

Student name: Gökay Gülsøy
Student number: 270201072

-CENG312-ASSIGNMENT 1 HTTP and DNS-

PART-1)

1.) Fundamental difference between GET and POST method according to figure 1 and figure 2 is that POST method authenticates the user credentials using Base-64 encoding which we can see in the authorization section, whereas GET method does not provide such an authentication mechanism.

2.) In the authorization section of POST request we can see a encoded credentials that we have passed from terminal for userid and password.

3.) Actually it is not safe because POST request encodes the userid and password for server authentication, but it is not using encryption because we are still making this request over HTTP not over HTTPS. But compared to GET it is safer at least.

Figure 1: GET request

No.	Time	Source	Destination	Protocol	Length	Info
+ 251	2023-04-08 21:22:55,288992121	192.168.0.29	34.127.31.83	HTTP	374	GET /favicon.ico HTTP/1.1
+ 266	2023-04-08 21:22:55,546641524	34.127.31.83	192.168.0.29	HTTP	821	HTTP/1.1 200 OK (image/x-icon)
+ 583	2023-04-08 21:23:04,290214564	128.119.245...	192.168.0.29	HTTP	496	HTTP/1.1 200 OK (text/html)
+ 581	2023-04-08 21:23:04,132181897	192.168.0.29	128.119.245...	HTTP/JS...	302	POST /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 , JavaScript Object Notation (application/json)

> Frame 251: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)
> Internet Protocol Version 4, Src: 192.168.0.29, Dst: 34.127.31.83
> Transmission Control Protocol, Src Port: 45216, Dst Port: 80, Seq: 1, Ack: 1, Len: 308
> Hypertext Transfer Protocol
> GET /favicon.ico HTTP/1.1\r\n
Host: www.washington.edu\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0\r\n
Accept: image/avif,image/webp,*/*\r\n
Accept-Language: en-GB,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Referer: http://www.washington.edu/\r\n
\r\n
[Full request URI: http://www.washington.edu/favicon.ico]
[HTTP request 1/1]
[Response in frame: 266]
0000 00 10 18 de ad 05 3c 58 c2 a5 ff aa 08 00 45 00 .<.....E
0001 01 68 1e ee 40 00 40 06 18 0b c0 a8 00 1d 22 7f .h @ @
0020 1f 53 b6 a9 00 50 89 4e 21 44 c2 c0 11 b9 88 18 .S ..P N ID.....
0030 01 f6 03 f2 00 00 01 01 08 0a 73 f7 f5 49 12 ed S ..I..
0040 ae 51 47 45 54 20 2f 66 61 76 69 63 of 6e 2e 69 .QGET /f avicon.i
0050 63 6f 20 48 54 54 50 2f 31 26 31 0d 0a 48 6f 73 co HTTP/ 1.1 - Hos
0060 74 3a 26 77 77 77 2e 77 61 73 68 69 6e 67 74 6f t: www.w ashingto
0070 6e 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e n.edu..U ser-Agen
0080 74 3a 26 4d 6f 7a 69 6c 66 61 2f 35 2e 38 28 28 t: Mozil la/5.0 (
0090 58 31 3b 29 55 62 75 6e 74 75 3b 28 4c 69 6e X11; Ubr ntu; Lin
00a0 75 78 26 78 38 36 5f 36 34 38 20 72 76 3a 31 38 ux x86_6 4; rv:10
00b0 39 2e 38 29 28 47 65 63 6b 6f 2f 32 39 31 30 30 9.0) Ge ko/20100
00c0 31 30 31 29 46 69 72 65 66 6f 78 2f 31 31 31 2e 101 Fire fox/111.
00d0 30 0d 0a 41 63 63 65 70 74 3a 26 69 6d 61 67 65 0..Accep t: image
00e0 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 /avif,image/webp

Figure 2: POST request

No.	Time	Source	Destination	Protocol	Length	Info
251	2023-04-08 21:22:55,268092121	192.168.0.29	34.127.31.83	HTTP	374	GET /favicon.ico HTTP/1.1
266	2023-04-08 21:22:55,546641524	34.127.31.83	192.168.0.29	HTTP	821	HTTP/1.1 200 OK (image/x-icon)
+ 583	2023-04-08 21:23:04,290214564	128.119.245.29	192.168.0.29	HTTP	496	HTTP/1.1 200 OK (text/html)
+ 581	2023-04-08 21:23:04,132181897	192.168.0.29	128.119.245.29	HTTP/JS...	302	POST /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 , JavaScript Object Notation (application/json)

Frame 581: 302 bytes on wire (2416 bits), 302 bytes captured (2416 bits) on interface wlo1, id 0
 Ethernet II, Src: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)
 Internet Protocol Version 4, Src: 192.168.0.29, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 60718, Dst Port: 80, Seq: 1, Ack: 1, Len: 236
 Hypertext Transfer Protocol
 POST /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 Authorization: Basic dXNlcm1kOnBhc3N3b3JkYrln
HTTP POST request with authentication using Base-64 encoding
 User-Agent: curl/7.81.0\r\n
 Accept: */*\r\n
 Content-Type: application/json\r\n
 Content-Length: 19\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
 [HTTP request 1/1]
 [Response in frame: 583]
 File Data: 19 bytes
 JavaScript Object Notation: application/json
 Line-based text data: application/json (1 lines)

```
0040: ba 80 50 4f 53 54 20 2f 77 69 72 65 73 68 61 72 . POST / wireshar
0050: 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 k-labs/H TTP-wire
0060: 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 6d 6c shark-fi le1.html
0070: 20 48 54 54 58 2f 31 2e 31 00 0a 48 6f 73 74 3a HTTP/1. 1-Host:
0080: 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 gaia.cs .umass.e
0090: 64 75 9d 0a [1] 75 74 68 6f 72 69 7a 61 74 69 6f du -Auth orizatio
00a0: 6e 3a 28 42 61 73 69 62 20 64 58 4e 6c 63 6d 6c n: Basic dXNlcm1
00b0: 6b 4f 6e 42 68 63 34 3e 33 62 33 4a 6b 0d 08 55 kOnBhc3N 3b3Jk .U
00c0: 73 65 72 2d 41 67 65 6e 74 3a 20 63 75 72 6c 2f ser-Agen t: curl/
00d0: 37 2e 38 31 2e 38 0d 0a 41 63 63 65 70 74 3a 20 7.81.0 . Accept:
00e0: 2a 2f 2a 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 */*Content-Typ
00f0: 65 3a 28 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6a e: appli cation/j
0100: 73 6f 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e son .Content-Len
0110: 67 74 68 3a 29 31 39 0d 0a 0d 0a e2 80 9c 70 72 gth: 19. ....pr
0120: 6f 64 75 63 74 49 64 3d 31 32 33 34 35 36 oductId= 123456
```

PART-2)

1.) FTP (File transfer) protocol.

