



Mawlana Bhashani Science and Technology University

Lab-Report

Report No: 05

Course code: ICT-4202

Course title: Wireless and Mobile Communication Lab

Date of Performance:

Date of Submission: 25.09.2020

Submitted by

Name: S M Shahriar Nashir

ID: IT-16039

4th year 2nd semester

Session: 2015-2016

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment No: 05

Experiment Name: Comparative Analysis of Wired and Wireless data using Wireshark

Objectives:

1. We have to find out the Wired data packages Using the Wireshark in order to compare with the wireless data packages.
2. Filter the packages
3. Find out the host, IP of the data packages
4. Create the Statistics for both of the data packages.
5. Finally compare the wired and wireless data packages simultaneously with the help of Wireshark.

Capturing Packets:

If we click any menu option, then it will show the available interfaces list.

After clicking the menu, we need to start Capturing on interface that has IP address/Source/Host.

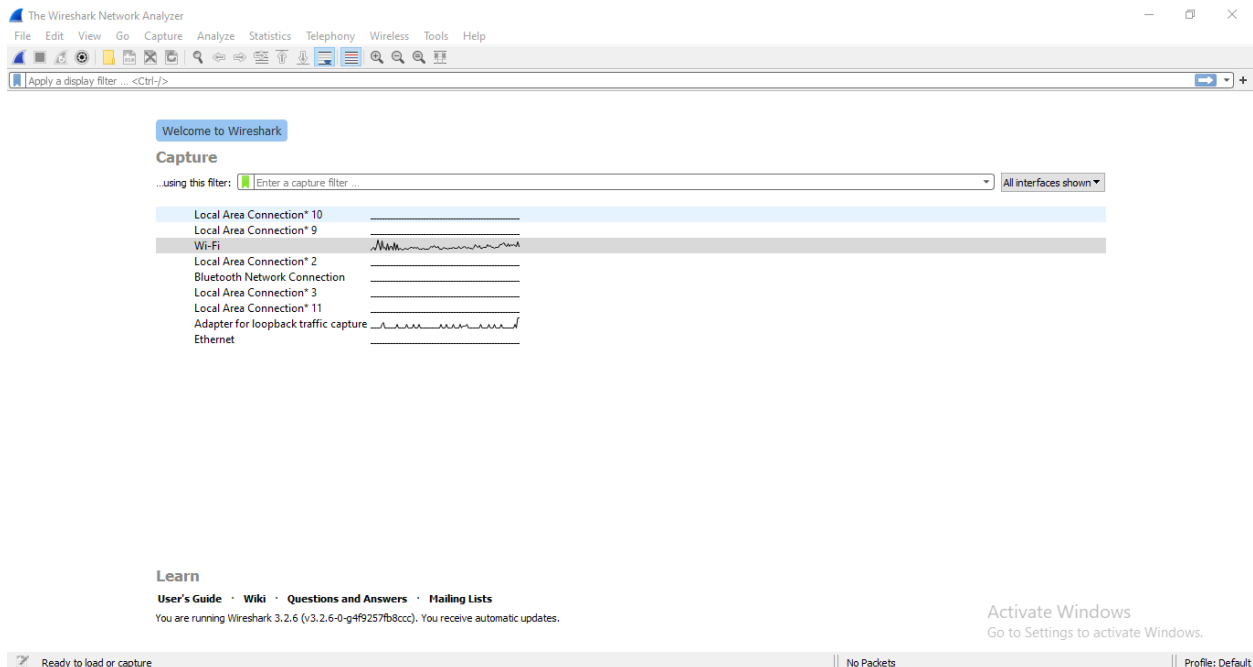


Figure 01: Wireshark Interface List

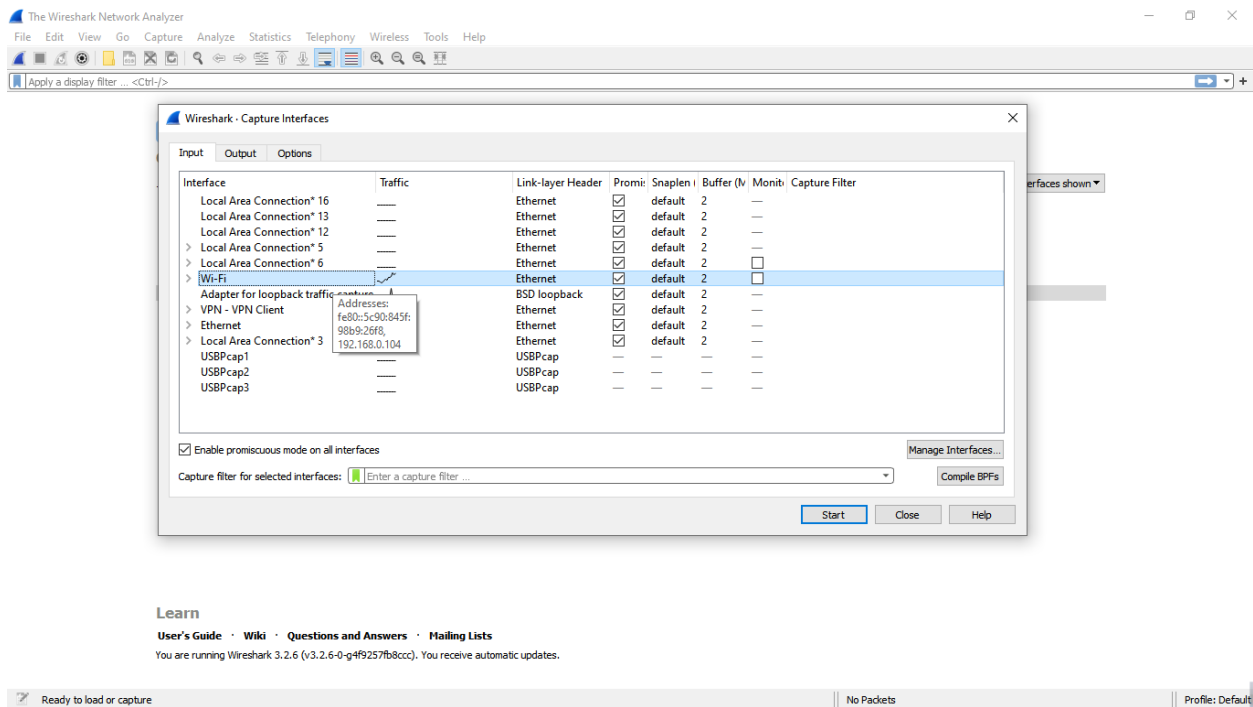


Figure 02-A: Start Capturing Interface that has for Wi-Fi (Wireless)

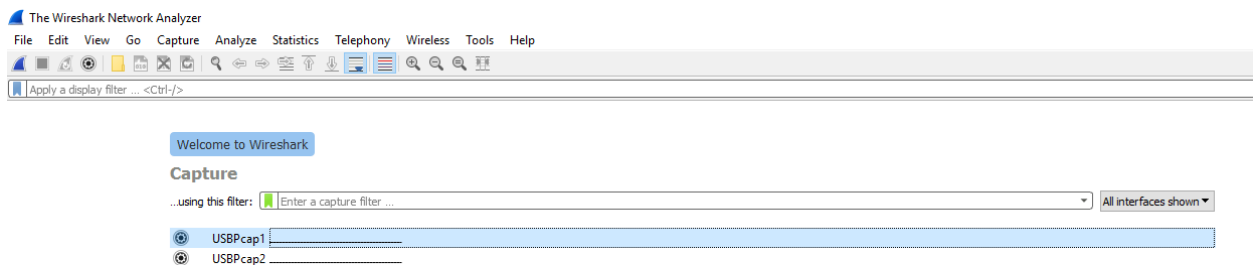


Figure 02-B: Start Capturing Interface that has for USB Tethering(Wired)

