MAWLANA BHASHANI SCIENCE AND TECHNOLOGY UNIVERSITY



DEPARTMENT OF ICT

Lab Report No: 02

Course Code : ICT-3208

Course Title : Network Planning and Designing Lab

Lab Report Name: Wireshark Lab

Submitted by
Md. Faruk Hosen

Submitted to
Nazrul Islam

ID: IT-17035 Assistant Professor,

Session: 2016-2017 Department of ICT, MBSTU

Year: 3rd Semester: 2nd Santosh, Tangail-1902

Date of Submission: 15 July 2020

Objective

- : 1. Wireshark basic and it's features.
 - 2. How to work with wireshark.
 - 3. Protocol Analysis with wireshark

Wireshark Lab

1. What is Wireshark? Why we use wireshark?

Ans: Wireshark:

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

Why use wireshark: We use wireshark because -

Wireshark is a powerful tool for -

- i. Troubleshooting network problems
- ii. examining security problems
- iii. debugging protocol implementations
- iv. learning network protocols internals.

2. What are the main features of wireshark?

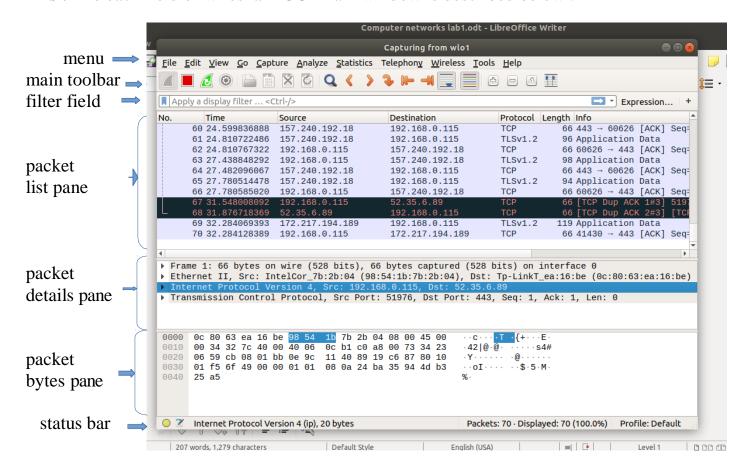
Ans: The main features of wireshark is:

- i. Capture live traffic
 - -data can be captured on wired or wireless medium.
 - -numerous protocols can be captured and analyzed.

- ii. Display packet in details
- iii. Open files containing packet data captured.
 - -from other programs(tcpdump/winDump).
- iv. Filtering is essential when dealing with lots of packets.
 - -filters can be applied on protocols, fields, values etc.
 - -filtering while capturing packets is possible.

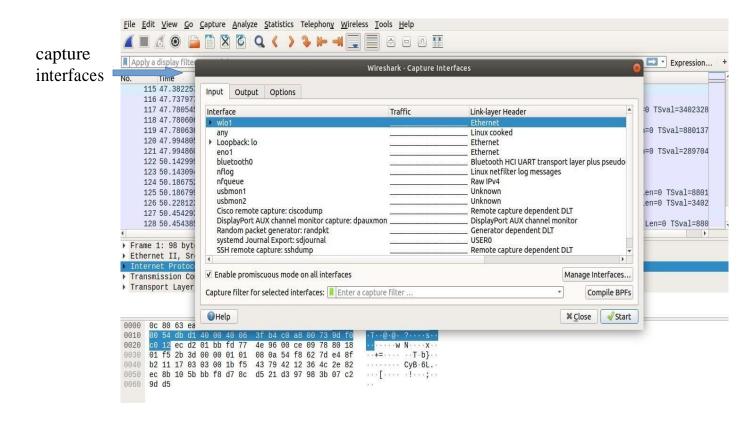
3. Describe each field of Wireshark GUI window?

Ans: The each field of wireshark GUI main window is described below:



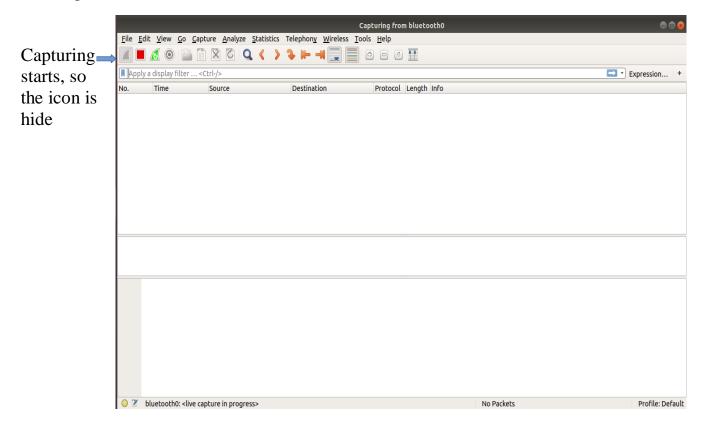
4. How to start capture in wireshark?