2.) FTP is used for transferring file from server to client over a computer

network.

3.) Name of the transferred file is cover.jpg and it's file type is .jpg file.

4.) In the given scenario client is establishing connection with FTP server

initially, then user provides username and server asks for password of user.

After FTP server authenticated the username and password, user has successfully

logged in. Then user requests cover.jpg file from server, server opens data connection

and transfers data then data connection was closed. Finally client makes a QUIT request

command and server closes control connection.

Figure 3: Request-Response Flow-1

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-03-30 11:35:32,576835	44.241.66.173	10.8.42.198	FTP	94	Response: 220 Welcome to the DLP Test FTP Server
2	2023-03-30 11:35:32,576227	10.8.42.198	44.241.66.173	FTP	68	Request: USER dluser
3	2023-03-30 11:35:32,818702	44.241.66.173	10.8.42.198	FTP	86	Response: 331 Please specify the password.
4	2023-03-30 11:35:32,818861	10.8.42.198	44.241.66.173	FTP	86	Request: PASS rNrKVTXg9z73RqJRMxWuGHbeu
5	2023-03-30 11:35:33,687032	44.241.66.173	10.8.42.198	FTP	77	Response: 230 Login successful.
6	2023-03-30 11:35:33,687129	10.8.42.198	44.241.66.173	FTP	59	Request: PWD
7	2023-03-30 11:35:33,923883	44.241.66.173	10.8.42.198	FTP	63	Response: 257 "/"
8	2023-03-30 11:35:33,924089	10.8.42.198	44.241.66.173	FTP	68	Request: EPSV
9	2023-03-30 11:35:34,165814	44.241.66.173	10.8.42.198	FTP	162	Response: 229 Entering Extended Passive Mode (1029).
10	2023-03-30 11:35:36,858245	10.8.42.198	44.241.66.173	FTP	62	Request: TYPE I
11	2023-03-30 11:35:37,095945	44.241.66.173	10.8.42.198	FTP	85	Response: 206 Switching to Binary mode.
12	2023-03-30 11:35:37,096542	10.8.42.198	44.241.66.173	FTP	78	Request: STOR cover.jpg
13	2023-03-30 11:35:37,336363	44.241.66.173	10.8.42.198	FTP	76	Response: 158 Ok to send data.
14	2023-03-30 11:35:39,117981	44.241.66.173	10.8.42.198	FTP	78	Response: 226 Transfer complete.
15	2023-03-30 11:35:39,128811	10.8.42.198	44.241.66.173	FTP	68	Request: QUIT
16	2023-03-30 11:35:39,366408	44.241.66.173	10.8.42.198	FTP	68	Response: 221 Goodbye.

▶ Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{ABEFC228-C742-47FC-967B-425A570F66B9}, id 0
 ▶ Ethernet II, Src: 7c:89:c2:b5:db:12 (7c:89:c2:b5:db:12), Dst: IntelCor_4a:4a:a7 (68:54:5a:4a:a7) (0x0000000000000000000000000000000000000000)
 ▶ Internet Protocol Version 4, Src: 44.241.66.173, Dst: 10.8.42.198
 ▶ Transmission Control Protocol, Src Port: 21, Dst Port: 60868, Seq: 1, Ack: 1, Len: 40
 ▶ File Transfer Protocol (FTP)
 ▶ 220 Welcome to the DLP Test FTP Server\r\n
Response code: Service ready for new user (220)
 Response arg: Welcome to the DLP Test FTP Server
 [Current working directory:]
FTP server is establishing a connection with a new client

0000	68	54	5a	4a	4a	a7	7c	89	c2	5b	db	12	08	00	45	00	htZJJ ...[....E
0010	00	50	ff	91	40	00	e8	06	ee	b1	2c	f1	42	ad	0a	08	.P @... .B...
0020	2a	00	15	ed	c4	61	f7	a8	5b	da	3d	0b	e4	50	18	*.... a... [=..P	
0030	00	d3	fe	e3	00	00	32	32	30	20	57	65	6c	63	6f	6d 22 0 Welcom
0040	65	20	74	67	20	74	68	65	20	44	4c	50	20	54	65	73	e to the DLP Tes
0050	74	20	46	54	50	20	53	65	72	76	65	72	0d	0a	t FTP Se	rver..	

Figure 4: Request-Response Flow-2

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-03-30 11:35:32,576835	44.241.66.173	10.8.42.198	FTP	94	Response: 220 Welcome to the DLP Test FTP Server
2	2023-03-30 11:35:32,576227	10.8.42.198	44.241.66.173	FTP	68	Request: USER dluser
3	2023-03-30 11:35:32,818702	44.241.66.173	10.8.42.198	FTP	88	Response: 331 Please specify the password.
4	2023-03-30 11:35:32,818861	10.8.42.198	44.241.66.173	FTP	88	Request: PASS rNrKVTXg9z73RqJRMxWuGHbeu
5	2023-03-30 11:35:33,687032	44.241.66.173	10.8.42.198	FTP	77	Response: 230 Login successful.
6	2023-03-30 11:35:33,687129	10.8.42.198	44.241.66.173	FTP	59	Request: PWD
7	2023-03-30 11:35:33,923883	44.241.66.173	10.8.42.198	FTP	63	Response: 257 "/"
8	2023-03-30 11:35:33,924089	10.8.42.198	44.241.66.173	FTP	68	Request: EPSV
9	2023-03-30 11:35:34,165814	44.241.66.173	10.8.42.198	FTP	162	Response: 229 Entering Extended Passive Mode (1029).
10	2023-03-30 11:35:36,858245	10.8.42.198	44.241.66.173	FTP	62	Request: TYPE I
11	2023-03-30 11:35:37,095945	44.241.66.173	10.8.42.198	FTP	85	Response: 206 Switching to Binary mode.
12	2023-03-30 11:35:37,096542	10.8.42.198	44.241.66.173	FTP	78	Request: STOR cover.jpg
13	2023-03-30 11:35:37,336363	44.241.66.173	10.8.42.198	FTP	76	Response: 158 Ok to send data.
14	2023-03-30 11:35:39,117981	44.241.66.173	10.8.42.198	FTP	78	Response: 226 Transfer complete.
15	2023-03-30 11:35:39,128811	10.8.42.198	44.241.66.173	FTP	68	Request: QUIT
16	2023-03-30 11:35:39,366408	44.241.66.173	10.8.42.198	FTP	68	Response: 221 Goodbye.

