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

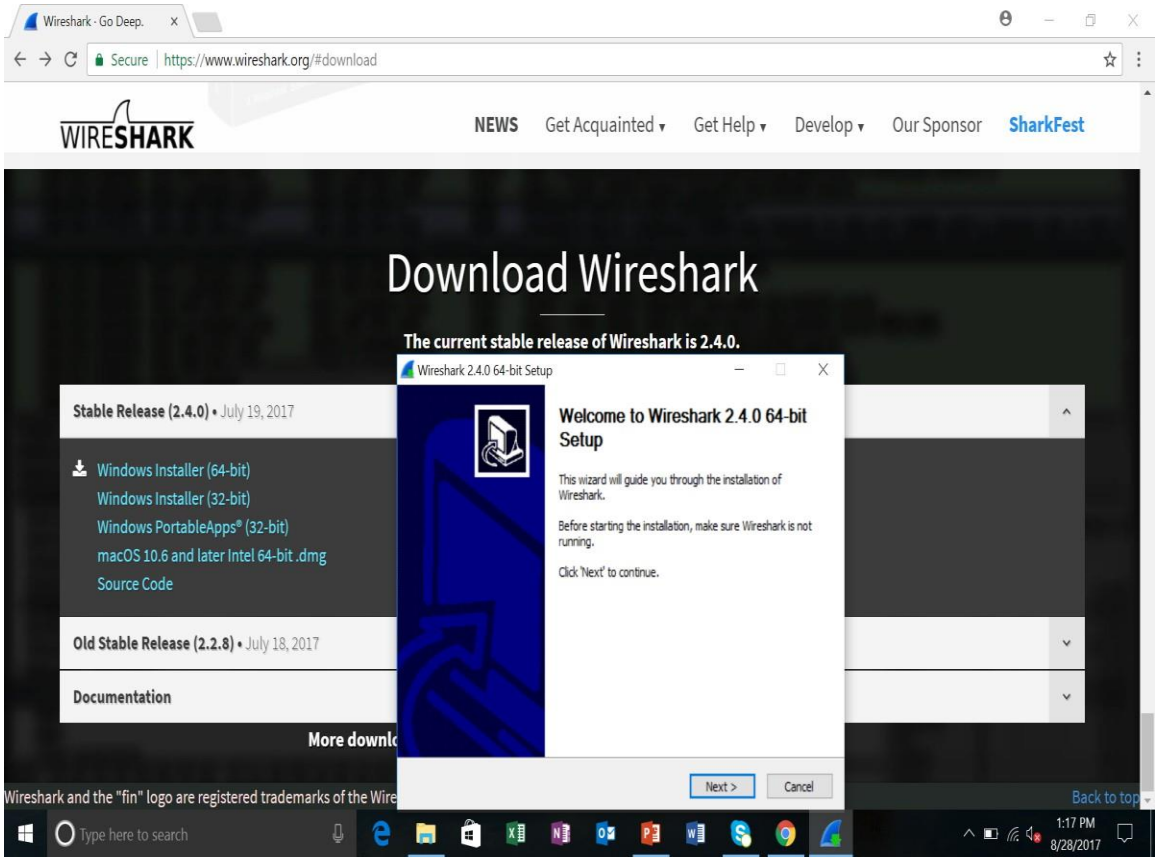
Wireshark Usage
Windows 10 Installation$_1$

