

Roland
Egheali

Wireshark assignment

ID 202513377

Lab-1

Part 1

1. Browser : HTTP/1.1
Server : HTTP/1.1
2. Accept language are en-LB, en-GB, en-US, es
~~belonere~~ ~~british~~ spanish english and belonere
arabic, and fr (French).
3. Computer IP: 192.168.123.29 Client
link(gara ...) IP is 128.119.245.72 server
4. 200 OK
5. Tue, 28 Oct 2025 05:59:07 GMT

6. 81 bytes

7. The User-agent header is not displayed in the packet listing window but visible in packet bytes.

Part 2:

8. In the first HTTP GET (frame 255) there is no If-mod since line.

9. The response HTTP/1.1 200 OK content length (371 bytes) indicates that data has been sent/returned

10. There is an If Modified since with Tue, 28 Oct 2025 05:59:01 GMT
HTTP GET (frame 337)

11. The response is 304 not modified hence the server did not return because it should use the cached copy.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
205	4.199518	192.168.123.29	128.119.245.12	HTTP	601	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
232	4.354953	128.119.245.12	192.168.123.29	HTTP	794	HTTP/1.1 200 OK (text/html)
271	4.466645	192.168.123.29	128.119.245.12	HTTP	547	GET /favicon.ico HTTP/1.1
291	4.600532	128.119.245.12	192.168.123.29	HTTP	645	HTTP/1.1 301 Moved Permanently (text/html)
337	7.476641	192.168.123.29	128.119.245.12	HTTP	713	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
348	7.865235	128.119.245.12	192.168.123.29	HTTP	411	HTTP/1.1 304 Not Modified

> Frame 337: Packet, 713 bytes on wire (5704 bits), 713 bytes captured (5704 bits) on interface \Device\NPF_{C634F1:0030 fa cc 71 5c 00 00 47 45 5a 20 2f 77 69 72 65 73} ...q\...f.../wires
> Ethernet II, Src: WNC_c4:fd:7a (58:96:71:c4:fd:7a), Dst: FidaInternat_1e:4d:2d (90:61:0c:1e:4d:2d) hark-lab s/HTTP-w
> Internet Protocol Version 4, Src: 192.168.123.29, Dst: 128.119.245.12 ireshark -file2.h
> Transmission Control Protocol, Src Port: 49667, Dst Port: 80, Seq: 1041, Ack: 1332, Len: 659 tml HTTP /1.1..Ho
v Hypertext Transfer Protocol st: gaia .cs.umas
v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n s.edu..C onnectio
Request Method: GET n: keep- alive..C
Request URI: /wireshark-labs/HTTP-wireshark-file2.html x-age=0. .Upgrade
Request Version: HTTP/1.1 ts: 1..U ser-Agen
Host: gaia.cs.umass.edu\r\n t: Mozil la/5.0 (
Connection: keep-alive\r\n Windows NT 10.0;
Cache-Control: max-age=0\r\n Win64; x64) App
Upgrade-Insecure-Requests: 1\r\n leWebKit /537.36
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 S
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/rtf+xml;q=0.9,application/vnd.ms-excel;q=0.5;q=0.7,application/atom+xml;q=0.9;q=0.5;q=0.3;q=0.2\r\n .0.0 Saf ari/537.
Accept-Encoding: gzip, deflate\r\n 36--Acce pt: text
Accept-Language: en-LB,en;q=0.9,es-LB;q=0.8,es;q=0.7,ar-LB;q=0.6,ar;q=0.5,en-GB;q=0.4,en-US;q=0.3,fr;q=0.2\r\n /html,ap plicatio
If-None-Match: "173-6d231b67176b7"\r\n n/xhtml+ xml,appl
If-Modified-Since: Tue, 28 Oct 2025 05:59:01 GMT\r\n ication/ xml;q=0.
\r\n 9,image/ avif,ima
\r\n ge/webp, image/ap

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
205	4.199518	192.168.123.29	128.119.245.12	HTTP	601	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
232	4.354953	128.119.245.12	192.168.123.29	HTTP	794	HTTP/1.1 200 OK (text/html)
271	4.466645	192.168.123.29	128.119.245.12	HTTP	547	GET /favicon.ico HTTP/1.1
291	4.600532	128.119.245.12	192.168.123.29	HTTP	645	HTTP/1.1 301 Moved Permanently (text/html)
337	7.476641	192.168.123.29	128.119.245.12	HTTP	713	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
348	7.865235	128.119.245.12	192.168.123.29	HTTP	411	HTTP/1.1 304 Not Modified

