



RUTGERS
UNIVERSITY | NEW BRUNSWICK

CS352: Internet Technology Summer 2019

Murtadha Aldeer

Wireshark Packet Sniffing Project

Protocol Analysis with Wireshark

Outline

- 1 Motivation and overview
- 2 Wireshark installation and use
- 3 Protocol analysis examples
- 4 Getting started

- Wireshark is a *network protocol analyzer*
 - captures network packets
 - displays packet data in details
 - www.wireshark.org
- First released in 1998 by Gerald Combs as Ethereal
 - many contributors around the world
- Open source and free software
- Graphical alternative to tcpdump

Motivation and Overview

Purpose

- Powerful tool for
 - troubleshooting network problems
 - examining security problems
 - debugging protocol implementations
 - learning network protocol internals
- Used in industry and academia

Wireshark Installation

Highlights

- Wireshark can be installed on various platforms
 - UNIX, MS, Linux, Mac OS, etc.
- Most recent release is v.3.0.2

Wireshark Installation

Overview

- Installation of Wireshark requires
 - downloading the relevant package
 - building the source into binary if the source is downloaded
 - install binaries to their destinations
 - detailed installation instructions found here
http://www.wireshark.org/docs/wsug_html/
- **Windows** installation includes Npcap
 - packet capture library
 - In case you were not able to see http packet given that you are connected to the network wirelessly using a laptop that runs Window 10, then you may need to install Npcap 0.996 (<https://nmap.org/npcap/#download>)
- Installation easy and intuitive

