Experiment No: AV-341-2025-Lab-4
HTTP Capture and Session Analysis

Saurabh Kumar
SC22B146
February 25, 2025

Date and Time of experiment: February 17, 2025, 15:00 IST

Objectives

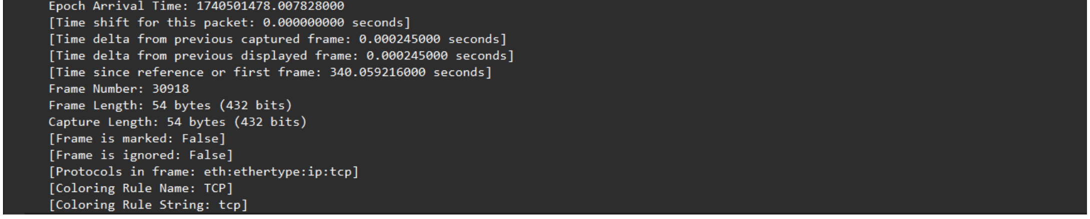
- Capture a set of packets, understand the encapsulation, and interpret them
- HTTP Session capture and identification
- Capture at least three different HTTP session packets (request and response)
  - GET-OK pair
  - Identify and Discuss at least two more Request-Response packet pairs.
    - Cache related
    - Cookie related
  - Identify and Discuss at least two header lines that we have not been discussed in the class.

Tools Used

- PC: 12th Gen Intel(R) Core(TM) i5-1240P 1.70 GHz, Windows 11, 64-bit, (Reduced to) 4 GB RAM
- Software used: Wireshark

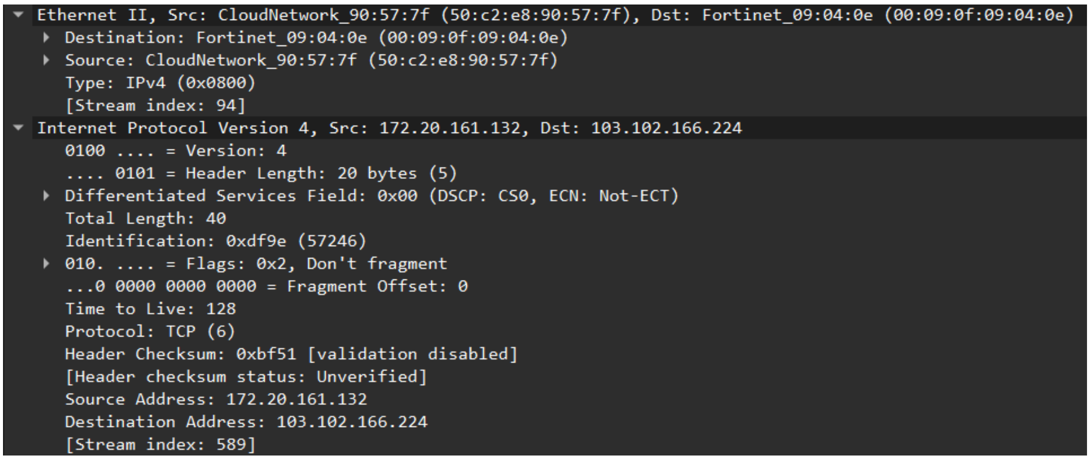
Procedure

1. Open Wireshark on Windows PC.
2. Apply a filter to capture packets from a particular website, e.g., wikipedia.org (with filter: ip.addr == 103.102.166.224.