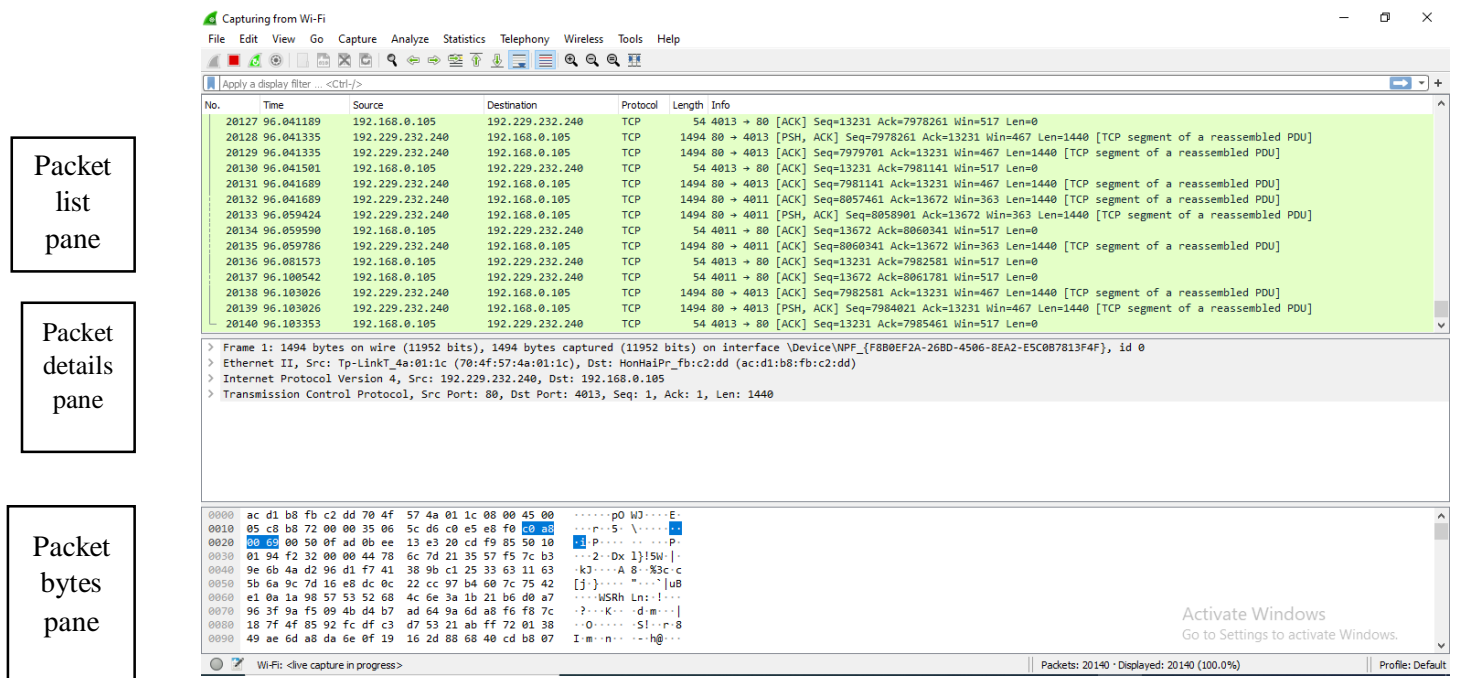


Figure 03-A: A sample packet capture window for Wireless Data Pack

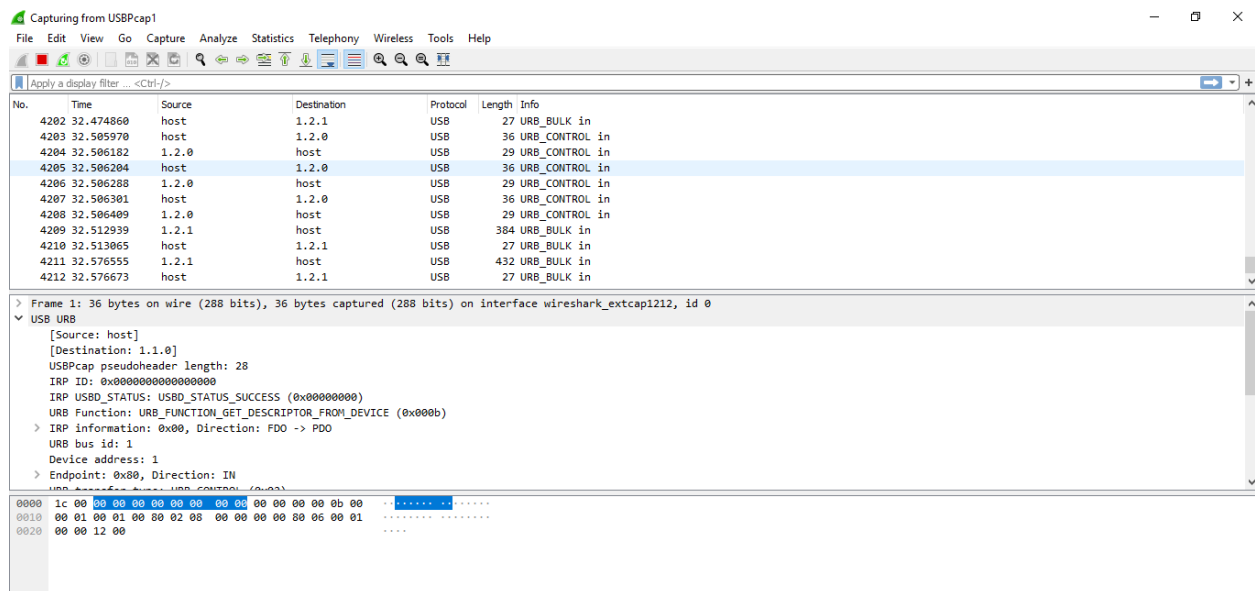


