

Bil 452 Hw-3

Fatih Furkan Has
141101024

1-) <http://www.nectec.or.th/users/htk/web-th.960318.html> bu sayfada Tayland'da bulunan webserverlerin listesi vardı oradan www.mut.ac.th adresini seçtim.

```
toor@001:~$ nslookup www.mut.ac.th
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.mut.ac.th
Address: 203.209.55.160
```

Sitenin adresi: 203.209.55.160

2-) Bu soru için Duisburg-Essen Üniversitesinin sitesi olan www.uni-due.de adresi seçtim. Ancak authoritative adresler bulunamamıştır.

```
toor@001:~$ nslookup -type=NS uni-due.de
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
uni-due.de      nameserver = ns1.uni-essen.de.
uni-due.de      nameserver = ws-leil1.win-ip.dfn.de.
uni-due.de      nameserver = ns2.uni-duisburg-essen.de.
uni-due.de      nameserver = ws-nue1.win-ip.dfn.de.
uni-due.de      nameserver = ns1.uni-duisburg-essen.de.
uni-due.de      nameserver = ns2.uni-essen.de.

Authoritative answers can be found from:

toor@001:~$
```

3-) Bu sorguyu Ubuntu'da attığımda "connection timeout" hatası alıyorum. Bilgisayarım Windows olmadığı için kendi bilgisayarımın bu soruyu yapamadım ancak başka bir Windows kurulu bilgisayarda bunu gözlemleyebildim.

```
toor@001:~$ nslookup www.mail.yahoo.com www.uni-due.de
;; connection timed out; no servers could be reached

toor@001:~$ nslookup mail.yahoo.com www.uni-due.de
;; connection timed out; no servers could be reached

toor@001:~$ nslookup mail.yahoo.com uni-due.de
;; connection timed out; no servers could be reached
```

ipconfig

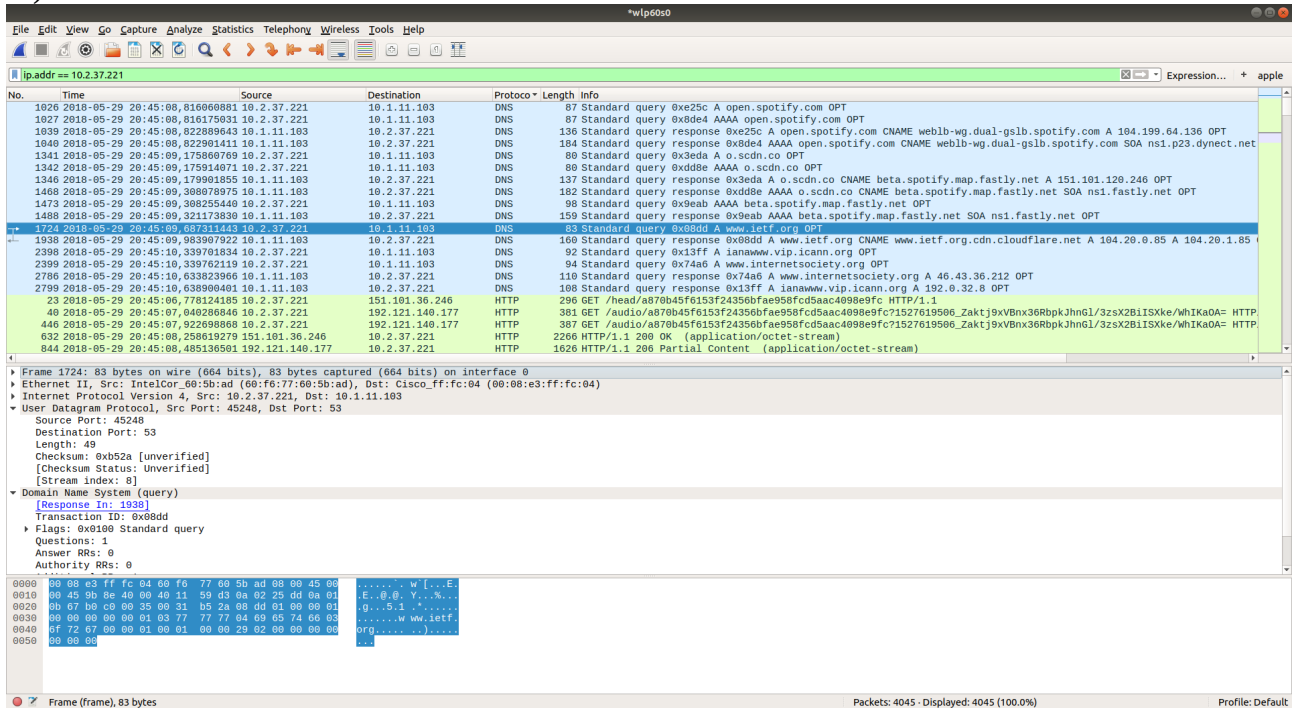
```
toor@001:~$ ifconfig
enp59s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether a4:4c:c8:6f:d8:78 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 694 bytes 59076 (59.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 694 bytes 59076 (59.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp60s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.2.37.221 netmask 255.255.252.0 broadcast 10.2.39.255
    inet6 fe80::d889:790:672d:ff14 prefixlen 64 scopeid 0x20<link>
    ether 60:f6:77:60:5b:ad txqueuelen 1000 (Ethernet)