Wireshark Usage

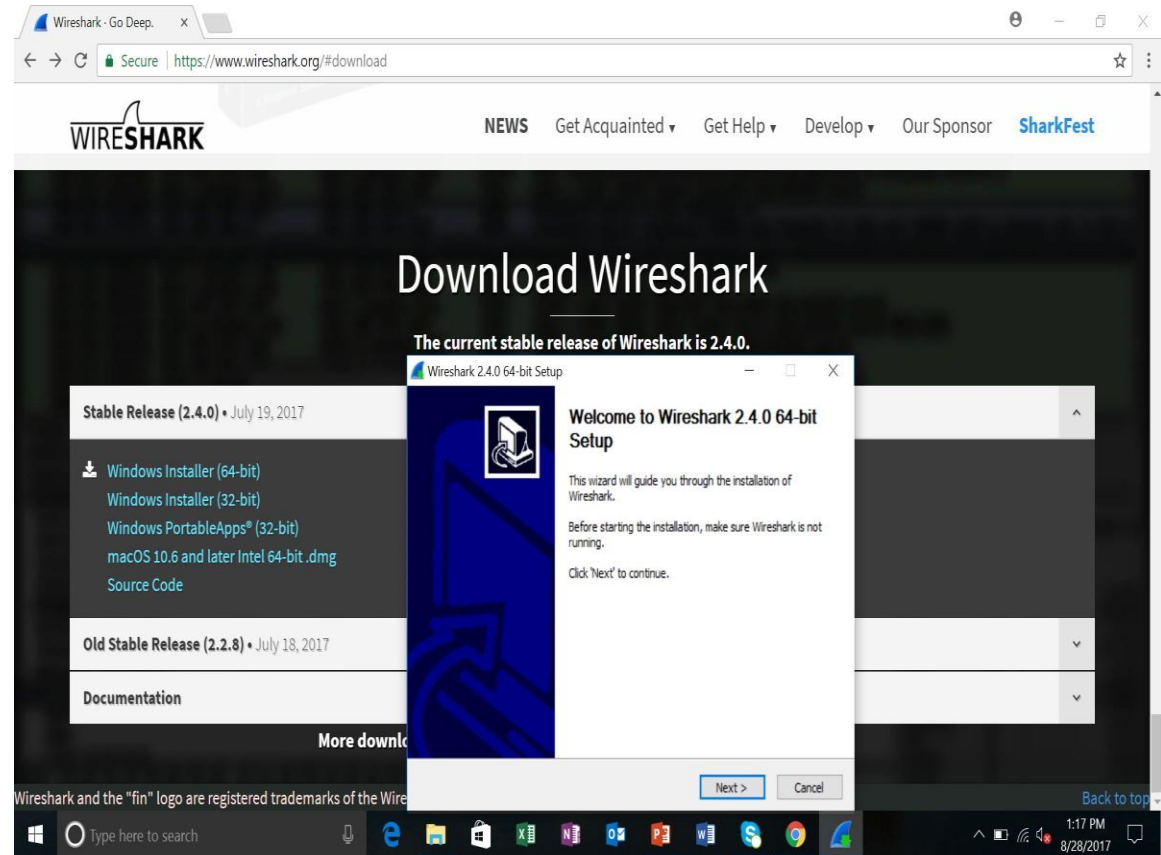
Windows 10 Installation₁

Go to
wireshark.org

Click on
Download
Wireshark

Save and run the
executable
.exe file

Installation
wizard is
intuitive



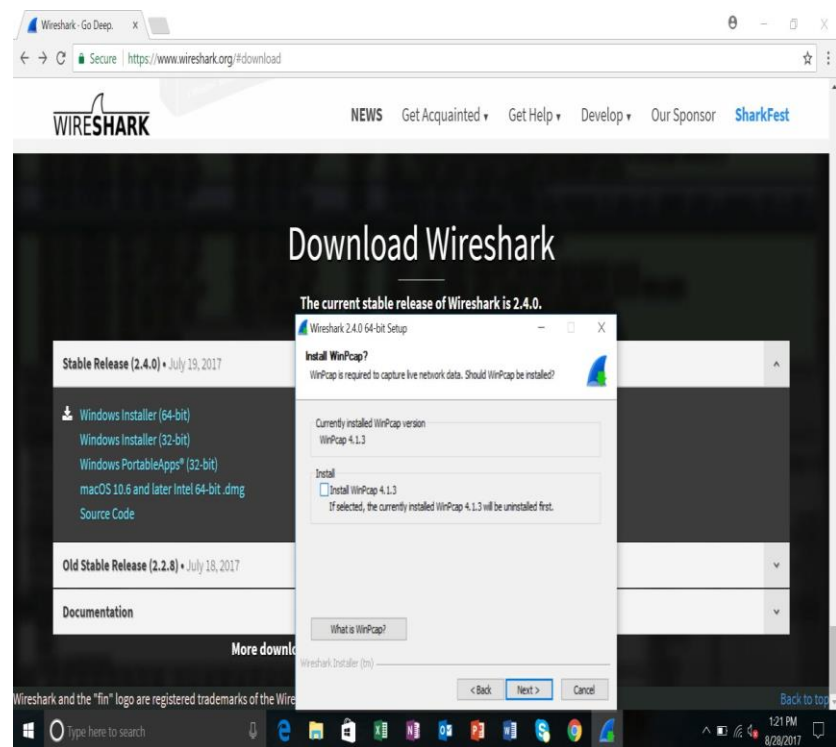
