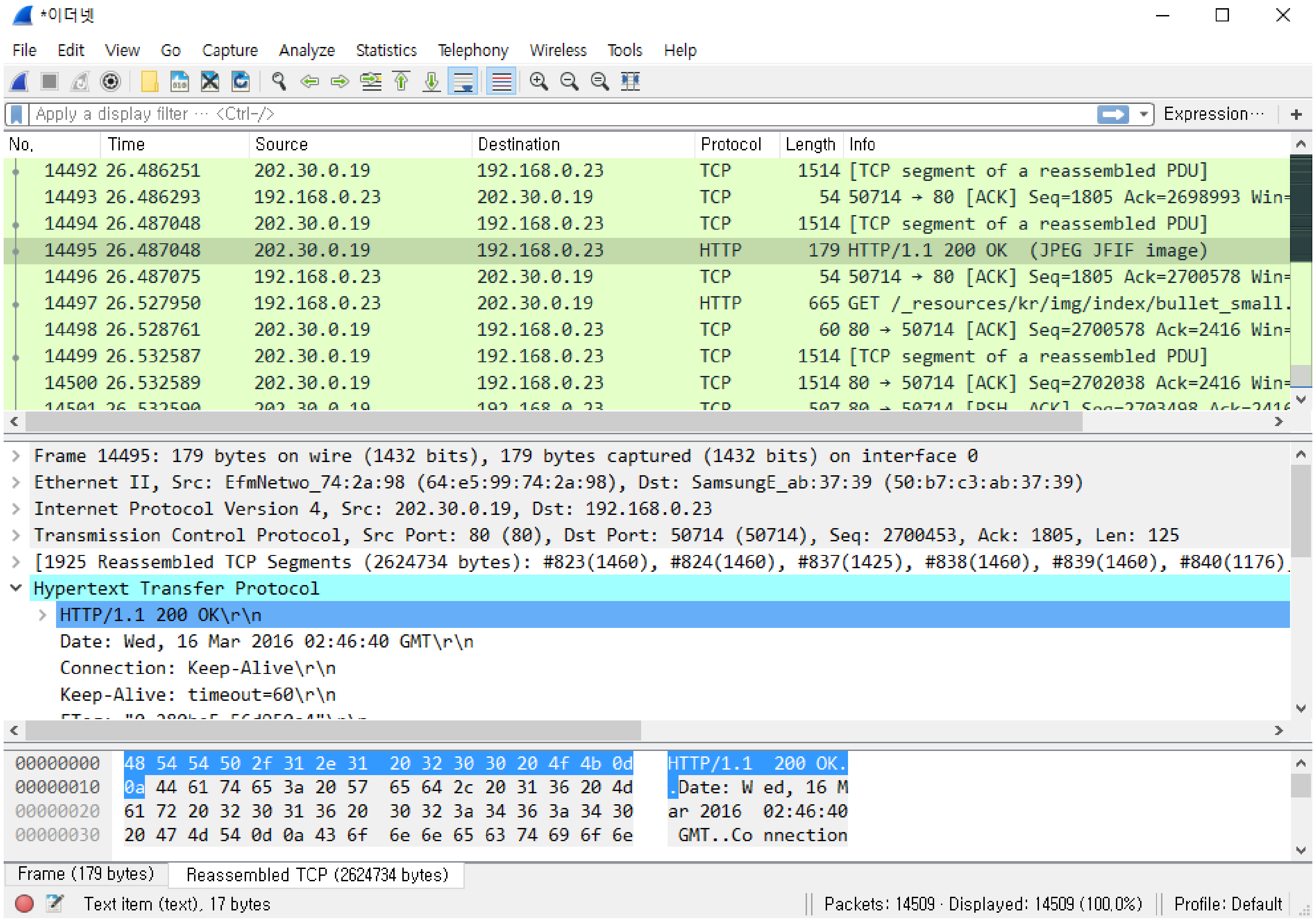
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Run WireShark