    RX packets 12021 bytes 12082570 (12.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7701 bytes 1830996 (1.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ubuntu’da yaptığım araştırmalara göre DNS cache özelliği olmadığı için bu sorular için ekran görüntüsü koyamıyorum. (ipconfig /displaydns ve ipconfig /flushdns)

4-)



Yukarıdaki ekran görüntüsünde görüldüğü gibi UDP (User Datagram Protocol) kullanılmıştır.

5-) Yine yukarıdaki ekran görüntüsüne bakarsak Destination Port: 53 Source Port: 45248’dır.

6-) Destination 10.1.11.103 olarak görünmektedir, ancak yine Ubuntu’dan kaynaklı olarak local DNS server’i bilgisini görememekteyim.

7-)



Type ‘A’ olarak görünmektedir ancak cevap ‘answer’ içermemektedir.

8-)



3 adet answer görülmektedir. 1 tanesi ‘CNAME’ tipinde diğer ikisi ‘A’ tipindedir. Type: CNAME (Canonical NAME for an alias) ve Address bilgilerini içermektedirler.

9-) Destination 104.20.0.85 adresidir ve bu response’da gelen adresle aynıdır.

10-)

No.	Time	Source	Destination	Protocol	Length	Info
1346	2018-05-29 20:45:09,179991855	10.1.11.103	10.2.37.221	DNS	137	Standard query response 0x3eda A o.scdn.co CNAME beta.spotify.map.fastly.net A 151.101.120.246 OPT
1468	2018-05-29 20:45:09,308078975	10.1.11.103	10.2.37.221	DNS	182	Standard query response 0xddd8 AAAA o.scdn.co CNAME beta.spotify.map.fastly.net SOA ns1.fastly.net OPT
1473	2018-05-29 20:45:09,308255440	10.2.37.221	10.1.11.103	DNS	98	Standard query 0x9eab AAAA beta.spotify.map.fastly.net OPT
1488	2018-05-29 20:45:09,321173830	10.1.11.103	10.2.37.221	DNS	159	Standard query response 0x9eab AAAA beta.spotify.map.fastly.net SOA ns1.fastly.net OPT
1724	2018-05-29 20:45:09,607311443	10.2.37.221	10.1.11.103	DNS	83	Standard query 0x08dd A www.ietf.org OPT
1938	2018-05-29 20:45:09,903907922	10.1.11.103	10.2.37.221	DNS	160	Standard query response 0x08dd A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85
2398	2018-05-29 20:45:10,339701834	10.2.37.221	10.1.11.103	DNS	92	Standard query 0x13ff A ianaww.vip.icann.org OPT
