LAB 1

1. TCP, HTTP, DNS, TLSv1.2, UDP

2.)GET Sep 19, 2024 12:52:17.295902000

OK Sep 19, 2024 12:52:17.597888000

3. My computer: 10.62.83.210 Address of gaia.cs.umass.edu: 128.119.245.12

4.)

GET

------

Hypertext Transfer Protocol

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

Request Method: GET

Request URI: /wireshark-labs/INTRO-wireshark-file1.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu\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/128.0.0.0 Safari/537.36 Edg/128.0.0.0\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: "51-622726c83dbbf"\r\n

If-Modified-Since: Thu, 19 Sep 2024 05:45:02 GMT\r\n

\r\n

[Response in frame: 42]

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

OK

------

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Thu, 19 Sep 2024 05:52:16 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: Thu, 19 Sep 2024 05:52:02 GMT\r\n

ETag: "51-62272858b2805"\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

[Request in frame: 37]

[Time since request: 0.301986000 seconds]

[Request URI: /wireshark-labs/INTRO-wireshark-file1.html]

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

File Data: 81 bytes

5.)

Transmission Control Protocol, Src Port: 62490, Dst Port: 80, Seq: 1, Ack: 1, Len: 598

Source Port: 62490

Destination Port: 80

[Stream index: 5]

[Stream Packet Number: 1]

[Conversation completeness: Incomplete (12)]

..0. .... = RST: Absent

...0 .... = FIN: Absent

.... 1... = Data: Present

.... .1.. = ACK: Present

.... ..0. = SYN-ACK: Absent

.... ...0 = SYN: Absent

[Completeness Flags: ··DA··]

[TCP Segment Len: 598]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1291655146

[Next Sequence Number: 599 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2254033311

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

Flags: 0x018 (PSH, ACK)

000. .... .... = Reserved: Not set

...0 .... .... = Accurate ECN: Not set

.... 0... .... = Congestion Window Reduced: Not set

.... .0.. .... = ECN-Echo: Not set

.... ..0. .... = Urgent: Not set

.... ...1 .... = Acknowledgment: Set

.... .... 1... = Push: Set

.... .... .0.. = Reset: Not set

.... .... ..0. = Syn: Not set

.... .... ...0 = Fin: Not set

[TCP Flags: ·······AP···]

Window: 64240

[Calculated window size: 64240]

[Window size scaling factor: -1 (unknown)]

Checksum: 0xba58 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[Time since first frame in this TCP stream: 0.000000000 seconds]

[Time since previous frame in this TCP stream: 0.000000000 seconds]

[SEQ/ACK analysis]

[Bytes in flight: 598]

[Bytes sent since last PSH flag: 598]

TCP payload (598 bytes)

6.

GET

A screenshot of a computer program

Description automatically generated

OK

A screenshot of a computer

Description automatically generated