# Review Questions

Week-05 Review questions covering Application Layer Protocols and their functions

## Objectives

\* Explore and identify the aspects of Application Layer protocols, DNS, HTTP, and SMTP

\* Identify how the Application Layer and the Transport Layer interact

\* Explain and infer the meaning of packet captures in WireShark

## Questions

1. Suppose you wanted to do a transaction from a remote client to a server as fast as possible. Would you use UDP or TCP? Why?

i)You would use UDP.With UDP, the transaction can be completed in one roundtrip time (RTT) - the client sends the transaction request into a UDP socket, and the server sends the reply back to the client's UDP socket. With TCP, a minimum of two RTTs are needed - one to set up the TCP connection, and another for the client to send the request and for the server to send back the reply.

2. Recall that TCP can be enhanced with TLS to provide process-to-process security services, including encryption. Does TLS operate at the transport layer or the application layer? If the application developer wants TCP to be enhanced with TLS, what does the developer have to do?

i)TLS operates at the application layer. To enhance TCP with TLS, the developer needs to implement TLS within the application code and configure it to secure the communication between the processes.

3. What is meant by a handshaking protocol?

i)A handshaking protocol, in the context of computer networking and communication, is a set of rules and procedures that two devices or entities follow to establish a connection and exchange information. It's like a formal greeting or introduction between two devices before they start transmitting data.

4. Why do HTTP, SMTP, and IMAP run on top of TCP rather than on UDP?

i)HTTP, SMTP, and IMAP use TCP instead of UDP because TCP provides reliable, error-checked, ordered delivery of data, which is essential for applications like web browsing and email.

5. Describe how Web caching can reduce the delay in receiving a requested object. Will Web caching reduce the delay for all objects requested by a user or for only some of the objects? Why?

i)Web caching can bring the desired content “closer” to the user, possibly to the same LAN to which the user’s host is connected. Web caching can reduce the delay for all objects, even objects that are not cached, since caching reduces the traffic on links.

6. What is the HOL blocking issue in HTTP/1.1? How does HTTP/2 attempt to solve it?

i)HTTP/1.1's HOL (Head-of-Line) blocking occurs when one delayed request holds up others on the same connection. HTTP/2 solves this by allowing multiple requests to be processed in parallel over a single connection, reducing the impact of HOL blocking through features like multiplexing, stream prioritization, flow control, and header compression.

7. True or False and why? A user requests a Web page that consists of some text and three images. For this page, the client will send one request message and receive four response messages.

i)False. The client would receive a response for each request so if it sent a request then it would get a response of the same amount. So if it send three requests it would get three responses and so on.

8. True or False and why? Two distinct Web pages (for example, `www.mit.edu/research.html` and `www.mit.edu/students.html`) can be sent over the same persistent connection.

i)True. Multiple web pages can be sent over the same persistent connection to improve efficiency and reduce connection overhead.

9. True or False and why? With non-persistent connections between browser and origin server, it is possible for a single TCP segment to carry two distinct HTTP request messages.

