

# Assignment Ethernet Wireshark

**Scenario\_1** Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message respected to [testing-ground.scraping.pro](http://testing-ground.scraping.pro) web page:

Q1. What is the 48-bit Ethernet address of your computer?

Ans- `12:50:ce:9e:51:dc` is the MAC address of my WiFi NIC.

```
▶ Frame 163: 436 bytes on wire (3488 bits), 436 bytes captured (3488 bits) on interface eth0
▼ Ethernet II, Src: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc), Dst: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
  ▶ Destination: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
  ▶ Source: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  ▶ Internet Protocol Version 4, Src: 192.168.1.6, Dst: 199.59.243.228
  ▶ Transmission Control Protocol, Src Port: 60353, Dst Port: 80, Seq: 1, Ack: 1, Len: 382
  ▶ Hypertext Transfer Protocol
```

Q2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of <http://testing-ground.scraping.pro/login?> What device has this as its Ethernet address?

Ans- The 48 bit destination address in the Ethernet frame is `f0:ed:b8:15:b5:d8`. No this is not the ethernet address of the destination website rather this the MAC address of my network's gateway router.

```
▶ Frame 163: 436 bytes on wire (3488 bits), 436 bytes captured (3488 bits) on interface eth0
▼ Ethernet II, Src: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc), Dst: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
  ▶ Destination: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
  ▶ Source: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  ▶ Internet Protocol Version 4, Src: 192.168.1.6, Dst: 199.59.243.228
  ▶ Transmission Control Protocol, Src Port: 60353, Dst Port: 80, Seq: 1, Ack: 1, Len: 382
  ▶ Hypertext Transfer Protocol
```

Q3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Ans- Hexadecimal value for the two-byte Frame type field is `0x0800` which corresponds to upper layer IPv4 protocol.

```
▼ Ethernet II, Src: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc),
  ▶ Destination: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
  ▶ Source: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)
  Type: IPv4 (0x0800)
  [Stream index: 0]
```

Q4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

Ans- After `54 bytes` from the very start of the Ethernet frame the ASCII "G" in "GET" appears. Below is the screen shot proof from wireshark, results are marked in red boxes. Also we can verify this by simple addition that the ethernet header is of 14 bytes + 20 bytes of IP header + 20 bytes of TCP header = 54

bytes.

Wireshark packet capture showing an HTTP GET request and its response. The packet list on the left shows packet 163 selected. The packet details pane shows the structure of the HTTP response, including the status line '200 OK (application/javascript)'. The packet bytes pane shows the raw data of the response, with a red box highlighting the first byte 'f0'.

**Scenario\_2** Answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message:

Q5. What is the value of the Ethernet source address? Is this the address of your computer, or <http://testing-ground.scraping.pro/login>? What device has this as its Ethernet address?

Ans- The value of the Ethernet source address is `f0:ed:b8:15:b5:d8`. This address neither belong to my computer NIC card nor to the website's NIC rather this address belongs to the MAC address of my network's gateway router.

Wireshark packet capture showing an Ethernet II frame. The packet list on the left shows packet 171 selected. The packet details pane shows the structure of the Ethernet frame, including the source and destination MAC addresses. The packet bytes pane shows the raw data of the frame, with a red box highlighting the first byte 'f0'.

Q6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Ans- Destination address in the Ethernet frame is `12:50:ce:9e:51:dc`. Yes this is the ethernet

address of my computer's WiFi NIC.

```
▶ Frame 171: 564 bytes on wire (4512 bits), 564 bytes captured
▼ Ethernet II, Src: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8),
  ▶ Destination: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)
  ▶ Source: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
    Type: IPv4 (0x0800)
    [Stream index: 0]
▶ Internet Protocol Version 4, Src: 199.59.243.228, Dst: 192.16
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 60353,
▶ [2 Reassembled TCP Segments (1760 bytes): #170(1250), #171(51
▶ Hypertext Transfer Protocol
▶ Line-based text data: text/html (14 lines)
```

Q7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Ans- Hexadecimal value for the two-byte Frame type field is `0x0800` which corresponds to upper layer IPv4 protocol.

Q8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

Ans- After `54 bytes` from the very start of the Ethernet frame the ASCII "O" in "OK" appears. we can verify this by simple addition that the ethernet header is of 14 bytes + 20 bytes of IP header + 20 bytes of TCP header = 54 bytes.