ECSE 308:
Introduction to
Communication Systems and Networks

L6: DNS & HTTP

Part 1: DNS
Part 2: HTTP

CEAB Data – Engineering tools

- The following engineering tools are used in this laboratory:
  - Wireshark network analyser
  - NS lookup command
  - DNS system
  - HTTP protocol

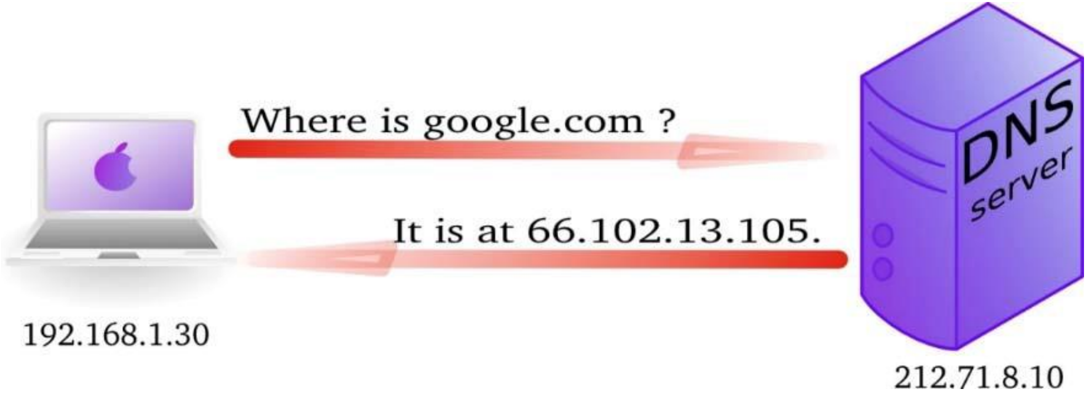
Part 1: DNS

Objectives: Use Wireshark to investigate the Domain Name System (DNS) protocol from the DNS client's standpoint

- DNS query/response structure
- Authoritative name servers
- DNS load balancing

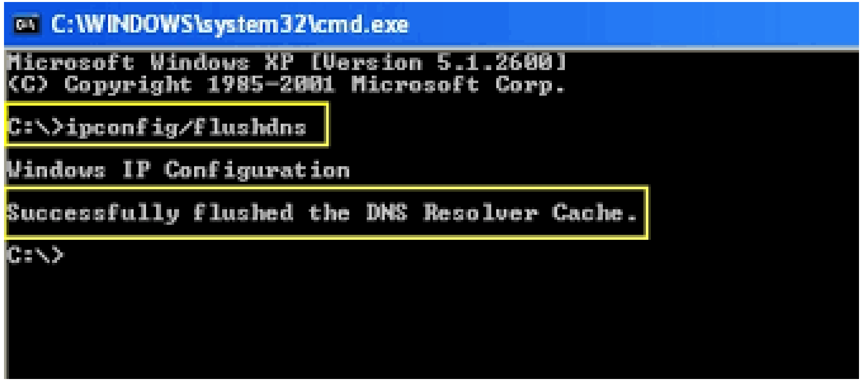
Domain Name System (DNS): Overview

- The DNS translates hostnames to IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.
- The client's role in the DNS is relatively simple; a client sends a query to its local DNS server. If the local DNS server can resolve query by using locally cached information, the query is answered and the process is completed. Otherwise, the resolution process continues with the client's DNS querying other DNS servers to resolve the name.



ipconfig

- *ipconfig:* ipconfig (for Windows) and ifconfig (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we will only describe ipconfig, although the Linux/Unix ifconfig is very similar. ipconfig can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on.
- Running ipconfig:
  - Windows: open the Command Prompt and run ipconfig on the command line.
  - Linux/Unix: type the ifconfig command on the command line.