Ans: To start capture, one can go to capture menu and select options. Now start capturing on interface that has an IP address. The capturing is also possible in another way.



5. When capturing starts, what is the situation of the wireshark main window?

Ans: Once the capturing starts, the main window will be blank until the data is exchanged on Network Interface Card (NIC).



6. When packets exchanged on NIC, what will be condition of wireshark GUI?

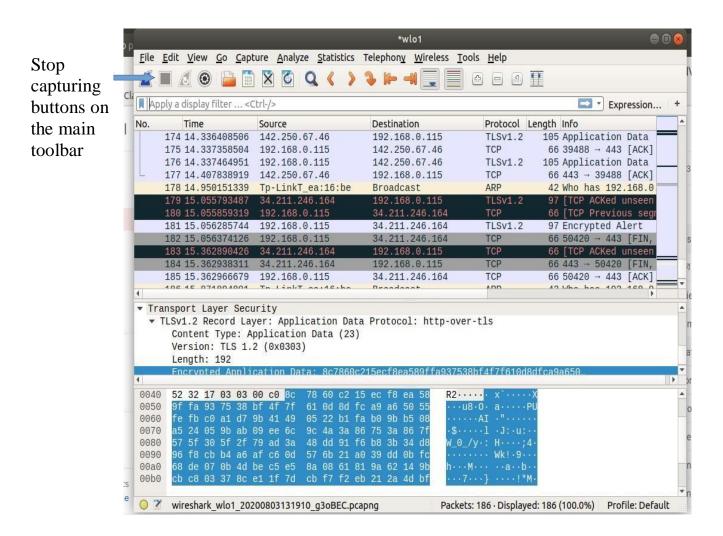
Ans: When packets exchanged on NIC, the packets will be dumped to main window.

∠ Wireshark ▼ Capturing from any <u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u> When packets **/ ■ <u>/</u> ⊕** ⊕ ↑ X Ø **Q ⟨ > 3 № →** ■ ■ ⊕ ⊕ ₫ Ⅲ exchanged on Apply a display filter ... < Ctrl-/ Expression... + Time Source
1788 169.757599516 Tp-LinkT_ea:16:be
1789 170.679132437 Tp-LinkT_ea:16:be
1790 171.499113481 172.217.194.189 NIC, the Protocol Length Info 44 Who has 192,168,0,102 ARP ARP 44 Who has 192.168.0.102 packets will 192.168.0.115 TLSv1.2 121 Application Data 1791 171.499162266 192.168.0.115 1792 172.726962075 Tp-LinkT_ea:16:be TCP ARP 68 42528 - 443 [ACK] Seq: 44 Who has 192.168.0.102 172.217.194.189 be dumped to 1793 174.877545418 Tp-LinkT_ea:16:be 1794 176.823186629 Tp-LinkT_ea:16:be 1795 177.437610078 192.168.0.1 44 Who has 192.168.0.1027 44 Who has 192.168.0.1027 ARP main window. IGMPv3 52 Membership Query, gene 44 Who has 192.168.0.102 107 Application Data 224.0.0.1 1796 178.973655831 Tp-LinkT_ea:16:be 1797 179.164574066 192.168.0.115 ARP TLSv1.2 172.217.26.174 107 Application Data 68 33882 → 443 [ACK] Seq: 1798 179.221040083 172.217.26.174 192.168.0.115 TLSv1.2 1799 179.221125624 192.168.0.115 172.217.26.174 ▼ Transport Layer Security ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls Content Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 34 00 00 00 01 00 06 0c 80 63 ea 16 be 00 00 08 00 45 80 00 5b 35 77 00 00 79 06 f9 ed ac d9 a3 c3 c0 a8 00 73 01 bb a5 e4 38 d5 51 54 ed 10 b5 49 80 18 01 47 7d c3 00 00 01 01 08 0a 0c fd 55 42 2d 3c ce f1 17 03 03 00 22 e7 ed e0 6f fc 07 75 8 · QT · · · I G} Payload is encrypted application data (tls.app_data), 34 bytes Packets: 1799 · Displayed: 1799 (100.0%) Profile: Default

7. How to stop capturing packets on wireshark?

Ans:

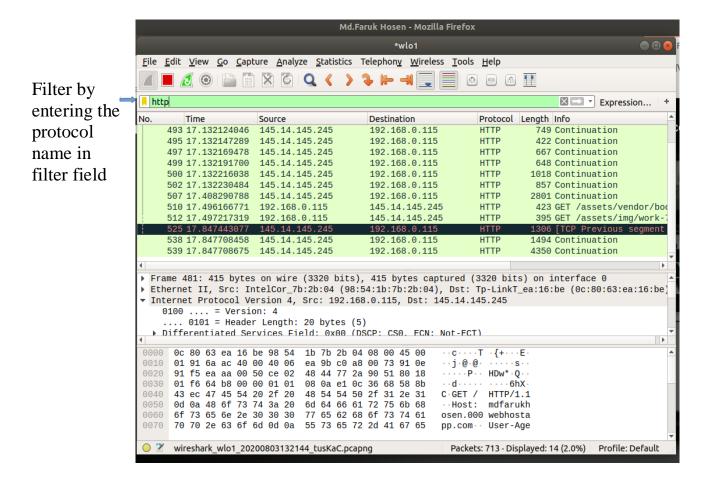
Capturing can be stopped by clicking on stop the running capture button on the main toolbar.



8. How to filtering protocol in wireshark?

Ans: Filter by entering the protocol field name in Apply a display filter and press enter.

Detailed filters can be applied by creating expressions.



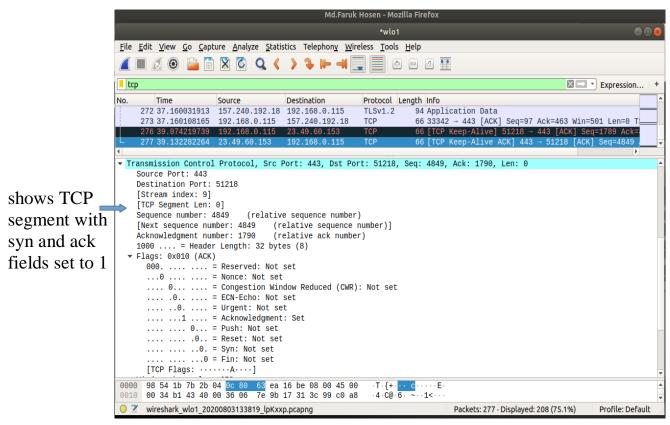
9. How to do protocol analysis with wireshark?

Ans: 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 .

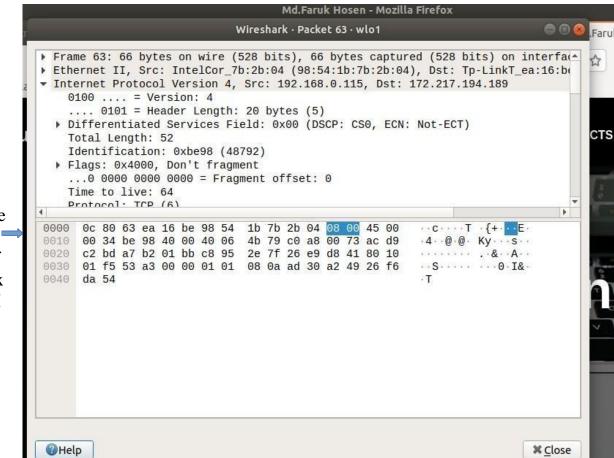
Analysis is performed manually. First of all, we see the TCP segment. The below example shows TCP segment with SYN and ACK fields set to 1.

Protocol detail pane figure:



Then we see the packet byte pane consists of offset, Hex and Ascii fields.

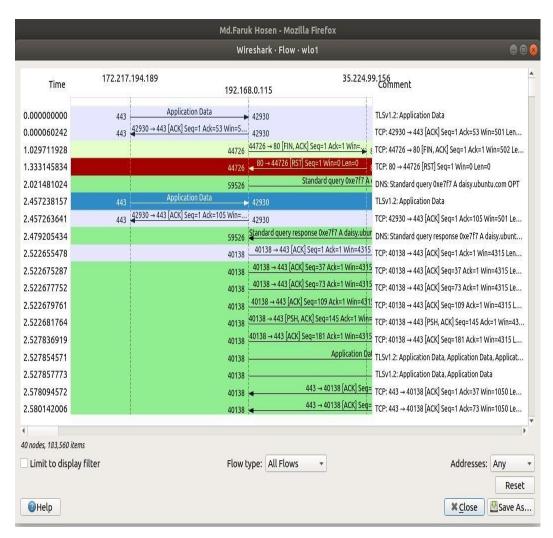
Packet byte pane:



packet byte pane consists of offset, Hex and ASCII fields. Then we see the statistics-flow graph example to analysis the protocol.

Flow Graph example:

In statistics menu, TCP plots and flow graphs are available



Conclusion:

From this lab, I know what is wireshark and how to work with wireshark and How to do protocol analysis using wireshark. When I do this lab, I was very excited to know how to see all protocols. Our course teacher Nazrul Islam Sir helps us a lot to teach new technology that is related with networking.