

# Packet Dissection Wireshark

```
> Frame 27: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
> Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xerox_00:00:00 (00:00:01:00:00:00)
> Internet Protocol Version 4, Src: 216.239.59.99, Dst: 145.254.160.237
> Transmission Control Protocol, Src Port: 80, Dst Port: 3371, Seq: 778787098, Ack: 918692089, Len: 160
> [2 Reassembled TCP Segments (1590 bytes): #26(1430), #27(160)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (3 lines)
```

7 layers associated with the packet:

- Frame/packet
- Source [mac]
- Source [ip]
- Protocol
- Protocol errors
- Application protocol
- Application data

- Frame (layer 1) – detail specific to the Physical layer of the OSI model

```
▼ Frame 27: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: May 13, 2004 06:17:11.266912000 Eastern Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1084443431.266912000 seconds
  [Time delta from previous captured frame: 0.040058000 seconds]
  [Time delta from previous displayed frame: 0.040058000 seconds]
  [Time since reference or first frame: 3.955688000 seconds]
  Frame Number: 27
  Frame Length: 214 bytes (1712 bits)
  Capture Length: 214 bytes (1712 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

- Source [MAC] (layer 2) – source + destination MAC address; data link layer of the OSI model

```
▼ Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xerox_00:00:00 (00:00:01:00:00:00)
  > Destination: Xerox_00:00:00 (00:00:01:00:00:00)
  > Source: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
  Type: IPv4 (0x0800)
```

- Source [MAC] (layer 3) – source + destination ip address; network layer of the OSI model

```

  ▾ Internet Protocol Version 4, Src: 216.239.59.99, Dst: 145.254.160.237
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
      Total Length: 200
      Identification: 0x85cf (34255)
    > Flags: 0x0000
      Fragment offset: 0
      Time to live: 55
      Protocol: TCP (6)
      Header checksum: 0xb612 [validation disabled]
      [Header checksum status: Unverified]
      Source: 216.239.59.99
      Destination: 145.254.160.237

```

- Protocol (layer 4) – details of protocol used TCP/UDP + source/destination ports – transport layer of the OSI model

```

  ▾ Transmission Control Protocol, Src Port: 80, Dst Port: 3371, Seq: 778787098, Ack: 918692089, Len: 160
    Source Port: 80
    Destination Port: 3371
    [Stream index: 1]
    [TCP Segment Len: 160]
    Sequence number: 778787098
    [Next sequence number: 778787258]
    Acknowledgment number: 918692089
    0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x018 (PSH, ACK)
    Window size value: 31460
    [Calculated window size: 31460]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xde29 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    > [SEQ/ACK analysis]
    > [Timestamps]
    TCP payload (160 bytes)
    TCP segment data (160 bytes)

```

- Protocol errors – continuation of layer 4 – showing specific segments from TCP needed to be reassembled

```

  ▾ [2 Reassembled TCP Segments (1590 bytes): #26(1430), #27(160)]
    [Frame: 26, payload: 0-1429 (1430 bytes)]
    [Frame: 27, payload: 1430-1589 (160 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 1590]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a5033503a20706f...]

```

- Application Protocol (layer 5) – details specific to protocol being used such as HTTP; application layer of the OSI model

```

v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    P3P: policyref="http://www.googleadservices.com/pagead/p3p.xml", CP="NOI DEV PSA PSD IVA PVD OTP OUR OTR IND OTC"\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    Content-Encoding: gzip\r\n
    Server: CAFE/1.0\r\n
    Cache-control: private, x-gzip-ok=""\r\n
  > Content-length: 1272\r\n
    Date: Thu, 13 May 2004 10:17:14 GMT\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.971397000 seconds]
    [Request in frame: 18]
    [Request URI [truncated]: http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2309191948673629&random=108444]
    Content-encoded entity body (gzip): 1272 bytes -> 3608 bytes
    File Data: 3608 bytes

```

- Application data – extension of layer 5 – application specific data

```

v Line-based text data: text/html (3 lines)
  <html><head><style><!--\n
    [truncated].ch{cursor:pointer;cursor:hand}a.ad:link { color: #000000 }
    [truncated]function ss(w,id) {window.status = w;return true;}function

```