

# LAB 3

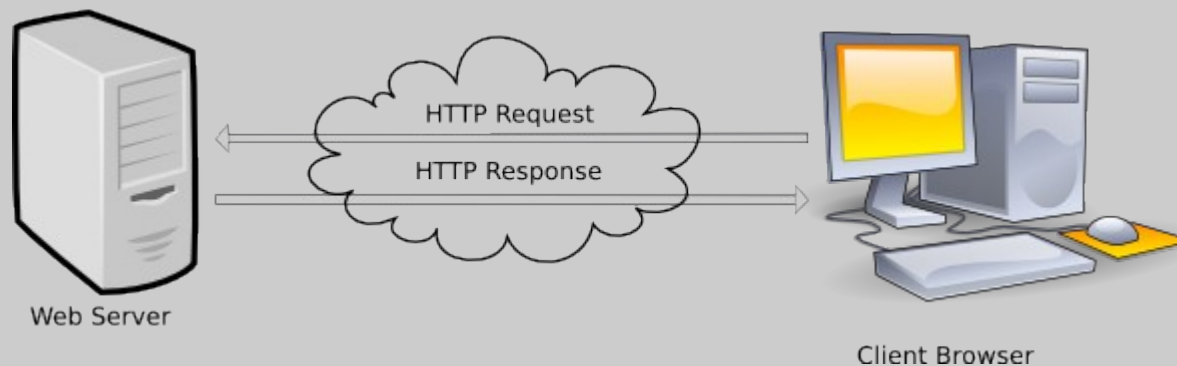
# Objectives:

→ Investigate HTTP protocol

# HTTP Protocol

## - What is HTTP?

- Hypertext Transfer Protocol (http) is application layer protocol.
- HTTP functions as a request-response protocol in the client-server computing model
- HTTP defines the structure of messages and how the client and server exchange these messages
- HTTP defines methods/verbs to indicate the desired action to be performed on the identified resource
- Request methods : GET, POST, PUT, DELETE ... etc.



- The server responds to the browser's request with a three-digit code which is the HTTP status code.
- HTTP status code:
  - 200 - OK
  - 404 - Not Found
  - 500 - Internal Server Error
  - 503 - Service Unavailable

# HTTP Request:

http.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
31783	1701.8846197...	192.168.1.4	52.85.22.116	HTTP	420	GET /Themes/AllWebLeads/styles/less/site.min.css HTTP/1.1
31786	1701.8875249...	207.200.22.28	192.168.1.4	HTTP	348	HTTP/1.1 404 Not Found (text/html)
31794	1701.9266032...	93.184.221.200	192.168.1.4	HTTP	1350	HTTP/1.1 200 OK (application/x-javascript)
31796	1701.9274061...	192.168.1.4	52.85.22.116	HTTP	417	GET /Themes/AllWebLeads/styles/bootstrap/JS/bootstrap.min.js HTTP/1.1
31797	1701.9282028...	192.168.1.4	52.85.22.116	HTTP	398	GET /Themes/AllWebLeads/scripts/global.js HTTP/1.1
31865	1702.0614729...	52.85.22.116	192.168.1.4	HTTP	1100	HTTP/1.1 200 OK (application/x-javascript)
32118	1703.1243563...	192.168.1.4	52.85.22.116	HTTP	394	GET /media/default/Logos/awl-logo.png HTTP/1.1
32119	1703.1246999...	192.168.1.4	52.85.22.116	HTTP	390	GET /media/default/Logos/lock.jpg HTTP/1.1
32120	1703.1249410...	192.168.1.4	52.85.22.116	HTTP	408	GET /media/default/Banners/request_freebrochure.png HTTP/1.1
32121	1703.1252922...	192.168.1.4	207.200.22.28	HTTP	889	GET /media/default/standard/spacer.gif HTTP/1.1
32122	1703.1256196...	192.168.1.4	52.85.22.116	HTTP	406	GET /media/default/Logos/bbb_horizontal_small.png HTTP/1.1
32144	1703.2236068...	52.85.22.116	192.168.1.4	HTTP	376	HTTP/1.1 200 OK (PNG)
32150	1703.2262681...	52.85.22.116	192.168.1.4	HTTP	1106	HTTP/1.1 200 OK (JPEG JFIF image)
32164	1703.2908995...	192.168.1.4	108.161.189.121	HTTP	440	GET /font-awesome/4.4.0/css/font-awesome.css HTTP/1.1
32170	1703.3470937...	207.200.22.28	192.168.1.4	HTTP	1497	HTTP/1.1 200 OK (GIF89a) (image/gif)
32187	1703.3927923...	108.161.189.121	192.168.1.4	HTTP	574	HTTP/1.1 200 OK (text/css)
32189	1703.3933834...	192.168.1.4	52.85.22.116	HTTP	401	GET /media/default/Logos/glassdoor-32x32.png HTTP/1.1
32190	1703.3935641...	192.168.1.4	52.85.22.116	HTTP	399	GET /media/default/Logos/facebook-logo.png HTTP/1.1
32191	1703.3937756...	192.168.1.4	52.85.22.116	HTTP	398	GET /media/default/Logos/twitter-logo.png HTTP/1.1
32205	1703.4825666...	52.85.22.116	192.168.1.4	HTTP	1628	HTTP/1.1 200 OK (PNG)
32207	1703.4832109...	192.168.1.4	52.85.22.116	HTTP	395	GET /media/default/Logos/instagram.png HTTP/1.1
32208	1703.4843282...	52.85.22.116	192.168.1.4	HTTP	935	HTTP/1.1 200 OK (PNG)
32211	1703.4855099...	192.168.1.4	52.85.22.116	HTTP	402	GET /media/default/Logos/lcfoundingmember.png HTTP/1.1