Go to wireshark.org

Click on *Download Wireshark*

Save and run the executable `.exe` file

Installation wizard is intuitive

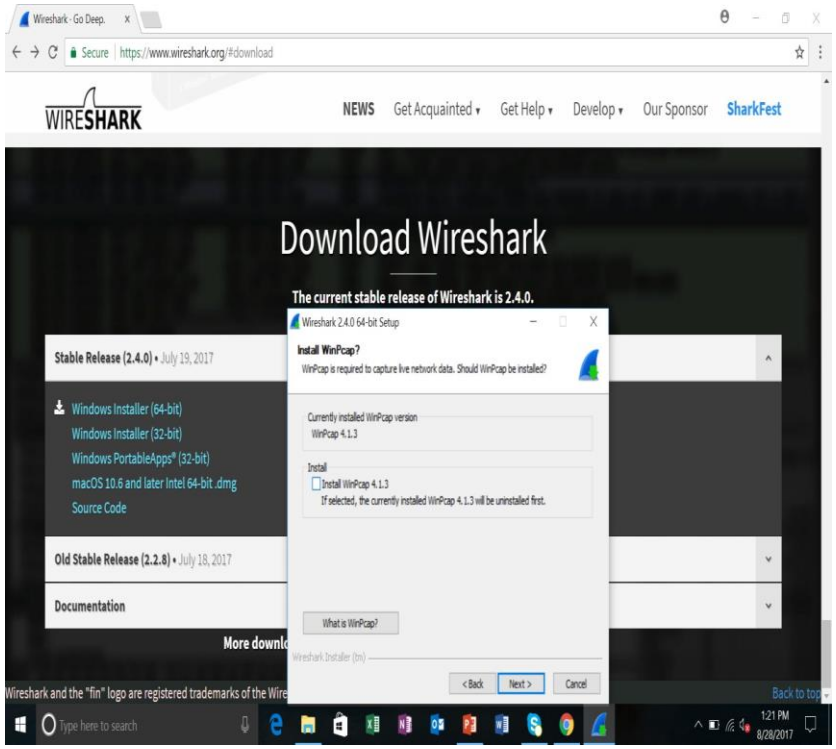


Wireshark Usage
Windows 10 Installation$_2$

pcap library is required to capture low- level network messages

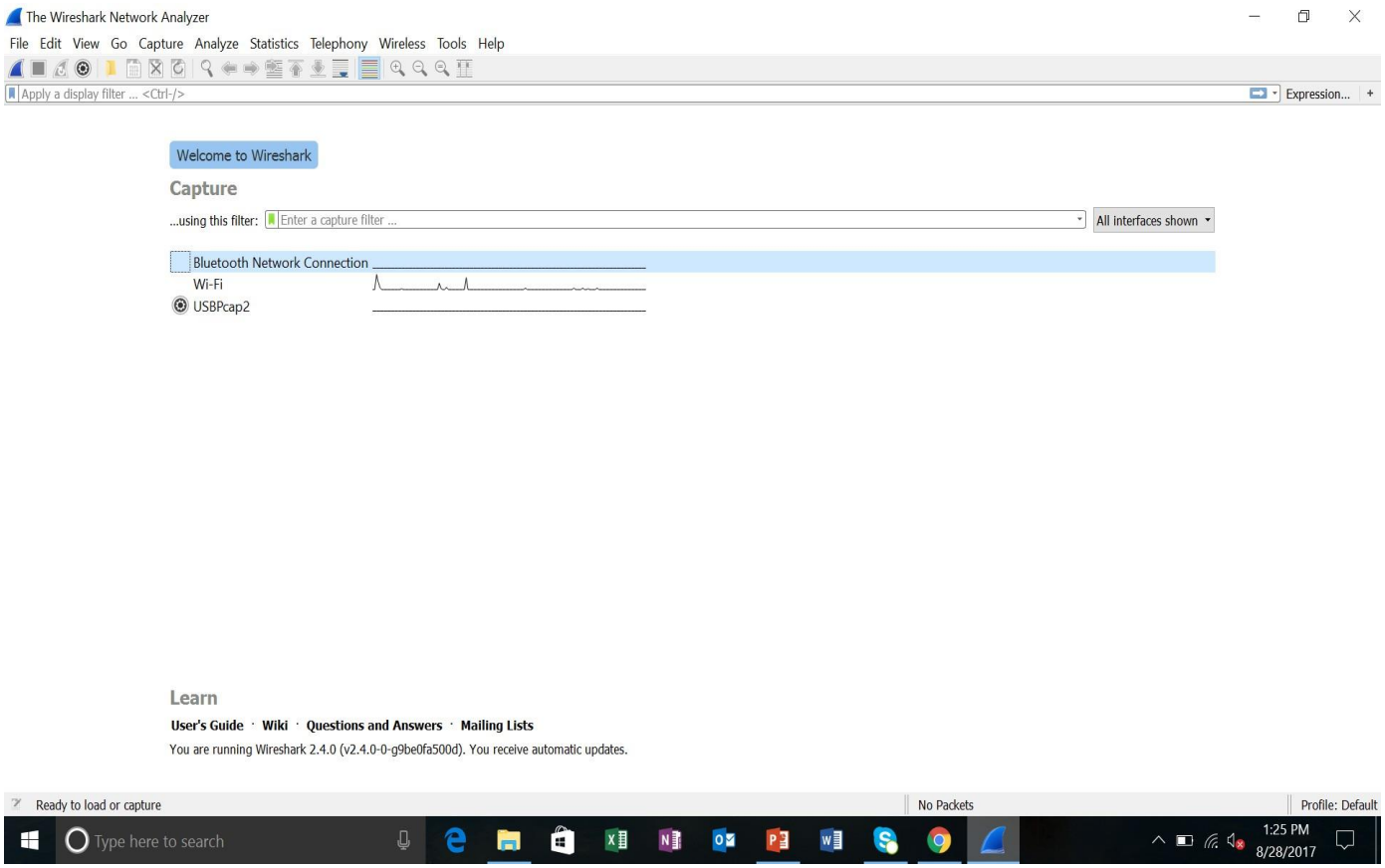
Npcap for windows
(comes with Windows 10 but may need upgarde)
`libpcap` for UNIX/Linux