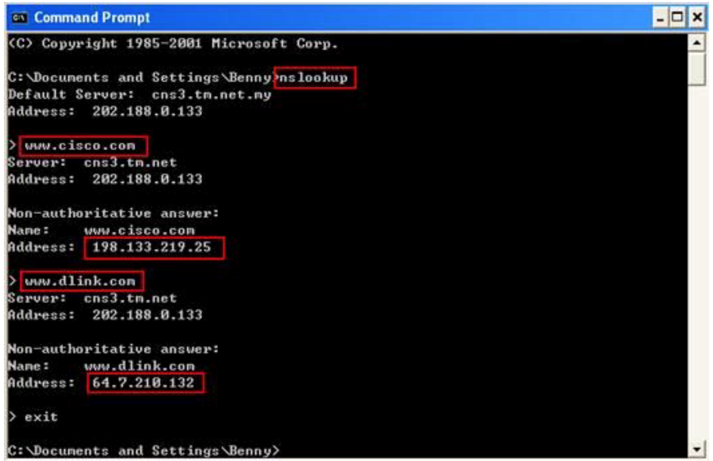
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\>
```

ipconfig commands

- ***ipconfig /all***
  - Displays all current TCP/IP network configuration values
- ***ipconfig /displaydns***
  - A host can cache DNS records it recently obtained. To see these cached records, we can use this command. Each entry shows the remaining Time to Live (TTL) in seconds.
- ***ipconfig /flushdns***
  - This command clears all entries of the DNS cache and reloads the entries from the hosts file.

nslookup

- This tool allows the user to query any specified DNS server for a DNS record.
- To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.
- Running nslookup:
  - Windows: open the Command Prompt and run nslookup on the command line.
  - Linux/Unix: just type the nslookup command on the command line.



```
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Benny>nslookup
Default Server:  cns3.tm.net.my
Address:  202.188.0.133