▶ Frame 3: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{ABEFC228-C742-47FC-967B-425A570F66B9}, id 0
 ▶ Ethernet II, Src: 7c:89:c2:b5:db:12 (7c:89:c2:b5:db:12), Dst: IntelCor_4a:4a:a7 (68:54:5a:4a:a7) (0x0000000000000000000000000000000000000000)
 ▶ Internet Protocol Version 4, Src: 44.241.66.173, Dst: 10.8.42.198
 ▶ Transmission Control Protocol, Src Port: 21, Dst Port: 60868, Seq: 1, Ack: 1, Len: 34
 ▶ File Transfer Protocol (FTP)
 ▶ 331 Please specify the password.\r\n
Response code: User name okay, need password (331)
 Response arg: Please specify the password.
 [Current working directory:]
Client enters its username and FTP server asks for the clients password

0000	68	54	5a	4a	4a	a7	7c	89	c2	5b	db	12	08	00	45	00	htZJJ ...[....E
0010	00	4a	ff	93	40	00	e8	06	ee	b5	2c	f1	42	ad	0a	08	.J @... .B...
0020	2a	00	15	ed	c4	61	f7	a8	83	da	3d	0b	f2	50	18	*.... a... [=..P	
0030	00	d3	e4	cd	00	00	33	33	31	20	58	6c	65	61	73	65 33 1 Please
0040	20	73	70	65	63	69	66	79	20	74	68	65	20	70	61	73	specify the pas
0050	73	77	6f	72	64	2e	0d	0a									word...

Figure 5: Request-Response Flow-3

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-03-30 11:35:32,576035	44.241.66.173	10.8.42.190	FTP	94	94 Response: 220 Welcome to the DLP Test FTP Server
2	2023-03-30 11:35:32,576227	10.8.42.190	44.241.66.173	FTP	68	68 Request: USER dluser
3	2023-03-30 11:35:32,818702	44.241.66.173	10.8.42.190	FTP	88	88 Response: 331 Please specify the password.
4	2023-03-30 11:35:32,818861	10.8.42.190	44.241.66.173	FTP	86	86 Request: PASS rNrKYTX9g7z3RgJRxwluGHbeu
5	2023-03-30 11:35:33,657632	44.241.66.173	10.8.42.190	FTP	77	77 Response: 230 Login successful.
6	2023-03-30 11:35:33,687129	10.8.42.190	44.241.66.173	FTP	59	59 Request: PWD
7	2023-03-30 11:35:33,923883	44.241.66.173	10.8.42.190	FTP	63	63 Response: 257 "/"
8	2023-03-30 11:35:33,924009	10.8.42.190	44.241.66.173	FTP	60	60 Request: EPSV
9	2023-03-30 11:35:34,165814	44.241.66.173	10.8.42.190	FTP	102	102 Response: 229 Entering Extended Passive Mode (1029).
10	2023-03-30 11:35:36,858245	10.8.42.190	44.241.66.173	FTP	62	62 Request: TYPE I
11	2023-03-30 11:35:37,095945	44.241.66.173	10.8.42.190	FTP	85	85 Response: 200 Switching to Binary mode.
12	2023-03-30 11:35:37,336363	10.8.42.190	44.241.66.173	FTP	70	70 Request: STOR cover.jpg
13	2023-03-30 11:35:39,128011	44.241.66.173	10.8.42.190	FTP	76	76 Response: 150 Ok to send data.
14	2023-03-30 11:35:39,117081	10.8.42.190	44.241.66.173	FTP	78	78 Response: 226 Transfer complete.
15	2023-03-30 11:35:39,128011	10.8.42.190	44.241.66.173	FTP	60	60 Request: QUIT
16	2023-03-30 11:35:39,366408	44.241.66.173	10.8.42.190	FTP	68	68 Response: 221 Goodbye.

Frame 5: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{ABEFC228-C742-47FC-967B-425A570F66B9}, id 0
Ethernet II, Src: 7c:89:c2:5b:db:12 (7c:89:c2:5b:db:12), Dst: IntelCor_4a:4a:a7 (68:54:5a:4a:4a:a7)
Internet Protocol Version 4, Src: 44.241.66.173, Dst: 10.8.42.190
Transmission Control Protocol, Src Port: 21, Dst Port: 60868, Seq: 75, Ack: 47, Len: 23
File Transfer Protocol (FTP)
- 230 Login successful.\r\n

Response code: User logged in, proceed (230)
Response arg: Login successful.
[Current working directory:]

Client enters its password and FTP server authenticates the given username and password

0000	68 54 5a 4a 4a a7 7c 89 c2 5b db 12 08 00 45 00	hTZJJ . [....E
0010	00 3f ff 95 48 00 e8 06 ee b2 2c f1 42 ad 0a 08	?@... , B...
0020	2a 00 15 ed c4 61 f7 a8 a5 da 3d 0c 12 50 18	*.... a... =.P
0030	00 d3 4a 3f 00 00 32 33 30 20 4c 6f 67 69 6e 20	.J? .23 & Login
0040	73 75 63 63 65 73 73 66 75 6c 2e 0d 0a	successf ul...

