

Q. Capture an IPv4 packet in Wireshark, list out all of the fields and their values. Calculate the checksum.

Wireshark packet capture showing an IPv4 packet. The packet list shows a TCP segment from 204.79.197.239 to 192.168.15.143. The packet details pane shows the full structure of the IP and TCP headers.

No.	Time	Source	Destination	Protocol	Length	Info
14	2.508395	192.168.15.143	204.79.197.239	TCP	63	12016 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
15	2.559140	204.79.197.239	192.168.15.143	TCP	74	443 → 12016 [ACK] Seq=1 Ack=2 Win=16383 Len=0 SLE=1 SRE=2
24	5.908894	192.168.15.143	142.250.195.142	UDP	152	50702 → 443 Len=102
25	6.031428	142.250.195.142	192.168.15.143	UDP	119	443 → 50702 Len=69
26	6.031428	142.250.195.142	192.168.15.143	UDP	71	443 → 50702 Len=21
27	6.031910	192.168.15.143	142.250.195.142	UDP	85	50702 → 443 Len=35
28	6.065745	192.168.15.143	142.250.195.142	UDP	82	50702 → 443 Len=32
29	6.108966	142.250.195.142	192.168.15.143	UDP	74	443 → 50702 Len=24

Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{5C0C9324-0550-4065-B307-FA608A0E1173}, id 0

Ethernet II, Src: Routerboardc_3a:5e:23 (cc:2d:e0:3a:5e:23), Dst: LCFCElectron_33:ce:47 (88:a4:c2:33:ce:47)

PPP-over-Ethernet Session

Point-to-Point Protocol

Internet Protocol Version 4, Src: 204.79.197.239, Dst: 192.168.15.143

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- ▼ Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 - 0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
 -00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 52
- Identification: 0x804d (32845)
- ▼ 010. = Flags: 0x2, Don't fragment
 - 0... = Reserved bit: Not set
 - .1... = Don't fragment: Set
 - ..0. = More fragments: Not set
 - ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 115
- Protocol: TCP (6)
- Header Checksum: 0x24e0 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 204.79.197.239
- Destination Address: 192.168.15.143

Transmission Control Protocol, Src Port: 443, Dst Port: 12016, Seq: 1, Ack: 2, Len: 0

```

▼ Internet Protocol Version 4, Src: 204.79.197.239, Dst: 192.168.15.143
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 52
  Identification: 0x804d (32845)
  ▼ 010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1... .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 115
  Protocol: TCP (6)
  Header Checksum: 0x24e0 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 204.79.197.239
  Destination Address: 192.168.15.143

```

② Capture a ^{IPv4} packet in Wireshark & calculate the checksum

→ The captured packet is shown above:

→ The fields and their values are: (In hex)

- 1) Version: 4
- 2) Header length: 5
- 3) Differentiated Services Code Point (DSCP): 20
- 4) Explicit congestion Notification: 00
- 5) Total length: 34
- 6) Identification: 804d
- 7) Flags: (Don't fragment) ~~2100~~ → 402
- 8) Time to Live: 73
- 9) Protocol: 06 (TCP)
- 10) Header checksum: 0000 (for calculation)
- 11) Source address: cc:4f:es:ef
- 12) Destination address: Co:a8:of:8f

Now, we convert all of the fields value to binary and divide each of them to 16 bits & calculate the sum of the values one by one & adding the carry over back to the LSB of the sum (if there's carry).

Now, the bits are :-

4520	=	0100010100100000	2
0034	=	0000000000110100	3+
804d	=	10000000001001101	3+
4000	=	0100000000000000	3+
7306	=	0111001100000110	3+
0000	=	0000000000000000	3+
cc4f	=	1100110001001111	3+
csef	=	1100010111101111	3+
Coa8	=	1100000010101000	3+
of8f	=	0000111110001111	3+

Here, sum is 3DB1C, Now adding carry to LSB we get, DB1F, Now, 1's complement is 24E0 which is check sum.