> www.cisco.com
Server:  cns3.tm.net
Address:  202.188.0.133

Non-authoritative answer:
Name:    www.cisco.com
Address:  198.133.219.25

> www.dlink.com
Server:  cns3.tm.net
Address:  202.188.0.133

Non-authoritative answer:
Name:    www.dlink.com
Address:  64.7.210.132

> exit

C:\Documents and Settings\Benny>
```

nslookup commands

- ***nslookup***
  - This command identifies which DNS server the computer is currently configured to use for its DNS lookups.
- ***nslookup "hostname"***
  - This command provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer; and (2) the answer itself, which is the host name and IP address of "hostname".
- ***nslookup –type=NS "hostname"***
- This command returns authoritative a DNS name server(s) for the given hostname.
- ***nslookup "hostname" "dns server"***
  - This command indicates that the query should be sent to the given DNS server rather than to the default DNS server.
- ***nslookup –option1 –option2 "hostname" "dns-server"***
  - This is the general syntax of nslookup commands. As we have seen in the above, nslookup can be run with zero, one, two or more options. Furthermore, the dnsserver is optional as well; if it is not given, the query is sent to the default local DNS server.

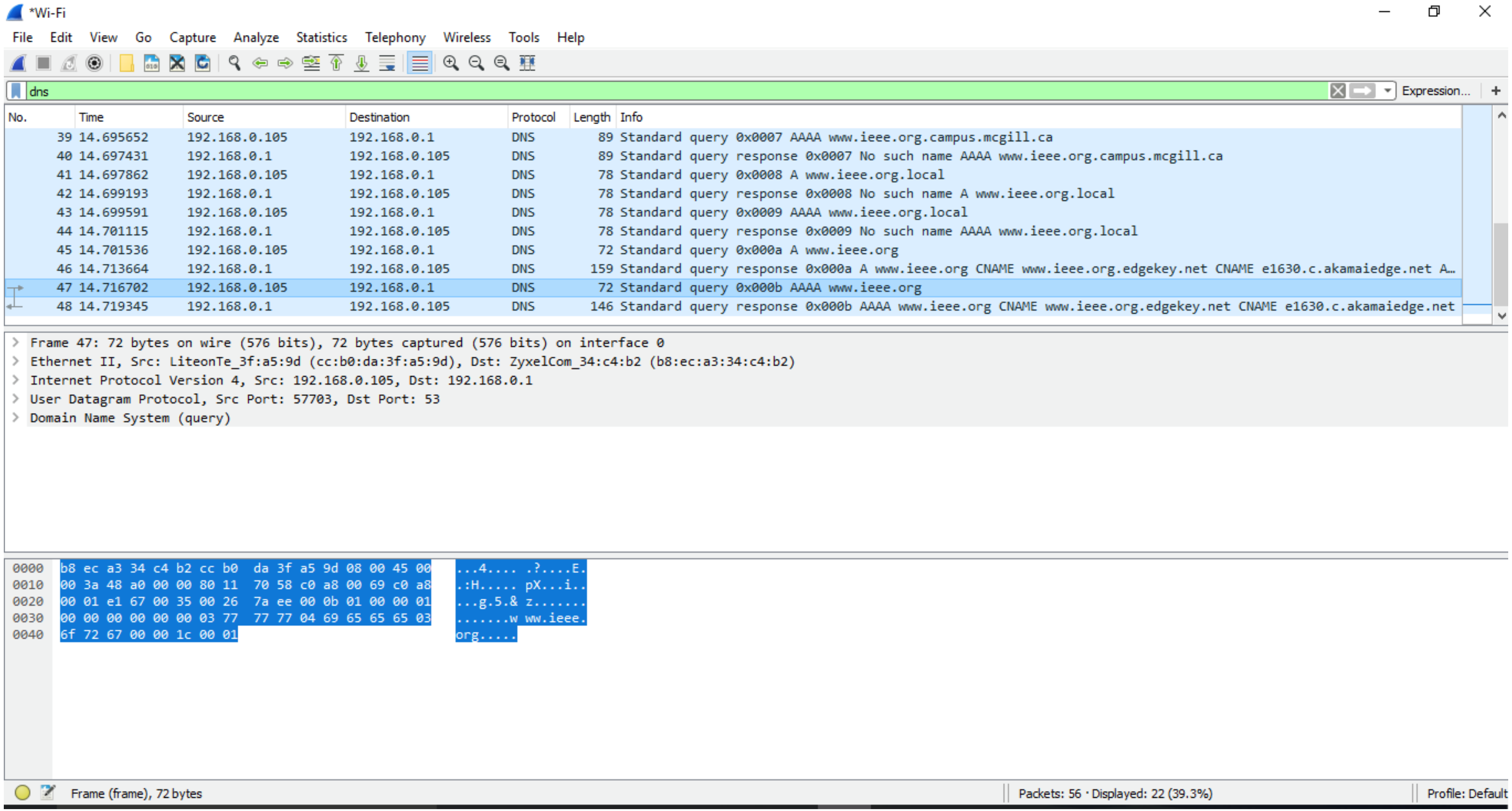
Questions

1. Use nslookup to determine the IP address of www.cbc.ca. What is the IP address of this web server?
2. Use nslookup to determine the authoritative DNS servers for McGill University.
3. Run nslookup to obtain the IP address of www.wikipedia.org by sending a query to 8.8.4.4 which is the IP address of the google public DNS server. If you cannot obtain an answer within preset time limit from this server, use instead 208.67.222.222 which is the IP address of a Cisco server named dns.umbrella.com

DNS queries and responses - Instructions

- Start packet capture; use dns in the filter field.
- Run Command Prompt and enter the command:
  - nslookup www.ieee.org
- Stop packet capture.

DNS queries & responses: example screenshot



```
dns
```

```
No.  Time       Source         Destination    Protocol Length Info
  39 14.695652  192.168.0.105  192.168.0.1    DNS        89 Standard query 0x0007 AAAA www.ieee.org.campus.mcgill.ca
  40 14.697431  192.168.0.1    192.168.0.105  DNS        89 Standard query response 0x0007 No such name AAAA www.ieee.org.campus.mcgill.ca
  41 14.697862  192.168.0.105  192.168.0.1    DNS        78 Standard query 0x0008 A www.ieee.org.local
  42 14.699193  192.168.0.1    192.168.0.105  DNS        78 Standard query response 0x0008 No such name A www.ieee.org.local
  43 14.699591  192.168.0.105  192.168.0.1    DNS        78 Standard query 0x0009 AAAA www.ieee.org.local
  44 14.701115  192.168.0.1    192.168.0.105  DNS        78 Standard query response 0x0009 No such name AAAA www.ieee.org.local
  45 14.701536  192.168.0.105  192.168.0.1    DNS        72 Standard query 0x000a A www.ieee.org
  46 14.713664  192.168.0.1    192.168.0.105  DNS       159 Standard query response 0x000a A www.ieee.org CNAME www.ieee.org.edgekey.net CNAME e1630.c.akamaiedge.net A…
  47 14.716702  192.168.0.105  192.168.0.1    DNS        72 Standard query 0x000b AAAA www.ieee.org
  48 14.719345  192.168.0.1    192.168.0.105  DNS       146 Standard query response 0x000b AAAA www.ieee.org CNAME www.ieee.org.edgekey.net CNAME e1630.c.akamaiedge.net
```