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



Wireshark Installation

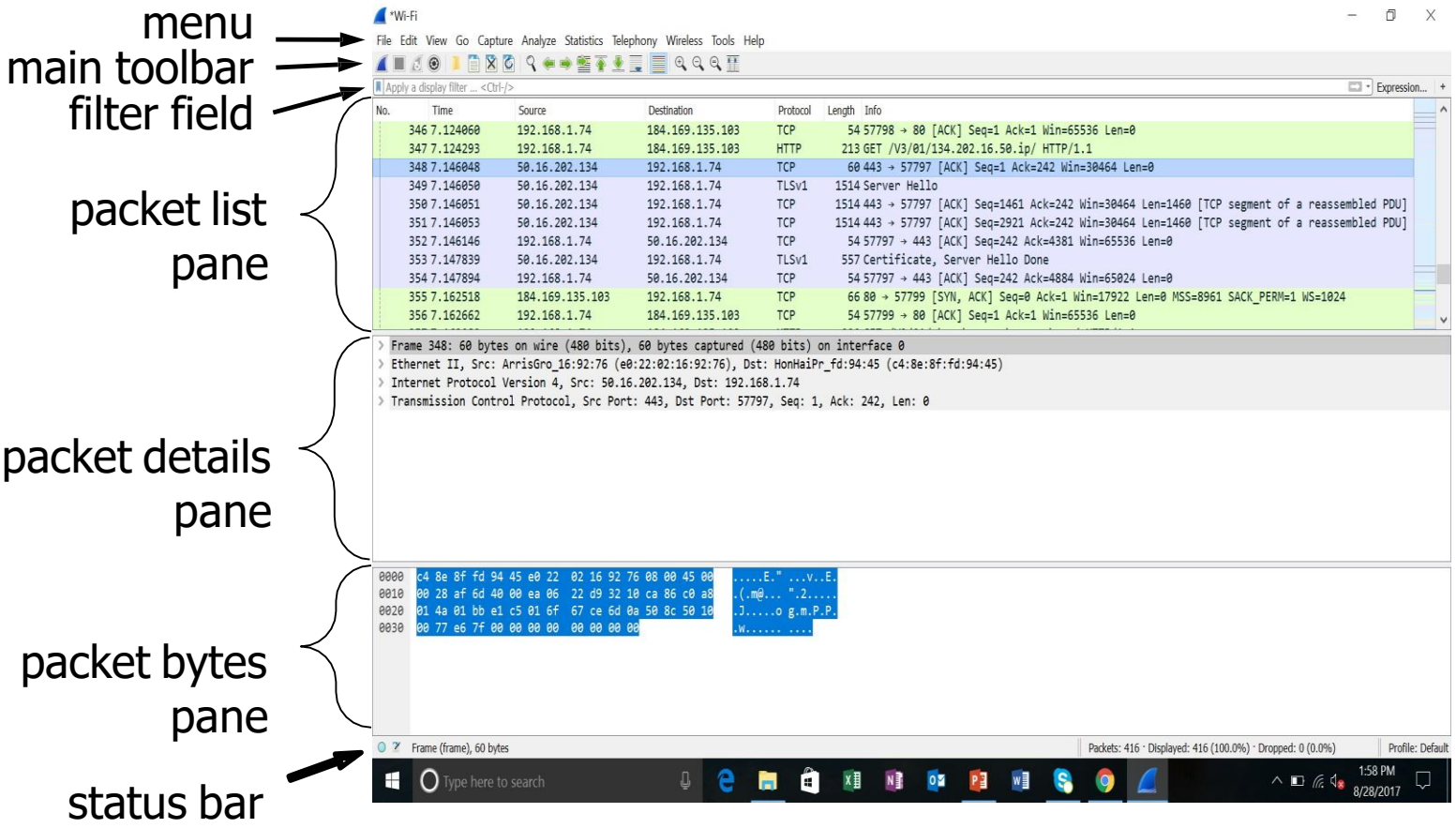
Windows 10 Installation$_3$



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

