CS331 Assignment 1

Github Link: https://github.com/aayush8991/CS-331-Assign1

Aayush Parmar (22110181)
Bhoumik Patidar (22110049)

Part 1: Metrics and Plots Report

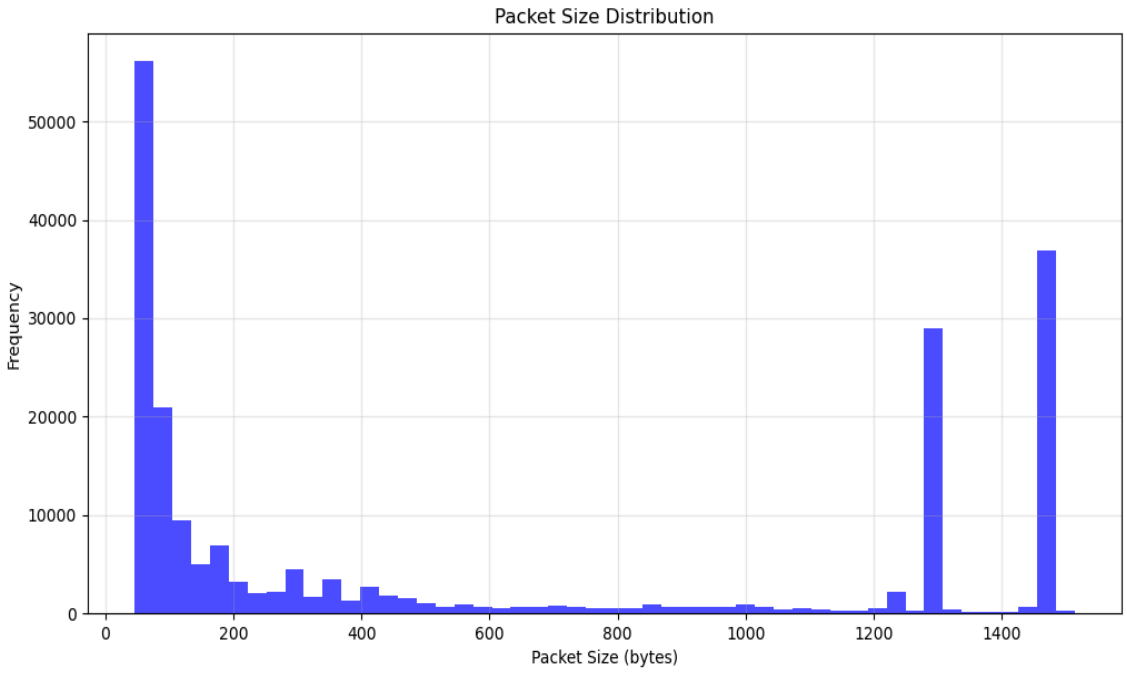
Following metrics were extracted for the data as captured by sniffer.py (code in github link above) by performing the pcap replay using tcpreplay.

1. Data Transfer Analysis

Total Data Transferred and Packet Statistics:

Total data: 134,996,148 bytes
Total packets: 246,519
Min packet size: 42 bytes
Max packet size: 1,514 bytes
Avg packet size: 547.61 bytes

Histogram of Packet Sizes:



2. Unique Source-Destination Pairs

Number of unique source-destination pairs: 9,615

The whole list of the pairs is present in pcap_detailed_analysis.txt uploaded on github repo.

---

3. IP Flow Statistics

The source IP flow counts are:

=== Top 10 Source IP Flows ===

10.240.0.249: 47,210 flows

23.52.40.154: 16,490 flows

151.101.2.133: 12,403 flows

52.123.129.14: 8,897 flows

142.250.193.36: 7,789 flows

10.0.136.7: 5,658 flows

10.240.1.72: 4,691 flows

142.250.70.100: 3,391 flows

10.240.8.31: 3,149 flows

10.7.11.235: 2,543 flows

The destination IP flow counts are:

=== Top 10 Destination IP Flows ===

10.240.0.249: 95,972 flows

224.0.0.251: 33,101 flows

10.7.11.235: 7,897 flows

255.255.255.255: 6,945 flows

10.0.136.7: 6,726 flows

10.240.31.255: 5,884 flows

23.52.40.154: 4,752 flows

239.255.255.250: 4,624 flows

142.250.193.36: 2,837 flows

10.240.8.31: 2,791 flows

The rest of the dictionary has been stored in a file named pcap_detailed_analysis.txt.

