Computer Networks

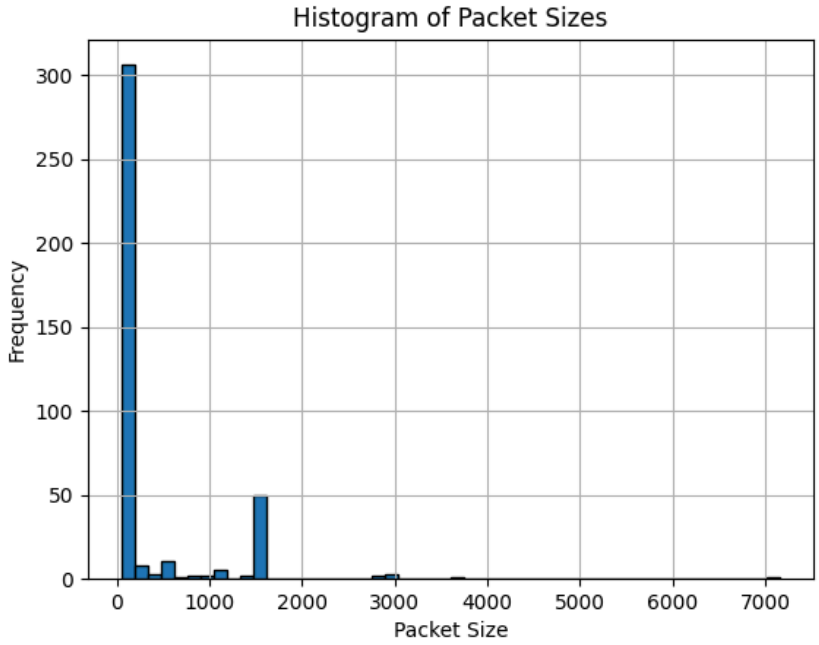
Part 1:

Data and Packet Metrics

- **Total Data Transferred:** 144,520 bytes
- **Total Packets Transferred:** 397
- **Minimum Packet Size:** 42 bytes
- **Maximum Packet Size:** 7,165 bytes
- **Average Packet Size:** 364.03 bytes

Maximum Packet Details

- **Packet Size:** 7,165 bytes
- **Source IP:** 10.0.2.15
- **Destination IP:** 52.168.117.175
- **Source Port:** 53,030
- **Destination Port:** 443
- **Packet Raw Data:** Ether / IP / TCP 10.0.2.15:53030 > 52.168.117.175:https PA / Raw



Part 2:

Q1: Extracting the IP Address from a TCP Packet

The IP address found in the TCP packet containing the message "< my ip address = >" is:
10.1.2.200

Q2: Counting Packets with the Identified IP Address

The total number of packets that contain the IP address **10.1.2.200** is:
80 packets

Q3: Extracting Laptop Name and TCP Checksum

(a) **Laptop Name Found in a TCP Packet:**
lenovo

(b) **TCP Checksum of the Packet Containing the Laptop Name:**
0x0a61

Q4: Counting Packets Containing "Order successful"

The total number of packets that contain the message "**Order successful**" is:
40 packets

Part 3: Capture the packets

1)

Syslog Protocol

- **Operation:** Syslog is used for message logging, allowing devices such as routers, switches, and servers to send log messages to a central server for monitoring and debugging.
- **Layer:** Application Layer
- **RFC:** RFC 5424

LDAP (Lightweight Directory Access Protocol)

- **Operation:** LDAP is used for querying and modifying directory services, commonly used for authentication and centralized user management in enterprise networks.
- **Layer:** Application Layer

- **RFC:** RFC 4519

NNTP (Network News Transfer Protocol)

- **Operation:** NNTP is used to distribute, retrieve, and post news articles (Usenet newsgroups) over the Internet. It is mainly used for online discussion forums.
- **Layer:** Application Layer
- **RFC:** RFC 3977

BGP (Border Gateway Protocol)

- **Operation:** BGP is used for exchanging routing information between autonomous systems (AS) on the Internet. It is essential for global Internet routing.
- **Layer:** Application Layer
- **RFC:** RFC 4271

SMTP (Simple Mail Transfer Protocol)

- **Operation:** SMTP is used for sending and forwarding email messages between mail servers. It operates on a push model, meaning emails are sent from a client to a mail server and then relayed to the recipient's server. SMTP works alongside protocols like IMAP and POP3 for email retrieval.
- **Layer:** Application Layer
- **RFC:** RFC 5321

2)

Netflix

- **IP Address:** 54.74.73.31:443
- **Request Line:** GET / HTTP/2
- **Response Headers:**
    - accept-ch: Sec-CH-UA-Platform-Version,Sec-CH-UA-Model
    - cache-control: no-cache, no-store
    - content-security-policy-report-only: Specifies security policies for content sources.
- **Request Headers:**
    - accept: Various MIME types accepted, including HTML, images, and application data.
    - accept-encoding: Supports compression formats like gzip, deflate, and br.
    - accept-language: en-US,en;q=0.9
- **Connection: Not Persistent**

GitHub

- **IP Address:** 20.207.73.82:443

- **Request Line:** GET / HTTP/2
- **Response Headers:**
    - content-type: text/html; charset=utf-8
    - date: Sat, 01 Feb 2025 15:51:54 GMT
    - etag: W/"59eb3c5ca3c41c4bf99e43c360a81bef"
- **Request Headers:**
    - accept: Similar to Netflix, allowing multiple MIME types.
    - accept-encoding: Supports gzip, deflate, br, and zstd.
    - accept-language: en-US,en;q=0.9
- **Connection: Not Persistent**