Figure 6: Request-Response Flow-4

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-03-30 11:35:32,576035	44.241.66.173	10.8.42.190	FTP	94	94 Response: 220 Welcome to the DLP Test FTP Server
2	2023-03-30 11:35:32,576227	10.8.42.190	44.241.66.173	FTP	68	68 Request: USER dluser
3	2023-03-30 11:35:32,818702	44.241.66.173	10.8.42.190	FTP	88	88 Response: 331 Please specify the password.
4	2023-03-30 11:35:32,818861	10.8.42.190	44.241.66.173	FTP	86	86 Request: PASS rNrKYTX9g7z3RgJRxwluGHbeu
5	2023-03-30 11:35:33,657632	44.241.66.173	10.8.42.190	FTP	77	77 Response: 230 Login successful.
6	2023-03-30 11:35:33,687129	10.8.42.190	44.241.66.173	FTP	59	59 Request: PWD
7	2023-03-30 11:35:33,923883	44.241.66.173	10.8.42.190	FTP	63	63 Response: 257 "/"
8	2023-03-30 11:35:33,924009	10.8.42.190	44.241.66.173	FTP	60	60 Request: EPSV
9	2023-03-30 11:35:34,165814	44.241.66.173	10.8.42.190	FTP	102	102 Response: 229 Entering Extended Passive Mode (1029).
10	2023-03-30 11:35:36,858245	10.8.42.190	44.241.66.173	FTP	62	62 Request: TYPE I
11	2023-03-30 11:35:37,095945	44.241.66.173	10.8.42.190	FTP	85	85 Response: 200 Switching to Binary mode.
12	2023-03-30 11:35:37,336363	10.8.42.190	44.241.66.173	FTP	70	70 Request: STOR cover.jpg
13	2023-03-30 11:35:39,117081	44.241.66.173	10.8.42.190	FTP	76	76 Response: 150 Ok to send data.
14	2023-03-30 11:35:39,128011	10.8.42.190	44.241.66.173	FTP	78	78 Response: 226 Transfer complete.
15	2023-03-30 11:35:39,128011	10.8.42.190	44.241.66.173	FTP	60	60 Request: QUIT
16	2023-03-30 11:35:39,366408	44.241.66.173	10.8.42.190	FTP	68	68 Response: 221 Goodbye.

Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{ABEFC228-C742-47FC-967B-425A570F66B9}, id 0
Ethernet II, Src: IntelCor_4a:4a:a7 (68:54:5a:4a:4a:a7), Dst: 7c:89:c2:5b:db:12 (7c:89:c2:5b:db:12)
Internet Protocol Version 4, Src: 10.8.42.190, Dst: 44.241.66.173
Transmission Control Protocol, Src Port: 60868, Dst Port: 21, Seq: 66, Ack: 186, Len: 16
File Transfer Protocol (FTP)
- STOR cover.jpg\r\n

Request command: STOR
Request arg: cover.jpg
[Current working directory: /]

Client requests cover.jpg file from FTP server

0000	7c 89 c2 5b db 12 68 54 5a 4a 4a a7 08 00 45 00	.[. hT ZJJ ..E
0010	00 38 2b 44 40 00 80 06 00 00 0a 08 2a be 2c f1	.8+D0... .*. .
0020	42 ad ed c4 00 15 da 3d 0c 25 61 f7 a9 14 50 18	B..... = %a ..P
0030	02 00 a4 8e 00 00 53 54 4f 52 20 63 6f 76 65 72ST OR cover
0040	2e 6a 70 67 0d 0a	.jpg ..

Figure 7: Request-Response Flow-5

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-03-30 11:35:32,576835	44.241.66.173	10.8.42.190	FTP	94	Response: 220 Welcome to the DLP Test FTP Server
2	2023-03-30 11:35:32,576227	10.8.42.190	44.241.66.173	FTP	68	Request: USER dlpuser
3	2023-03-30 11:35:32,818702	44.241.66.173	10.8.42.190	FTP	88	Response: 331 Please specify the password.
4	2023-03-30 11:35:32,818861	10.8.42.190	44.241.66.173	FTP	86	Request: PASS rNrKYTXg7z3RgJRmxWuGHbeu
5	2023-03-30 11:35:33,687932	44.241.66.173	10.8.42.190	FTP	77	Response: 230 Login successful.
6	2023-03-30 11:35:33,687129	10.8.42.190	44.241.66.173	FTP	59	Request: PWD
7	2023-03-30 11:35:33,923883	44.241.66.173	10.8.42.190	FTP	63	Response: 257 "/"
8	2023-03-30 11:35:33,924089	10.8.42.190	44.241.66.173	FTP	60	Request: EPSV
9	2023-03-30 11:35:34,165814	44.241.66.173	10.8.42.190	FTP	102	Response: 229 Entering Extended Passive Mode (1029).
10	2023-03-30 11:35:36,858245	10.8.42.190	44.241.66.173	FTP	62	Request: TYPE I
11	2023-03-30 11:35:37,095945	44.241.66.173	10.8.42.190	FTP	85	Response: 200 Switching to Binary mode.
12	2023-03-30 11:35:37,096542	10.8.42.190	44.241.66.173	FTP	78	Request: STOR cover.jpg
13	2023-03-30 11:35:37,336363	44.241.66.173	10.8.42.190	FTP	76	Response: 156 Ok to send data.
14	2023-03-30 11:35:39,117981	44.241.66.173	10.8.42.190	FTP	78	Response: 226 Transfer complete.
15	2023-03-30 11:35:39,128811	10.8.42.190	44.241.66.173	FTP	60	Request: QUIT
16	2023-03-30 11:35:39,366408	44.241.66.173	10.8.42.190	FTP	68	Response: 221 Goodbye.

FTP server checks whether the requested file exists and finds it, then opens a data connection

```
0000 68 54 5a 4a 4a a7 7c 89 c2 5b db 12 08 00 45 00 hTZJJ | . [ ... E
0010 00 3e ff 9a 40 00 e8 06 ee ba 2c f1 42 ad 0a 08 .> @ . . . , B ...
0020 2a be 00 15 ed c4 61 f7 a9 14 da 3d 0c 35 50 18 * . . . a . . . =5P.
0030 00 d3 18 f7 00 00 31 35 30 20 4f 6b 20 74 6f 20 .....15 0 Ok to
0040 73 65 6e 64 20 64 61 74 61 2e 0d 0a send dat a ...
```