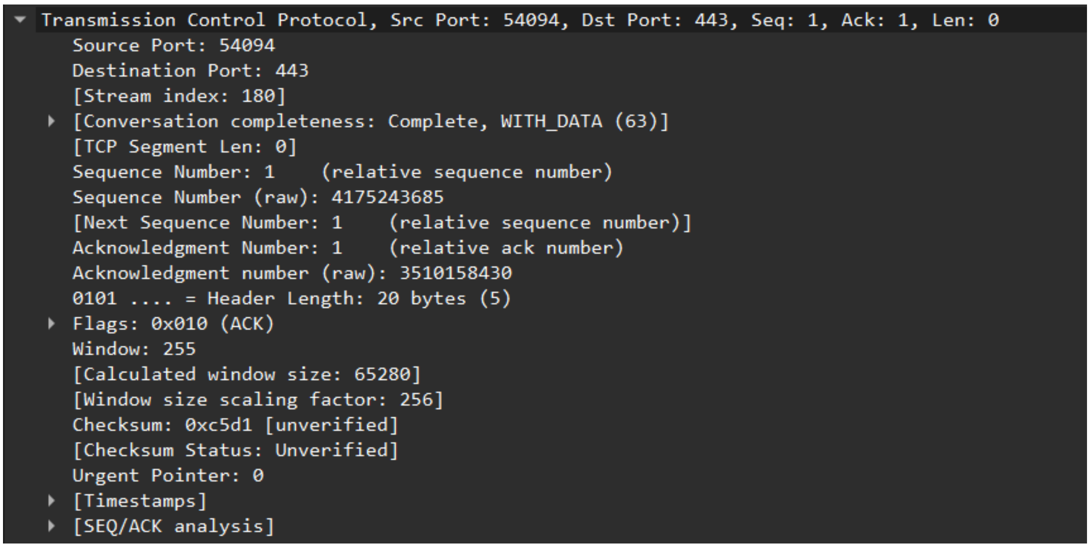
```
▾ Frame 30918: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B4722742-94ED-4B90-812E-C3DC51B8B97E}, id 0
    Section number: 1
  ▸ Interface id: 0 (\Device\NPF_{B4722742-94ED-4B90-812E-C3DC51B8B97E})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 25, 2025 22:07:58.007828000 India Standard Time
    UTC Arrival Time: Feb 25, 2025 16:37:58.007828000 UTC
    Epoch Arrival Time: 1740501478.007828000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000245000 seconds]
    [Time delta from previous displayed frame: 0.000245000 seconds]
    [Time since reference or first frame: 340.059216000 seconds]
    Frame Number: 30918
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
```

Figure 1: Frame header



```
▾ Ethernet II, Src: CloudNetwork_90:57:7f (50:c2:e8:90:57:7f), Dst: Fortinet_09:04:0e (00:09:0f:09:04:0e)
  ▸ Destination: Fortinet_09:04:0e (00:09:0f:09:04:0e)
  ▸ Source: CloudNetwork_90:57:7f (50:c2:e8:90:57:7f)
    Type: IPv4 (0x0800)
    [Stream index: 94]
▾ Internet Protocol Version 4, Src: 172.20.161.132, Dst: 103.102.166.224
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xdf9e (57246)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xbf51 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.161.132
    Destination Address: 103.102.166.224
    [Stream index: 589]
```

Figure 2: Ethernet and IP header

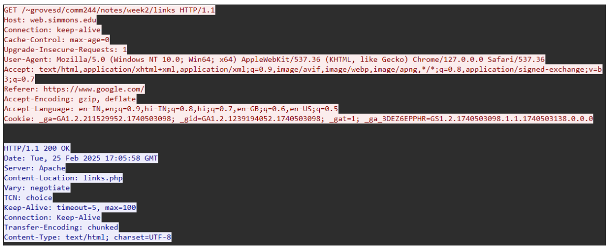


```
▾ Transmission Control Protocol, Src Port: 54094, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 54094
    Destination Port: 443
    [Stream index: 180]
  ▸ [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4175243685
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3510158430
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x010 (ACK)
    Window: 255
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
    Checksum: 0xc5d1 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
```

Figure 3: TCP header

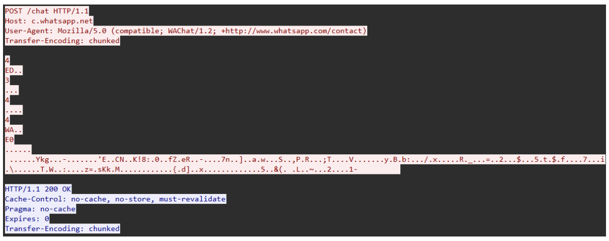
Packet headers for each layers are shown.