2399	2018-05-29 20:45:10,339721119	10.2.37.221	10.1.11.103	DNS	94	Standard query 0x74a6 A www.internetsociety.org OPT
2786	2018-05-29 20:45:10,633823966	10.1.11.103	10.2.37.221	DNS	110	Standard query response 0x74a6 A www.internetsociety.org A 46.43.36.212 OPT
2799	2018-05-29 20:45:10,638908401	10.1.11.103	10.2.37.221	DNS	108	Standard query response 0x13ff A ianaww.vip.icann.org A 102.0.32.0 OPT
23	2018-05-29 20:45:06,778124185	10.2.37.221	151.101.36.246	HTTP	206	GET /head/a870b45f6153f24350bfae958fcd5aac4098e9fc HTTP/1.1
40	2018-05-29 20:45:07,040286846	10.2.37.221	192.121.140.177	HTTP	381	GET /audio/a870b45f6153f24350bfae958fcd5aac4098e9fc/1527619506_Zaktj9xVBnx36Rbpkjhnl/3zsx2B1ISkxw/wh1Ka0A= HTTP/1.1
446	2018-05-29 20:45:07,922088868	10.2.37.221	192.121.140.177	HTTP	387	GET /audio/a870b45f6153f24350bfae958fcd5aac4098e9fc/1527619506_Zaktj9xVBnx36Rbpkjhnl/3zsx2B1ISkxw/wh1Ka0A= HTTP/1.1
632	2018-05-29 20:45:08,258018279	151.101.36.246	10.2.37.221	HTTP	2266	HTTP/1.1 200 OK (application/octet-stream)
844	2018-05-29 20:45:08,405136591	192.121.140.177	10.2.37.221	HTTP	1626	HTTP/1.1 206 Partial Content (application/octet-stream)
846	2018-05-29 20:45:08,406248691	10.2.37.221	192.121.140.177	HTTP	388	GET /audio/a870b45f6153f24350bfae958fcd5aac4098e9fc/1527619506_Zaktj9xVBnx36Rbpkjhnl/3zsx2B1ISkxw/wh1Ka0A= HTTP/1.1
1099	2018-05-29 20:45:08,870383485	10.2.37.221	151.101.120.246	HTTP	263	GET /image/17a8cd7ad09f7707f770bdc823a5f97ad7e9b3a HTTP/1.1
1116	2018-05-29 20:45:08,886407649	10.2.37.221	151.101.120.246	HTTP	263	GET /image/fcb0e86c409bce0b50e65969223eafaa38b7cce HTTP/1.1
1237	2018-05-29 20:45:09,307186065	10.2.37.221	151.101.120.246	HTTP	262	GET /image/17a8cd7ad09f7707f770bdc823a5f97ad7e9b3a HTTP/1.1
1241	2018-05-29 20:45:09,016046523	10.2.37.221	192.121.140.177	HTTP	388	GET /audio/a870b45f6153f24350bfae958fcd5aac4098e9fc/1527619506_Zaktj9xVBnx36Rbpkjhnl/3zsx2B1ISkxw/wh1Ka0A= HTTP/1.1
1252	2018-05-29 20:45:09,096404976	151.101.120.246	10.2.37.221	HTTP	4552	HTTP/1.1 200 OK (JPEG JFIF image)
1336	2018-05-29 20:45:09,175348311	151.101.120.246	10.2.37.221	HTTP	1261	HTTP/1.1 200 OK (JPEG JFIF image)