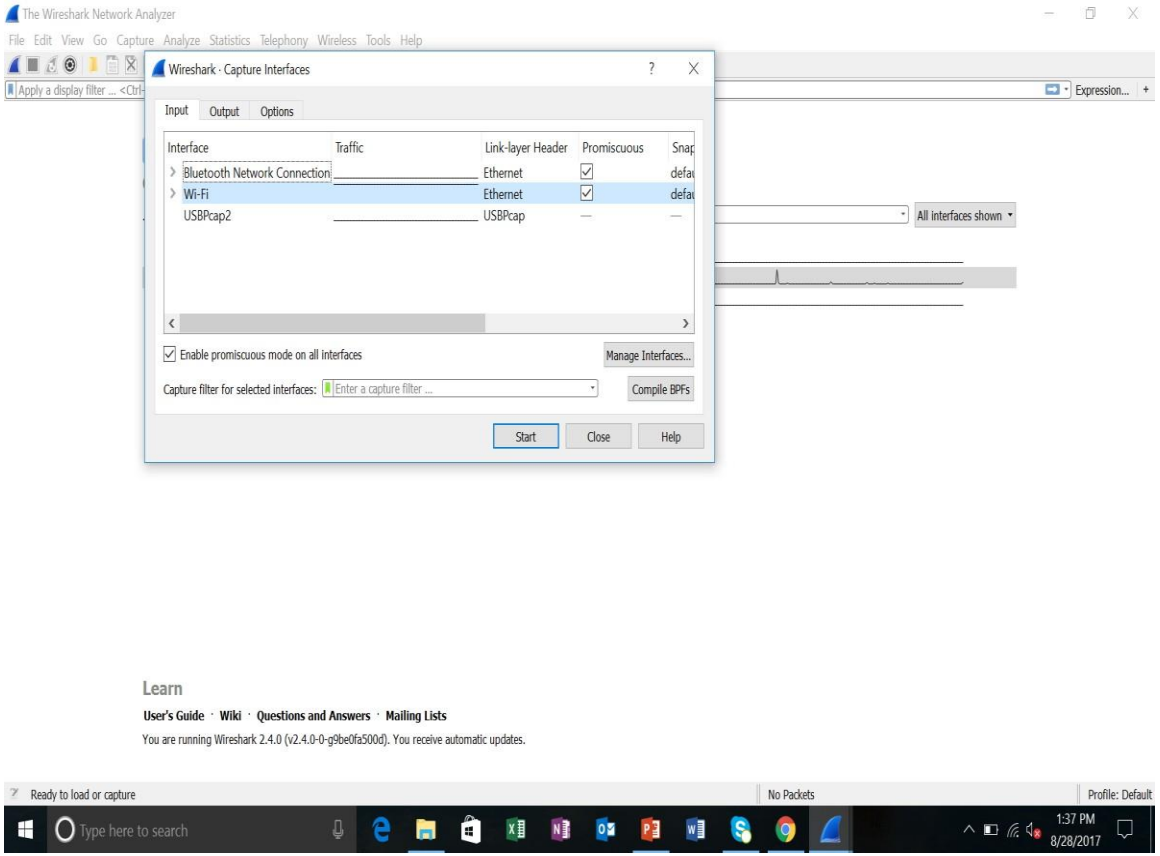


Wireshark Usage
Starting Capture

To capture: go to Capture menu and select Options…

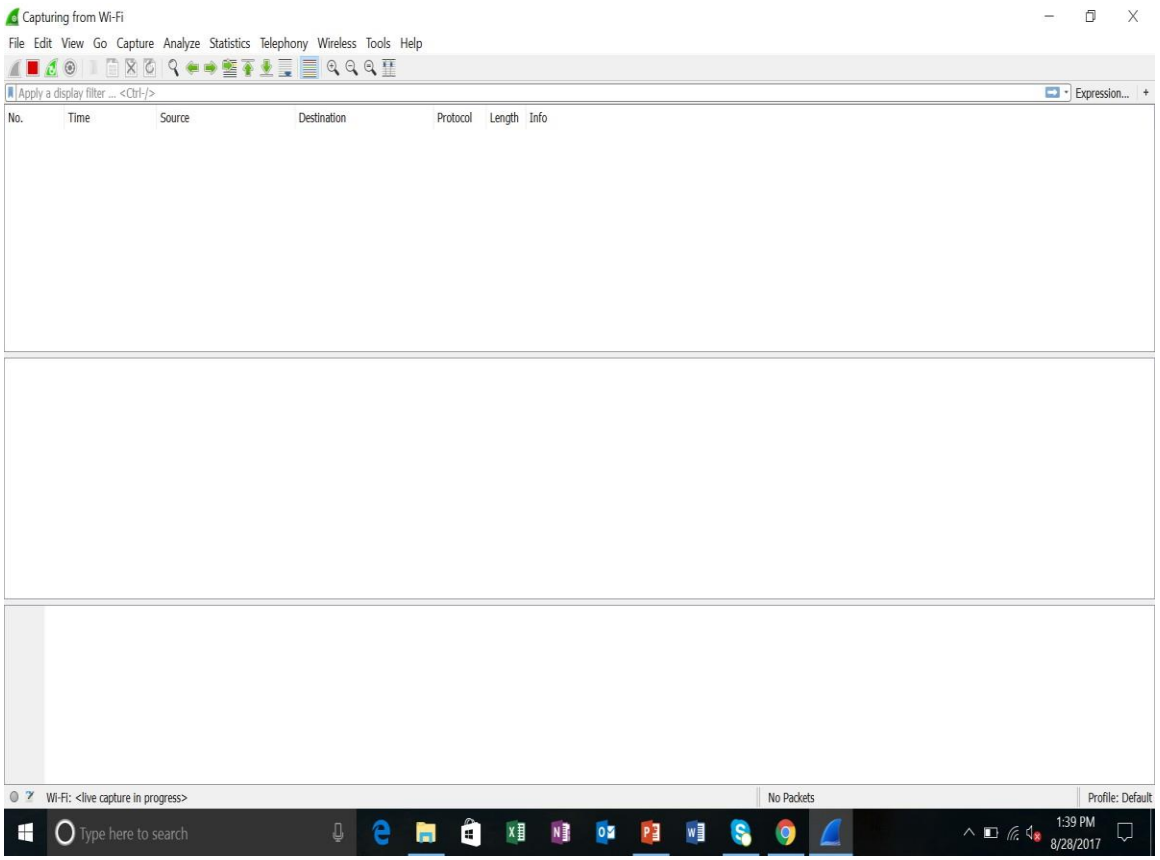
Start capturing on interface that has IP address