Frame 32122: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface 0

Ethernet II, Src: IntelCor\_08:b3:ee (ac:2b:6e:08:b3:ee), Dst: HuaweiTe\_88:52:85 (14:b9:68:88:52:85)

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 52.85.22.116

Transmission Control Protocol, Src Port: 33454, Dst Port: 80, Seq: 355, Ack: 194113, Len: 340

Hypertext Transfer Protocol

GET /media/default/Logos/bbb\_horizontal\_small.png HTTP/1.1\r\n

Host: d1eaiqbqfywfp7.cloudfront.net\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:58.0) Gecko/20100101 Firefox/58.0\r\n

Accept: \*/\*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://www.allwebleads.com/kurose-ross\r\n

Connection: keep-alive\r\n

\r\n

[Full request URI: http://d1eaiqbqfywfp7.cloudfront.net/media/default/Logos/bbb\_horizontal\_small.png]

[HTTP request 2/4]

[Prev request in frame: 31783]

[Next request in frame: 32257]

Text item (text), 60 bytes

Packets: 79863 · Displayed: 269 (0.3%) · Load time: 0:0.747 · Profile: Default

# HTTP Response:

http.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
31783	1701.8846197...	192.168.1.4	52.85.22.116	HTTP	420	GET /Themes/AllWebLeads/styles/less/site.min.css HTTP/1.1
31786	1701.8875249...	207.200.22.28	192.168.1.4	HTTP	348	HTTP/1.1 404 Not Found (text/html)
31794	1701.9266032...	93.184.221.200	192.168.1.4	HTTP	1350	HTTP/1.1 200 OK (application/x-javascript)
31796	1701.9274061...	192.168.1.4	52.85.22.116	HTTP	417	GET /Themes/AllWebLeads/styles/bootstrap/JS/bootstrap.min.js HTTP/1.1
31797	1701.9282028...	192.168.1.4	52.85.22.116	HTTP	398	GET /Themes/AllWebLeads/scripts/global.js HTTP/1.1
31865	1702.0614729...	52.85.22.116	192.168.1.4	HTTP	1100	HTTP/1.1 200 OK (application/x-javascript)
32118	1703.1243563...	192.168.1.4	52.85.22.116	HTTP	394	GET /media/default/Logos/awl-logo.png HTTP/1.1
32119	1703.1246999...	192.168.1.4	52.85.22.116	HTTP	390	GET /media/default/Logos/lock.jpg HTTP/1.1
32120	1703.1249410...	192.168.1.4	52.85.22.116	HTTP	408	GET /media/default/Banners/request_freebrochure.png HTTP/1.1
32121	1703.1252922...	192.168.1.4	207.200.22.28	HTTP	889	GET /media/default/standard/spacer.gif HTTP/1.1
32122	1703.1256196...	192.168.1.4	52.85.22.116	HTTP	406	GET /media/default/Logos/bbb_horizontal_small.png HTTP/1.1
32144	1703.2236068...	52.85.22.116	192.168.1.4	HTTP	376	HTTP/1.1 200 OK (PNG)
32150	1703.2262681...	52.85.22.116	192.168.1.4	HTTP	1106	HTTP/1.1 200 OK (JPEG JFIF image)
32164	1703.2908995...	192.168.1.4	108.161.189.121	HTTP	440	GET /font-awesome/4.4.0/css/font-awesome.css HTTP/1.1