1555	2018-05-29 20:45:09,307186065	10.2.37.221	151.101.120.246	HTTP	262	GET /image/17a8cd7ad09f7707f770bdc823a5f97ad7e9b3a HTTP/1.1
1628	2018-05-29 20:45:09,459328597	151.101.120.246	10.2.37.221	HTTP	5880	HTTP/1.1 200 OK (JPEG JFIF image)
1721	2018-05-29 20:45:09,56803772	192.121.140.177	10.2.37.221	HTTP	1626	HTTP/1.1 206 Partial Content (application/octet-stream)
1723	2018-05-29 20:45:09,569524675	10.2.37.221	192.121.140.177	HTTP	388	GET /audio/a870b45f6153f24350bfae958fcd5aac4098e9fc/1527619506_Zaktj9xVBnx36Rbpkjhnl/3zsx2B1ISkxw/wh1Ka0A= HTTP/1.1
1964	2018-05-29 20:45:10,909041926	10.2.37.221	104.20.1.85	HTTP	446	GET / HTTP/1.1
1986	2018-05-29 20:45:10,022278637	104.20.1.85	10.2.37.221	HTTP	74	HTTP/1.1 200 OK (text/html)
1988	2018-05-29 20:45:10,040928324	10.2.37.221	104.20.1.85	HTTP	475	GET /static/CACHE/css/b27d083853f9b.css HTTP/1.1
1989	2018-05-29 20:45:10,041805923	10.2.37.221	104.20.1.85	HTTP	479	GET /static/js/vendor/modernizr-2.6.2.min.42306a279a9e.js HTTP/1.1
2022	2018-05-29 20:45:10,071692082	10.1.12.104	10.2.37.221	HTTP	202	HTTP/1.1 200 OK (application/javascript)
2036	2018-05-29 20:45:10,071666831	10.2.37.221	104.20.1.85	HTTP	458	GET /static/CACHE/js/b72eb3d3acd5.js HTTP/1.1
2057	2018-05-29 20:45:10,081700807	104.20.1.85	10.2.37.221	HTTP	557	HTTP/1.1 200 OK (text/css)
2147	2018-05-29 20:45:10,134148135	10.2.37.221	104.20.1.85	HTTP	475	GET /static/CACHE/css/0fc5c8d1d363.css HTTP/1.1
2207	2018-05-29 20:45:10,103097169	104.20.1.85	10.2.37.221	HTTP	1582	HTTP/1.1 200 OK (text/css)
2247	2018-05-29 20:45:10,204042766	10.2.37.221	104.20.1.85	HTTP	558	GET /static/fonts/montserrat/montserrat-regular-webfont.woff2?16fc7d9cf54b HTTP/1.1
2264	2018-05-29 20:45:10,217152599	104.20.1.85	10.2.37.221	HTTP	1486	HTTP/1.1 200 OK (application/javascript)
2265	2018-05-29 20:45:10,218208877	10.2.37.221	104.20.1.85	HTTP	508	GET /static/img/ietf-logo_e4b6ca9dd271.gif HTTP/1.1
2289	2018-05-29 20:45:10,236605197	104.20.1.85	10.2.37.221	HTTP	414	HTTP/1.1 200 OK

Evet oldu yukarıda görüldüğü gibi resim alınmadan önce DNS sorguları yapıldı ve bu sorgu tamamlanana kadar resim alınmadı.