Other ways of capturing possible



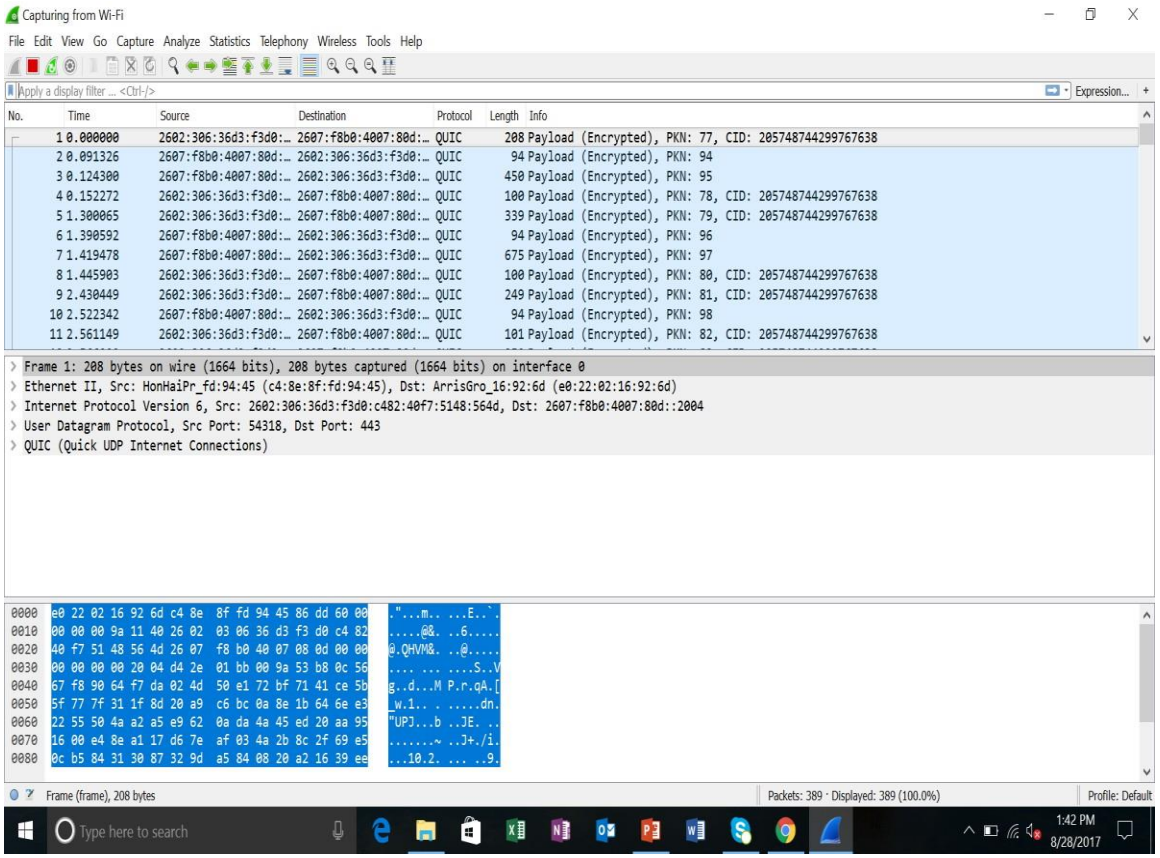
Wireshark Usage
Capturing$_1$

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



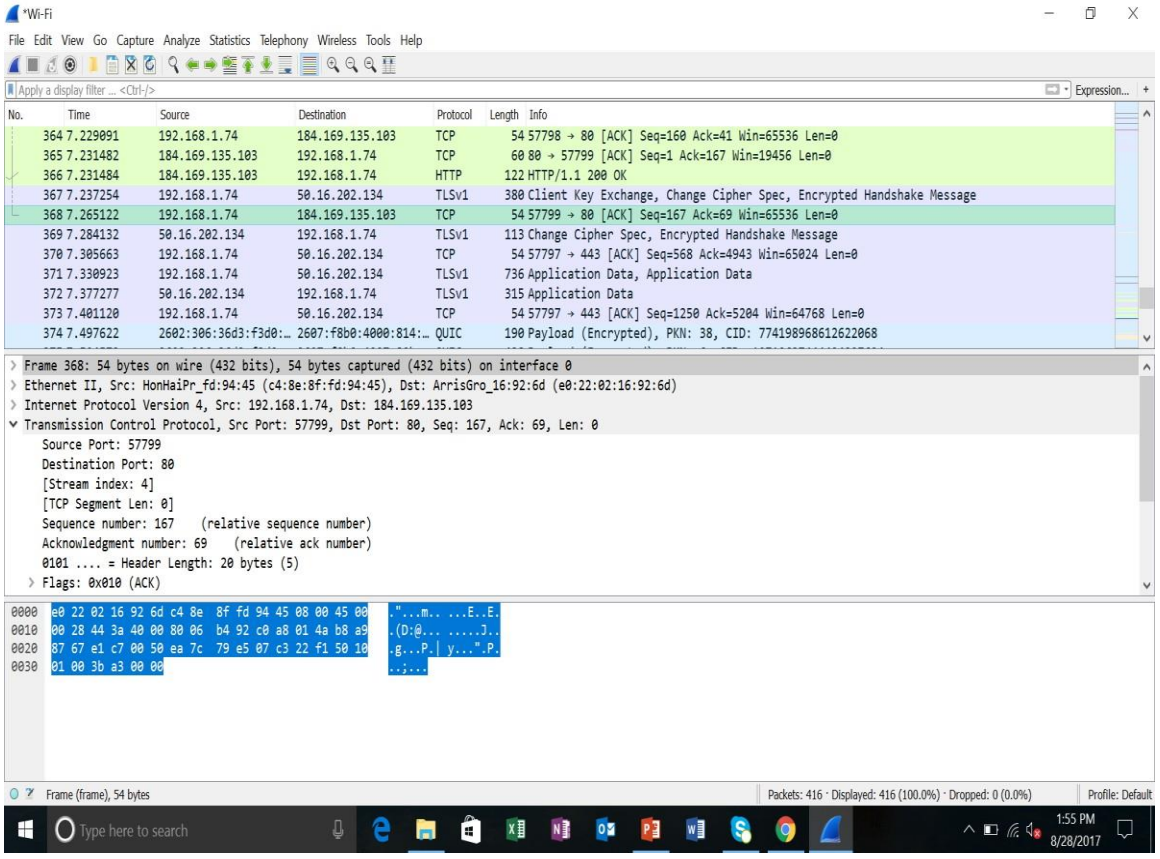
Wireshark Usage
Capturing$_2$