Figure 03-B: A sample packet capture window for Wired Data Pack

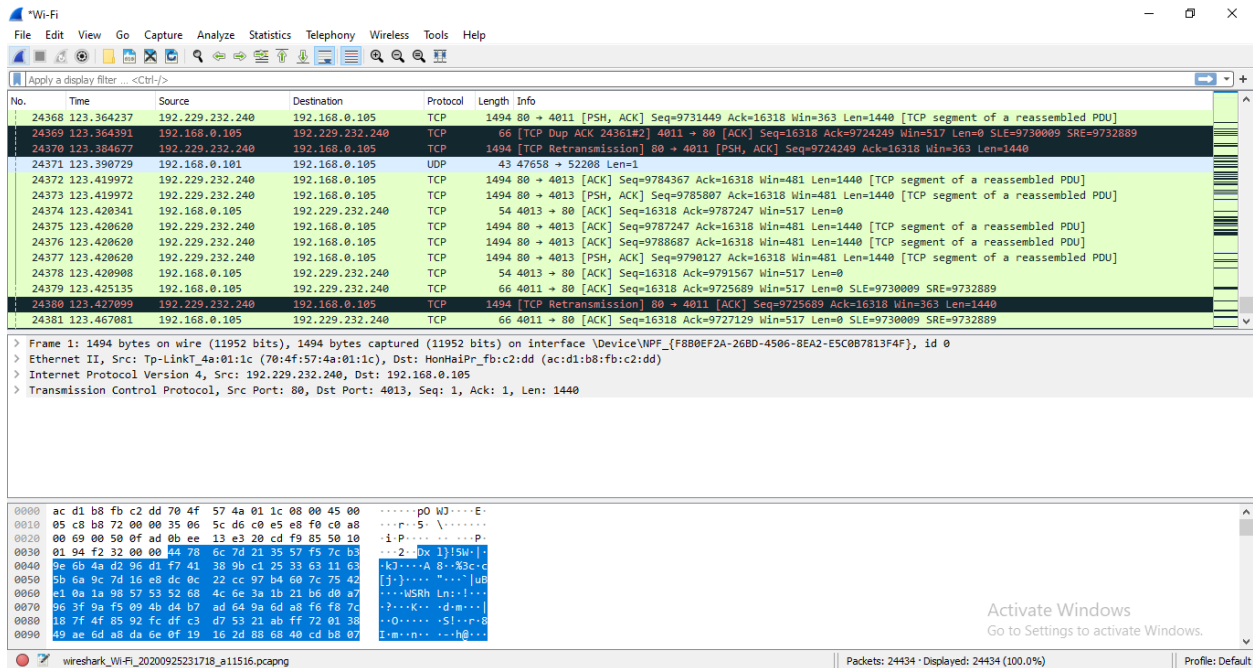