11-)

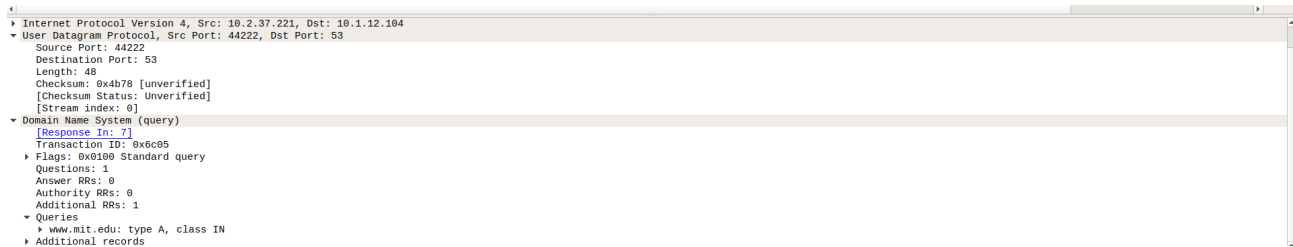
No.	Time	Source	Destination	Protocol	Length	Info
5	2018-05-29 21:23:10,657157520	10.2.37.221	10.1.12.104	DNS	82	Standard query 0x6c05 A www.mit.edu OPT
6	2018-05-29 21:23:10,657216330	10.2.37.221	10.1.12.104	DNS	82	Standard query 0x0fbd AAAA www.mit.edu OPT
7	2018-05-29 21:23:10,816209282	10.1.12.104	10.2.37.221	DNS	171	Standard query response 0x6c05 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104
8	2018-05-29 21:23:10,125875014	10.1.12.104	10.2.37.221	DNS	211	Standard query response 0x0fbd AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AA
9	2018-05-29 21:23:10,127614101	10.2.37.221	104.87.1.194	DNS	62	Standard query 0x2647 A on
29	2018-05-29 21:23:20,127977525	10.2.37.221	104.87.1.194	DNS	62	Standard query 0x2647 A on
30	2018-05-29 21:23:30,128026241	10.2.37.221	104.87.1.194	DNS	62	Standard query 0x2647 A on
62	2018-05-29 21:23:44,716882999	10.2.37.221	10.1.12.104	DNS	78	Standard query 0xc3b3 A mit.edu OPT
63	2018-05-29 21:23:44,716946632	10.2.37.221	10.1.12.104	DNS	78	Standard query 0xa29f AAAA mit.edu OPT
64	2018-05-29 21:23:44,772545479	10.1.12.104	10.2.37.221	DNS	134	Standard query response 0xa29f AAAA mit.edu AAAA 2a02:26f0:7b:383::255e AAAA 2a02:26f0:7b:385::255e OPT
65	2018-05-29 21:23:44,781249663	10.1.12.104	10.2.37.221	DNS	94	Standard query response 0xc3b3 A mit.edu A 69.192.64.128 OPT
66	2018-05-29 21:23:44,782777952	10.2.37.221	69.192.64.128	DNS	82	Standard query 0xef34 A on
74	2018-05-29 21:23:19,982226818	10.2.37.221	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
77	2018-05-29 21:23:51,993605218	10.2.37.221	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
2	2018-05-29 21:23:14,533077689	54.230.226.114	10.2.37.221	TCP	66	443 - 58874 [ACK] Seq=1 Ack=78 Win=122 Len=0 TSval=602563462 TSecr=972058438
4	2018-05-29 21:23:14,716882999	10.2.37.221	54.230.226.114	TCP	66	58874 - 443 [ACK] Seq=78 Ack=3156 Win=1428 Len=0 TSval=972059774 TSecr=602563507
10	2018-05-29 21:23:19,410840850	10.2.37.221	91.189.92.19	TCP	66	37820 - 443 [ACK] Seq=1 Ack=1 Win=490 Len=0 TSval=1719599298 TSecr=1990655967
11	2018-05-29 21:23:19,471084217	91.189.92.19	10.2.37.221	TCP	66	[TCP ACKed unseen segment] 443 - 37820 [ACK] Seq=1 Ack=2 Win=277 Len=0 TSval=1990663483 TSecr=1719569294