> Frame 232: Packet, 794 bytes on wire (6352 bits), 794 bytes captured (6352 bits) on interface \Device\NPF_{C634F1: 0000 50 96 71 c4 fd 7a 90 61 0c 1e 4d 2d 08 00 45 00 X-q-z-a --M--E-
> Ethernet II, Src: FidaInternat1e:4d:2d (00:61:0c:1e:4d:2d), Dst: WNC_c4:fd:7a (58:96:71:c4:fd:7a) 0010 03 0c 91 18 40 00 fd 06 38 89 80 77 f5 0c c0 a8 ---@--- 8--w---
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.123.29 0020 7b 1d 00 50 c2 03 35 8f eb 19 46 20 99 e4 50 18 {...P...5...F...P...
> Transmission Control Protocol, Src Port: 80, Dst Port: 49667, Seq: 1, Ack: 548, Len: 748 0030 15 2e a0 43 00 00 48 54 54 50 2f 31 2e 31 20 32 ...C...HT P/1.1 2
> Hypertext Transfer Protocol 0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 46 72 69 00 OK--D ate: Fri
v HTTP/1.1 200 OK\r\n 0050 2c 20 32 30 20 46 65 62 20 32 30 32 36 20 31 37 , 20 Feb 2026 17
Response Version: HTTP/1.1 0060 3a 34 30 3a 30 33 20 47 4d 54 0d 0a 53 65 72 76 :40:03 G MT--Serv
Status Code: 200 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
[Status Code Description: OK] 0080 32 20 28 41 6c 6d 61 4c 69 6e 75 78 29 20 4f 70 2 (AlmaLinux) Op
Response Phrase: OK 0090 65 6e 53 53 4c 2f 33 2e 35 2e 31 20 6d 6f 64 5f enSSL/3. 5.1 mod_
Date: Fri, 20 Feb 2026 17:40:03 GMT\r\n 00a0 66 63 67 69 64 2f 32 2e 33 2e 39 20 6d 6f 64 5f fcgid/2. 3.9 mod_
Server: Apache/2.4.62 (AlmaLinux) OpenSSL/3.5.1 mod_fcgid/2.3.9 mod_perl/2.0.12 Perl/v5.32.1\r\n 00b0 70 65 72 6c 2f 32 2e 30 2e 31 32 20 50 65 72 6c perl/2.0 .12 Perl
Last-Modified: Tue, 28 Oct 2025 05:59:01 GMT\r\n 00c0 2f 76 35 2e 33 32 2e 31 0d 0a 4c 61 73 74 2d 4d /v5.32.1 --Last-M
ETag: "173-64231b67176b7"\r\n 00d0 6f 64 69 66 69 65 64 3a 20 54 75 65 2c 20 32 38 odified: Tue, 28
Accept-Ranges: bytes\r\n 00e0 20 4f 63 74 20 32 30 32 35 20 30 35 3a 35 39 3a Oct 2025 05:59:
Content-Type: text/html; charset=UTF-8\r\n 00f0 30 31 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 01 GMT-- ETag: "1
X-CFLO-Cache-Result: TCP_HIT\r\n 0100 37 33 2d 36 34 32 33 31 62 36 37 31 37 36 62 37 73-64231 b67176b7
Content-Length: 371\r\n 0110 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 "...Accep t-Ranges
Connection: Keep-Alive\r\n 0120 3a 20 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 : bytes --Content
Accept-Range: bytes 0130 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c -Type: t ext/html
Keep-Alive: 300 0140 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 0d ; charse t=UTF-8-
X-CFLO-Cache-Result: TCP_HIT\r\n 0150 0a 58 2d 43 46 4c 4f 2d 43 61 63 68 65 2d 52 65 -X-CFLO- Cache-Re
0160 73 75 6c 74 3a 20 54 43 50 5f 48 49 54 0d 0a 43 sult: TC P_HIT-C
0170 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 33 ontent-L ength: 3

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
205	4.199518	192.168.123.29	128.119.245.12	HTTP	601	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
232	4.354953	128.119.245.12	192.168.123.29	HTTP	794	HTTP/1.1 200 OK (text/html)
271	4.466645	192.168.123.29	128.119.245.12	HTTP	547	GET /favicon.ico HTTP/1.1
291	4.600532	128.119.245.12	192.168.123.29	HTTP	645	HTTP/1.1 301 Moved Permanently (text/html)
337	7.476641	192.168.123.29	128.119.245.12	HTTP	713	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
348	7.865235	128.119.245.12	192.168.123.29	HTTP	411	HTTP/1.1 304 Not Modified