3. Capture a HTTP packet by using the filter 'http'. Right click on a packet. Go to Follow → HTTP Stream.



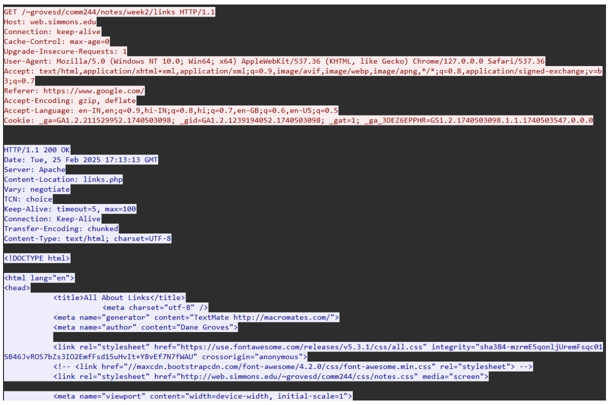
```
GET /~grovesd/comm244/notes/week2/links HTTP/1.1
Host: web.simmons.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.7
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-IN,en;q=0.9,hi-IN;q=0.8,hi;q=0.7,en-GB;q=0.6,en-US;q=0.5
Cookie: _ga=GA1.2.211529952.1740503098; _gid=GA1.2.1239194052.1740503098; _gat=1; _ga_3DEZ6EPPHR=GS1.2.1740503098.1.1.1740503138.0.0.0


HTTP/1.1 200 OK
Date: Tue, 25 Feb 2025 17:05:58 GMT
Server: Apache
Content-Location: links.php
Vary: negotiate
TCN: choice
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Figure 4: Following HTTP Stream



```
POST /chat HTTP/1.1
Host: c.whatsapp.net
User-Agent: Mozilla/5.0 (compatible; WAChat/1.2; +http://www.whatsapp.com/contact)
Transfer-Encoding: chunked

4
ED..
3
...
4
....
4
WA..
E0
......
 ......Ykg...-.......'E..CN..K!8:.0..fZ.eR..-....7n..]..a.w...S..,P.R...;T....V.......y.B.b:.../.x.....R._...=..2...$...5.t.$.f....7...i
.\......T.W..:....z=.sKk.M...........{.d]..x............5..&(. .L..~...2....1-

HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Transfer-Encoding: chunked
```

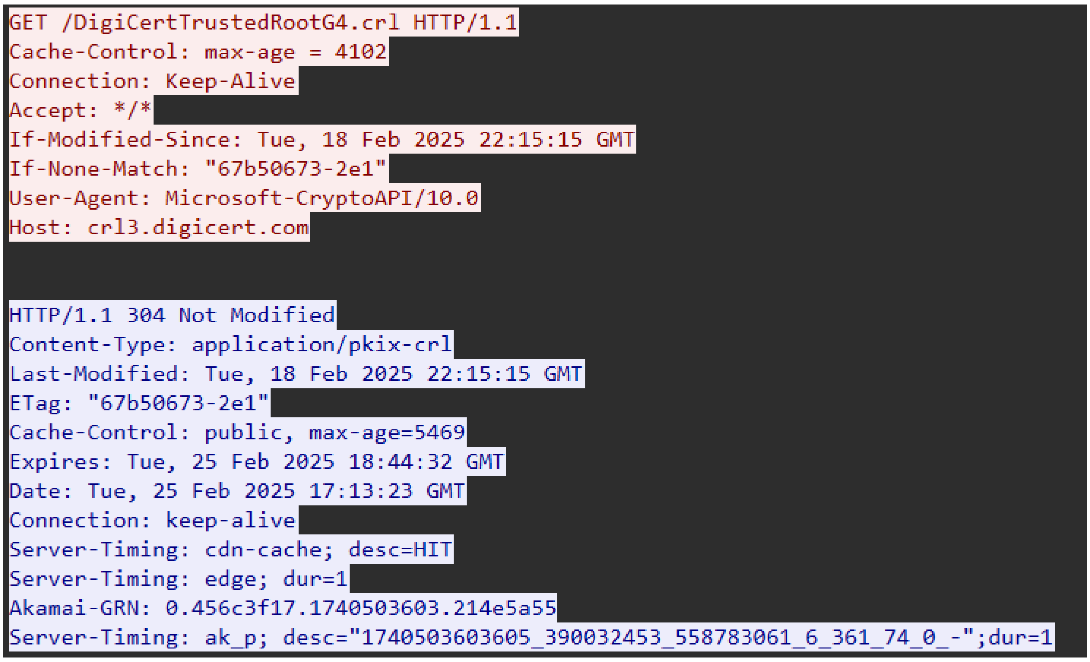
Figure 5: Following 2nd HTTP Stream