Wireshark Usage

Windows 10 Installation₂

pcap library is required to capture low-level network messages

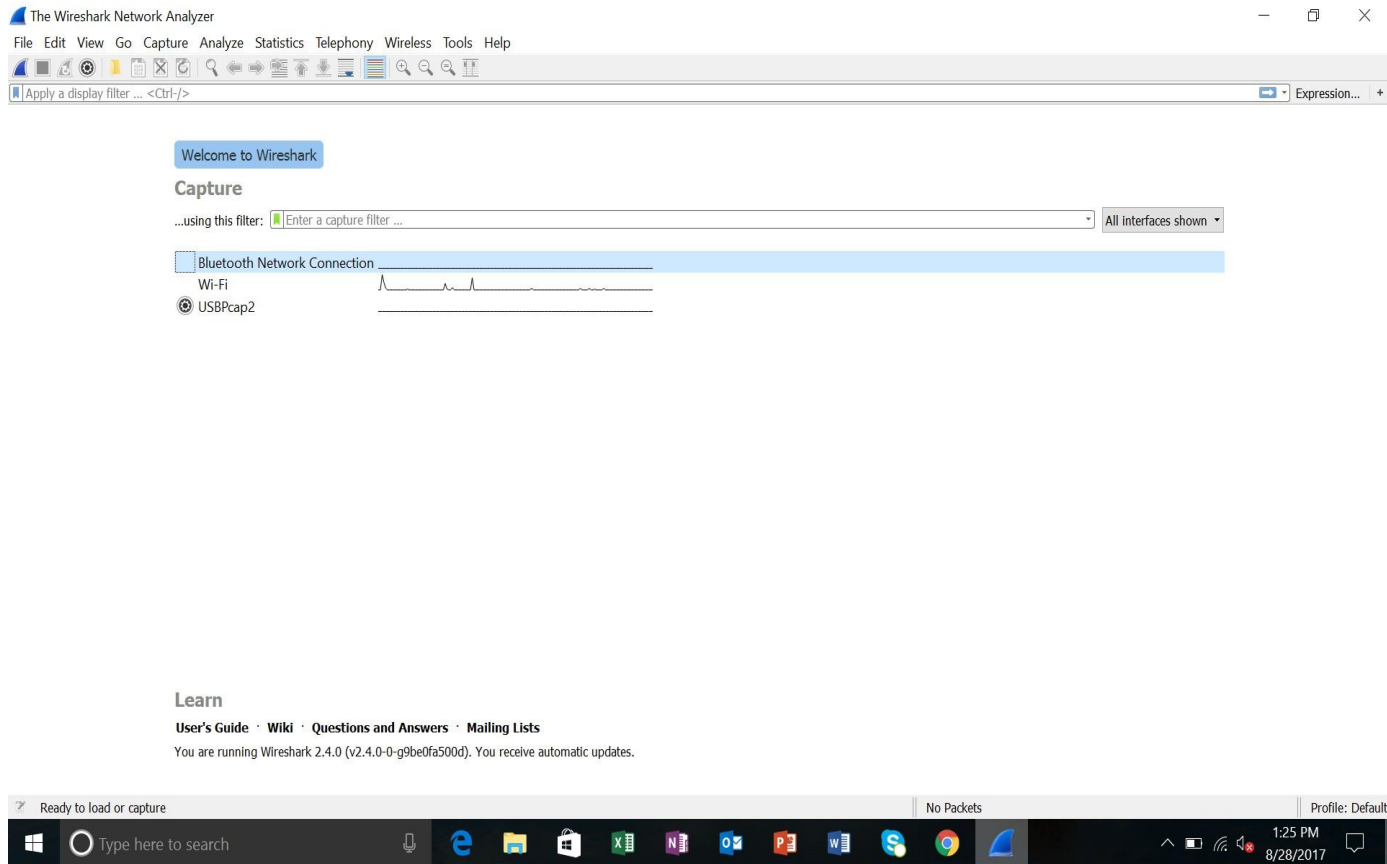
Npcap for windows
(comes with Windows 10 but may need upgrade)
libpcap for UNIX/Linux