Canara Bank

- **IP Address:** 107.162.160.8:443
- **Request Line:** GET / HTTP/1.1
- **Response Headers:**
    - connection: close
    - content-security-policy: Defines security rules for scripts, styles, and images.
    - content-type: text/html; charset=utf-8
- **Request Headers:**
    - accept: Accepts various content types, similar to Netflix and GitHub.
    - accept-encoding: Supports gzip, deflate, br, and zstd.
    - accept-language: en-US,en;q=0.9
- **Connection: Persistent**

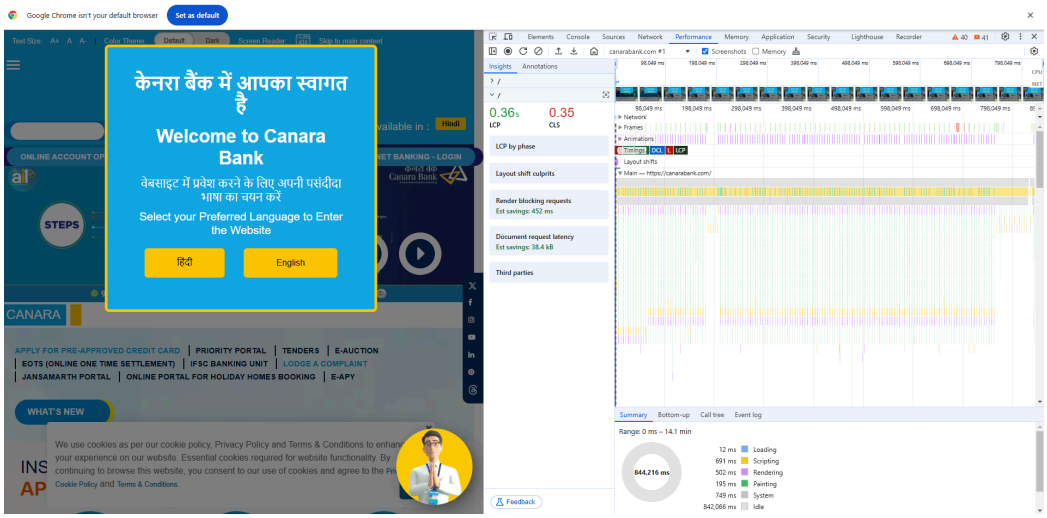
We are not encountering any HTTP error codes, but this could potentially be the error.

1. 404 Not Found:
    - The server cannot find the requested page. This error occurs when the URL does not point to a valid resource on the server.
2. 500 Internal Server Error:
    - The server encountered an unexpected condition that prevented it from fulfilling the request. This error is often due to issues within the server's code or configuration.
3. 403 Forbidden:
    - The server understands the request but refuses to authorize it. This can happen if the user doesn't have permission to access the requested resource.

3)

Browser : Chrome

screenshot of the performance metrics for canara bank



For Netflix:

Set-Cookie:	flwssn=ce5e6d19-c9f1-43fd-a0dd-29fb6c37c776; Max-Age=10800; Domain=.netflix.com; Path=/

Cookie:	flwssn=ce5e6d19-c9f1-43fd-a0dd-29fb6c37c776; nfvdid=BQFmAAEBENI07JO1qbZJ3wUA6B6vaspAHjxbUvKS-bhq8ORU5rfw88xTCdSQtZnf8_tXqMHBvOVo5ciKw4TJiAydPu0IoKZ2WW9FmTNd7EcJ3gzQgDYggQ%3D%3D; SecureNetflixId=v%3D3%26mac%3DAQEAEQABABQRm8EygEP10mRaienRAGRbCFnBwHYd5-o.%26dt%3D1738424463633; NetflixId=v%3D3%26ct%3DBgjHlOvcAxLAAUtVVrnyaBJL4ujTaGnqmu8WVBWJOfHlizPV0FDJb23VHN-XyXd2MsNFDgEsigjH8XOJNV9N-xUzkiWSn45e7_RwfpYY77DALjykwYF7XgNmZsaL2IXU-5eUq3W8GYiNPUgDjk7K5ks_tOSpJ7Iw6A4Xh8IKkG1OeSQMp_y4RaRS9gdbX93zzm34ev0nULDhQ5cmcGjQ3mJ_p8ybhR-DpNeLqRRWhhQ8eeMVd8TEZG8dn0q288aIr0n8BUA6ck65ExgGIg4KDHCsqNooit5cbmonZg..; OptanonConsent=isGpcEnabled=0&datestamp=Sat+Feb+01+2025+21%3A19%3A47+GMT%2B0530+(India+Standard+Time)&version=202411.1.0&browserGpcFlag=0&isIABGlobal=false&hosts=&consentId=47f66887-3c40-4d3d-b423-4b88edcda0c3&interactionCount=1&isAnonUser=1&landingPath=https%3A%2F%2Fwww.netflix.com%2Fin%2F&groups=C0001%3A1%2CC0002%3A1%2CC0003%3A1%2CC0004%3A1

The associated flags for the given cookie are:

1. **Max-Age=10800**: This indicates that the cookie will expire after 10,800 seconds (or 3 hours).
2. **Domain=.netflix.com**: The cookie is valid for any subdomain of netflix.com.

3. **Path=/**: The cookie is valid for the entire domain (i.e., all paths within the domain)