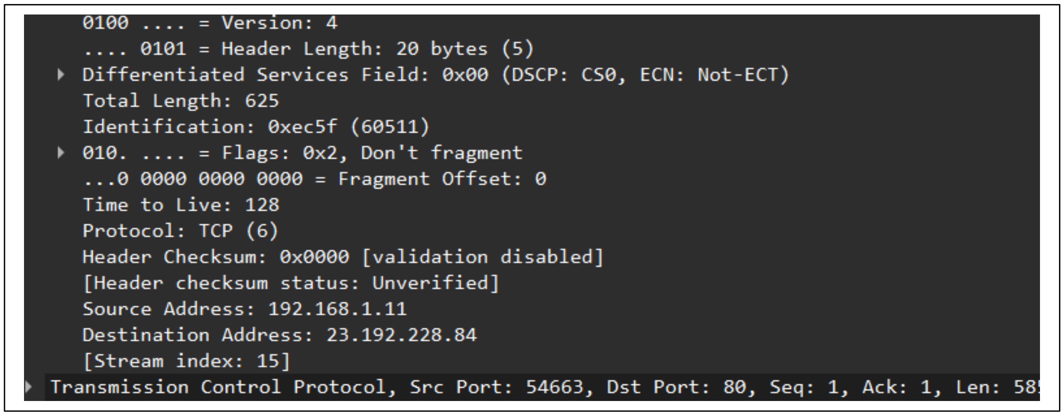
Wireshark Lab 01: Introduction to Packet Capturing

E/21/291

1. What is your IP address?

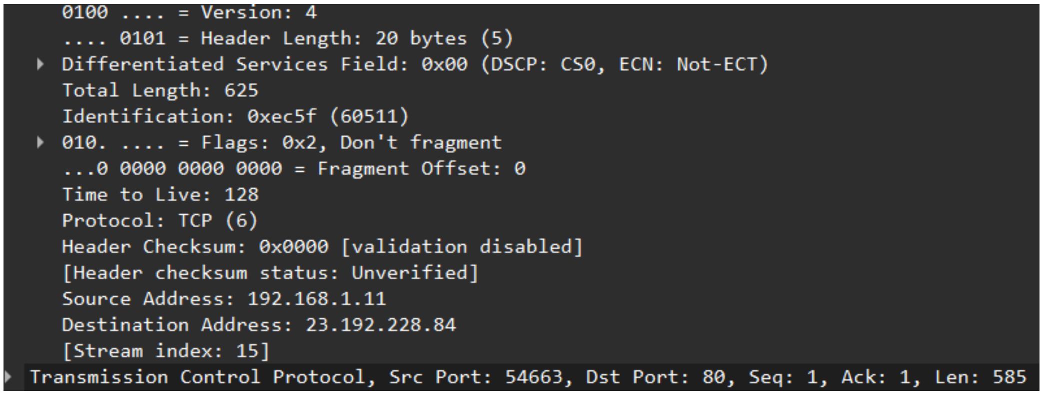
192.168.1.11



```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 625
    Identification: 0xec5f (60511)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.11
    Destination Address: 23.192.228.84
    [Stream index: 15]
▸ Transmission Control Protocol, Src Port: 54663, Dst Port: 80, Seq: 1, Ack: 1, Len: 58
```

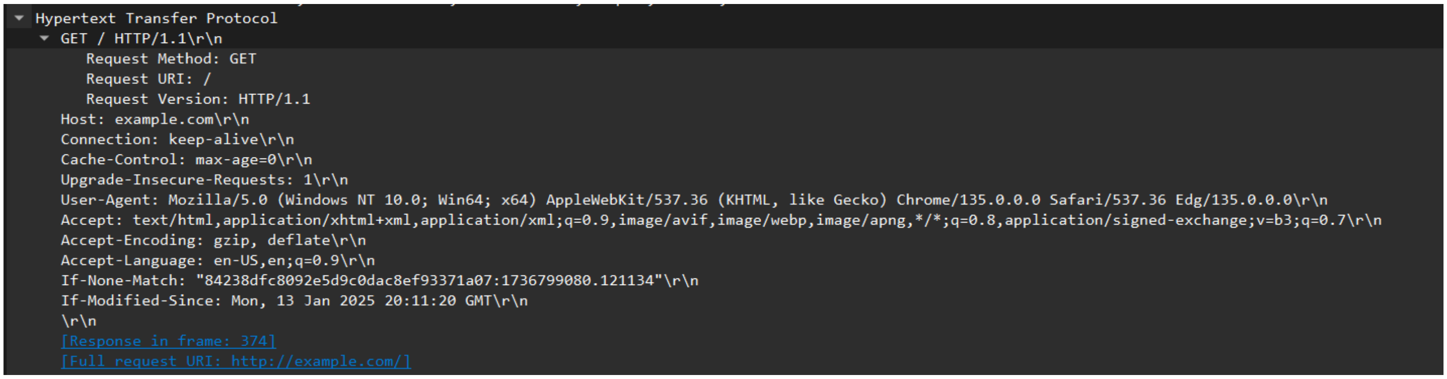
2. What is the IP address of example.com ?

