Questions:

1. The IETF, stands for Internet Engineering Task Force, is a community of people that are vendors, network designers, and more, that their job is to develop and promote the internet standards. It is a voluntary organization, and it helps at the advancement and evolution of the internet. Their primary mission is to develop and share standards that are ensuring functionality of the internet.
2. A communication is a set of conventions, that are telling us how the data transmission needs to look like. Those protocols are telling us the format, sequencing, errors, and timing of the data transmission.
3. RFC which stands for Request for Comments, is a many documents that are used by the IETF and other similar organizations. Using these documents, those organizations publish and develop protocols and standards.
4. HTTP, stands for Hypertext Transfer Protocol, is a protocol that is used on the WWW (world wide web), for data communication. HTTP is mostly used to request and get web pages, like html documents, stylesheets, images, and more from the web servers.
5. http and https are protocols for transferring data in the internet, but the are very different from each other when you talk about security and such. The s in https stands for secure, which basically by its name you can understand that https is a secure http. There are a few main differences between these protocols, such as;

in http, there is not TLS/SSL, so there is no way of authenticating the server’s identity or making sure the data is private and secure. In http there is TLS and SSL, it relies on them, and the meaning of it is that the use of it is valid and secure, because TLS(transport layer security) and SSL(secure sockets layer) are protocols that give encryption and secure communication.

In http, the protocol works on top of the TCP/IP (transmission control protocol/ internet protocol), tcp gives reliable communication and ensures data integrity. https uses TCP/IP as well.

1. http works as a request-repsonse protocol so there is a client and a server. Usually the client is a web browser/ app. The client make a request from the server that has web resources that it can respond to the client with it.
2. User agent is a string that includes information about the client or device when making an http request, such as the application of the client, the version, the operating system, and more.

A web server is software or hardware that is responsible for giving web content and respond to http requests from clients, it handles the delivery and prcessing of the web resources to users.

A proxy is a server is responsible for mediation between clients and servers. It is used for routing, caching, and filtering. Proxies can deal with http requests and are offering security, caching, routing, privacy and anonymity and more.

1. Proxies have many purposes that related to the network communication. They handle anonymity and privacy; proxy mask the ip of the user when the client sends a request to the web server. It is very secure and can filter web content, so it denies access to websites that seem harmful.
2. The term state for protocols refers to the way the communication is being preserved throughout a few transaction. Protocols with a state, keep information about their current state of a session between the parties that communicate with each other.
3. http does not have a state, it is a stateless protocol.
4. First the client makes a request, by using http method (GET, POST, PUT, DELETE). Then, the client sends the request using TCP/IP protocol. The server processes the request and makes a response considering the http method the client used. The client receives the respond and processes it. The process repeats until the session is over and the connection is closed.
5. Requests headers provide information about the client, the headers can be found in the http request send by the client.
6. Cookies are used for managing sessions, tracking users, and more. Cookies can be found in the web browser when a user is visiting a website. They store information about the user’s communication with the website that the user is visiting, that information is sent back to the website each time the user visits it.
7. in an http request there is the http method which is (GET, POST, PUT, DELETE), the url that is the location of the resources on the server that the client wants to communicate with, the http version, the request headers, the request body which is optional and consists of the data the client sends to the server if there is any, custom headers and cookies which are also optional.
8. In an http response you can find the http version and status code (200 for success, 404 not found etc), the response headers, the response body with the actual content of the requested resource, and custom headers which is optional.
9. http3 is the third version of http and http2 is the second version. http2 uses the TCP transport protocol, and http3 uses QUIC transport protocol that is build on to of UDP. http2 allows multiple requests and responses to be send with the same TCP connection, http3 does that but better, with QUIC protocol. Http2 uses on security supplied by TLS/SSL encryption, which works but not on all cases. http3 is more secure and uses encryption with QUIC protocol.