```
> Frame 47: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: LiteonTe_3f:a5:9d (cc:b0:da:3f:a5:9d), Dst: ZyxelCom_34:c4:b2 (b8:ec:a3:34:c4:b2)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 57703, Dst Port: 53
> Domain Name System (query)
```

```
0000  b8 ec a3 34 c4 b2 cc b0  da 3f a5 9d 08 00 45 00   ...4.... .?....E.
0010  00 3a 48 a0 00 00 80 11  70 58 c0 a8 00 69 c0 a8   .:H..... pX...i..
0020  00 01 e1 67 00 35 00 26  7a ee 00 0b 01 00 00 01   ...g.5.& z.......
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 65 65 03   .......w ww.ieee.
0040  6f 72 67 00 00 1c 00 01                            org.....
```

Frame (frame), 72 bytes | Packets: 56 · Displayed: 22 (39.3%) | Profile: Default

Questions

4. What are the destination port number for the DNS query message and the source port number of the DNS response message?
5. What is the destination IP address of the DNS query? Is this the IP address of your default local DNS server?
6. Examine the DNS query. What is the “Type” of the DNS query? What does this “Type” mean? What are the other values for this field?
7. Which bit in the “Flags” field indicates that the message is a query or a response?
8. Which field of the response message contains the IP address of www.ieee.org?
9. Provide a screenshot.

III. Authoritative name servers - Instructions

○ Again repeat the previous instructions, but instead use the command:

○ nslookup –type=NS www.wireshark.org

Questions

10. What is the destination IP address of the DNS query? What does this address correspond to?
11. Determine the “Type” of DNS query. What is the authoritative name server of www.wireshark.org. What is the role of an authoritative name server?
12. Provide a screenshot.

DNS Load Balancing - Instruction

- Start Wireshark packet capture.
- Open Command Prompt and use an appropriate ipconfig to clear your DNS cache.
- In the Command Prompt, enter the command:
  - nslookup www.google.com
- After getting the results for the previous command, run another command
  - “nslookup www.google.com 208.67.222.222”.
- Stop Wireshark packet capture.

Questions

13. What are the destination IP addresses for the two DNS queries? What do these IP addresses correspond to?
14. What IP addresses are returned by these two queries? Do they return the same IP addresses for www.google.com ? Explain your answer.
15. Provide a screen shot.

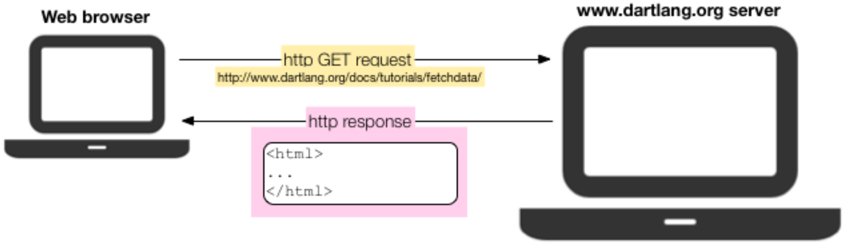
Part 2: Hyper-Text Transfer Protocol (HTTP)

Objectives: Use Wireshark to collect traces and investigate the different aspects of the HTTP protocol operation:

- Simple HTTP GET request/response
- Long HTTP response
- HTTP caching mechanism
- HTML pages with embedded objects
- HTTP request methods

Simple HTTP GET request/response

- ***Overview:***
  - We will investigate the basic HTTP GET request/response interaction by retrieving a simple HTML file which is very short, and has no embedded objects.



HTTP GET request/response: Instructions

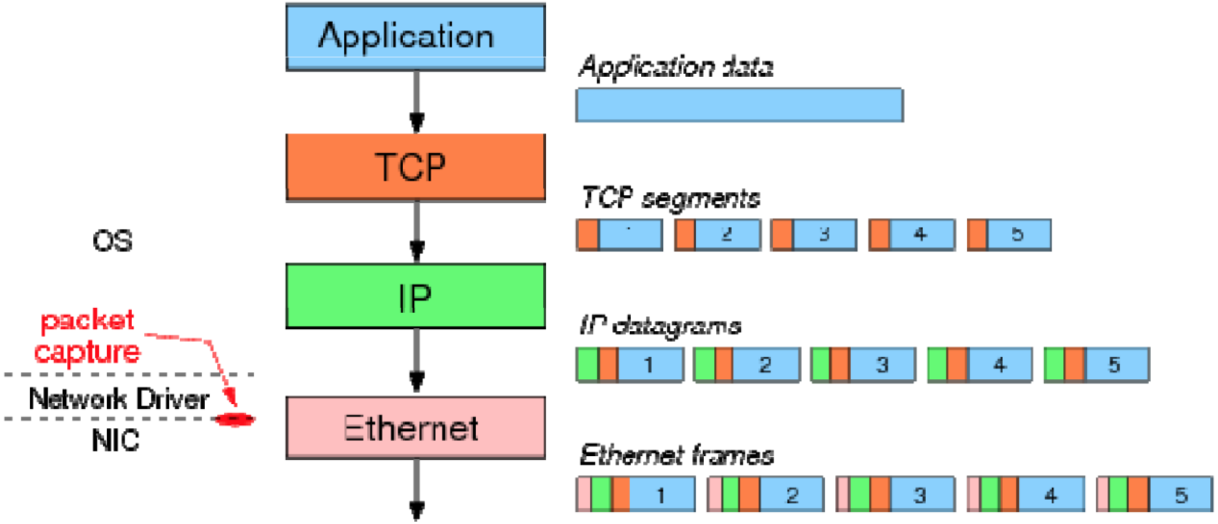
- Start up your web browser.
- Open up the Wireshark. In the filter field, type “http” (without the quotation marks), so that only captured HTTP messages will be displayed later in the packet-listing window.
- Note: After you have changed the expression in the filter input box, do not forget to press the Apply button (or the Enter/Return key twice), to apply this filter string to the displayed trace file.
- Start Wireshark packet capture.
- Go back to your web browser and enter:
    - http://assorted-potential.glitch.me/
- Stop Wireshark packet capture.

HTTP GET request/response: Questions

1. What HTTP request method is used to retrieve the HTML file?
2. What is the URI of the requested file?
3. What HTTP version is your browser running? What are the other versions of HTTP?
4. What languages does your browser accept for response?
5. What is the IP address of your computer?
6. What is the server’s IP address?