32170	1703.3470937...	207.200.22.28	192.168.1.4	HTTP	1497	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
32187	1703.3927923...	108.161.189.121	192.168.1.4	HTTP	574	HTTP/1.1 200 OK (text/css)
32189	1703.3933834...	192.168.1.4	52.85.22.116	HTTP	401	GET /media/default/Logos/glassdoor-32x32.png HTTP/1.1
32190	1703.3935641...	192.168.1.4	52.85.22.116	HTTP	399	GET /media/default/Logos/facebook-logo.png HTTP/1.1
32191	1703.3937756...	192.168.1.4	52.85.22.116	HTTP	398	GET /media/default/Logos/twitter-logo.png HTTP/1.1
32205	1703.4825666...	52.85.22.116	192.168.1.4	HTTP	1628	HTTP/1.1 200 OK (PNG)
32207	1703.4832109...	192.168.1.4	52.85.22.116	HTTP	395	GET /media/default/Logos/instagram.png HTTP/1.1
32208	1703.4843282...	52.85.22.116	192.168.1.4	HTTP	935	HTTP/1.1 200 OK (PNG)
32211	1703.4855099...	192.168.1.4	52.85.22.116	HTTP	402	GET /media/default/Logos/lcfoundingmember.png HTTP/1.1

Frame 32144: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface 0

Ethernet II, Src: HuaweiTe\_88:52:85 (14:b9:68:88:52:85), Dst: IntelCor\_08:b3:ee (ac:2b:6e:08:b3:ee)

Internet Protocol Version 4, Src: 52.85.22.116, Dst: 192.168.1.4

Transmission Control Protocol, Src Port: 80, Dst Port: 33460, Seq: 10835, Ack: 661, Len: 310

[8 Reassembled TCP Segments (10110 bytes): #32130(1400), #32132(1400), #32134(1400), #32136(1400), #32138(1400), #32140(1400), #32142(1400), #32144(310)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Content-Type: image/png\r\n

Content-Length: 9563\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=604800\r\n

Last-Modified: Tue, 19 Jul 2016 16:41:12 GMT\r\n

Accept-Ranges: bytes\r\n

ETag: "04d25bdce1d11:0"\r\n

Server: Microsoft-IIS/7.5\r\n

X-Powered-By: ASP.NET\r\n

X-Frame-Options: SAMEORIGIN\r\n

Access-Control-Allow-Origin: \*\r\n

Date: Mon, 18 Dec 2017 09:40:24 GMT\r\n

Age: 557098\r\n

Text item (text), 17 bytes

Packets: 79863 · Displayed: 269 (0.3%) · Load time: 0:0.747 · Profile: Default



## Let's have fun

1. Capture all HTTP packets.
1. What version of HTTP is the server and your browser running?
2. What is the IP address of your computer and of Server you trying to access ?
3. What is the status code returned from the server?
4. When was the HTML file that you are retrieving last modified at the server?
5. How many bytes of content are being returned to your browser?
6. What is the default port number for the http service?
7. Find all running process that using HTTP protocol. (use lsof command)