Figure 04-A: Stopping Capture for Wi-Fi (Wireless)

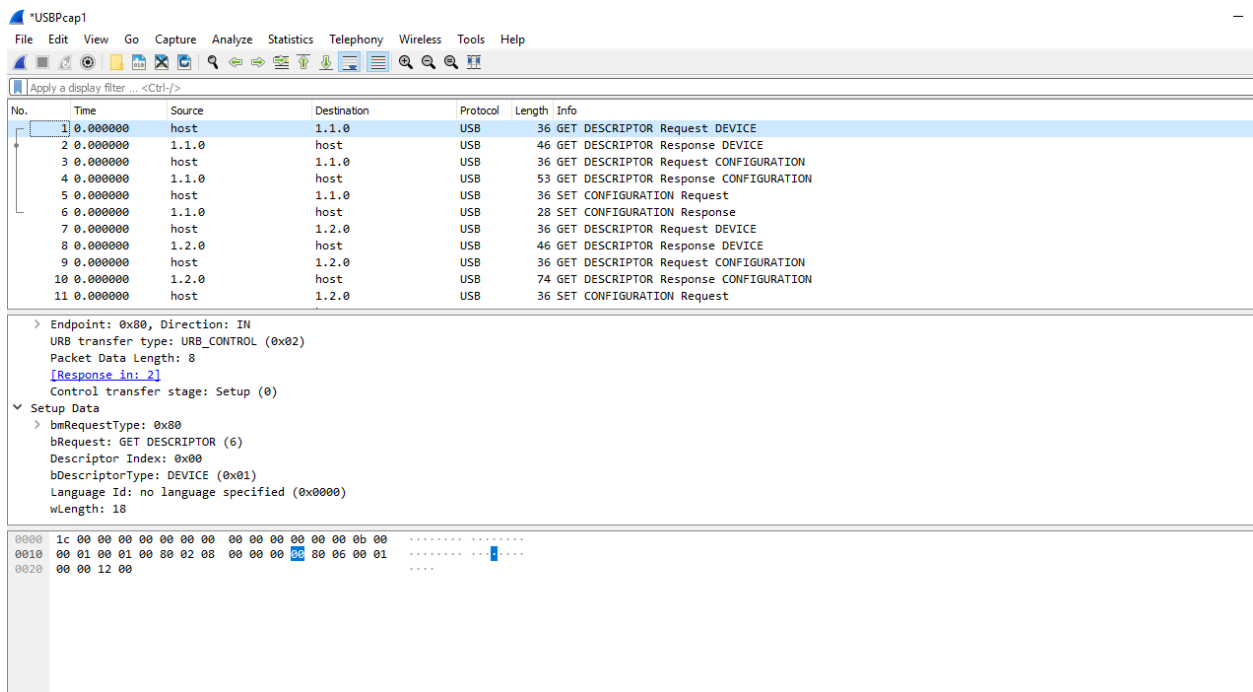


Figure 04-B: Stopping Capture for Wi-Fi (Wired)

Filtering:

The image shows the Wireshark interface with a packet capture of UDP traffic. The packet list pane shows 18 packets, all of type UDP, with source and destination IP addresses 192.168.0.101 and 192.168.0.105. The packet details pane shows the selected packet (No. 49) with details for Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
49	0.284999	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
97	0.890758	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
131	0.988391	192.168.0.105	147.135.136.51	UDP	145	34984 → 8644 Len=103
160	1.222904	147.135.136.51	192.168.0.105	UDP	319	8644 → 34984 Len=277
173	1.311143	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
264	1.818752	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
345	2.335153	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
360	2.372839	192.168.0.105	151.177.99.101	UDP	107	6881 → 57320 Len=65
464	2.840667	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
577	3.345335	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
689	3.851268	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
799	4.358805	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
913	4.862019	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1
1018	5.376413	192.168.0.101	192.168.0.105	UDP	43	47658 → 52208 Len=1

Frame 49: 43 bytes on wire (344 bits), 43 bytes captured (344 bits) on interface \Device\NPF{F8B0EF2A-268D-4506-8EA2-E5C087813F4F}, id 0
Ethernet II, Src: XiaomiCo_5e:41:d4 (d8:32:e3:5e:41:d4), Dst: NonHqPr_fb:c2:dd (ac:d1:b8:fb:c2:dd)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.105
User Datagram Protocol, Src Port: 47658, Dst Port: 52208
Data (1 byte)

0000 ac d1 b8 fb c2 dd d8 32 e3 5e 41 d4 00 00 45 002..A...E
0010 00 1d 43 26 40 00 40 11 75 8b c0 a8 00 65 c0 a8 ..C&@ @ u....e..
0020 00 69 ba 2a cb f0 00 09 66 a1 91 .!*....f..

Activate Windows
Go to Settings to activate Windows.

User Datagram Protocol: Protocol | Packets: 24434 · Displayed: 361 (1.5%) · Dropped: 0 (0.0%) | Profile: Default

Figure 05-A: Filter by Protocol Wireless Data Packages

The image shows the Wireshark interface with a packet capture of TCP traffic. The packet list pane shows 18 packets, all of type TCP, with source and destination IP addresses 192.0.2.1 and 192.0.2.1. The packet details pane shows the selected packet (No. 49) with details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the packet.

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 53 tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80
HTTP	http
No ARP and no DNS	not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.port in {80 25}