7. What is the relationship between source and destination IP addresses of the first GET and the source and destination IP addresses of the first response?
8. What is the status code of the first response message? What does this code indicate? What code is returned if the requested file cannot be found on the server?
9. When was the last time that the received HTML file was modified at the server?
10. What is the size of the content that is returned to your browser?

Long HTTP response: Overview

○ In the previous exercise, we retrieved a short HTML file. Here, we will see what happens when we download a long HTML file.



The Address Resolution Protocol

- Start up your web browser.
- Open up the Wireshark.
- Start Wireshark packet capture.
- Enter the following URL into your browser
  - http://nettle-notify.glitch.me/
- Stop Wireshark packet capture, and type “http” in the filter field.

ARP Questions

11. How many HTTP GET request messages are sent by your web browser?
12. By inspecting the entire trace, determine the number of packets that contain HTTP header. Explain your answer.
13. How many TCP segments are transmitted to your computer? Why multiple segments are required to retrieve this single HTML file?
14. Determine the length of these TCP segments. Do they have the same size? Explain your answer.
15. Which message and what field in that message indicate that the server was able to process the request successfully?

HTTP caching mechanism

- Overview:
    - In this exercise, we will focus on the caching mechanism of the HTTP protocol. Most web browsers keep the recently retrieved HTTP objects in their cache memory. When they receive a request to retrieve an HTTP object, they first check whether the object is cached or not. If the object exists in the cache memory, a conditional GET request is sent to the server. The server sends the object if it is modified, otherwise it sends a “Not Modified” response.
- Note:
    - Before performing the instructions, make sure your browser’s cache is empty.
    - Firefox: select Tools->Clear Recent History and check the Cache box
    - Internet Explorer: select Tools->Internet Options->Delete File; these actions will remove cached files from your browser’s cache.
    - Chrome may not work properly for this part.

HTTP caching: Instruction

- Start up your web browser, and make sure your browser’s cache is cleared.
- Open up the Wireshark.
- Start Wireshark packet capture.
- Enter the following URL into your browser
    - http://nettle-notify.glitch.me/
- Quickly enter the same URL into your browser again (or use the refresh button on your browser)
- Do NOT stop Wireshark packet capture, and type “http” in the filter field.

HTTP caching: Questions

16. What is the status code of the first response message?
17. What is the value of the content size of the first response message?
18. What is the etag (identity tag) of the first response message?

NOTE: To answer the remaining question, use a “Reload/Refresh” command in the browser. This will generate an additional trace of http frames (queries and responses) in the Wireshark viewer.

16. What is the application of etag in conditional HTTP request? Which line in the new query contains the etag value of the first response message above?
17. Which HTTP GET in the new sequence contains the “IF-MODIFIED-SINCE” line? What is the usage of this field?
18. What is the status code of the first response message in the new sequence (answer should be 304; if you do not see this, apply the reload command as noted above and look at the subsequent response)? What does this code mean?
19. What is the content length of this response? Explain.

Retrieving a web page with embedded objects

- Overview:
  - In this experiment, we will retrieve an HTML file with embedded objects, i.e., a file that includes other objects (in the example below, image files) that are stored on another server(s).