Figure 8: Request-Response Flow-6

No.	Time	Source	Destination	Protocol	Length	Info
-	1 2023-03-30 11:35:32,576835	44.241.66.173	10.8.42.190	FTP	94	Response: 220 Welcome to the DLP Test FTP Server
2	2023-03-30 11:35:32,576227	10.8.42.190	44.241.66.173	FTP	68	Request: USER dlpuser
3	2023-03-30 11:35:32,818702	44.241.66.173	10.8.42.190	FTP	88	Response: 331 Please specify the password.
4	2023-03-30 11:35:32,818861	10.8.42.190	44.241.66.173	FTP	86	Request: PASS rNrKYTXg7z3RgJRmxWuGHbeu
5	2023-03-30 11:35:33,687932	44.241.66.173	10.8.42.190	FTP	77	Response: 230 Login successful.
6	2023-03-30 11:35:33,687129	10.8.42.190	44.241.66.173	FTP	59	Request: PWD
7	2023-03-30 11:35:33,923883	44.241.66.173	10.8.42.190	FTP	63	Response: 257 "/"
8	2023-03-30 11:35:33,924089	10.8.42.190	44.241.66.173	FTP	60	Request: EPSV
9	2023-03-30 11:35:34,165814	44.241.66.173	10.8.42.190	FTP	102	Response: 229 Entering Extended Passive Mode (1029).
10	2023-03-30 11:35:36,858245	10.8.42.190	44.241.66.173	FTP	62	Request: TYPE I
11	2023-03-30 11:35:37,095945	44.241.66.173	10.8.42.190	FTP	85	Response: 200 Switching to Binary mode.
12	2023-03-30 11:35:37,096542	10.8.42.190	44.241.66.173	FTP	78	Request: STOR cover.jpg
13	2023-03-30 11:35:37,336363	44.241.66.173	10.8.42.190	FTP	76	Response: 156 Ok to send data.
14	2023-03-30 11:35:39,117981	44.241.66.173	10.8.42.190	FTP	78	Response: 226 Transfer complete.
15	2023-03-30 11:35:39,128811	10.8.42.190	44.241.66.173	FTP	60	Request: QUIT
16	2023-03-30 11:35:39,366408	44.241.66.173	10.8.42.190	FTP	68	Response: 221 Goodbye.

FTP server closes the data connection after transferring the cover.jpg file

```
0000 68 54 5a 4a 4a a7 7c 89 c2 5b db 12 08 00 45 00 hTZJJ | . [ ... E
0010 00 40 ff 9b 40 00 e8 06 ee b7 2c f1 42 ad 0a 08 @ . @ . . , B ...
0020 2a be 00 15 ed c4 61 f7 a9 2a da 3d 0c 35 50 18 * . . . a . . . =5P.
0030 00 d3 5c 19 00 00 32 32 36 20 54 72 61 6e 73 66 ..\..22 6 Transf
0040 65 72 20 63 6f 6d 70 6c 65 74 65 2e 0d 0a er compl etc...
```

Response code (ftp.response.code), 3 bytes

Packets: 16 · Displayed: 16 (100.0%)

Profile: Default

Figure 9: Request-Response Flow-7

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-03-30 11:35:32,576035	44.241.66.173	10.8.42.190	FTP	94	Response: 220 Welcome to the DLP Test FTP Server
2	2023-03-30 11:35:32,576227	10.8.42.190	44.241.66.173	FTP	68	Request: USER dlplayer
3	2023-03-30 11:35:32,818702	44.241.66.173	10.8.42.190	FTP	88	Response: 331 Please specify the password.
4	2023-03-30 11:35:32,818861	10.8.42.190	44.241.66.173	FTP	86	Request: PASS rNrKYTXg97z3RqJRMxWuGHbeu
5	2023-03-30 11:35:33,687032	44.241.66.173	10.8.42.190	FTP	77	Response: 230 Login successful.
6	2023-03-30 11:35:33,687129	10.8.42.190	44.241.66.173	FTP	59	Request: PWD
7	2023-03-30 11:35:33,923883	44.241.66.173	10.8.42.190	FTP	63	Response: 557 "/"
8	2023-03-30 11:35:33,924009	10.8.42.190	44.241.66.173	FTP	60	Request: EPSV
9	2023-03-30 11:35:34,165814	44.241.66.173	10.8.42.190	FTP	102	Response: 229 Entering Extended Passive Mode (1029).
10	2023-03-30 11:35:36,858245	10.8.42.190	44.241.66.173	FTP	62	Request: TYPE I
11	2023-03-30 11:35:37,895945	44.241.66.173	10.8.42.190	FTP	85	Response: 200 Switching to Binary mode.
12	2023-03-30 11:35:37,896542	10.8.42.190	44.241.66.173	FTP	78	Request: STOR cover.jpg
13	2023-03-30 11:35:37,336363	44.241.66.173	10.8.42.190	FTP	76	Response: 150 Ok to send data.
14	2023-03-30 11:35:39,117981	44.241.66.173	10.8.42.190	FTP	78	Response: 226 Transfer complete.
15	2023-03-30 11:35:39,128011	10.8.42.190	44.241.66.173	FTP	60	Request: QUIT
16	2023-03-30 11:35:39,366408	44.241.66.173	10.8.42.190	FTP	68	Response: 221 Goodbye.

Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{ABEFC228-C742-47FC-967B-425A570F66B9}, id 0
Ethernet II, Src: IntelCor_4a:4a:a7 (68:54:5a:4a:4a:a7), Dst: 7c:89:c2:5b:db:12 (7c:89:c2:5b:db:12)
Internet Protocol Version 4, Src: 10.8.42.190, Dst: 44.241.66.173
Transmission Control Protocol, Src Port: 68668, Dst Port: 21, Seq: 82, Ack: 232, Len: 6
File Transfer Protocol (FTP)
QUIT\r\n

Request command: QUIT
[Current working directory: /]

0000 7c 89 c2 5b db 12 68 54 5a 4a 4a a7 08 00 45 00 |...[...hT ZJJ...E.
0010 00 2e 2c 9d 40 00 80 06 00 00 a0 08 2a be 2c f1 .,.@...*..
0020 42 ad ed c4 00 15 da 3d 0c 35 61 f7 a9 42 50 18 B.....=..5a..BP.
0030 02 00 a4 84 00 00 51 55 49 54 0d 0aQI II..