Figure 05-B: Filter by Protocol Wired Data Packages

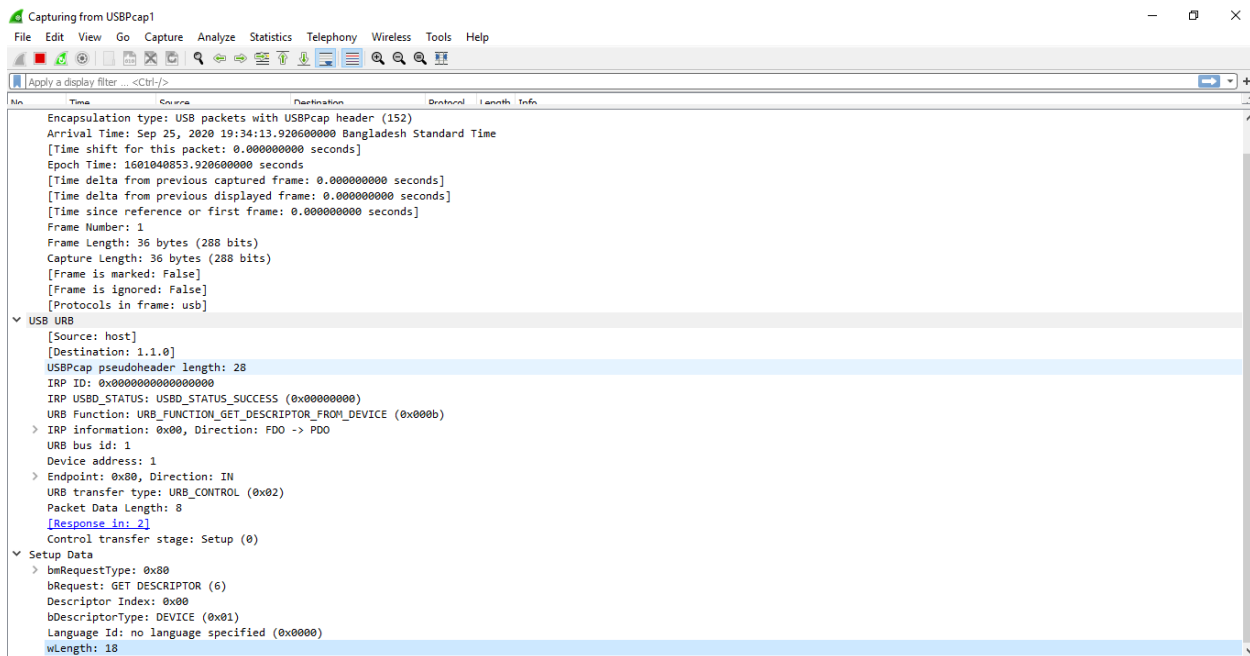


Figure 06-A: Packet Details Pane (Frame segment) for Wired Data Packages.

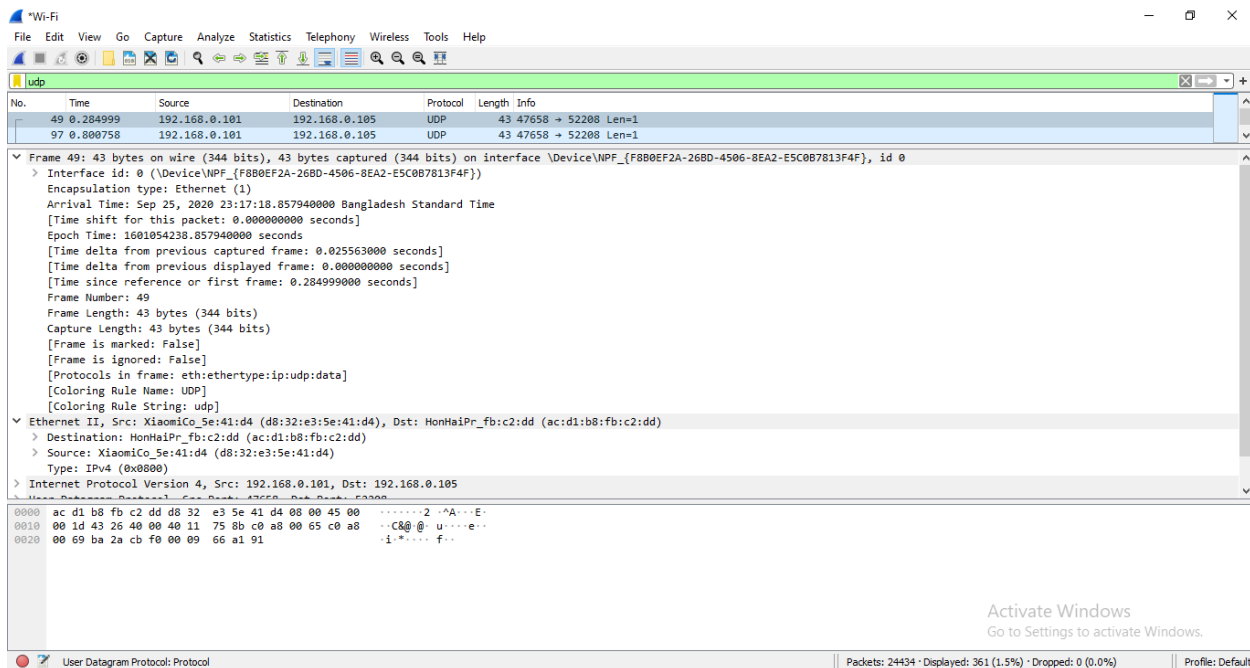


Figure 06-B: Packet Details Pane (Frame segment) for Wireless Data Packages.

