Lab 1

1. TCP and HTTP
2. 0.031263 seconds
3. Internet address of gaia.cs.umass.edu: 192.168.1.230; Internet address of my PC: 128.119.245.12
4. Firefox
5. 80
6.

No. Time Source Destination Protocol Length Info

1614 13.578792 192.168.1.230 128.119.245.12 HTTP 446 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/ 1.1

Frame 1614: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface

\Device\NPF_{D460A571-65B8-45F5-9AFA-0C57941903A6}, id 0

Ethernet II, Src: ASUSTekCOMPU_d3:f8:f4 (f0:2f:74:d3:f8:f4), Dst: TechnicolorD_eb:39:c9 (d4:35:1d:eb:39:c9)

Internet Protocol Version 4, Src: 192.168.1.230, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 52795, Dst Port: 80, Seq: 1, Ack: 1, Len: 392 Source Port: 52795

Destination Port: 80

[Stream index: 10]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 392]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2716584868

[Next Sequence Number: 393 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 3693505695

0101 .... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window: 1026

[Calculated window size: 262656]

[Window size scaling factor: 256]

Checksum: 0x39b5 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[SEQ/ACK analysis]

TCP payload (392 bytes)

Hypertext Transfer Protocol

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp, */*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade
-
Insecure
-
Requests
: 1\r\n
\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/2]

[Response in frame: 1616]

[Next request in frame: 1618]

No. Time Source Destination Protocol Length Info

1616 13.610055 128.119.245.12 192.168.1.230 HTTP 492 HTTP/1.1 200 OK (text/html)

Frame 1616: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface

\Device\NPF_{D460A571-65B8-45F5-9AFA-0C57941903A6}, id 0

Ethernet II, Src: TechnicolorD_eb:39:c9 (d4:35:1d:eb:39:c9), Dst: ASUSTekCOMPU_d3:f8:f4 (f0:2f:74:d3:f8:f4) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.230

Transmission Control Protocol, Src Port: 80, Dst Port: 52795, Seq: 1, Ack: 393, Len: 438 Source Port: 80

Destination Port: 52795

[Stream index: 10]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 438]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 3693505695

[Next Sequence Number: 439 (relative sequence number)]

Acknowledgment Number: 393 (relative ack number)

Acknowledgme
nt number
(raw):
2716585260
0101 .... =
Header Length:
20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window: 237

[Calculated window size: 30336]

[Window size scaling factor: 128]

Checksum:
0x9787
[unverified

]
[Checksum
Status:
Unverified]

Urgent Pointer: 0

[Timestamps]

[SEQ/ACK analysis]

TCP payload (438 bytes)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Wed, 07 Feb 2024 00:08:28 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n Last-Modified: Tue, 06 Feb 2024 06:59:01 GMT\r\n

ETag: "51-610b11cfd3c31"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/2]

[Time since request: 0.031263000 seconds]

[Request in frame: 1614]

[Next request in frame: 1618]

[Next response in frame: 1619]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

File Data: 81 bytes

Line-based text data: text/html (3 lines)