> Frame 295: Packet, 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits) on interface \Device\NPF_{C634F13A-...}

> Ethernet II, Src: WNC_c4:fd:7a (58:96:71:c4:fd:7a), Dst: FidaInternat1e:4d:2d (90:61:0c:1e:4d:2d)

> Internet Protocol Version 4, Src: 192.168.123.29, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 49667, Dst Port: 80, Seq: 1, Ack: 547

> Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file2.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/145.0.0.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9,es-LB;q=0.8,es;q=0.7,ar-LB;q=0.6,ar;q=0.5,en-GB;q=0.4,en-US;q=0.3,fr;q=0.2\r\n\r\n

[Response in frame: 232]

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

0030 ff ff 6a df 00 00 47 45 5a 20 2f 77 69 72 65 73 ..j...[REDACTED]/wires

0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w

0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68 ireshark -file2.h

0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1..Ho

0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umass

0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu..C onnectio

0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive..U

00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-

00b0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1..Use

00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla

00d0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Ni ndows NT

00e0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 10.0; W in64; x6

00f0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) Apple WebKit/5

0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, 11

0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko) Chrome

0120 2f 31 34 35 2e 30 2e 30 2e 30 2e 30 2e 53 61 66 61 72 /145.0.0 .0 Safan

0130 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 i/537.36 ..Accept

0140 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/h tml,appl

0150 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d ication/ xhtml+xm

0160 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d l,applic ation/xm

0170 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 i;q=0.9, image/av

0180 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d if,image /webp,im

0190 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 age/apng ,*/*;q=0

01a0 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 .8,appli cation/s

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No. Time Source Destination Protocol Length Info

1016	19.794640	192.168.123.29	34.104.35.123	HTTP	366	GET /edgedl/diffgen-puffin/%7B8a69d345-d564-463c-aff1-a69d9e530f96%7D/a3f2d141b7a03707891235e41e54ac55e3ed278cff1189ad3934866daf9072a...
6795	32.883433	192.168.123.29	128.119.245.12	HTTP	602	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
6809	32.943624	128.119.245.12	192.168.123.29	HTTP	502	HTTP/1.1 200 OK (text/html)
6822	32.996377	192.168.123.29	128.119.245.12	HTTP	548	GET /favicon.ico HTTP/1.1
6990	33.335359	128.119.245.12	192.168.123.29	HTTP	644	HTTP/1.1 301 Moved Permanently (text/html)

> Frame 6809: Packet, 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits) on interface \Device...

> Ethernet II, Src: FidaInternat_1e:4d:2d (00:61:0c:1e:4d:2d), Dst: WNC_c4:fd:7a (58:96:71:c4:fd:7a)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.123.29

> Transmission Control Protocol, Src Port: 80, Dst Port: 64705, Seq: 1, Ack: 550, Len: 448

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n\r\nDate: Fri, 20 Feb 2026 17:30:42 GMT\r\n\r\nServer: Apache/2.4.62 (AlmaLinux) OpenSSL/3.5.1 mod_fcgid/2.3.9 mod_perl/2.0.12 Perl/v5.32.1\r\n\r\nLast-Modified: Tue, 28 Oct 2025 05:59:01 GMT\r\n\r\nETag: "51-64231b6715777"\r\n\r\nAccept-Ranges: bytes\r\n\r\nContent-Type: text/html; charset=UTF-8\r\n\r\nX-CFLO-Cache-Result: TCP_HIT\r\n\r\nContent-Length: 81\r\n\r\nConnection: Keep-Alive\r\n\r\nAge: 06\r\n\r\n\r\n[Request in frame: 6795]\r\n[Time since request: 60.191000 milliseconds]\r\n[Request URI: /wireshark-labs/INTRO-wireshark-file1.html]

0030 15 1f e5 fe 00 00 48 54 54 50 2f 31 2e 31 20 32HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 46 72 69 80 OK..D ate: Fri

0050 2c 20 32 30 20 46 65 62 20 32 30 32 36 20 31 37 , 20 Feb 2026 17

0060 3a 33 30 3a 3a 32 20 47 4d 54 0d 0a 53 65 72 76 :30:42 G MT..Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6