PS: During installation, you will need to enable
"Support raw 802.11 traffic
(and monitor mode) for wireless adapters"



Wireshark Installation

Windows 10 Installation₃



Wireshark Usage

Main Features

- Capture live traffic
 - data can be captured on wired or wireless medium
 - numerous protocols can be captured and analyzed
- Display packet in details
- Filtering is essential when dealing with lots of packets
 - filters can be applied on protocols, fields, values, etc.
 - filtering while capturing packets is possible

Wireshark GUI

Main Window

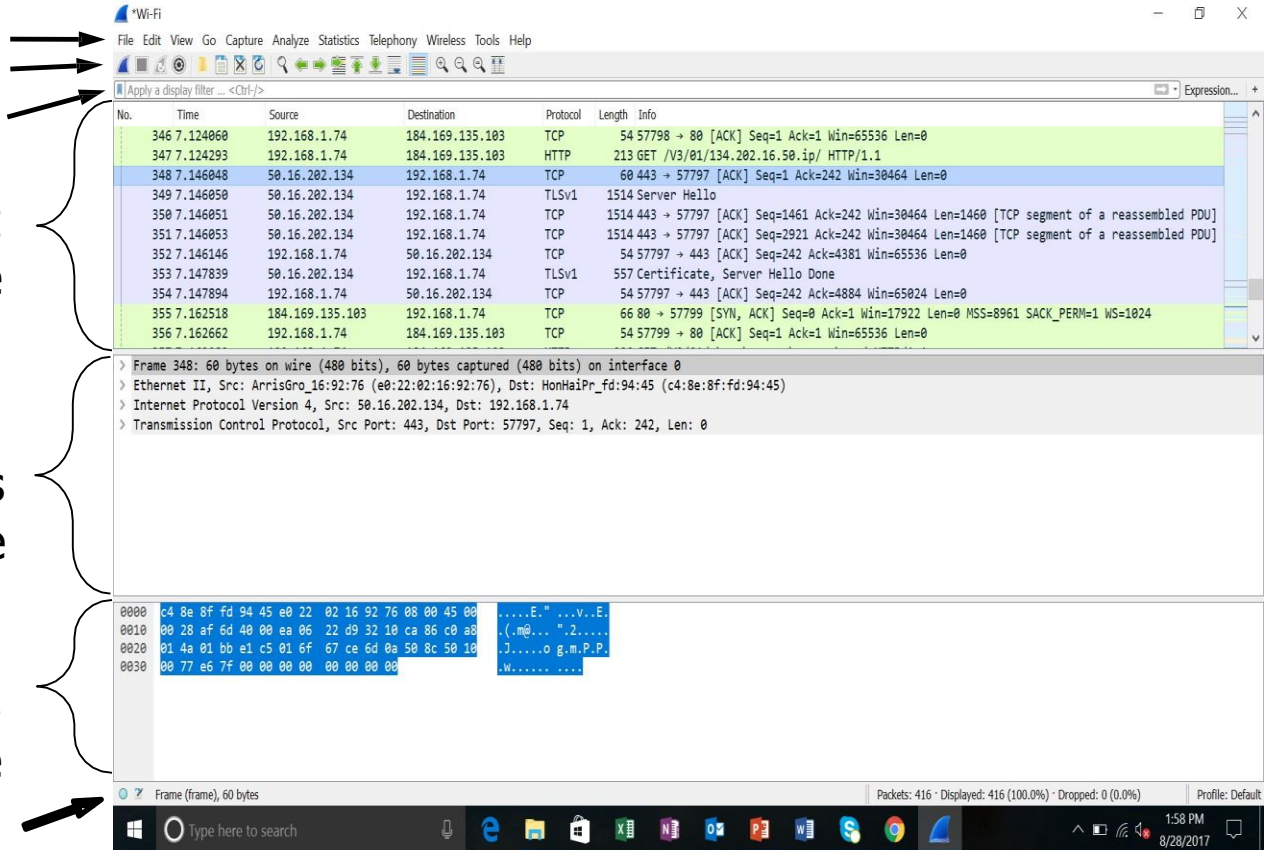
menu
main toolbar
filter field

packet list
pane

packet details
pane

packet bytes
pane

status bar



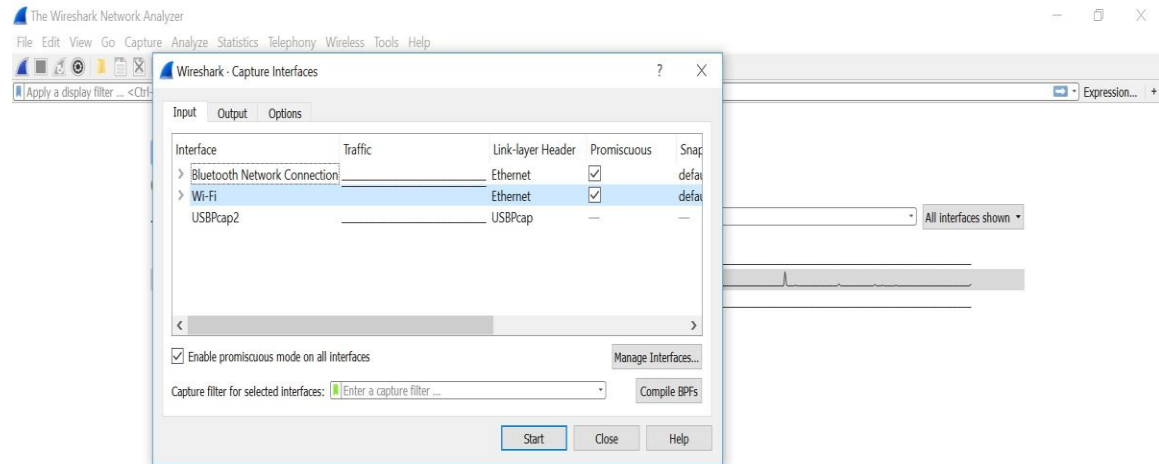
Wireshark Usage

Starting Capture

To capture:
go to Capture
menu and
select
Options...

Start
capturing on
interface that
has IP address

Other ways of
capturing
possible



Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

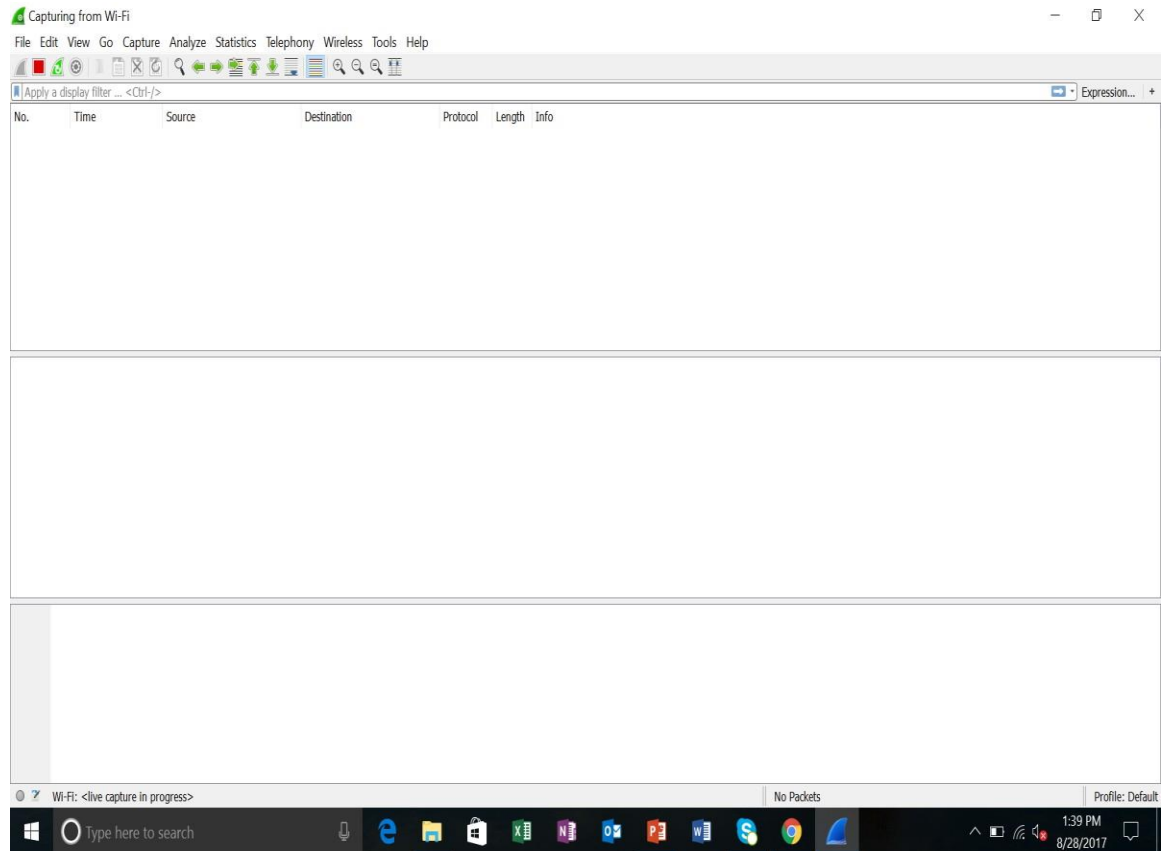
You are running Wireshark 2.4.0 (v2.4.0-0-g9be0fa500d). You receive automatic updates.