```
GET /~grovesd/comm244/notes/week2/links HTTP/1.1
Host: web.simmons.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.7
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-IN,en;q=0.9,hi-IN;q=0.8,hi;q=0.7,en-GB;q=0.6,en-US;q=0.5
Cookie: _ga=GA1.2.211529952.1740503098; _gid=GA1.2.1239194052.1740503098; _gat=1; _ga_3DEZ6EPPHR=GS1.2.1740503098.1.1.1740503547.0.0.0


HTTP/1.1 200 OK
Date: Tue, 25 Feb 2025 17:13:13 GMT
Server: Apache
Content-Location: links.php
Vary: negotiate
TCN: choice
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>

<html lang="en">
<head>
           <title>All About Links</title>
                      <meta charset="utf-8" />
           <meta name="generator" content="TextMate http://macromates.com/">
           <meta name="author" content="Dane Groves">

           <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-mzrmE5qonljUremFsqc01
SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">
           <!-- <link href="//maxcdn.bootstrapcdn.com/font-awesome/4.2.0/css/font-awesome.min.css" rel="stylesheet"> -->
           <link rel="stylesheet" href="http://web.simmons.edu/~grovesd/comm244/css/notes.css" media="screen">

           <meta name="viewport" content="width=device-width, initial-scale=1">
```

Figure 6: Following 3rd HTTP Stream

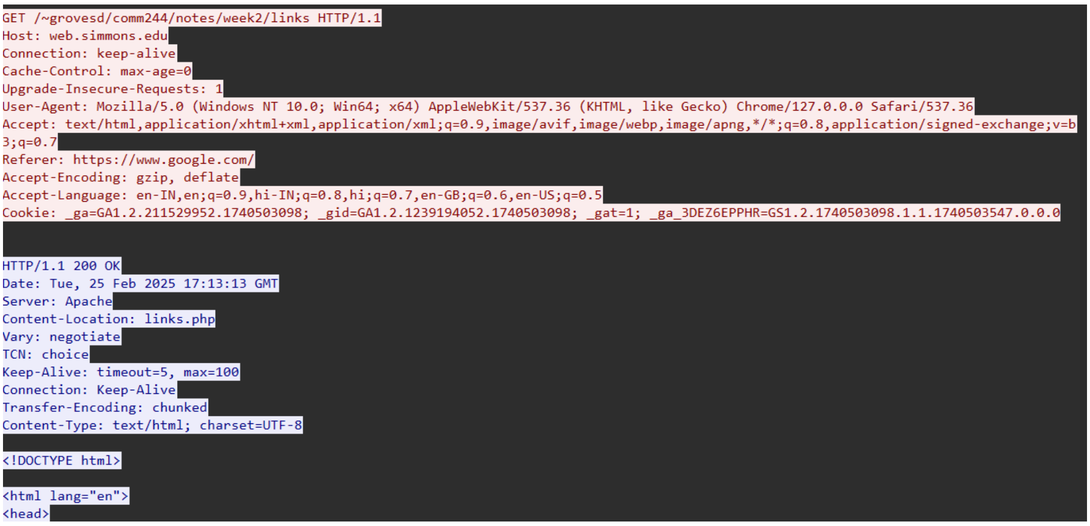
4. Follow another http packet with filter 'http.response.code == 304'.