- Wireshark Start Screen



*이더넷
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

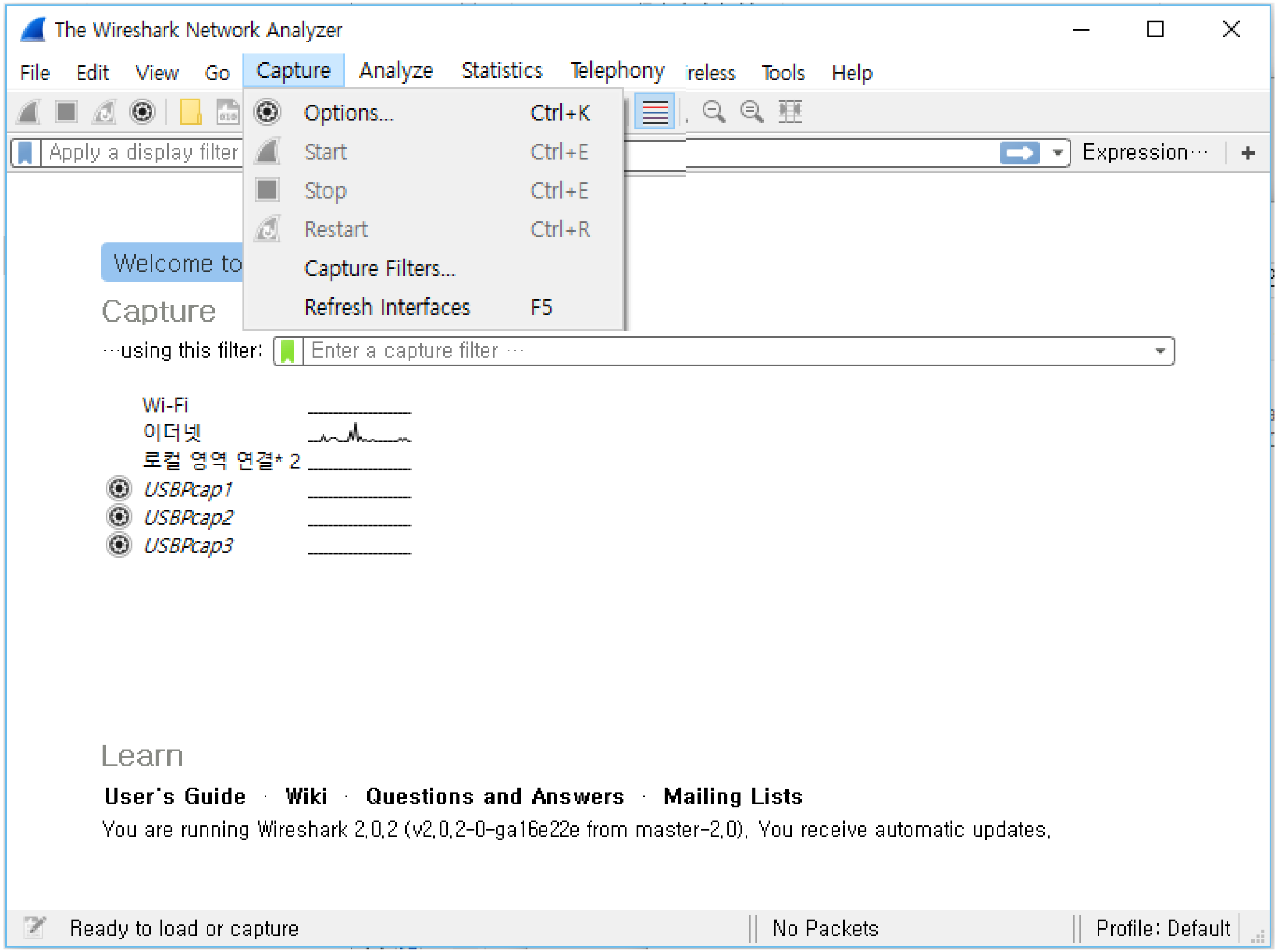
```
No.   Time       Source        Destination   Protocol Length Info
14492 26.486251  202.30.0.19   192.168.0.23  TCP      1514 [TCP segment of a reassembled PDU]
14493 26.486293  192.168.0.23  202.30.0.19   TCP        54 50714 → 80 [ACK] Seq=1805 Ack=2698993 Win=
14494 26.487048  202.30.0.19   192.168.0.23  TCP      1514 [TCP segment of a reassembled PDU]
14495 26.487048  202.30.0.19   192.168.0.23  HTTP      179 HTTP/1.1 200 OK  (JPEG JFIF image)
14496 26.487075  192.168.0.23  202.30.0.19   TCP        54 50714 → 80 [ACK] Seq=1805 Ack=2700578 Win=
14497 26.527950  192.168.0.23  202.30.0.19   HTTP      665 GET /_resources/kr/img/index/bullet_small.
14498 26.528761  202.30.0.19   192.168.0.23  TCP        60 80 → 50714 [ACK] Seq=2700578 Ack=2416 Win=
14499 26.532587  202.30.0.19   192.168.0.23  TCP      1514 [TCP segment of a reassembled PDU]
14500 26.532589  202.30.0.19   192.168.0.23  TCP      1514 80 → 50714 [ACK] Seq=2702038 Ack=2416 Win=
14501 26.532590  202.30.0.19   192.168.0.23  TCP       507 80 → 50714 [PSH, ACK] Seq=2703498 Ack=2416
```

```
> Frame 14495: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface 0
> Ethernet II, Src: EfmNetwo_74:2a:98 (64:e5:99:74:2a:98), Dst: SamsungE_ab:37:39 (50:b7:c3:ab:37:39)
> Internet Protocol Version 4, Src: 202.30.0.19, Dst: 192.168.0.23
> Transmission Control Protocol, Src Port: 80 (80), Dst Port: 50714 (50714), Seq: 2700453, Ack: 1805, Len: 125
> [1925 Reassembled TCP Segments (2624734 bytes): #823(1460), #824(1460), #837(1425), #838(1460), #839(1460), #840(1176)
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 16 Mar 2016 02:46:40 GMT\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=60\r\n
    ETag: "0-280b5-56d050a4"\r\n
```

```
00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
00000010  0a 44 61 74 65 3a 20 57  65 64 2c 20 31 36 20 4d   .Date: W ed, 16 M
00000020  61 72 20 32 30 31 36 20  30 32 3a 34 36 3a 34 30   ar 2016  02:46:40
00000030  20 47 4d 54 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e    GMT..Co nnection
```

