1.
- a.
  DNS Server Contacted: 1.1.1.1
  Request Epoch Time: 1603822039.762266412 Seconds
  Response Epoch Time: 1603822039.775940328 Seconds
  Total Time Taken: 0.137 Seconds
- b.
  I could see around 40 diffrent objects like PNGs, JPEGs, CSS, Javascripts, text and json requests getting loaded.
  This tells me that the whole webpage is broken into various small objects that are then sent over the network one by one. In the trace I could see that the Images were requested towards the end, suggesting that the more important components (like text) are prioritized than others (like images) so that a user can atleast start reading the content of the page as soon as possible while the images load.
- c.
  - Laptop to Server: 9 Connections. Port Numbers: 365(36, 40, 42, 48, 50, 52, 54, 56, 60) to 80 i.e. port 36536 to port 80 and so on.
  - Server to Laptop: 9 more Connections. Reverse of the previous port number
- d. 8 of the previous connections (except 80 to 36536) from server to laptop were used to fetch content using HTTP.
- e. Let 1.5*RTT be the duration of the handshake.
  RTT=Epoch Time of Syn-Ack - Epoch Time of Syn
  - port 36540's handshake.
    Epoch time of Syn: 1603823949.608056036 Seconds
    Epoch Time for Syn-Ack: 1603823949.657342096 Seconds.
    Handshake Duration: 0.739 Seconds
  - Port 36550's handshake.
    Epoch time of Syn: 1603823950.693742231 Seconds
    Epoch time of Syn-Ack: 1603823950.743294313 Seconds
    Handshake Duration: 0.743 Seconds

  The duration of port 36550 might be greater that that of 36540 because the network was busy for handling requests from other ports as well (36552, 36554, 36556).
  Since the duration of a handshake is high, one can send multiple data requests between two handshakes to decrease latencies.
- f.
  Epoch Time of DNS request: 1603823949.589542953 Seconds
  Epoch Time of last HTTP object request: 1603823951.628573533 Seconds
  Time to Load: 2.039 Seconds
- g.
  I could not see any HTTP traffic being generated. This is because Indian Express uses https which is secure and encrypted.

2.
- a. Indian Express might be using HTTPS which is encrypted and does not allow third party apps to sniff packets. Since the browser requested the information, it has access to it and thus I was able to see the objects.
- b. I could see around 220 different object in the inspector window of Firefox.
  I could also see some objects from non Indian express domain.

  - One was from google accounts, maybe for sign in purposes.
  - I also saw some objects from google analytics, indicating that Indian express might have outsourced some of its user activity analytics to google.
  - Some were from doubleclick. For advertisements.
  - Some objects from scorecard research which is a firm similar to google analytics and collects data online.
  - Some from wzrkt.com, a SaaS analytics firm.
- c. There was a png file called sprite of about 70.67 KBs which took about 11ms to be received (not considering the waiting time.) The average throughput is 6.42 MB/s.
- d. I could see around 210 objects on nytimes.com.
  This tells me that a good webpage should be broken into smaller objects and be loaded in some order so that the user can start surfing as soon as possible even if ze have connectivity issues.
- e. Yes in my opinion the optimizations that the browser do is important. If it loads text first, I can stat reading the articles at the earliest. Since they are multiple port connections open, the browser can download small objects in parallel. Also the round trip time of small objects would be comparatively less, making the upload of essential items very fast, improving the user experience.
- f.

Network	Throughput	Load Time
Regular 2G	2.22 KBps	1.35 mins
Good 2G	7.47 KBps	42.92 secs
Regular 3G	9 KBps	37.34 secs
Good 3G	16.28 KBps	10.47 secs
Regular 4G	39.04 KBps	4.85 secs
DSL	24.88 KBps	8.65 secs

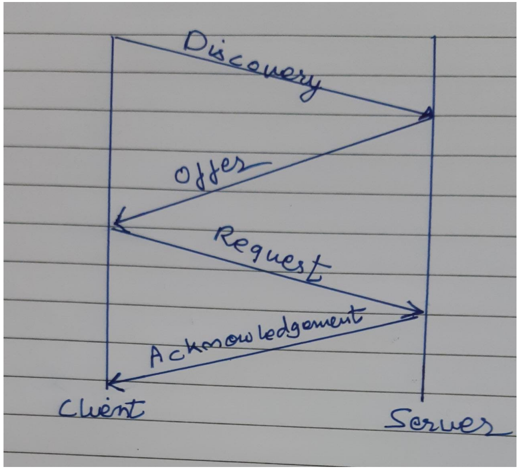
According to [1], Chrome adds a browser level delay for the emulation. We specify the uplink and downlink speeds, so the browser itself might ask for objects with that speed. Maybe the browser would also be a less aggressive in pipe-lining for slower connections
1. https://www.debugbear.com/blog/network-throttling-methods

Computational capabilities can also effect the performance on a network. The device may not have the relevant drivers to upload/download at the maximum speed which the ISP provides. For an in-order arrival, the packets are first put in a buffer and then only passed further to the application. If a device has a very low capacity buffer, even if the packet arrives at the client, it might have to be dropped due to buffer overflow, resulting in more waiting time.

- g.
  - DoubleClick, Google Analytics, Scorecard
    - Information about the web browser and laptop OS was sent.
    - who is referring to the service (indian express) was also sent.
    - They did not show cookies.
  - Google Accounts
    - In addition to information sent for doubleclick, some client id and cookie was also sent.
    - The cookie information contained various ids like NID, SID ANID etc. SID contains encrypted record of user's google account id. It is also used along NID and ANID to customize ads.
  - wzrkt.com
    - In addition to information sent for doubleclick, some cookie was also sent.
    - The cookie information contained some alpha-numeral string, possibly a user id.

In my opinion third party apps store some ids as cookies so as to identify users and provide customized services.
Third party cookies are not blocked in my browser.

3. - a.
     DHCP used UDP as a transport layer protocol.
     DHCP is used to configure devices on a network by assigning them a IP address.
     Initially it sends a discover message, requesting for an IP address. The server in return reserves IP addresses for the client and sends an offer to it. The client then requests for a particular IP address to a server. The client may receive multiple offers but sends a request for a single address only. The concerned server sends acknowledgement for the IP address and some other configuration information. The visual diagram of the protocol is drawn below.



   - b. I saw some requests from my ip to 1.1.1.1, my DNS server. I also saw some requests from 127.0.0.1 to 127.0.0.53. The transport layer protocol was UDP. Within the DNS Query, messages transferred included transaction ID, flags, the domain name to be resolved and some other information.
   - c. After filtering for ICMP messages I found that the responses of TTL exceeded are coming through the protocol. I also got some destination unreachable messages.
     Traceroute send 3 messages for each TTL value starting from 1. For sending it uses UDP protocol, by default.
   - d.
     - Youtube: I saw TLSv1.2 protocol in a lot of packets.
     - Microsoft Teams: UDP protocol was used mainly. I also saw packets with STUN, TCP and TLSv1.2 protocol.
     - Facebook Video: Many TLSv1.2 packets, along with SSDP, TCP and very few UDP requests.

     I also saw DNS requests in all the above.