12	2018-05-29 21:23:19,690979344	10.2.37.221	192.0.7.220	TCP	54	42474 - 443 [ACK] Seq=1 Ack=1 Win=1452 Len=0
15	2018-05-29 21:23:20,022059255	192.0.7.220	10.2.37.221	TCP	54	[TCP ACKed unseen segment] 443 - 42474 [ACK] Seq=1 Ack=2 Win=62 Len=0
16	2018-05-29 21:23:20,740447273	104.199.64.141	10.2.37.221	TCP	77	4070 - 46512 [PSH, ACK] Seq=1 Ack=1 Win=42 Len=11 TSval=4020014413 TSecr=711757897
17	2018-05-29 21:23:20,740488599	10.2.37.221	104.199.64.141	TCP	66	46512 - 4070 [ACK] Seq=1 Ack=12 Win=3927 Len=0 TSval=711779993 TSecr=4020014413
18	2018-05-29 21:23:21,170683169	10.2.37.221	91.189.92.48	TCP	66	42038 - 443 [ACK] Seq=1 Ack=1 Win=490 Len=0 TSval=1750288950 TSecr=724299273
19	2018-05-29 21:23:21,217035824	91.189.92.48	10.2.37.221	TCP	66	4070 - 46512 [ACK] Seq=1 Ack=1 Win=490 Len=0 TSval=711779993 TSecr=724299273
Frame 82: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0						
Ethernet II, Src: IntelCor_00:1b:0b:00:00:00 (00:1b:0b:00:00:00), Dst: Cisco_ff:fc:04 (00:0e:e3:ff:fc:04)						
Internet Protocol Version 4, Src: 10.2.37.221, Dst: 19.1.12.104						
User Datagram Protocol, Src Port: 44222, Dst Port: 53						
Source Port: 44222						
Destination Port: 53						
Length: 48						
Checksum: 0x4b78 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 0]						
Domain Name System (query)						
[Response in: 7]						
Transaction ID: 0x6c05						
Flags: 0x0100 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 1						
Queries						
0000	00 00 e3 ff fc 04 00 fe	77 00 5b ad 00 00 45 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0010	00 44 8b 33 40 00 40 11	69 2e 0a 82 25 dd 0a 91	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0020	00 68 ac be 00 35 00 30	4b 78 6c 95 01 00 00 01	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0030	00 00 00 00 00 01 03 77	77 07 03 69 74 00 05	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0040	00 75 00 01 00 01 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
Frame (frame), 82 bytes						
Packets: 77 · Displayed: 75 (97.4%)						
Profile: Default						

Destination port: 53

Source port: 4422

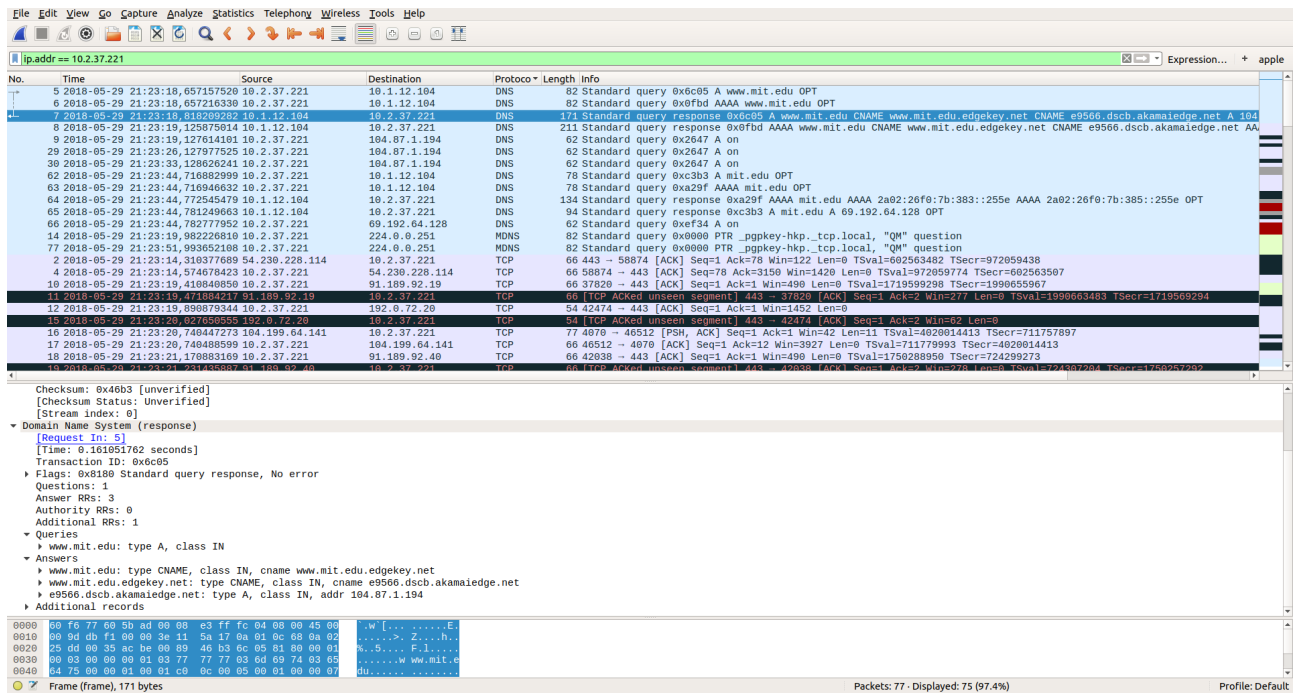
12-) Query 10.1.12.104 adresine gönderilmiştir.