0080 32 20 28 41 6c 6d 61 4c 69 6e 75 78 29 20 4f 70 2 (AlmaLinux) Op

0090 65 6e 53 53 4c 2f 33 2e 35 2e 31 20 6d 6f 64 5f enSSL/3. 5.1 mod_

00a0 66 63 67 69 64 2f 32 2e 33 2e 39 20 6d 6f 64 5f fcgid/2. 3.9 mod_

00b0 70 65 72 6c 2f 32 2e 30 2e 31 32 20 50 65 72 6c perl/2.0 .12 Perl

00c0 2f 76 35 2e 33 32 2e 31 0d 0a 4c 61 73 74 2d 4d /v5.32.1 ..Last-M

00d0 6f 64 69 66 69 65 64 3a 20 54 75 65 2c 20 32 38 odified: Tue, 28

00e0 20 4f 63 74 20 32 30 32 35 20 30 35 3a 35 39 3a Oct 202 5 05:59:

00f0 30 31 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 35 01 GMT.. ETag: "5

0100 31 2d 36 34 32 33 31 62 36 37 31 35 37 37 37 22 1-64231b 6715777"

0110 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a ..Accept -Ranges:

0120 20 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d bytes.. Content-

0130 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 3b Type: te xt/html;

0140 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 0d 0a charset =UTF-8..

0150 58 2d 43 46 4c 4f 2d 43 61 63 68 65 2d 52 65 73 X-CFLO-C ache-Res

0160 75 6c 74 3a 20 54 43 50 5f 48 49 54 0d 0a 43 6f ult: TCP_HIT..Co

0170 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 38 31 ntent-Le ngth: 81

0180 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 ..Connec tion: Ke

0190 65 70 2d 41 6c 69 76 65 0d 0a 41 67 65 3a 20 36 ep-Alive ..Age: 6

01a0 36 0d 0a 0d 0a 3c 68 74 6d 6c 3e 0a 43 6f 6e 67 6.....<ht ml> Cong

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1016	19.794640	192.168.123.29	34.104.35.123	HTTP	366	GET /edgedl/diffgen-puffin/%7B8a69d345-d564-463c-aff1-a69d9e530f96%7D/a3f2d141b7a0370789123541e54ac55e3ed278cff1189ad3934866daf9072a...
6795	32.883433	192.168.123.29	128.119.245.12	HTTP	602	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
6809	32.943624	128.119.245.12	192.168.123.29	HTTP	502	HTTP/1.1 200 OK (text/html)
6822	32.996377	192.168.123.29	128.119.245.12	HTTP	548	GET /favicon.ico HTTP/1.1
6990	33.335359	128.119.245.12	192.168.123.29	HTTP	644	HTTP/1.1 301 Moved Permanently (text/html)

> Frame 6795: Packet, 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface \Device\NPF...
> Ethernet II, Src: WNC_c4:fd:7a (58:96:71:c4:fd:7a), Dst: FidaInternat_1e:4d:2d (90:61:0c:1e:4d:2d)
> Internet Protocol Version 4, Src: 192.168.123.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64705, Dst Port: 80, Seq: 2, Ack: 1, Len: 548
v Hypertext Transfer Protocol
v GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Request Method: GET
Request URI: /wireshark-labs/INTRO-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US;q=0.9,en-US;q=0.8,en-US;q=0.7,en-US;q=0.6,en-US;q=0.5,en-US;q=0.4,en-US;q=0.3\r\n
[Response in frame: 6809]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

0030 fe 9b 9f 8d 00 00 47 45 54 20 2f 77 09 72 65 73GET /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0e 48 html HTT F/1.1..H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 ss.edu.. Connecti
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive..
00a0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure
00b0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Request s: 1..Us
00c0 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
00d0 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indows N
00e0 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64; x
00f0 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 64) Appl eWebKit/
0100 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 537.36 (KHTML, l
0110 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d ike Geck o) Chrom
0120 65 2f 31 34 35 2e 30 2e 30 2e 30 20 53 61 66 61 e/145.0. 0.0 Safa
0130 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 ri/537.3 6..Accep
0140 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 t: text/ html,app
0150 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication /xhtml+
0160 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 8 n1,appli cation/x
0170 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 n1;q=0.9 ,image/a
0180 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 vif,imag e/webp,i
0190 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d nage/apn g,*/*;q=
01a0 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 0.8,appl ication/

Lab 2

Part 1

- 1_ IP of `www.iitb.ac.in` = 103.21.124.133
- 2_ IP of DNS : 192.168.123.254
- 3_ Non authoritative because it was cached.
- 4_ `dns2.iitb.ac.in`