=== Maximum Data Flow ===

Source: 23.52.40.154:443

Destination: 10.240.0.249:59231

Data transferred: 19,798,738 bytes

4. Performance Evaluation (pps & mbps)

A.Same Machine (VM)

The tcpreplay at 500pps:

```
Statistics for network device: eth0
        Successful packets:        3302
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

The captured packets are as below:

```
Total Packets: 3303
Total Data: 2567450 bytes
Min Packet Size: 54 bytes
Max Packet Size: 1514 bytes
Avg Packet Size: 779.91 bytes
```

B. Different Machines (Two VMs)

Running tcpreplay at 500 pps {2.19Mbps) on Kali Linux and forwarding packets to sniffer program running on Ubuntu, we get the following results

- On speed of 1250 pps there is no loss in packets.

```
ubuntu@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Bhoumik_CN_A1/CS-331-Assign1$ sudo tcpreplay -p 1250 -i eth0
 7.pcap
^C User interrupt...
sendpacket_abort
Actual: 4512 packets (3694340 bytes) sent in 3.60 seconds
Rated: 1023772.9 Bps, 8.19 Mbps, 1250.36 pps
Statistics for network device: eth0
        Successful packets:        4511
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

```
=== Capture Summary ===
Duration: 13.24 seconds
Total Packets: 4512
Total Data: 3693698 bytes
Min Packet Size: 54 bytes
Max Packet Size: 1514 bytes
Avg Packet Size: 820.64 bytes
```

- On speed of 1500 pps loss of packets is there

```
ubuntu@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Bhoumik_CN_A1/CS-331-Assign1$ sudo tcpreplay -p 1500 -i eth0
 7.pcap
^C User interrupt...
sendpacket_abort
Actual: 8299 packets (7146237 bytes) sent in 5.53 seconds
Rated: 1291828.3 Bps, 10.33 Mbps, 1500.21 pps
Statistics for network device: eth0
        Successful packets:        8298
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

```
=== Capture Summary ===
Duration: 15.21 seconds
Total Packets: 8255
Total Data: 7105389 bytes
Min Packet Size: 54 bytes
Max Packet Size: 1514 bytes
Avg Packet Size: 861.89 bytes
```

Part 2: Packet Analysis

1. No Matching Packets Found

2. SYN Packet Analysis

Total SYN Packets Matching Criteria: 223

Complete list is present on github as tcp_analysis_results.txt.

3. Specific IP and Port Matches

```
Analyzing packets for specific IP and port conditions...
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Specific Match Found: Source IP: 18.234.0.179, Destination IP: 10.7.11.235, Source Port: 443, Destination Port: 53251
Total number of packets matching the specific IP and port criteria: 11
```

4. Sequence and Acknowledgment Match