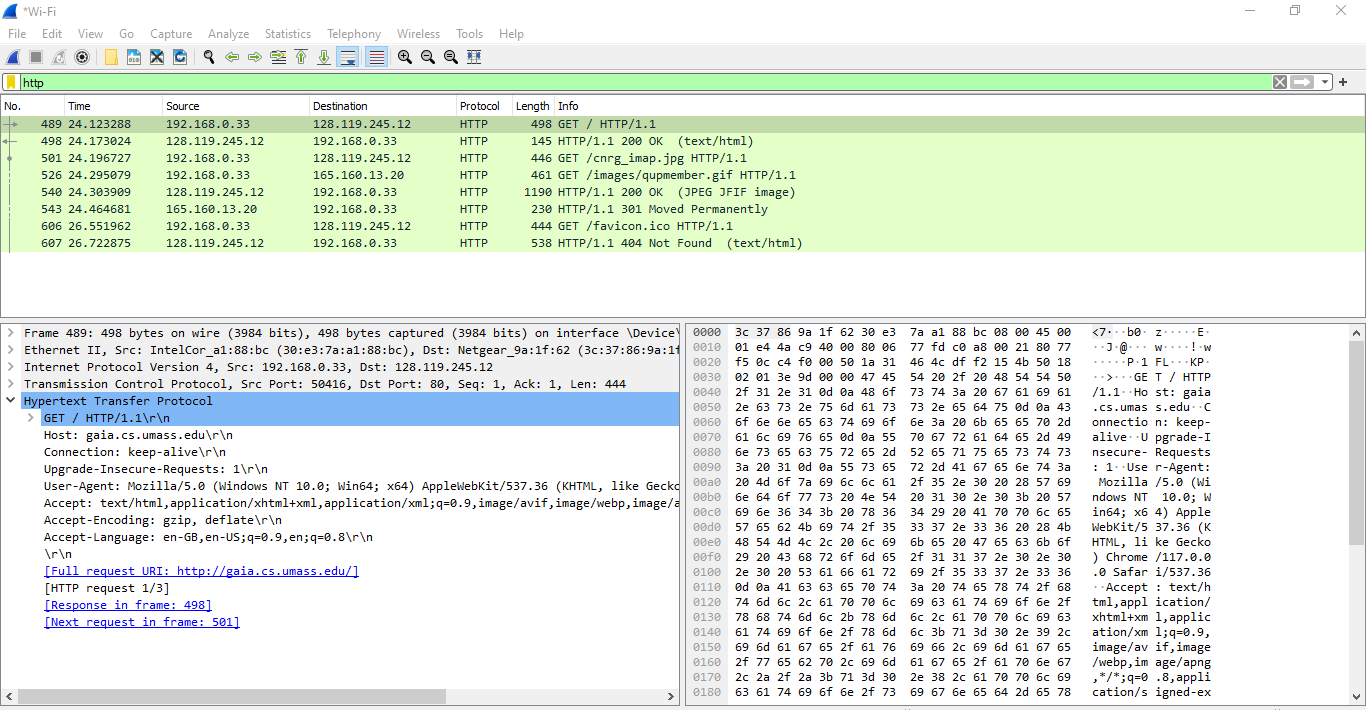
i) False. Non-persistent connections do not allow a single TCP segment to carry two distinct HTTP request messages. Each request typically has its own connection.

10. True or False and why? The `Date:` header in the HTTP response message indicates when the object in the response was last modified.

i)False. The Date: header in an HTTP response indicates when the response was generated, not when the object was last modified.

11. While running WireShark, open a browser and go to the URL [http://gaia.cs.umass.edu/](http://gaia.cs.umass.edu/ "http site"), note the \*\*http\*\*. Using the WireShark Capture, of that answer the following questions: What is the URL of the document requested by the browser?

i)



12. What version of HTTP is the browser running?

i)The browser is running version 1.1 of HTTP.

13. Does the browser request a non-persistent or a persistent connection?

i) The browser requests a persistent connection with the host. This can be understood because a message is sent stating “Keep-Alive”. This means that the connection should not terminate following the sending of the file requested.

14. What is the IP address of the host on which the browser is running?

i)This is a trick question. This information is not contained in an HTTP message anywhere. So there is no way to tell this from looking at the exchange of HTTP messages alone. One would need information from the IP datagrams (that carried the TCP segment that carried the HTTP GET request) to answer this question .

15. Obtain the HTTP/1.1 specification (RFC 2616 via a search engine). Answer the following questions: Explain the mechanism used for signaling between the client and server to indicate that a persistent connection is being closed.

i)Persistent connections are discussed in section 8 of RFC 2616 (the real goal of this question was to get you to retrieve and read an RFC). Sections 8.1.2 and 8.1.2.1 of the RFC indicate that either the client or the server can indicate to the other that it is going to close the persistent connection. It does so by including the connection-token "close" in the Connection-header field of the http request/reply.

16. Can the client, the server, or both signal the close of a connection?

i)Both the client and the server can independently signal the close of a connection, and it's a normal part of the TCP (Transmission Control Protocol) communication protocol used in many network applications.

17. What encryption services are provided by HTTP?

i)There are no encryption services provided by HTTP. HTTPS, its secure counterpart, offers data encryption, authentication, data integrity, and secure key exchange.

18. Can a client open three or more simultaneous connections with a given server?

i)Yes, a client can open three or more simultaneous connections with a given server, although the suggested number of concurrent persistent connections is two.

19. Either a server or a client may close a transport connection between them if either one detects the connection has been idle for some time. Is it possible that one side starts closing a connection while the other side is transmitting data via this connection? Explain.

i) Closing the connection by one side is possible while the other side is transmitting. This is because HTTP is stateless and therefore neither party knows the others state.

## Deliverables

Place your answers to each question next to the \*i)\*. Copy this template into your own local private repo under the itmo-540 folder. Create a subfolder called: `week-05` and place this document into that folder, push the code to GitHub and submit the URL to this document.

Kurose, James F.; Ross, Keith. Computer Networking (p. 166). Pearson Education. Kindle Edition.