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



Wireshark Usage
Stopping Capture

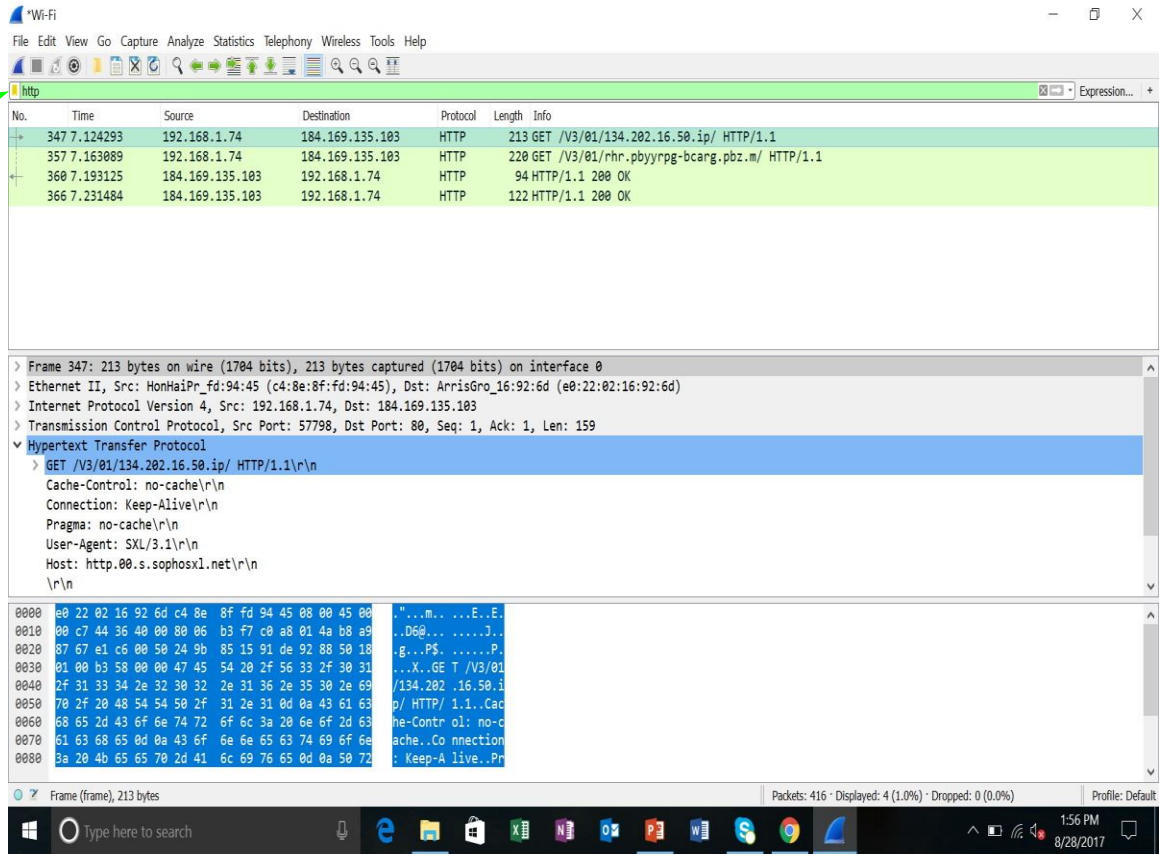
Capturing can be stopped by clicking on Stop the running capture button on the main toolbar