To find the authoritative name server,

I run `nslookup dns2.iitb.ac.in`

which queries the DNS system for its IP address

Answer : 103.21.126.129


```
Command Prompt
Microsoft Windows [Version 10.0.26200.7840]
(c) Microsoft Corporation. All rights reserved.

C:\Users\roland.hf>nslookup www.iitb.ac.in
DNS request timed out.
    timeout was 2 seconds.
Server:  Unknown
Address:  192.168.123.254

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:    www.iitb.ac.in
Address: 103.21.124.133

C:\Users\roland.hf>nslookup -type=NS iitb.ac.in
DNS request timed out.
    timeout was 2 seconds.
Server:  Unknown
Address:  192.168.123.254

Non-authoritative answer:
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in
iitb.ac.in      nameserver = dns1.iitb.ac.in

C:\Users\roland.hf>
```

```
Command Prompt X + v

    timeout was 2 seconds.
Name:    www.iitb.ac.in
Address: 103.21.124.133

C:\Users\roland.hf>nslookup -type=NS iitb.ac.in
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address: 192.168.123.254

Non-authoritative answer:
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in
iitb.ac.in      nameserver = dns1.iitb.ac.in

C:\Users\roland.hf>nslookup dns2.iitb.ac.in
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address: 192.168.123.254

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:    dns2.iitb.ac.in
Address: 103.21.126.129

C:\Users\roland.hf>
```


Part 2

- 5_ The first DNS response is sent over UDP packet 483
- 6_ Matching DNS response is ~~over~~ over UDP packet 497
- 7_ DNS uses port 53 ; the query is UDP 61735 → 53
and response UDP 53 → 61735
- 8_ The DNS query sent is to 192.168.1.23.254
- 9_ The DNS query message contains 1 question 0 answers
- 10_ 1 question 1 answer
- 11_ The DNS query pair but the HTTP Get response cannot be identified for
http://gaia.cs No DNS query was made
to resolve. The browser can reuse the cached
IP without any DNS query, which
improves efficiency.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.123.29

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000057	fe80::e4bc:d413:27e...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
467	8.139027	192.168.123.253	192.168.123.29	HTTP/X...	529	HTTP/1.1 200 OK
461	8.135983	192.168.123.29	192.168.123.253	HTTP	254	GET /gatedesc.xml HTTP/1.1
994	12.810124	192.168.123.254	192.168.123.29	DNS	177	Standard query response 0x20d4 A cdn.jsdelivr.net CNAME jsdelivr.map.fastly.net A 151.101.193.229 A 151.101.1.229 A 151.101.65.2...
993	12.767052	192.168.123.29	192.168.123.254	DNS	76	Standard query 0x20d4 A cdn.jsdelivr.net
968	11.920342	192.168.123.254	192.168.123.29	DNS	121	Standard query response 0x77da A ogs.google.com CNAME www3.l.google.com A 172.217.20.110
967	11.880504	192.168.123.29	192.168.123.254	DNS	74	Standard query 0x77da A ogs.google.com
966	11.865105	192.168.123.254	192.168.123.29	DNS	96	Standard query response 0xeada A fonts.googleapis.com A 142.251.209.106
965	11.819357	192.168.123.29	192.168.123.254	DNS	80	Standard query 0xeada A fonts.googleapis.com
539	9.430518	192.168.123.254	192.168.123.29	DNS	155	Standard query response 0x0976 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
491	8.770358	192.168.123.254	192.168.123.29	DNS	93	Standard query response 0x7c39 A gain.cs.umass.edu A 128.119.245.12
ARR 276508	107.168.173.254	107.168.173.29	DNS	118	Standard query response 0x77a1 A starknath.hackthebox.com A 104.18.10.207 A 104.18.11.207	

> Frame 491: Packet, 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{C634F13A-1BE8-4000-8000-000000000000}

> Ethernet II, Src: FidaInternat_1e:4d:2d (90:61:0c:1e:4d:2d), Dst: WNC_c4:fd:7a (58:96:71:c4:fd:7a)

> Internet Protocol Version 4, Src: 192.168.123.254, Dst: 192.168.123.29

> User Datagram Protocol, Src Port: 53, Dst Port: 61735

Source Port: 53

Destination Port: 61735

Length: 59

Checksum: 0x3752 [unverified]

[Checksum Status: Unverified]

[Stream index: 20]

[Stream Packet Number: 2]

> [Timestamps]

UDP payload (51 bytes)

> Domain Name System (response)

Transaction ID: 0x7c39

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

> Queries

> Answers

[Request ID: 483]

[Time: 224.737000 milliseconds]

0000 58 96 71 c4 fd 7a 90 61 0c 1e 4d 2d 08 00 45 00 X-q-z-a--H--E

0010 08 4f dd a2 00 09 1e 11 48 8f c0 a8 7b fe c0 a8 0-.....F-{-...

