LAB-1 Assignment

(1) UDP, TLS, TCP, STP, SSDP, NBNS, MDNS, LLMNR, LLC, IPv4, IGMP, DNS, DHCP, ARP

(2) Time: 0.283680439 (s)

(3) Source Internet Address: 172.18.3.182
Destination Internet Address: 128.119.245.12

(4) User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0\r\n

(5) Destination Port: 80

(6) GET

/tmp/wireshark_anyCMJ691.pcapng 2295 total packets, 2 shown

```
No.     Time               Source                Destination           Protocol Length Info
   1766 15:49:29.498275926 172.18.3.182          128.119.245.12        HTTP     531    GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 1766: 531 bytes on wire (4248 bits), 531 bytes captured (4248 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 172.18.3.182, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56178, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
    Source Port: 56178
    Destination Port: 80
    [Stream index: 11]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 475]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1936649022
    [Next Sequence Number: 476    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2555279524
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0xa441 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (475 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): 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
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0\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
    If-Modified-Since: Wed, 23 Aug 2023 05:59:01 GMT\r\n
    If-None-Match: "51-60390cee3bf48"\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 1800]
```

OK

/tmp/wireshark_anyCMJ691.pcapng 2295 total packets, 2 shown

```
No.     Time               Source                Destination           Protocol Length Info
   1800 15:49:29.765338939 128.119.245.12        172.18.3.182          HTTP     295    HTTP/1.1 304 Not
Modified
Frame 1800: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.3.182
Transmission Control Protocol, Src Port: 80, Dst Port: 56178, Seq: 1, Ack: 476, Len: 239
    Source Port: 80
    Destination Port: 56178
    [Stream index: 11]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 239]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2555279524
    [Next Sequence Number: 240    (relative sequence number)]
    Acknowledgment Number: 476    (relative ack number)
    Acknowledgment number (raw): 1936649497
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x3a07 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (239 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Wed, 23 Aug 2023 10:19:29 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-60390cee3bf48"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.267063013 seconds]
    [Request in frame: 1766]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

(7) www.washington.edu/

Protocols: UDP, TLS, TCP, STP, SSDP, NBNS, MDNS, LLMNR, LLC, IPv4, IGMP, DNS, DHCP, ARP
Time: 0.480436283
Source Internet Address: 172.18.3.182
Destination Internet Address: 34.127.31.83

example.com/

Protocols: UDP, TLS, TCP, STP, SSDP, NBNS, MDNS, LLMNR, LLC, IPv4, IGMP, DNS, DHCP, ARP
Time: 0.221253036
Source Internet Address: 172.18.3.182
Destination Internet Address: 93.184.216.34

www.iith.ac.in

Protocols: UDP, TLS, TCP, STP, SSDP, NBNS, MDNS, LLMNR, LLC, IPv4, IGMP, DNS, DHCP, ARP
Time: 0.011414865
Source Internet Address: 172.18.3.182
Destination Internet Address: 192.168.36.56

www.youtube.com

Protocols: UDP, TLS, TCP, STP, SSDP, NBNS, MDNS, LLMNR, LLC, IPv4, IGMP, DNS, DHCP, ARP
Time: 0.031907729
Source Internet Address: 172.18.3.182
Destination Internet Address: 142.250182.10

(8) When I hit the domain names in the browser, the browser simply showed the landing page of the website full of images, text and different resources.

While observing the same in parallel in wireshark, i got to know that a large number of packets exchanges took place just for the landing page of the website to show up.