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



Protocol Analysis with Wireshark

Protocol Analysis

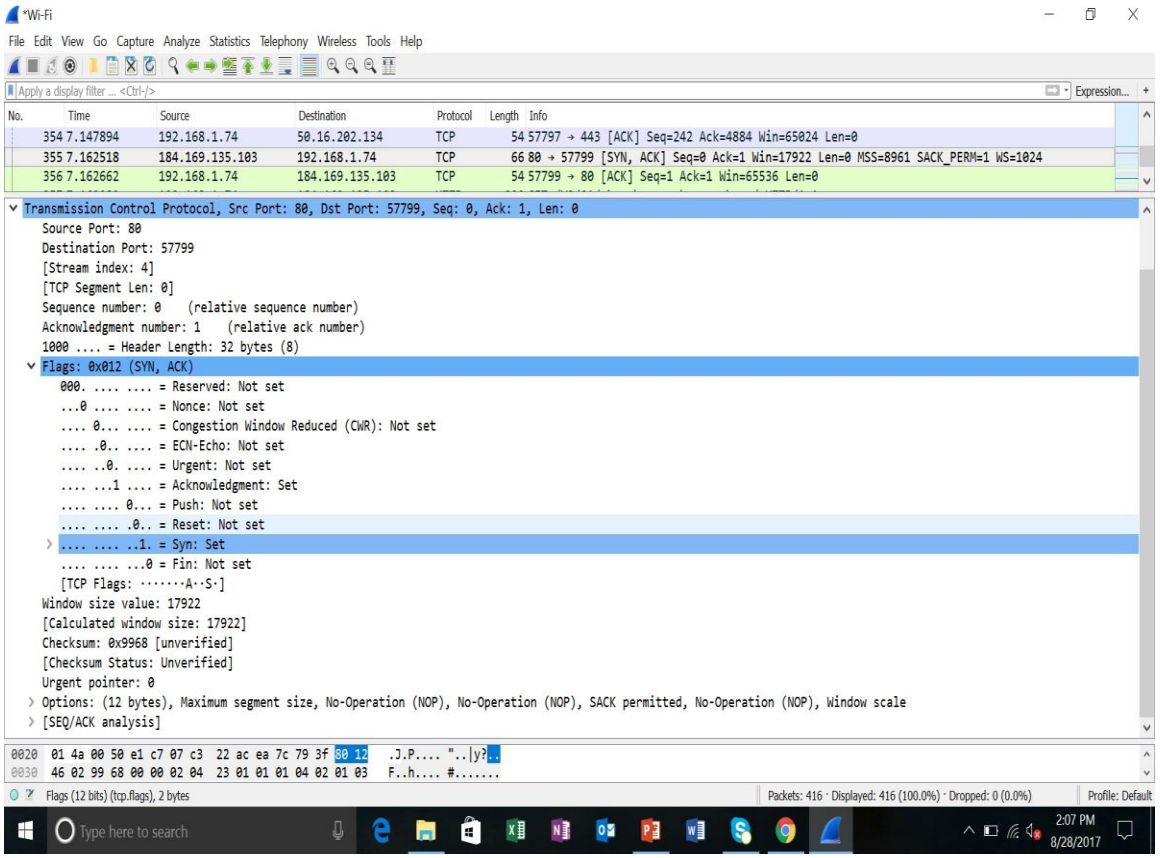
- Packets and protocols can be analysed after capture
- Individual fields in protocols can be easily seen
- Graphs and flow diagrams can be helpful in analysis