Wireshark Usage

Capturing₁

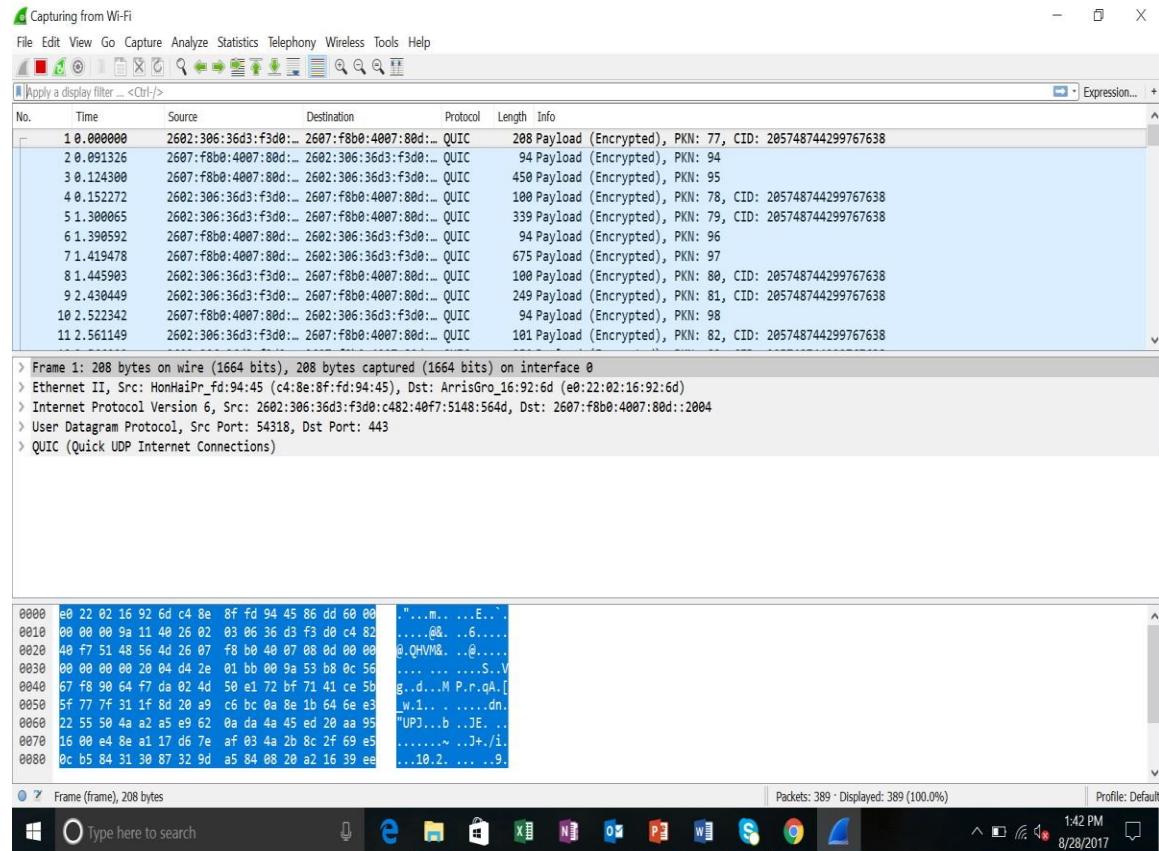
Once the capturing starts, main window will be blank until the data is exchanged on network interface (NIC)