Request command (ftp.request.command), 4 bytes

Packets: 16 - Displayed: 16 (100.0%)

Profile: Default

Figure 10: Request-Response Flow-8

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-03-30 11:35:32,576035	44.241.66.173	10.8.42.190	FTP	94	Response: 220 Welcome to the DLP Test FTP Server
2	2023-03-30 11:35:32,576227	10.8.42.190	44.241.66.173	FTP	68	Request: USER dlplayer
3	2023-03-30 11:35:32,818702	44.241.66.173	10.8.42.190	FTP	88	Response: 331 Please specify the password.
4	2023-03-30 11:35:32,818861	10.8.42.190	44.241.66.173	FTP	86	Request: PASS rNrKYTXg97z3RqJRMxWuGHbeu
5	2023-03-30 11:35:33,687032	44.241.66.173	10.8.42.190	FTP	77	Response: 230 Login successful.
6	2023-03-30 11:35:33,687129	10.8.42.190	44.241.66.173	FTP	59	Request: PWD
7	2023-03-30 11:35:33,923883	44.241.66.173	10.8.42.190	FTP	63	Response: 557 "/"
8	2023-03-30 11:35:33,924009	10.8.42.190	44.241.66.173	FTP	60	Request: EPSV
9	2023-03-30 11:35:34,165814	44.241.66.173	10.8.42.190	FTP	102	Response: 229 Entering Extended Passive Mode (1029).
10	2023-03-30 11:35:36,858245	10.8.42.190	44.241.66.173	FTP	62	Request: TYPE I
11	2023-03-30 11:35:37,895945	44.241.66.173	10.8.42.190	FTP	85	Response: 200 Switching to Binary mode.
12	2023-03-30 11:35:37,896542	10.8.42.190	44.241.66.173	FTP	78	Request: STOR cover.jpg
13	2023-03-30 11:35:37,336363	44.241.66.173	10.8.42.190	FTP	76	Response: 150 Ok to send data.
14	2023-03-30 11:35:39,117981	44.241.66.173	10.8.42.190	FTP	78	Response: 226 Transfer complete.
15	2023-03-30 11:35:39,128011	10.8.42.190	44.241.66.173	FTP	60	Request: QUIT
16	2023-03-30 11:35:39,366408	44.241.66.173	10.8.42.190	FTP	68	Response: 221 Goodbye.

Frame 16: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{ABEFC228-C742-47FC-967B-425A570F66B9}, id 0
Ethernet II, Src: IntelCor_4a:4a:a7 (68:54:5a:4a:4a:a7), Dst: IntelCor_4a:4a:a7 (68:54:5a:4a:4a:a7)
Internet Protocol Version 4, Src: 7c:89:c2:5b:db:12 (7c:89:c2:5b:db:12), Dst: 44.241.66.173
Transmission Control Protocol, Src Port: 68668, Dst Port: 21, Seq: 232, Ack: 88, Len: 14
File Transfer Protocol (FTP)
221 Goodbye.\r\n

Response code: Service closing control connection (221)
Response arg: Goodbye.
[Current working directory: /]

0000 68 54 5a 4a 4a a7 7c 89 c2 5b db 12 08 00 45 00 hTZJJ |...[...E.
0010 00 36 ff 9c 40 00 e8 06 ee c0 2c f1 42 ad 0a 08 .6 @...,.B.
0020 2a be 00 15 ed c4 61 f7 a9 42 da 3d 0c 3b 50 18 *...a-B=;P.
0030 00 d3 3c 23 00 00 62 32 31 20 47 6f 6f 64 62 79 <# 22 1 Goody
0040 65 2e 0d 0a e...

Response code (ftp.response.code), 3 bytes

Packets: 16 - Displayed: 16 (100.0%)

Profile: Default

PART-3)

Section-1)

1.) Writing IP addresses instead of DNS name is known as name-to-address

translation.

2.) Because IP addresses are not usually human-readable or easy to recognize

even if they are better for routers. For the sake of easy understanding of domains,

DNS names are used.

3.) Query made was a recursive DNS query as we can see from figure 11 below.

4.) DNS name of the IP address 193.140.248.136 is webpro.iyte.edu.tr as we can

see from figure 12. below.

Figure 11: DNS-query

No.	Time	Source	Destination	Protocol	Length	Info
↑	2 2623-04-09 12:32:06,281189862	192.168.0.29	46.196.235.35	DNS	99	Standard query 0xc51f PTR 136.248.140.193.in-addr.arpa OPT
↓	3 2623-04-09 12:32:06,286525591	46.196.235.35	192.168.0.29	DNS	131	Standard query response 0xc51f PTR 136.248.140.193.in-addr.arpa PTR webpro.iyte.edu.tr OPT

> Frame 2: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa), Dst: Broadcom_de:ad:b5 (00:10:18:de:ad:b5)
> Internet Protocol Version 4, Src: 192.168.0.29, Dst: 46.196.235.35
> User Datagram Protocol, Src Port: 59339, Dst Port: 53
▼ Domain Name System (query)
 Transaction ID: 0xc51f
 Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
 0.... = Truncated: Message is not truncated
 1.... = Recursion desired: Do query recursively
 0... = Z: Reserved (0)
 0.... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
▼ Queries
 > 136.248.140.193.in-addr.arpa: type PTR, class IN
▼ Additional records
 > <Root>: type OPT
 [Response In: 3]

Making a recursive DNS query to find
the DNS name of the IP address 193.140.248.136