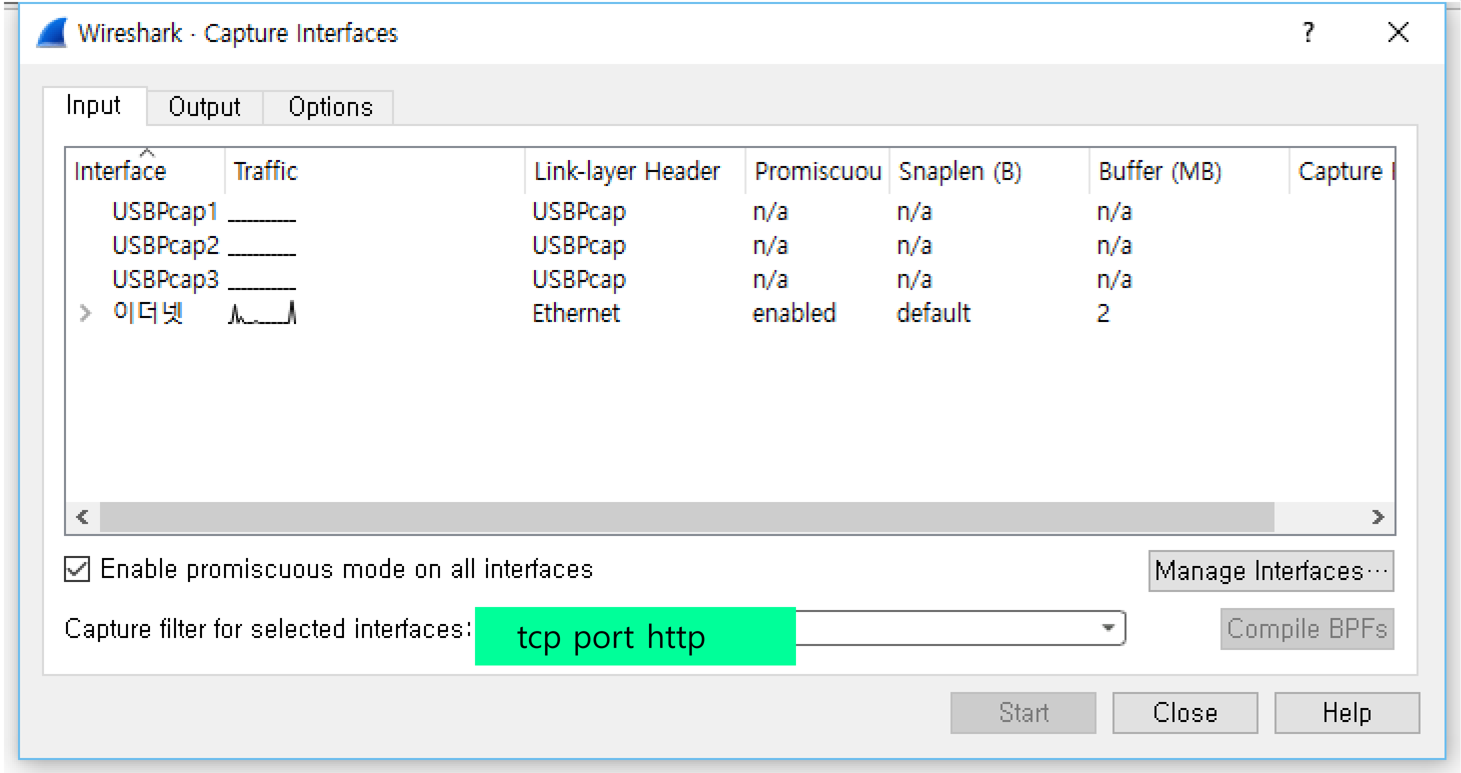
Frame (179 bytes)
Reassembled TCP (2624734 bytes)
Text item (text), 17 bytes
Packets: 14509 · Displayed: 14509 (100.0%)
Profile: Default

Capture Options



You are running Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0). You receive automatic updates.