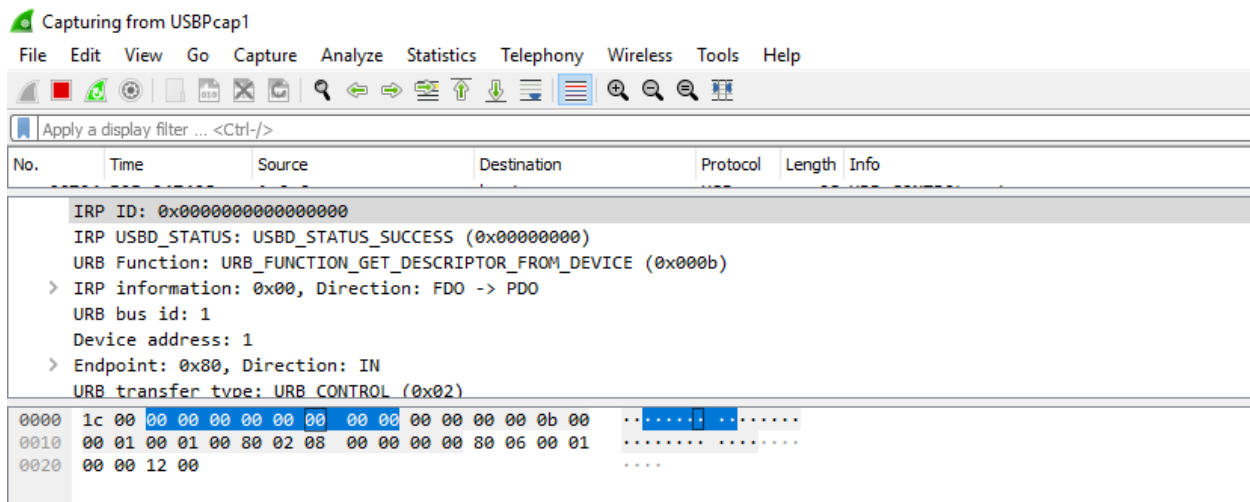


Figure 07-A: Packet Byte Pane for Wireless (USB Tethering)

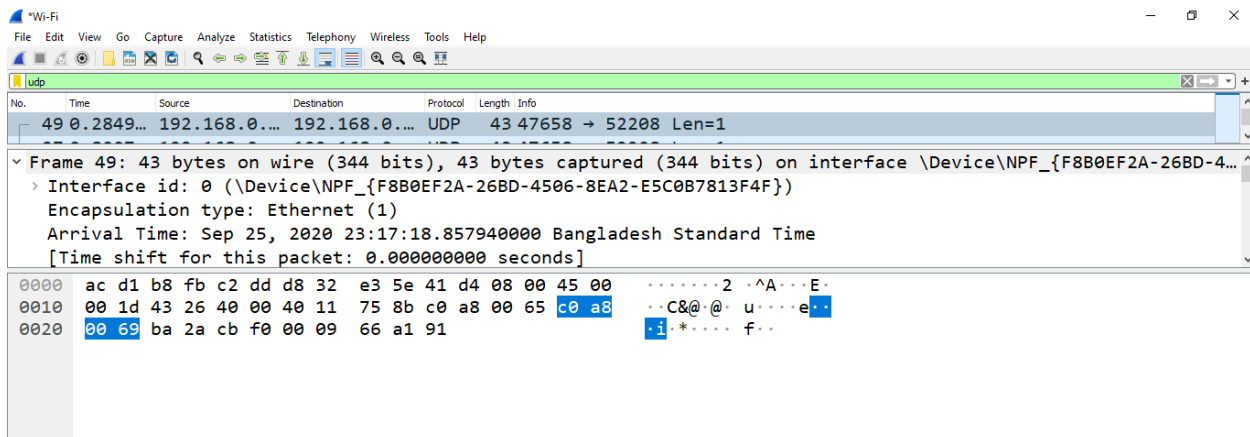


Figure 07-B: Packet Byte Pane (For Wi-Fi)

Conclusion:

As we know Wi-Fi is obviously more convenient than wired Ethernet cables, but Ethernet still offers significant advantages. Between Wired and Wireless Network, wired network is much more efficient than wireless network. Because wired data packages transfer rate are very much smoother than Wireless. From this experience we have learnt that we can also supervise or troubleshoot any problem whether it is wired or wireless by using Wireshark.