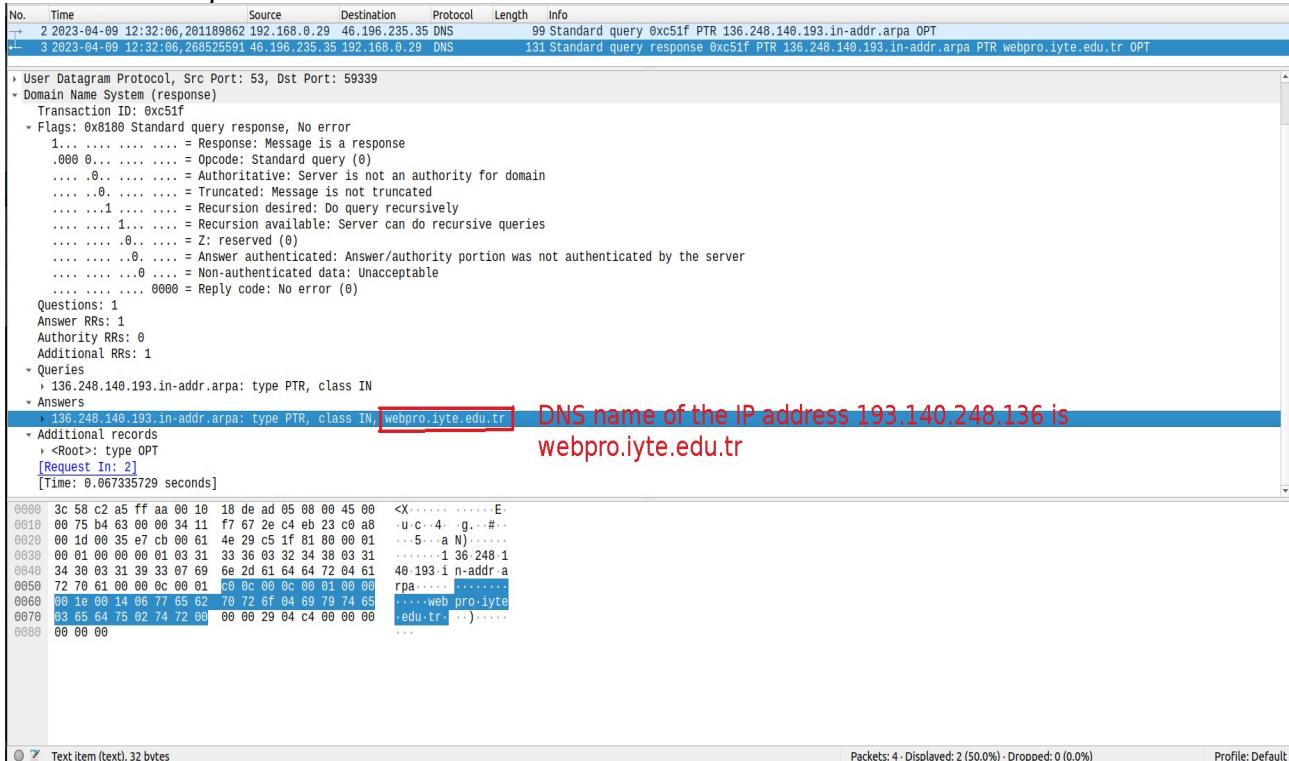
0000 00 10 18 de ad 05 3c 58 c2 a5 ff aa 08 00 45 00<XE
0010 00 55 dc 22 00 00 40 11 c3 c8 c0 a8 00 1d 2e c4 U " @
0020 eb 23 e7 cb 00 35 00 41 da ff c5 1f 01 00 00 01 #...5 A
0030 00 00 00 00 00 01 03 31 33 36 03 32 34 38 03 311 36.248.1
0040 34 30 03 31 39 33 07 69 6e 2d 61 64 64 72 04 61 40 193 i n-addr.a
0050 72 70 61 00 00 0c 00 01 00 00 29 05 c0 00 00 00 rpa.....)
0060 00 00 00

Do query recursively? (dns.flags.recdesired), 2 bytes

Packets: 4 · Displayed: 2 (50.0%) · Dropped: 0 (0.0%)

Profile: Default

Figure 12: DNS-response



PART-3)

Section-2)

1-) In the DNS query given in the figure 13 below we can see that DNS type is A which is known as address mapping record or DNS host record that stores a host name and its IPv4 address. In the DNS query given in the figure 14 below we can see that DNS type is AAAA which stores hostname and it's IPv6 address.

In the DNS query given in the figure 15 we can see that DNS type CNAME was also used to alias a hostname to some other host name, if client requests a record of type CNAME which is pointing to another hostname, DNS resolution process will also repeat for this new hostname.

2.) We make a DNS request to www.microsoft.com using Google's DNS server running at IP address 8.8.8.8 instead of our local DNS server as we can see in figure 17.

Figure 13: Type-A DNS query

No.	Time	Source	Destination	Protocol	Length	Info
3	2023-04-09 13:15:49	817544581 192.168.0.29	46.196.235.35	DNS	88	Standard query 0x3cc8 A www.microsoft.com OPT
4	2023-04-09 13:15:49	859737873 46.196.235.35	192.168.0.29	DNS	255	Standard query response 0x3cc8 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.microsoft.com
5	2023-04-09 13:15:49	861427234 192.168.0.29	46.196.235.35	DNS	97	Standard query 0x8588 AAAA e13678.dscb.akamaiedge.net OPT
6	2023-04-09 13:15:49	889143666 46.196.235.35	192.168.0.29	DNS	153	Standard query response 0x8588 AAAA e13678.dscb.akamaiedge.net AAAA 2a02:26f0:c700:28d::356e AAAA 2a02:26f0:c...

> User Datagram Protocol, Src Port: 37847, Dst Port: 53
 - Domain Name System (query)
 Transaction ID: 0x3cc8
 Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
0 = Truncated: Message is not truncated
1 = Recursion desired: Do query recursively
0.... = Z: reserved (0)
0.... = Non-authenticated data: Unacceptable
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 1
 Queries
 - www.microsoft.com: type A, class IN [Type-A DNS query was made]
 Name: www.microsoft.com
 [Name Length: 17]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Additional records
 > <Root>: type OPT
 [Response In: 4]

```
0000 00 10 18 de ad 05 3c 58 c2 a5 ff aa 08 00 45 00 .....<X .....E
0010 00 4a 28 51 00 00 48 11 77 a5 c0 a8 00 1d 2e c4 J(Q @. w.....
0020 eb 23 93 d7 00 35 00 36 da f4 3c c8 01 00 00 00 01 #.. 5 6 ..<....
0030 00 00 00 00 00 01 03 77 77 77 09 6d 69 63 72 6f .....Fw Ww-micro...
0040 73 6f 66 74 03 63 6f 6d 00 00 01 00 01 00 00 29 softi.com .....
0050 05 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....*
```

Text item (text), 23 bytes Packets: 7 · Displayed: 4 (57.1%) · Dropped: 0 (0.0%) Profile: Default

Figure 14: Type-AAAA DNS query

No.	Time	Source	Destination	Protocol	Length	Info
3	2023-04-09 13:15:49	817544581 192.168.0.29	46.196.235.35	DNS	88	Standard query 0x3cc8 A www.microsoft.com OPT
4	2023-04-09 13:15:49	859737873 46.196.235.35	192.168.0.29	DNS	255	Standard query response 0x3cc8 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.microsoft.com
5	2023-04-09 13:15:49	861427234 192.168.0.29	46.196.235.35	DNS	97	Standard query 0x8588 AAAA e13678.dscb.akamaiedge.net OPT
6	2023-04-09 13:15:49	889143666 46.196.235.35	192.168.0.29	DNS	153	Standard query response 0x8588 AAAA e13678.dscb.akamaiedge.net AAAA 2a02:26f0:c700:28d::356e AAAA 2a02:26f0:c...