Wireshark Usage

Capturing₂

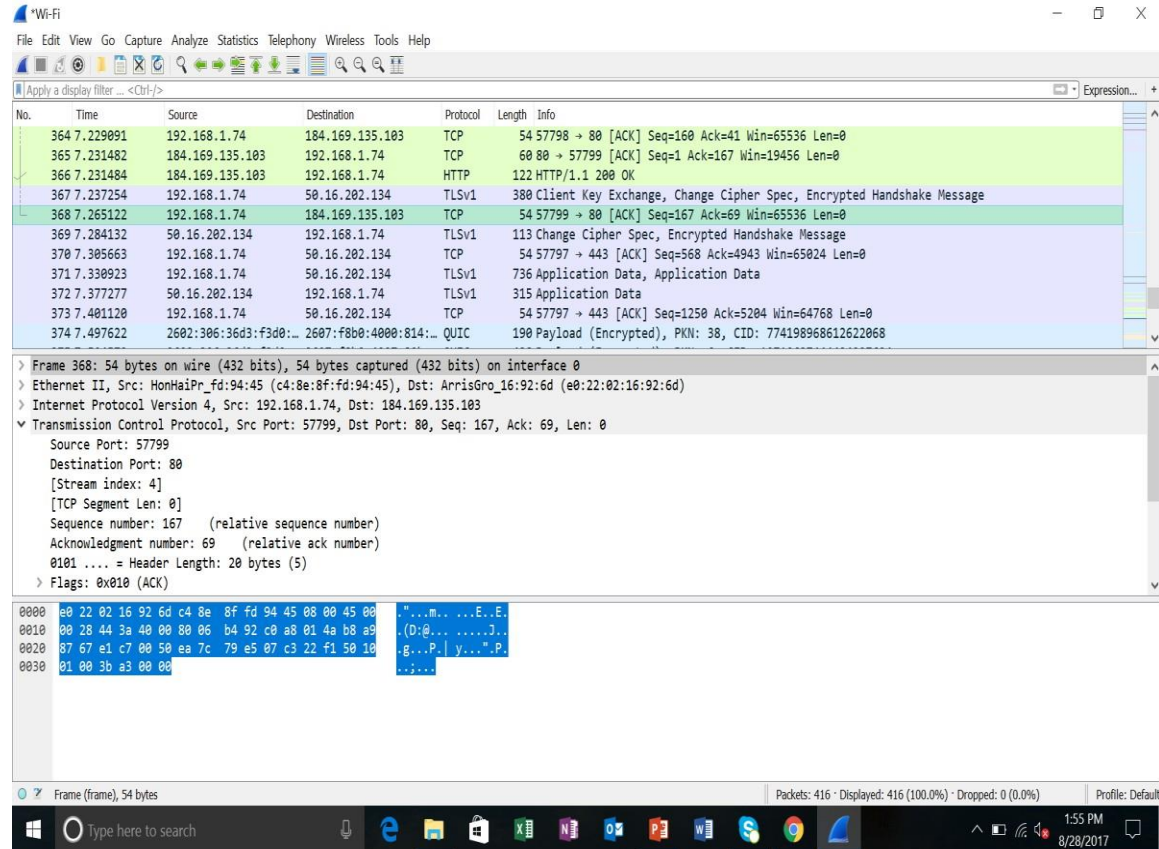
When packets exchanged on NIC, the packets will be dumped to main window



Wireshark Usage

Stopping Capture

Capturing can be stopped by clicking on Stop the running capture button on the main toolbar



Wireshark Usage

Filtering

Filter by entering the protocol or field name in Apply a display filter and enter

Detailed filters can be applied by creating expressions

The image shows the Wireshark network protocol analyzer 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. The main display area is divided into three panes. The top pane shows a list of captured packets, with the filter 'http' applied in the filter bar. The middle pane shows the details of the selected packet (No. 347), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates 'Frame (frame), 213 bytes' and 'Packets: 416 · Displayed: 4 (1.0%) · Dropped: 0 (0.0%)'.

No.	Time	Source	Destination	Protocol	Length	Info
347	7.124293	192.168.1.74	184.169.135.103	HTTP	213	GET /V3/01/134.202.16.50.ip/ HTTP/1.1
357	7.163089	192.168.1.74	184.169.135.103	HTTP	220	GET /V3/01/rhr.pbyyrg-bcarg.pbz.m/ HTTP/1.1
360	7.193125	184.169.135.103	192.168.1.74	HTTP	94	HTTP/1.1 200 OK
366	7.231484	184.169.135.103	192.168.1.74	HTTP	122	HTTP/1.1 200 OK

Frame 347: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface 0
> Ethernet II, Src: HonHaiPr_94:45 (c4:8e:8f:fd:94:45), Dst: ArrisGro_16:92:6d (e0:22:02:16:92:6d)
> Internet Protocol Version 4, Src: 192.168.1.74, Dst: 184.169.135.103
> Transmission Control Protocol, Src Port: 57798, Dst Port: 80, Seq: 1, Ack: 1, Len: 159
v Hypertext Transfer Protocol
GET /V3/01/134.202.16.50.ip/ HTTP/1.1\r\nCache-Control: no-cache\r\nConnection: Keep-Alive\r\nPragma: no-cache\r\nUser-Agent: SXL/3.1\r\nHost: http.00.s.sophosx1.net\r\n\r\n