```
Python
Analyzing packets for Sequence + Acknowledgment conditions...
Sequence + Acknowledgment Match Found: Source IP: 10.240.8.31, Destination IP: 10.7.11.235, Source Port: 8009, Destination Port: 53669, Sequence: 1376971233
```

Part 3: Capture the Packets (20 Points)

1. Wireshark Packet Capture and Protocol Analysis

Five Application-Layer Protocols Not Commonly Discussed in Classrooms

a. XMPP (Extensible Messaging and Presence Protocol)

- Usage: Used for real-time communication such as instant messaging, presence information, and multimedia streaming. Operates on top of TCP and uses XML for message exchange.
- Layer : Application
- RFC: RFC 6120

b. IMAP (Internet Message Access Protocol)

- Usage: Allows email clients to access messages stored on a mail server, providing functionalities like message syncing and server-side folder management.
- Layer : Application
- RFC: RFC 3501

c. TLS 1.3 (Transport Layer Security Version 1.3)

- TLS 1.3 is a cryptographic protocol that provides secure communication over a network by encrypting data transmissions between clients and servers. It improves upon previous versions by reducing handshake latency, enhancing security, and removing outdated cryptographic algorithms.
- Layer : Transport
- RFC: RFC 8446

d. SIP (Session Initiation Protocol)

- Usage: Used to initiate, maintain, and terminate multimedia communication sessions, including VoIP calls, video conferencing, and instant messaging.
- Layer : Application
- RFC: RFC 3261

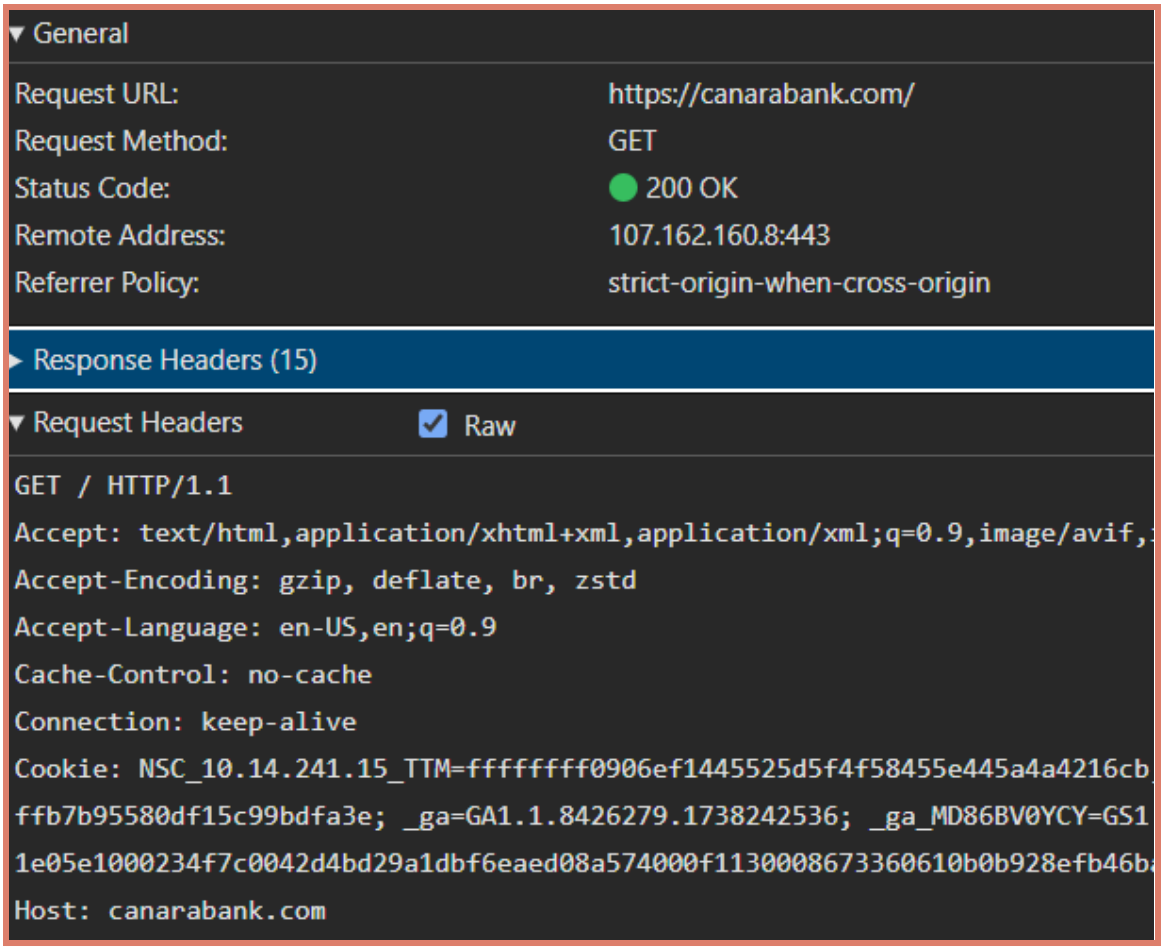
E. QUIC ((Quick UDP Internet Connections)

- QUIC is a designed to provide faster, more reliable, and secure internet connections by reducing connection establishment latency and improving congestion control. It is widely used by HTTP/3 to enhance web performance.
- Layer : Transport
- RFC: RFC 9000

---

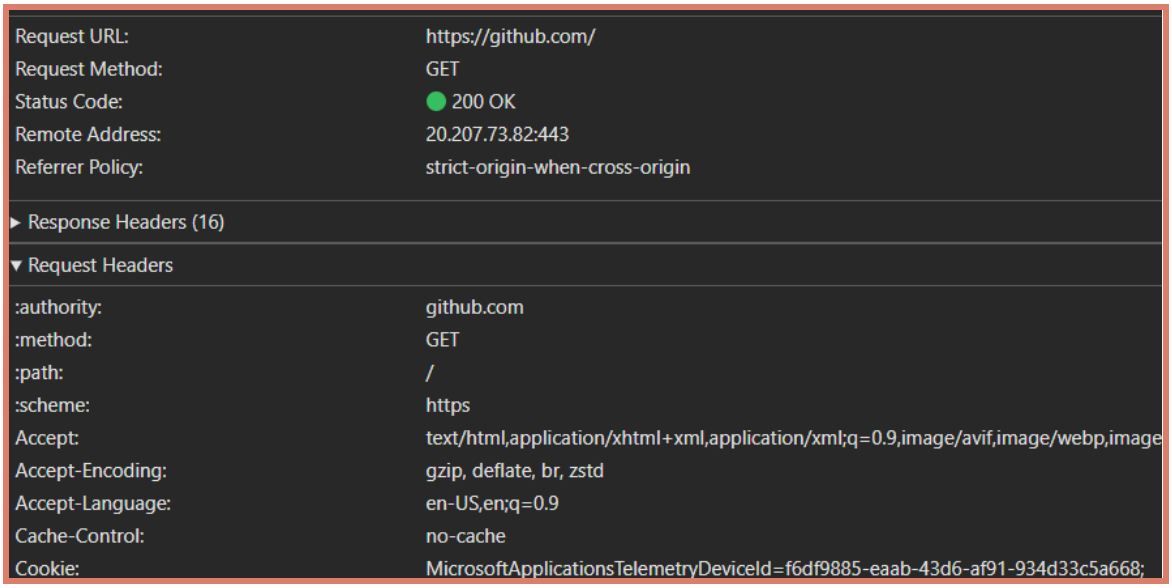
2. Website Analysis: canarabank.in, github.com, netflix.com