```
GET /DigiCertTrustedRootG4.crl HTTP/1.1
Cache-Control: max-age = 4102
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Tue, 18 Feb 2025 22:15:15 GMT
If-None-Match: "67b50673-2e1"
User-Agent: Microsoft-CryptoAPI/10.0
Host: crl3.digicert.com


HTTP/1.1 304 Not Modified
Content-Type: application/pkix-crl
Last-Modified: Tue, 18 Feb 2025 22:15:15 GMT
ETag: "67b50673-2e1"
Cache-Control: public, max-age=5469
Expires: Tue, 25 Feb 2025 18:44:32 GMT
Date: Tue, 25 Feb 2025 17:13:23 GMT
Connection: keep-alive
Server-Timing: cdn-cache; desc=HIT
Server-Timing: edge; dur=1
Akamai-GRN: 0.456c3f17.1740503603.214e5a55
Server-Timing: ak_p; desc="1740503603605_390032453_558783061_6_361_74_0_-";dur=1
```

Figure 7: Cache based packet

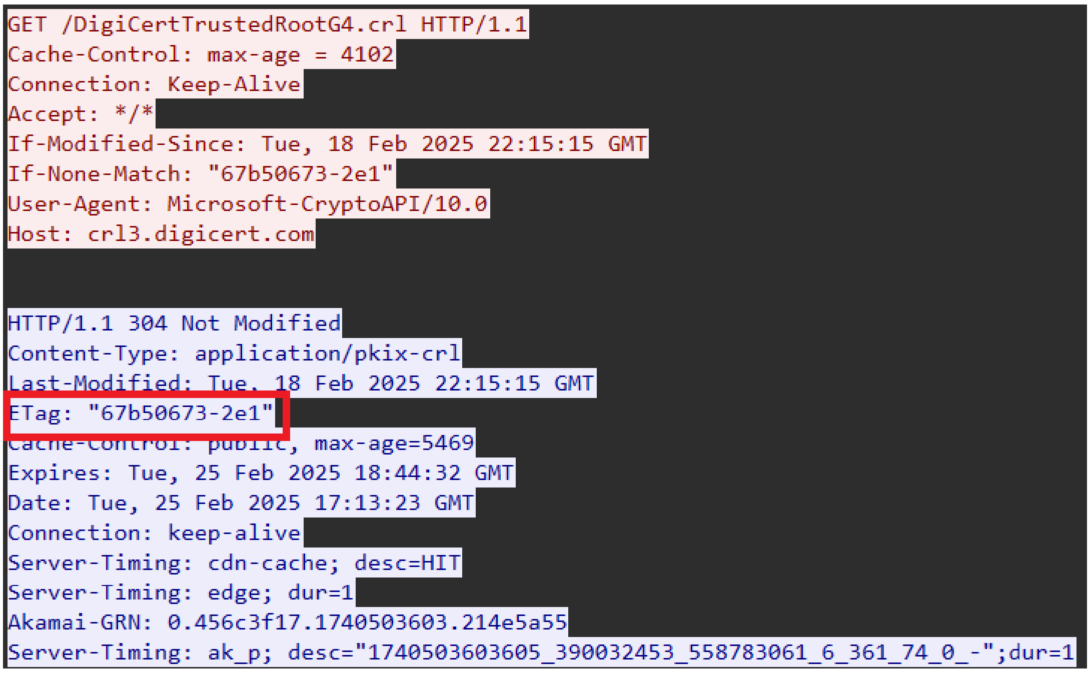
5. Follow another http packet with filter 'http.cookie'.



```
GET /~grovesd/comm244/notes/week2/links HTTP/1.1
Host: web.simmons.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.7
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-IN,en;q=0.9,hi-IN;q=0.8,hi;q=0.7,en-GB;q=0.6,en-US;q=0.5
Cookie: _ga=GA1.2.211529952.1740503098; _gid=GA1.2.1239194052.1740503098; _gat=1; _ga_3DEZ6EPPHR=GS1.2.1740503098.1.1.1740503547.0.0.0


HTTP/1.1 200 OK
Date: Tue, 25 Feb 2025 17:13:13 GMT
Server: Apache
Content-Location: links.php
Vary: negotiate
TCN: choice
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>