Capture Option



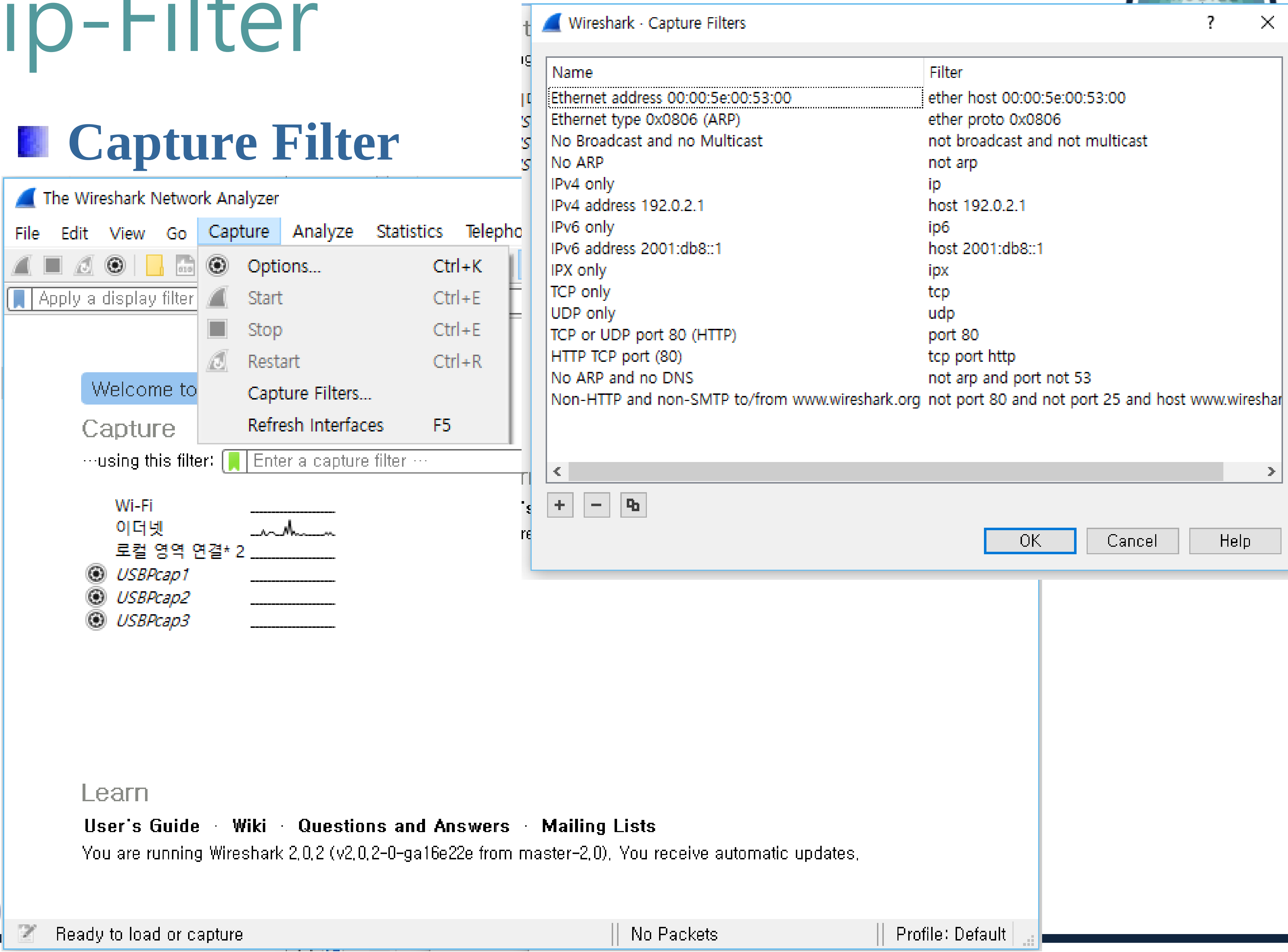
Interface	Traffic	Link-layer Header	Promiscuou	Snaplen (B)	Buffer (MB)	Capture I
USBPcap1		USBPcap	n/a	n/a	n/a	
USBPcap2		USBPcap	n/a	n/a	n/a	
USBPcap3		USBPcap	n/a	n/a	n/a	
› 이더넷		Ethernet	enabled	default	2	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: tcp port http

Tip-Filter

Capture Filter



You are running Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0). You receive automatic updates.

Name	Filter
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
IPX only	ipx
TCP only	tcp
UDP only	udp
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshar

MOBILE PLANET

Platform, networks & service Lab