0020 7b 1d 00 35 f1 27 00 3b 37 52 7c 39 81 80 00 01 {-5-'; 7R|9....

0030 00 01 00 00 00 00 04 67 61 69 61 02 63 73 05 75g aia cs u

0040 6d 61 73 73 03 65 64 75 00 00 01 00 01 c0 0c 00 mass-edu

0050 01 00 01 00 00 00 4f 00 04 80 77 f5 0c0: --W...

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.123.29

No.	Time	Source	Destination	Protocol	Length	Info
491	8.770358	192.168.123.254	192.168.123.29	DNS	93	Standard query response 0x7c39 A gaia.cs.umass.edu A 128.119.245.12
488	8.765694	192.168.123.254	192.168.123.29	DNS	118	Standard query response 0x22a1 A stackpath.bootstrapcdn.com A 104.18.10.207 A 104.18.11.207
487	8.765694	192.168.123.254	192.168.123.29	DNS	139	Standard query response 0x8be7 A code.jquery.com A 151.101.2.137 A 151.101.66.137 A 151.101.130.137 A 151.101.194.137
486	8.573585	192.168.123.254	192.168.123.29	DNS	148	Standard query response 0x9c6a HTTPS ogads-pa.clients6.google.com SOA ns1.google.com
485	8.545779	192.168.123.29	192.168.123.254	DNS	86	Standard query 0x22a1 A stackpath.bootstrapcdn.com
484	8.545779	192.168.123.29	192.168.123.254	DNS	75	Standard query 0x8be7 A code.jquery.com
483	8.545621	192.168.123.29	192.168.123.254	DNS	77	Standard query 0x7c39 A gaia.cs.umass.edu
328	5.600894	192.168.123.254	192.168.123.29	DNS	159	Standard query response 0x1932 A optimizationguide-pa.googleapis.com A 216.239.32.223 A 216.239.34.223 A 216.239.36.223 A 216.239.38.223
305	5.497570	192.168.123.29	192.168.123.254	DNS	95	Standard query 0x1932 A optimizationguide-pa.googleapis.com
304	5.497411	192.168.123.29	192.168.123.254	DNS	95	Standard query 0x0976 HTTPS optimizationguide-pa.googleapis.com
257	4.986105	192.168.123.254	192.168.123.29	DNS	156	Standard query response 0x452b HTTPS apis.google.com CNAME plus.l.google.com SOA ns1.google.com
236	4.088587	192.168.123.254	192.168.123.29	DNS	122	Standard query response 0x3040 A site.google.com FQDN plus.l.google.com A 142.251.200.78

> Frame 483: Packet, 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{C634F13A-1BEB-4000-8000-000000000000}

> Ethernet II, Src: WNC_c4:fd:7a (58:96:71:c4:fd:7a), Dst: FidaInternat_1e:4d:2d (90:61:0c:1e:4d:2d)

> Internet Protocol Version 4, Src: 192.168.123.29, Dst: 192.168.123.254

> User Datagram Protocol, Src Port: 61735, Dst Port: 53

Source Port: 61735

Destination Port: 53

Length: 43

Checksum: 0x9e29 [unverified]

[Checksum Status: Unverified]

[Stream index: 20]

[Stream Packet Number: 1]

> [Timestamps]

UDP payload (35 bytes)

> Domain Name System (query)

Transaction ID: 0x7c39

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

[Response In: 491]

0000 00 61 0c 1e 4d 2d 58 96 71 c4 fd 7a 08 00 45 00 a -M-X q -2 -E

0010 00 3f af 49 00 00 80 11 12 f8 c0 a8 7b 1d c0 a8 ? I{...

0020 7b fe f1 27 00 35 00 2b 9e 29 7c 39 01 00 00 01 {...'.5.+)|9....

0030 00 00 00 00 00 04 67 61 69 61 02 63 73 05 75g aia:cs:u

0040 6d 61 73 73 03 65 64 75 00 00 01 00 01 mass:edu