   23.192.228.84



```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 625
    Identification: 0xec5f (60511)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.11
    Destination Address: 23.192.228.84
    [Stream index: 15]
▸ Transmission Control Protocol, Src Port: 54663, Dst Port: 80, Seq: 1, Ack: 1, Len: 585
```

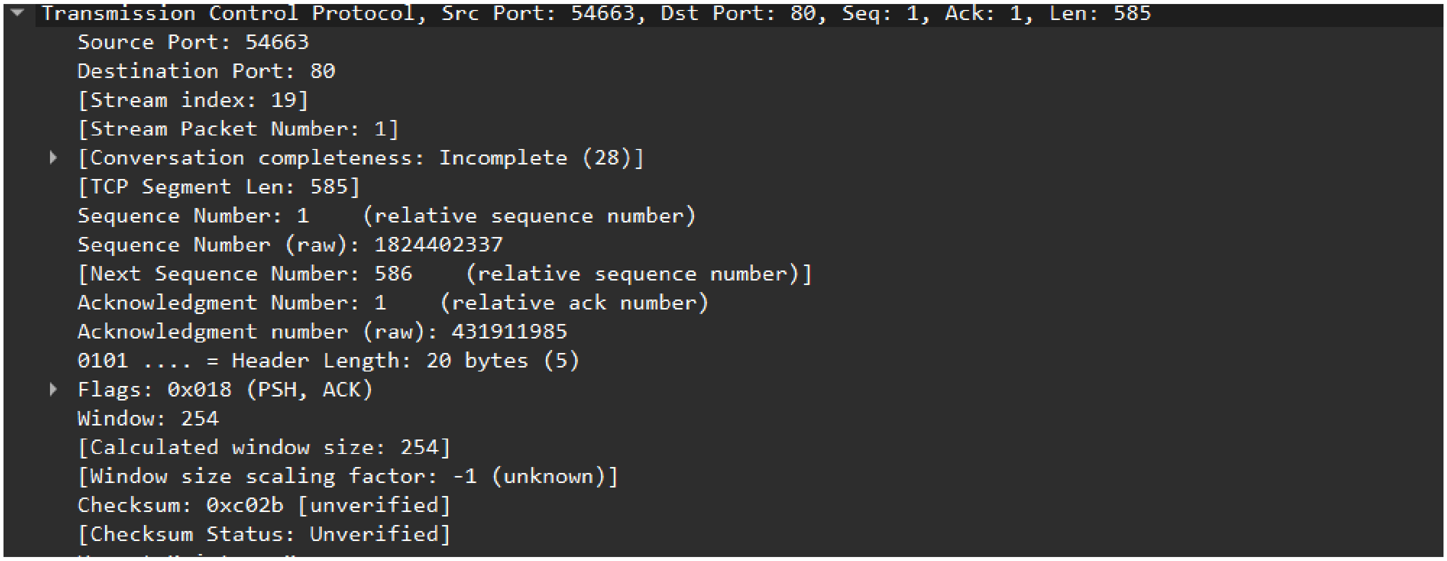
3. What is the full request sent to example.com?



```
▾ Hypertext Transfer Protocol
  ▾ GET / HTTP/1.1\r\n
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: example.com\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 Edg/135.0.0.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"\r\n
    If-Modified-Since: Mon, 13 Jan 2025 20:11:20 GMT\r\n
    \r\n
    [Response in frame: 374]
    [Full request URI: http://example.com/]
```

4. What TCP port was used for HTTP request?

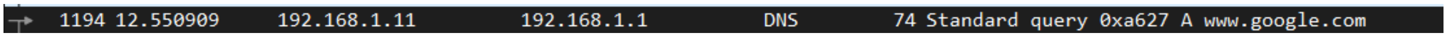
   54663



```
Transmission Control Protocol, Src Port: 54663, Dst Port: 80, Seq: 1, Ack: 1, Len: 585
   Source Port: 54663
   Destination Port: 80
   [Stream index: 19]
   [Stream Packet Number: 1]
   [Conversation completeness: Incomplete (28)]
   [TCP Segment Len: 585]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 1824402337
   [Next Sequence Number: 586    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 431911985
   0101 .... = Header Length: 20 bytes (5)
   Flags: 0x018 (PSH, ACK)
   Window: 254
   [Calculated window size: 254]
   [Window size scaling factor: -1 (unknown)]
   Checksum: 0xc02b [unverified]
   [Checksum Status: Unverified]
```

5. What happens when you access https://www.google.com?

   The request can be captured using DNS filter as follows



```
1194 12.550909     192.168.1.11          192.168.1.1          DNS        74 Standard query 0xa627 A www.google.com
```