

2: Wireshark capture:

The image shows a Wireshark network traffic capture. The top pane displays a list of packets. Packet 728 is selected, and the bottom pane shows its details.

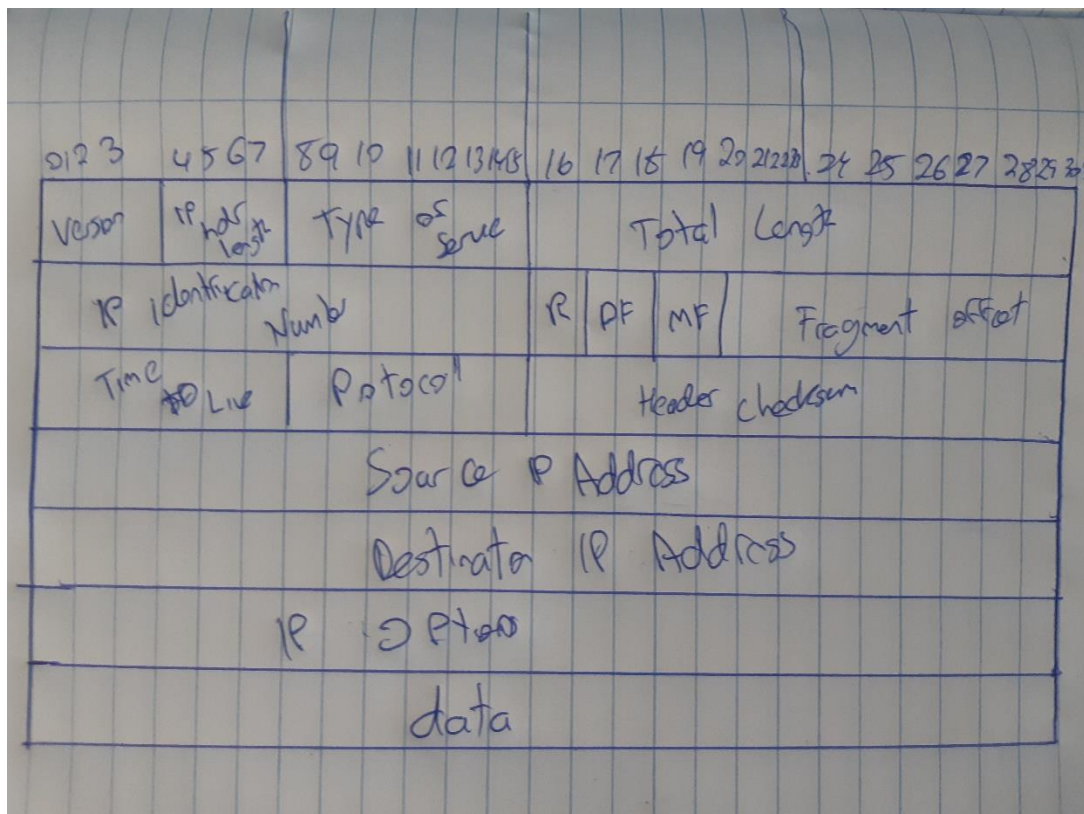
No.	Time	Source	Destination	Protocol	Length	Info
725	50.282232	192.168.1.106	213.163.93.40	UDP	237	52010 → 50001 Len=195
726	50.304019	192.168.1.106	213.163.93.40	UDP	239	52010 → 50001 Len=197
727	50.321090	192.168.1.106	213.163.93.40	UDP	246	52010 → 50001 Len=204
728	50.343095	192.168.1.106	213.163.93.40	UDP	241	52010 → 50001 Len=199
729	50.360113	192.168.1.106	213.163.93.40	UDP	244	52010 → 50001 Len=202
730	50.375373	fe80::f689:93e1:5b...	ff02::fb	MDNS	139	Standard query 0x002c PTR _674A0243._sub._googlecast._
731	50.381172	192.168.1.106	213.163.93.40	UDP	247	52010 → 50001 Len=205
732	50.402160	192.168.1.106	213.163.93.40	UDP	240	52010 → 50001 Len=198
733	50.424207	192.168.1.106	213.163.93.40	UDP	238	52010 → 50001 Len=196

Packet 728 details:

- Frame 728: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF_{71B2E5E4-3513-4F08-9D89-D60747C708}
- Ethernet II, Src: ASUSTekC_38:d4:b2 (b0:6e:bf:38:d4:b2), Dst: Tp-LinkT_e4:11:8c (30:b5:c2:e4:11:8c)
- Internet Protocol Version 4, Src: 192.168.1.106, Dst: 213.163.93.40
- User Datagram Protocol, Src Port: 52010, Dst Port: 50001
- Data (199 bytes)

The bottom pane shows the raw packet data in hexadecimal and ASCII format.

3: Draw IP Header



4: Explain header (from (2)):

Version: 30 b5 c2

Version of IP protocol used

Header Length: 45

Length of the header in 32-bit, minimum of 20

Type of Service: 08 00

How the datagram should be handled

Total length: 00 e3

Length of the entire packet

Identification: c7 86

Identify different packets from one another

Fragment offset: 00 00

Used for reassembling packets if it's too large

Time to Live: 80

Limits the datagram's lifespan, if it doesn't make it by this time to its destination it is removed

Protocol: 11

Defined protocol, this one is UDP

Header checksum: 00 00

Error checking of the header, discarded if incorrect

Source IP: c0 a8 01 6a

IP it is sent from

Destination: d5 a3 5d 28

IP it is sending to

5: Differences between captures

Major difference is that the IPv4 capture from the link is so large that it is fragmented into small parts so that it can be passed to its destination. Other differences between the captures is that the linked capture has a much larger data payload, another difference is that it is IPv4 protocol and my capture is a UDP protocol. The checksum is in a different place, also the header part of the capture is shorter than my capture, it only barely takes up more than the 20 byte minimum while my capture has a few more bytes of information.

6: Differences between captures

Ori and the blind forest: Tight platforming, stunning visuals and audio, short and difficult story.

Bioshock: RPG/FPS mix, great theme and setting, deep story based on Objectivism from the book: Atlas Shrugged by Ayn Rand.

Borderlands: Cell shading art style, great multiplayer co-op, open world, comedy dialogue.