0000 00 22 02 16 92 6d c4 8e 8f fd 94 45 08 00 45 00 ...m...E.E.
0010 00 c7 44 36 40 00 00 06 b3 f7 c0 a8 01 4a b8 a9 ...D6@...J...
0020 87 67 e1 c6 00 50 24 9b 85 15 91 de 92 88 50 18 ...g...PS...P...
0030 01 00 b3 58 00 00 47 45 54 20 2f 56 33 2f 30 31 ...X..GE T /V3/01
0040 2f 31 33 34 2e 32 30 32 2e 31 36 2e 35 30 2e 69 /134.202.16.50.i
0050 70 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 43 61 63 p/ HTTP/ 1.1...Cac
0060 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 he-Contr ol: no-c
0070 61 63 68 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e ache..Co nnection
0080 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 50 72 : Keep-A live..Pr

Protocol Analysis with Wireshark

Protocol Analysis

- Packets and protocols can be analysed after capture
- Individual fields in protocols can be easily seen
- Graphs and flow diagrams can be helpful in analysis

Protocol Analysis and Examples

Packet Details Pane

Analysis is performed manually

Example shows TCP segment with SYN and ACK fields set to 1

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The packet list pane shows three packets. The selected packet is packet 356, a TCP segment from 192.168.1.74 to 184.169.135.103, sequence 54 57799, length 80. The packet details pane shows the following information:

- Transmission Control Protocol, Src Port: 80, Dst Port: 57799, Seq: 0, Ack: 1, Len: 0
- Source Port: 80
- Destination Port: 57799
- [Stream index: 4]
- [TCP Segment Len: 0]
- Sequence number: 0 (relative sequence number)
- Acknowledgment number: 1 (relative ack number)
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x012 (SYN, ACK)
- 000. = Reserved: Not set
- ...0 = Nonce: Not set
- 0... = Congestion Window Reduced (CWR): Not set
- 0... = ECN-Echo: Not set
- 0... = Urgent: Not set
- 1... = Acknowledgment: Set
- 0... = Push: Not set
- 0... = Reset: Not set
- 1... = Syn: Set
- 0... = Fin: Not set
- [TCP Flags:A..S.]
- Window size value: 17922
- [Calculated window size: 17922]
- Checksum: 0x9968 [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
- > [SEQ/ACK analysis]

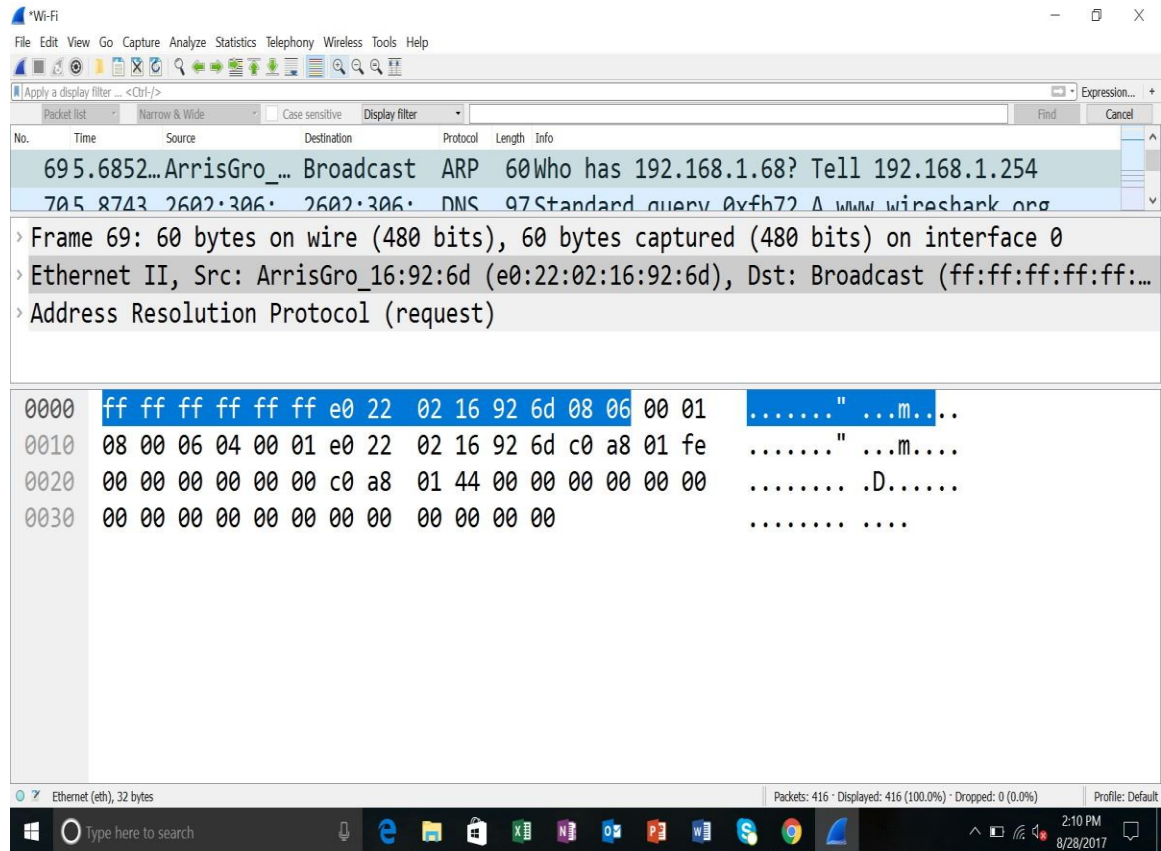
The packet bytes pane shows the raw data of the packet, with the first 12 bytes highlighted in blue, corresponding to the TCP header. The status bar at the bottom indicates 'Packets: 416 · Displayed: 416 (100.0%) · Dropped: 0 (0.0%)' and 'Profile: Default'.