<html lang="en">
<head>
```

Figure 8: Cookie based packet

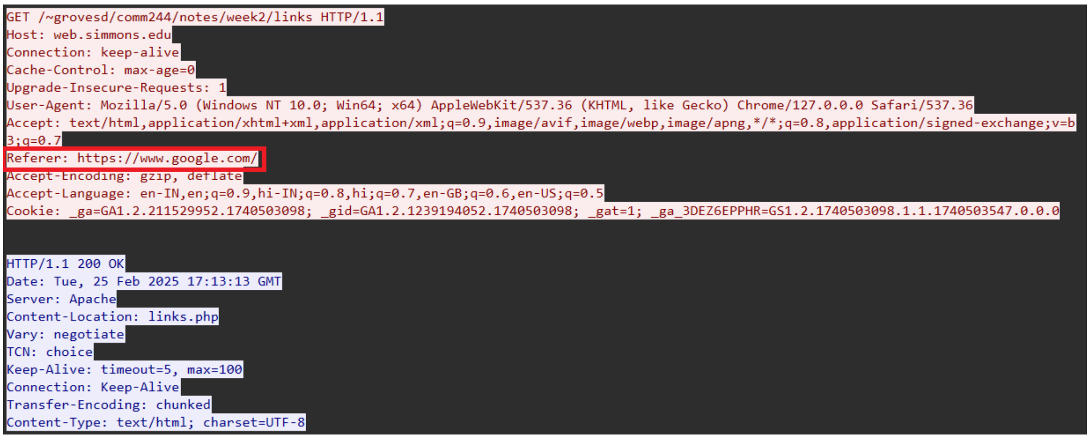
6. Follow another http packet with filter 'http contains "ETag"'.



```
GET /DigiCertTrustedRootG4.crl HTTP/1.1
Cache-Control: max-age = 4102
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Tue, 18 Feb 2025 22:15:15 GMT
If-None-Match: "67b50673-2e1"
User-Agent: Microsoft-CryptoAPI/10.0
Host: crl3.digicert.com


HTTP/1.1 304 Not Modified
Content-Type: application/pkix-crl
Last-Modified: Tue, 18 Feb 2025 22:15:15 GMT
ETag: "67b50673-2e1"
Cache-Control: public, max-age=5469
Expires: Tue, 25 Feb 2025 18:44:32 GMT
Date: Tue, 25 Feb 2025 17:13:23 GMT
Connection: keep-alive
Server-Timing: cdn-cache; desc=HIT
Server-Timing: edge; dur=1
Akamai-GRN: 0.456c3f17.1740503603.214e5a55
Server-Timing: ak_p; desc="1740503603605_390032453_558783061_6_361_74_0_-";dur=1
```

Figure 9: ETag header

7. Follow another http packet with filter 'http contains "Referer"'.



```
GET /~grovesd/comm244/notes/week2/links HTTP/1.1
Host: web.simmons.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.7
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-IN,en;q=0.9,hi-IN;q=0.8,hi;q=0.7,en-GB;q=0.6,en-US;q=0.5
Cookie: _ga=GA1.2.211529952.1740503098; _gid=GA1.2.1239194052.1740503098; _gat=1; _ga_3DEZ6EPPHR=GS1.2.1740503098.1.1.1740503547.0.0.0


HTTP/1.1 200 OK
Date: Tue, 25 Feb 2025 17:13:13 GMT
Server: Apache
Content-Location: links.php
Vary: negotiate
TCN: choice
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Figure 10: Referer header

Observations

- A particular type of packet can be captured by searching with the corresponding filter, e.g., for a particular address, or a protocol.
- Encapsulation refers to adding headers to data as it moves through the layers of a network. Different header for each layer can be viewed in Wireshark as shown.
- HTTP packet can be captured by using the filter 'http'. Follow the HTTP stream to view the request and response sent in the communication, as shown. The request contains various field like GET, connection, host, user-agent with the corresponding values. The response contains field like status code, server, content-length, content-type and the html content.
- A cache based packet can be recognised by the status code '304 Not Modified', filtered using 'ttp.response.code == 304'. This means the client used a previously stored copy instead of downloading again.
- A cookie based packet can be identified with filter 'http.cookie'. They are used for session management and tracking.
- Two additional headers:
  - Etag: Used for cache validation by uniquely identifying a resource version.
  - Referer: Indicates the previous page that linked to the requested resource.

Conclusions

- Wireshark provides various tools like filtering to capture a packet with particular identification. It allows following stream to view request-response communication to see the actual communication going on between the server and the client. Additionally, each layer in the communication adds an header which can be viewed in the Wireshark.