1 a) 5 different protocol are as follows

- MDNS (Multicast DNS): A local network can resolve hostnames to IP addresses using the MDNS protocol without the need of a central DNS server. The Application Layer (Layer 7) of the OSI architecture is where MDNS operates. RFC number is 6762.

- ARP (Address Resolution Protocol): On a local network, ARP is used to translate an IP address to a real MAC (Media Access Control) address. ARP enables a device to find the MAC address related to the IP address when it wants to interact with another on the same network. It functions at the Link Layer (Layer 2) of the OSI model. ARP is not governed by a single RFC, its operation is defined in various RFCs, including RFC 826.

- TLSv (Transport Layer Security):TLS is a cryptographic protocol that is used to secure network communication, enabling encrypted and secure connections between a client and a server. It safeguards the integrity and privacy of data. TLS operates at Layer 4 of the OSI model, which is the Transport Layer. RFC 5246.

- QUIC (Quick UDP Internet Connections): QUIC is a transport layer protocol created for fast and secure internet communication. To enable quicker connections and encryption by default, it includes elements of both transport and application layer protocols. The Transport Layer (Layer 4), as well as the Application Layer (Layer 7), are where QUIC operates. QUIC is described in several RFCs, with RFC 9000 serving as the primary standard.

- BGP (Border Gateway Protocol): BGP is a routing protocol that is used on the Internet to allow autonomous systems to exchange routing and reachability data. To ensure proper data transfer, it aids in routing decisions. BGP deals especially with routing and path selection at the Network Layer (Layer 3), which is where it functions in the OSI paradigm. RFC is 4271

b) Connection is as follows

Source ip: 142.250.183.100
Destination ip: 10.7.52.19
Packet request timestamp=262.831953734
Packet response timestamp=262.832154848
RTT=262.832154848-262.831953734
=0.00201114 sec= 2.01 msec

- Github.com: Protocol: GitHub primarily uses HTTP/HTTPS.

  Versions: They have been using HTTP/2(also known as h2), and for secure connections, TLS/SSL protocols. h2 is an application-level protocol that operates over a TLS connection.
- Netflix.com: Protocol: Netflix primarily uses HTTP/HTTPS.

  Versions: They have been using HTTP/1.1, HTTP/2(also known as h2), h3 and for secure connections, TLS/SSL protocols.
- Google.com: Google primarily uses HTTP/HTTPS.

  Versions: They have been using h2, h3 and for secure connections, TLS/SSL protocols.

Here is a table summarizing the key differences ans similarities between HTTP/1.1, HTTP/2, and HTTP/3:

Feature	HTTP/1.1	HTTP/2	HTTP/3
Persistent connections	Yes	Yes	Yes
Header compression	Yes	Yes	Yes
Pipelining	Yes	No	No
Multiplexing	No	Yes	Yes
Server push	No	Yes	Yes
Header size limit	8KB	Unlimited	Unlimited
Transport layer	TCP	QUIC	QUIC

Summarizing above table:

- All three protocols use the same request and response message formats.
- All three protocols support the same methods, such as GET, POST, PUT, and DELETE.
- The main difference between HTTP/1.1 and HTTP/2 is that HTTP/2 uses multiplexing, while HTTP/1.1 does not. Multiplexing allows multiple requests and responses to be sent over the same connection, which can significantly improve performance for large files.
- The main difference between HTTP/2 and HTTP/3 is that HTTP/3 uses QUIC, while HTTP/2 uses TCP. QUIC is a newer protocol that is designed to be more efficient and reliable than TCP.

3) Cookies are as follows

1. cookies set
2. SERVERID

3. _ga
4. -gid
5. -gat
6. cookieconsent_status

Cookies characteristics are

- all are sent over the HTTP protocol.
- They are all first-party cookies
- They are all non-essential cookies, which means that they are not required for the website to function.