Protocol Analysis and Examples

Packet Byte Pane

Zoom in or out is possible in main toolbar

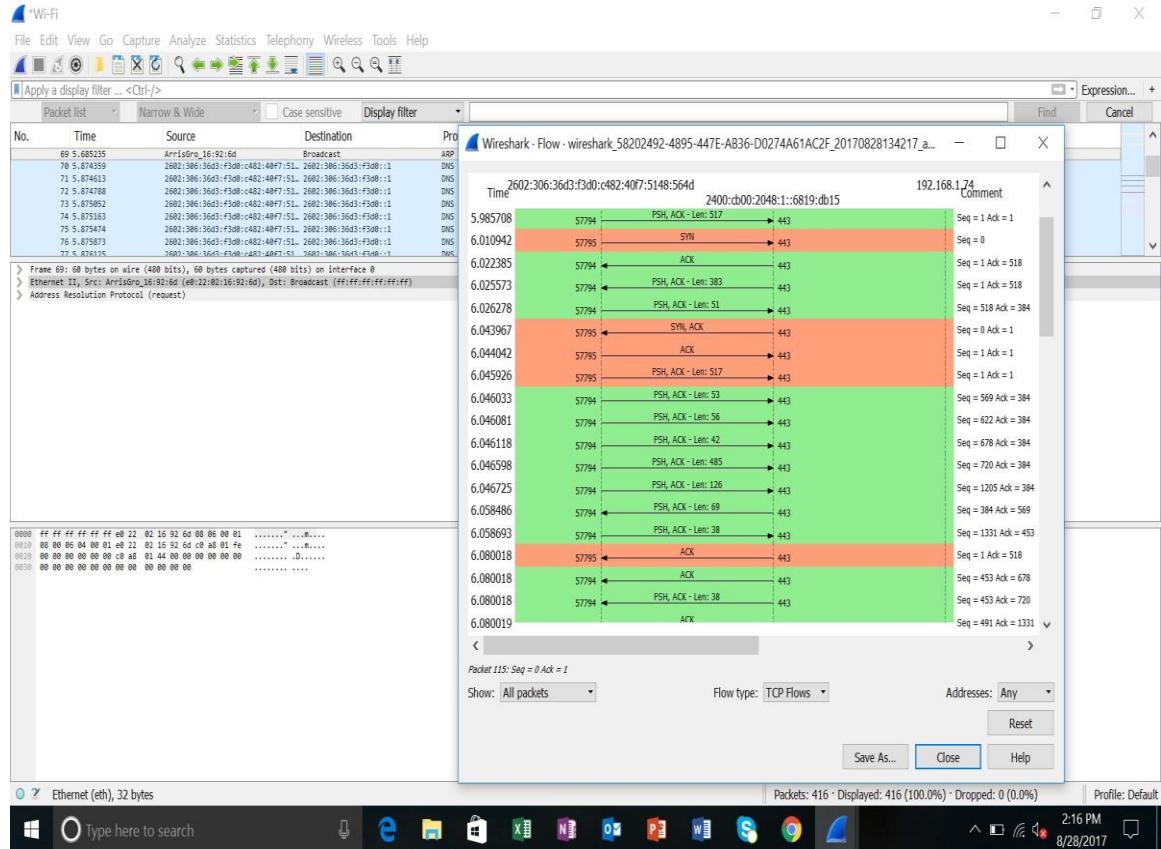
Packet Byte pane consists of offset, Hex, and ASCII fields



Protocol Analysis and Examples

Statistics – Flow Graph Example

TCP plots and
flow graphs
are available
in
Statistics
menu



Getting Started

Installation

- Install Wireshark and familiarise
- Download first Getting Started v7.0 exercise
<http://www-net.cs.umass.edu/wireshark-labs/>

Protocol Analysis with Wireshark

Acknowledgements

Some material in these slides comes from:

- Kurose & Ross,
Computer Networking: A Top-Down Approach, 7th ed.
- Wireshark
<https://www.wireshark.org/>
- WinPcap
<https://nmap.org/npcap/#download>