```
<imgsrc="https://upload.wikimedia.org/wikipedia/en/thumb/2/29/McGill_University_CoA.svg/1280px-
McGill_University_CoA.svg.png" style="float:right;width:200px;">

<imgsrc="https://cdn.glitch.com/5402db22-98ed-4857-a024e24d7b3eb6c0%2Fim1.jpg?v=1574010595863"
style="width:200px;">
```

HTTP caching: Instruction

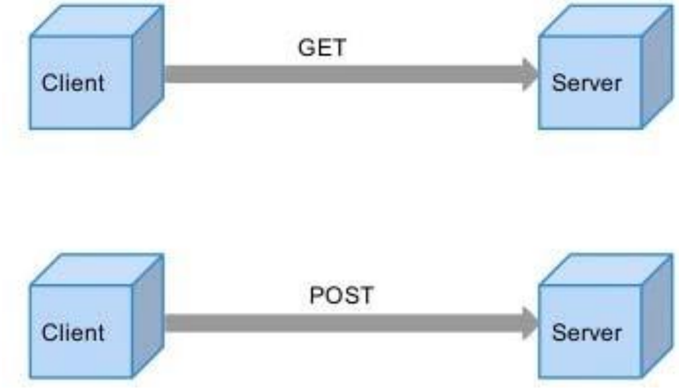
- Start up your web browser, and make sure your browser's cache is cleared.
- Open up the Wireshark.
- Start Wireshark packet capture.
- Go back to your web browser and enter:
  - http://plastic-midnight.glitch.me/
- Stop Wireshark packet capture, and type "http" in the filter field.

HTTP caching: Questions

23. How many HTTP GET requests are sent by your web browser?
24. What is the content type of each response message?
25. Did your browser forward the URLs of the two images separately or in the same commands? How were the images eventually transferred to your computer?
26. Has the HTTP used persistent or non-persistent connection? Explain your answer.

HTTP request methods: Overview

- In this last exercise, we will examine a trace file in which the user tried to connect to a password-protected website. We will see what HTTP messages are exchanged in this scenario.



HTTP request methods: Instructions

- Open the wireshark trace file “HTTP-Authentication.pcapng”, available on myCourses.
- Type “http” in the filter field so that only captured HTTP messages will be displayed later in the packet-listing window.

HTTP request methods: Questions

27. What is the requested URL in the frame#101? What HTTP field contains the username and password information? What are the submitted values for the username and the password?
28. What HTTP request method is used in the frame#172? What HTTP field contains the username and password information? Explain the difference between this request method and the GET method.
29. What is the status code of the frame#174? What is the description of this code?