13-)



Type 'A' 1 query içermekte ve answer yok.

14-)



3 cevap içermektedir ve adresleri göstermektedir. 1 tane 'CNAME' ve iki tane 'A' tipinde

16-)

Wireshark packet capture showing a DNS query from 10.2.37.221 to 10.1.12.104. The packet is a Standard query for AAAA mit.edu. The packet details pane shows the query structure with flags and questions.

Frame 11: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: IntelCor_00:5b:ad (60:f6:77:00:5b:ad), Dst: Cisco_ff:fc:04 (00:08:e3:ff:fc:04)
Internet Protocol Version 4, Src: 10.2.37.221, Dst: 10.1.12.104
User Datagram Protocol, Src Port: 46338, Dst Port: 53
Domain Name System (query)

Packets: 43 - Displayed: 41 (95.3%) Profile: Default

10.1.12.104 adresine gönderilmiştir.

17-)

Wireshark packet capture showing a DNS query from 10.2.37.221 to 10.1.12.104. The packet is a Standard query for AAAA mit.edu. The packet details pane shows the query structure with flags and questions.

Frame 11: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: IntelCor_00:5b:ad (60:f6:77:00:5b:ad), Dst: Cisco_ff:fc:04 (00:08:e3:ff:fc:04)
Internet Protocol Version 4, Src: 10.2.37.221, Dst: 10.1.12.104
User Datagram Protocol, Src Port: 46338, Dst Port: 53
Domain Name System (query)

Transaction ID: 0x6ff6
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
mit.edu: type A, class IN
Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)

Packets: 43 - Displayed: 41 (95.3%) Profile: Default

‘A’ tipinde bir query içermektedir. Answer yoktur.

18-)

Wireshark packet capture showing a DNS query and response. The query is for 'mit.edu' and the response is a standard query response. The packet list shows the query and response packets. The packet details pane shows the query and response details. The packet bytes pane shows the raw data of the query and response.

Wireshark packet capture showing a DNS query and response. The query is for 'mit.edu' and the response is a standard query response. The packet list shows the query and response packets. The packet details pane shows the query and response details. The packet bytes pane shows the raw data of the query and response.

Yukarıda ekran görüntülerinde görüldüğü gibi herhangi bir nameserver bilgisine ulaşılamamıştır. Bunu tekrardan Ubuntu kaynaklı bir problem olarak açıklayabilirim.

```
toor@001:~$ nslookup -type=NS mit.edu
;; connection timed out; no servers could be reached
```

Connection timed out hatası ile karşılaştım.

20-)

Wireshark packet capture showing a DNS query from 10.2.37.221 to 10.1.12.104. The packet is a Standard query for bitsy.mit.edu. The response is a Standard query response with the IP address 10.1.12.104.

Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Ethernet II, Src: IntelCor_00:5b:ad (00:f6:77:00:5b:ad), Dst: Cisco_ff:fc:04 (00:08:e3:ff:fc:04)
Internet Protocol Version 4, Src: 10.2.37.221, Dst: 10.1.12.104
User Datagram Protocol, Src Port: 43936, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xdb4e
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
bitsy.mit.edu: type A, class IN
Additional records
<Root>: type OPT

0010 00 46 30 6b 40 00 40 11 c3 f4 0a 02 25 dd 0a 01 .F0k0.0.%...
0020 0c 06 ad 1c 00 35 00 32 79 6b db 4e 01 00 00 01 .h...5.2 yk.N....
0030 00 00 00 00 01 05 02 69 74 73 79 03 6d 69 74b itsy.mit
0040 83 05 64 75 00 01 00 01 00 00 29 02 00 00 00 .edu....[...]
0050 [...]

Text item (text), 11 bytes

Packets: 48 - Displayed: 48 (100.0%) Profile: Default

10.1.12.104 adresine gönderilmiştir.

21-)

Wireshark packet capture showing a DNS query from 10.2.37.221 to 10.1.12.104. The packet is a Standard query for bitsy.mit.edu. The response is a Standard query response with the IP address 10.1.12.104.

Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Ethernet II, Src: IntelCor_00:5b:ad (00:f6:77:00:5b:ad), Dst: Cisco_ff:fc:04 (00:08:e3:ff:fc:04)
Internet Protocol Version 4, Src: 10.2.37.221, Dst: 10.1.12.104
User Datagram Protocol, Src Port: 43936, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xdb4e
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
bitsy.mit.edu: type A, class IN
Name: bitsy.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

0010 00 46 30 6b 40 00 40 11 c3 f4 0a 02 25 dd 0a 01 .F0k0.0.%...
0020 0c 06 ad 1c 00 35 00 32 79 6b db 4e 01 00 00 01 .h...5.2 yk.N....
0030 00 00 00 00 01 05 02 69 74 73 79 03 6d 69 74b itsy.mit
0040 83 05 64 75 00 01 00 01 00 00 29 02 00 00 00 .edu....[...]
0050 [...]

Text item (text), 11 bytes

Packets: 48 - Displayed: 48 (100.0%) Profile: Default

Response 'A' tipinde query içermektedir.

22-)

The image shows a Wireshark packet capture analysis. The top pane displays a list of network packets. The selected packet (No. 10) is a DNS Standard query response from 10.2.37.221 to 10.1.12.104. The middle pane shows the packet details, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and Domain Name System (response) section. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet 10: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0

Ethernet II, Src: Cisco_Ff:fc:04 (08:08:e3:ff:fc:04), Dst: IntelCor_08:5b:ad (08:f6:77:60:5b:ad)

Internet Protocol Version 4, Src: 10.1.12.104, Dst: 10.2.37.221

User Datagram Protocol, Src Port: 53, Dst Port: 43036

Domain Name System (response)

Request In: 3

[Time: 0.22047517 seconds]

Transaction ID: 0xd4e

Flags: 0x180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 1

Queries

bitsy.mit.edu: type A, class IN

Answers

bitsy.mit.edu: type A, class IN, addr 18.72.0.3

Additional records

<Root>: type OPT

0020 25 dd 00 35 a8 1c 00 42 84 f0 db 4e 81 00 00 01 %..5..B...N....

0030 00 01 00 00 01 05 62 69 74 73 79 03 6d 69 74bitsy.mit

0040 03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00 .edu....d.....

0050 00 07 00 00 04 12 48 00 00 00 00 29 10 00 00 00H[...]....

0060 00 00 00 00

Text item (text), 16 bytes

Packets: 48 - Displayed: 48 (100.0%)

Profile: Default

Tek bir answer içermektedir. Server'in ip adresi vardır bu answerda.