Protocol Analysis and Examples

Packet Details Pane

Analysis is performed manually

Example shows TCP segment with SYNand ACK fields set to 1

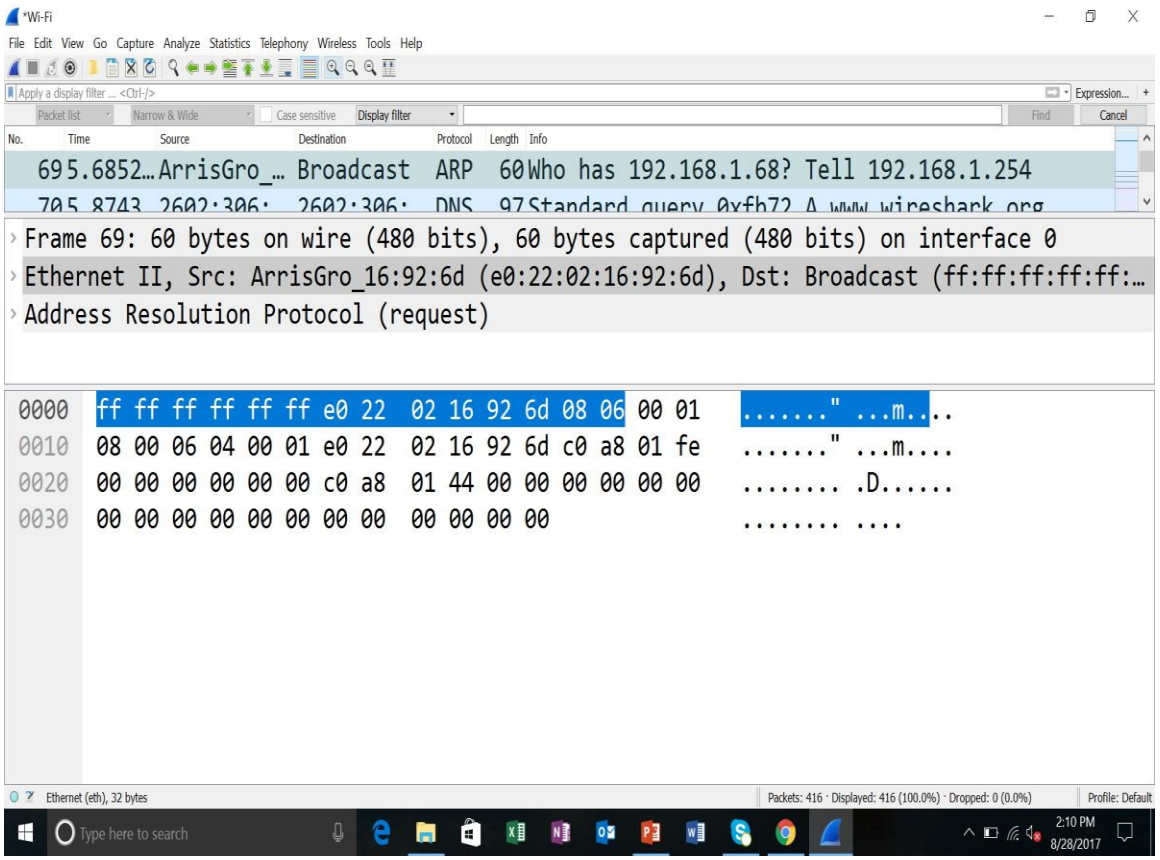


Protocol Analysis and Examples

Packet Byte Pane

Zoom in or out is possible in main toolbar

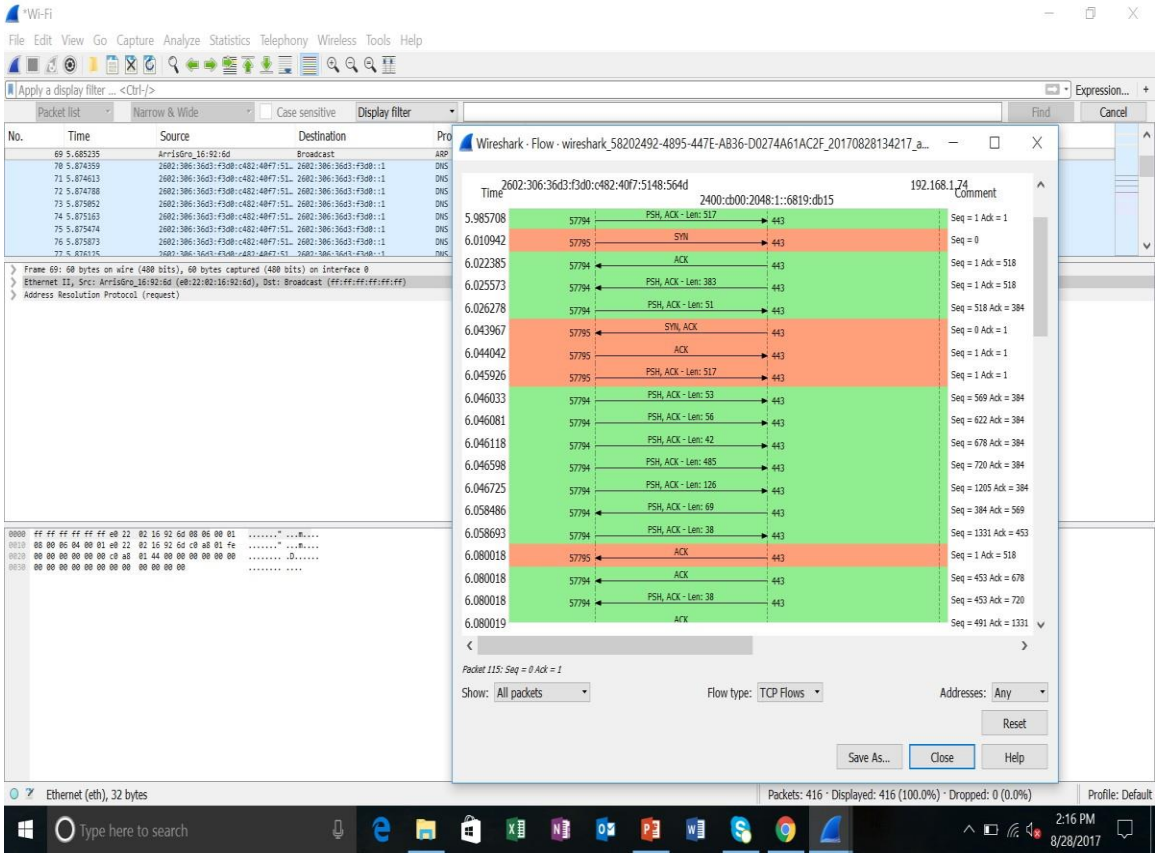
Packet Byte pane consists of offset, Hex, and ASCII fields



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