> User Datagram Protocol, Src Port: 34787, Dst Port: 53
 - Domain Name System (query)
 Transaction ID: 0x8588
 Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
0 = Truncated: Message is not truncated
1 = Recursion desired: Do query recursively
0.... = Z: reserved (0)
0.... = Non-authenticated data: Unacceptable
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 1
 Queries
 - e13678.dscb.akamaiedge.net: type AAAA, class IN [Type-AAAA DNS query was made]
 Name: e13678.dscb.akamaiedge.net
 [Name Length: 26]
 [Label Count: 4]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 Additional records
 > <Root>: type OPT
 [Response In: 6]

```
0000 00 10 18 de ad 05 3c 58 c2 a5 ff aa 08 00 45 00 .....<X .....E
0010 00 53 d1 8f 00 00 40 11 ce 5d c0 a8 00 1d 2e c4 S...@. 1...
0020 eb 23 87 e3 00 35 00 3f da fd 85 88 01 00 00 01 #.. 5 ?
0030 00 00 00 00 00 01 06 65 31 33 36 37 38 04 64 73 .....e 13678.ds...
0040 63 62 0a 61 6b 61 6d 61 69 65 64 67 65 03 6e 65 cb:akama iedge.ne
0050 74 00 00 1c 00 01 00 00 29 05 c0 00 00 00 00 00 .....*
0060 00
```

Text item (text), 32 bytes Packets: 7 · Displayed: 4 (57.1%) · Dropped: 0 (0.0%) Profile: Default

Figure 15: Type-CNAME DNS query

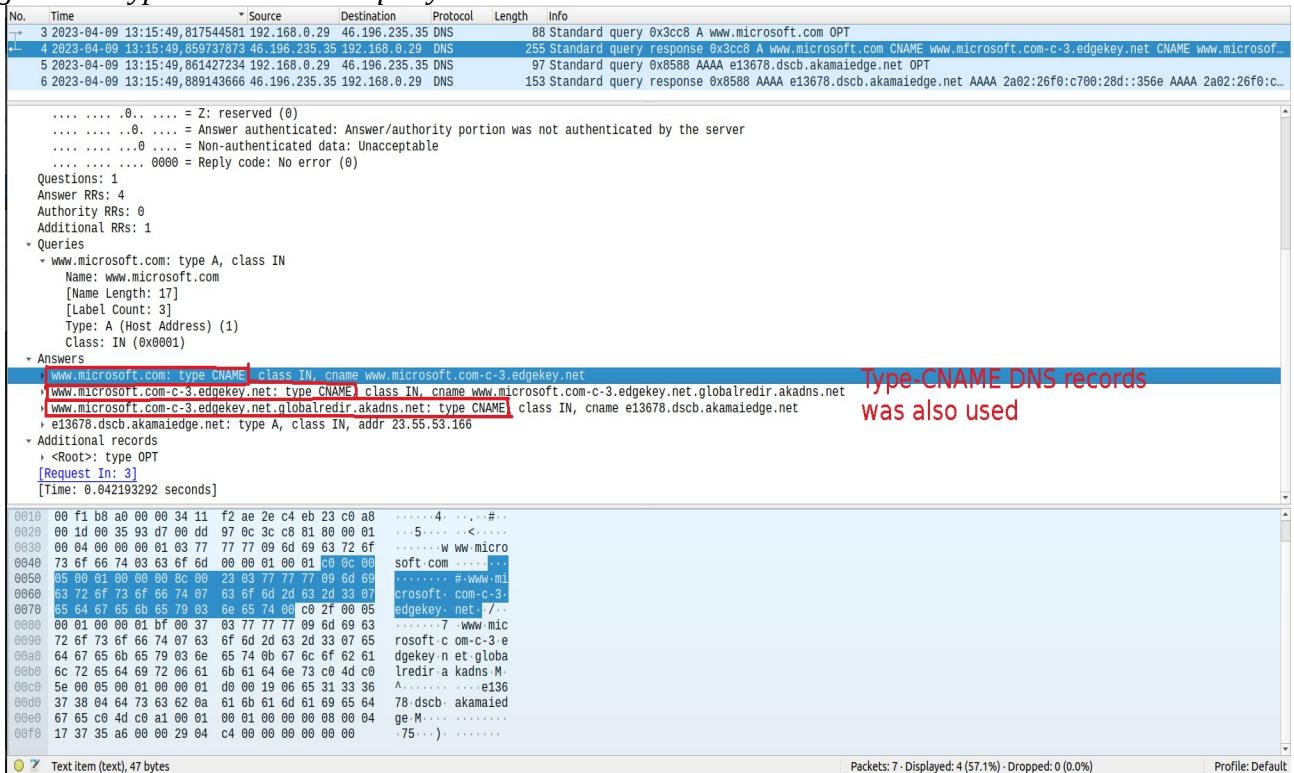


Figure 16: DNS lookup with our local DNS server

```
gokay@gokaycomputer:~$ nslookup www.microsoft.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
www.microsoft.com canonical name = www.microsoft.com-c-3.edgekey.net.
www.microsoft.com-c-3.edgekey.net canonical name = www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net.
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net canonical name = e13678.dscb.akamaiedge.net.

gokay@gokaycomputer:~$
```

DNS lookup with our local DNS server

Figure 17: DNS lookup with Google's DNS server

```
gokay@gokaycomputer:~$ nslookup www.microsoft.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
www.microsoft.com canonical name = www.microsoft.com-c-3.edgekey.net.
www.microsoft.com-c-3.edgekey.net canonical name = www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net.
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net canonical name = e13678.dscb.akamaiedge.net.

gokay@gokaycomputer:~$
```

DNS lookup with Google's DNS server whose IP address is 8.8.8.8