a. CanaraBank.in



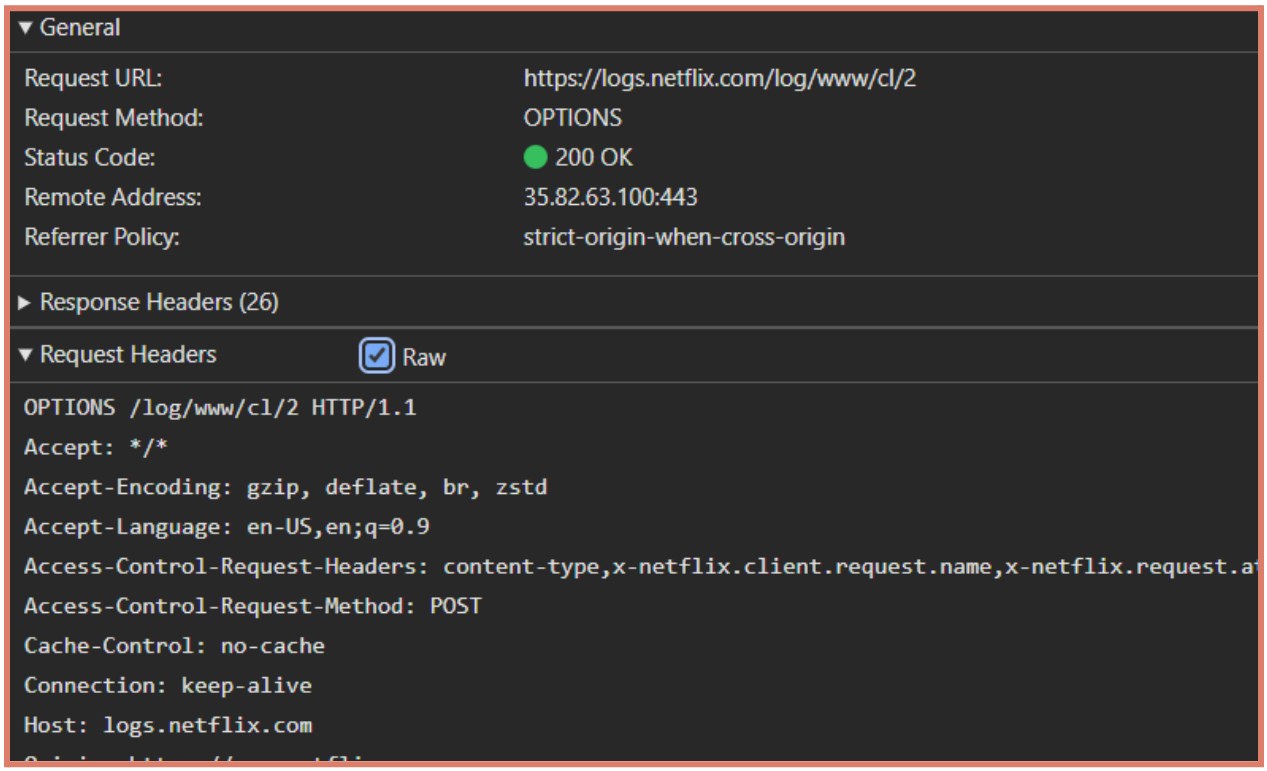
The Connection is PERSISTENT

Github



The connection is PERSISTENT.

Netflix.com



The connection is PERSISTENT.

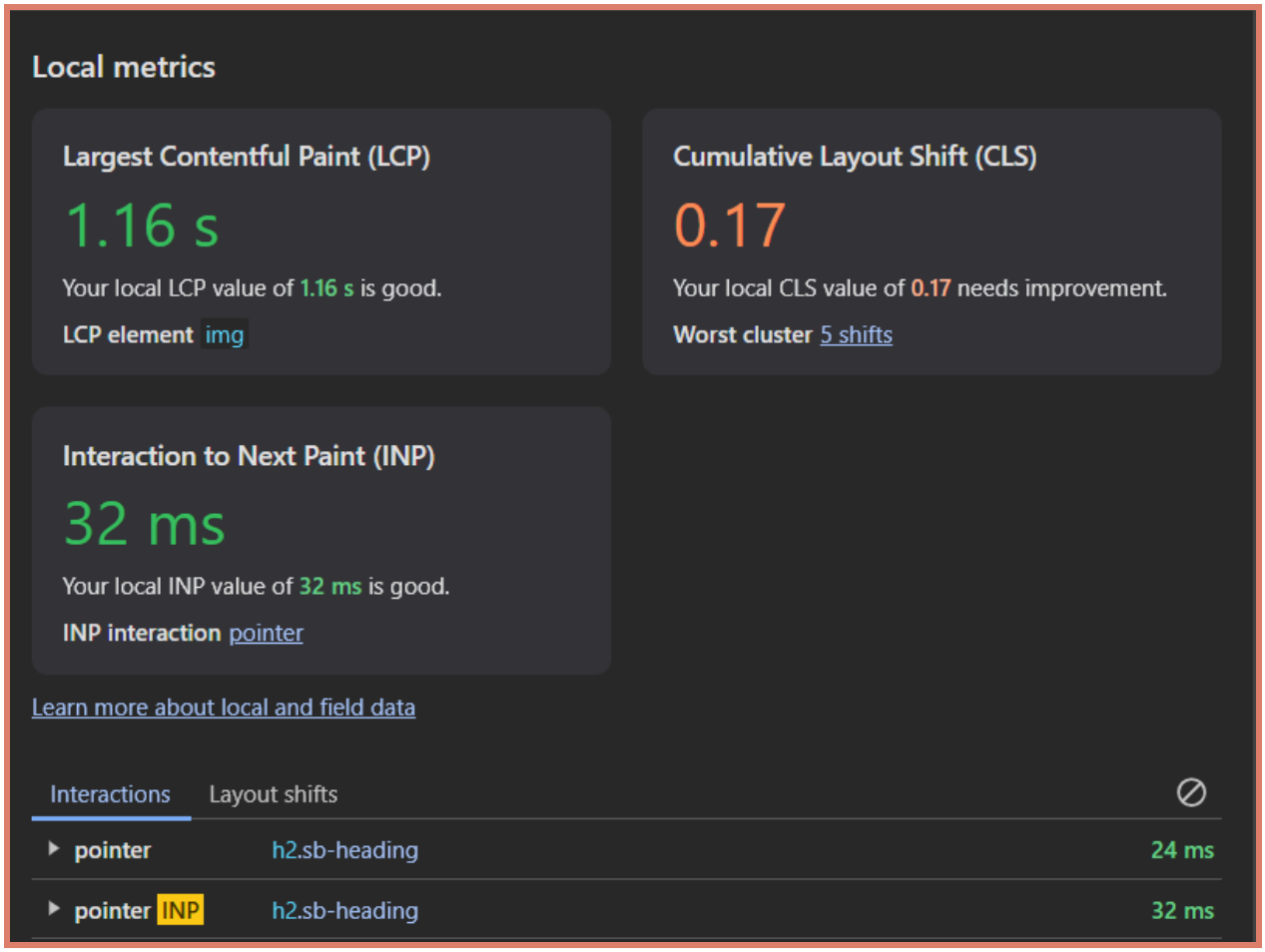
b. The header field names are:
   1. Accept-Encoding: `gzip, deflate, br, zstd`
   2. Accept-Language: `en-US,en;q=0.9`

3. Access-Control-Request-Headers: `content-type,x-netflix.client.request.name,x-netflix.request.a`
4. Access-Control-Request-Method: POST

HTTP Error Codes Encountered

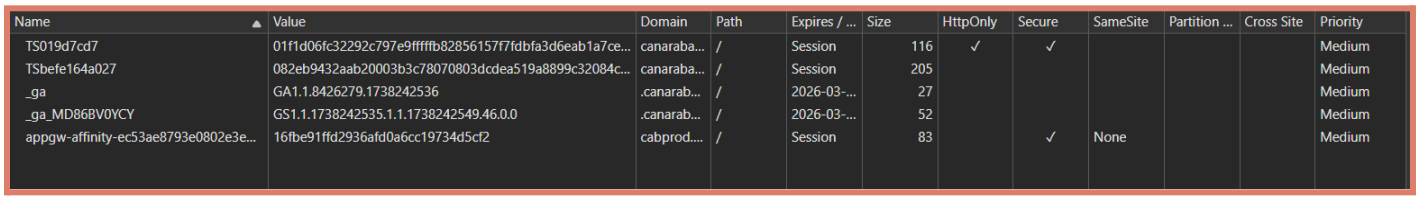
1. 404 Not Found: Occurs when the server cannot find the requested resource. Often due to incorrect URLs or missing files.
    - Example: `HTTP/1.1 404 Not Found`
2. 500 Internal Server Error: Indicates a server-side error due to misconfiguration or application issues.
    - Example: `HTTP/1.1 500 Internal Server Error`
3. 403 Forbidden: The server understands the request but refuses to authorize it, often due to permissions.
    - Example: `HTTP/1.1 403 Forbidden`

c. Browser Performance Metrics and Cookies on Google Chrome



- Cookies and Associated Flags Captured in Request and Response Headers:
    - `Accurate ECN`: Not set
    - `Congestion Window Reduced`: Not set

- ECN-Echo: Not set
- Acknowledgment: Set
- Push: Not set
- Reset: Not set
- Syn: Set
- Fin: Not set



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Cross Site	Priority
TS019d7cd7	01f1d06fc32292c797e9fffffb82856157f7fdbfa3d6eab1a7ce...	canaraba...	/	Session	116	✓	✓				Medium
TSbefe164a027	082eb9432aab20003b3c78070803dcdea519a8899c32084c...	canaraba...	/	Session	205						Medium
_ga	GA1.1.8426279.1738242536	.canarab...	/	2026-03-...	27						Medium
_ga_MD86BV0YCY	GS1.1.1738242535.1.1.1738242549.46.0.0	.canarab...	/	2026-03-...	52						Medium
appgw-affinity-ec53ae8793e0802e3e...	16fbe91ffd2936afd0a6cc19734d5cf2	cabprod....	/	Session	83		✓	None			Medium