

EEM-413 Bilgisayar Ağları Lab2 (DNS)

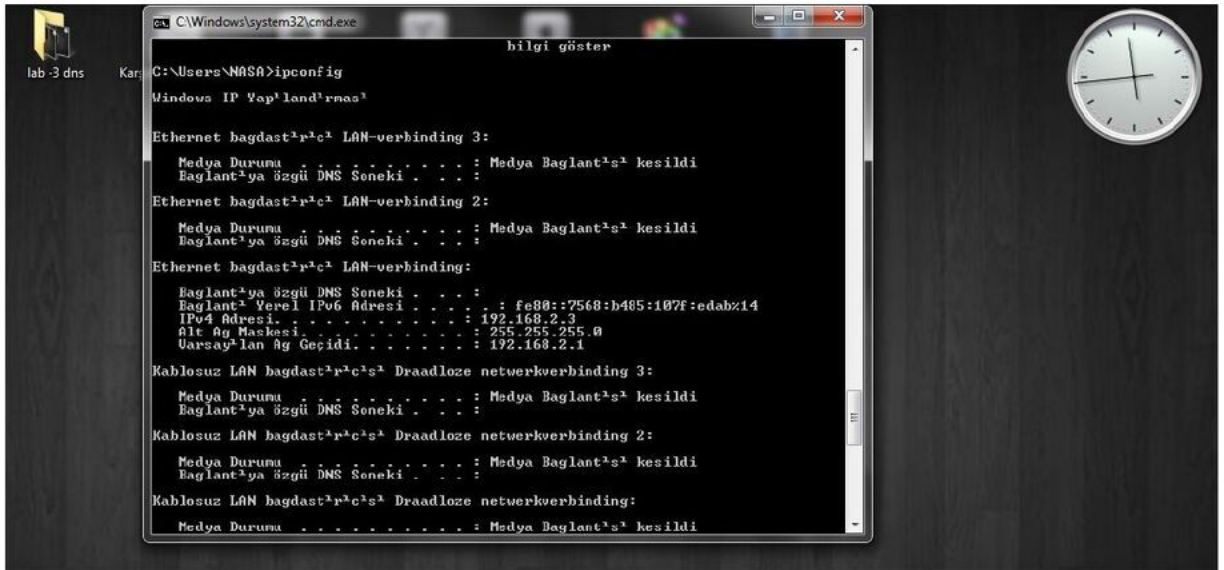
Nslookup www.mit.edu yazıldığında ;



Nslookup -type = NS mit.edu yazıldığında ;



Nslookup www.aiit.or.kr bitsy.mit.edu



ipconfig /flushdns

```
C:\Windows\system32\cmd.exe

Tunnel bagdast^r^c^  isatap.{F0F9010A-BE8A-4C4E-94BE-96} :
Medya Durumu . . . . . : Medya Baglant^s^ kesildi
Baglant^ya 8zgü DNS Soneki . . . . . :
C:\Users\NASA>ipconfig /flushdns

Windows IP Yap^land^rmas^
DNS 8özücü önbellegi basar^yla temizlendi.
C:\Users\NASA>
```

1-)Asia için www.rediff.com denendiğinde nslookup aşağıdaki gibi olmaktadır.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Sürüm 6.1.7600]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm haklar saklıdır.
C:\Users\NASA>nslookup www.rediff.com
Sunucu: RT
Address: 192.168.2.1

Güvenilir olmayan yanıt:
Ad: a1586.v3.akanai.net
Addresses: 80.239.247.68
80.239.247.31
Aliases: www.rediff.com
www-b.rediff.com.edgesuite.net

C:\Users\NASA>_
```

2-) nslookup -type=NS.udi.org Avrupadaki bi üniversite sitesi

```
C:\Windows\system32\cmd.exe - nslookup -type=NS.udi.edu
Microsoft Windows [Sürüm 6.1.7600]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm haklar saklıdır.
C:\Users\NASA>nslookup www.rediff.com
Sunucu: RT
Address: 192.168.2.1

Güvenilir olmayan yanıt:
Ad: a1586.v3.akanai.net
Addresses: 80.239.247.68
80.239.247.31
Aliases: www.rediff.com
www-b.rediff.com.edgesuite.net

C:\Users\NASA>nslookup -type=NS.udi.edu
unknown query type: NS.udi.edu
Varsayılan Sunucu: RT
Address: 192.168.2.1

> _
```

3-) nslookup mail.yahoo.com ya baktığımızda ;



```
C:\Windows\system32\cmd.exe - nslookup -type=NS.udi.edu
Ad: a1586.w3.akamai.net
Addresses: 80.239.247.68
Aliases: 80.239.247.31
www.rediff.com
www-b.rediff.com.edgesuite.net

C:\Users\NASA>nslookup -type=NS.udi.edu
unknown query type: NS.udi.edu
Varsayılan Sunucu: RT
Address: 192.168.2.1

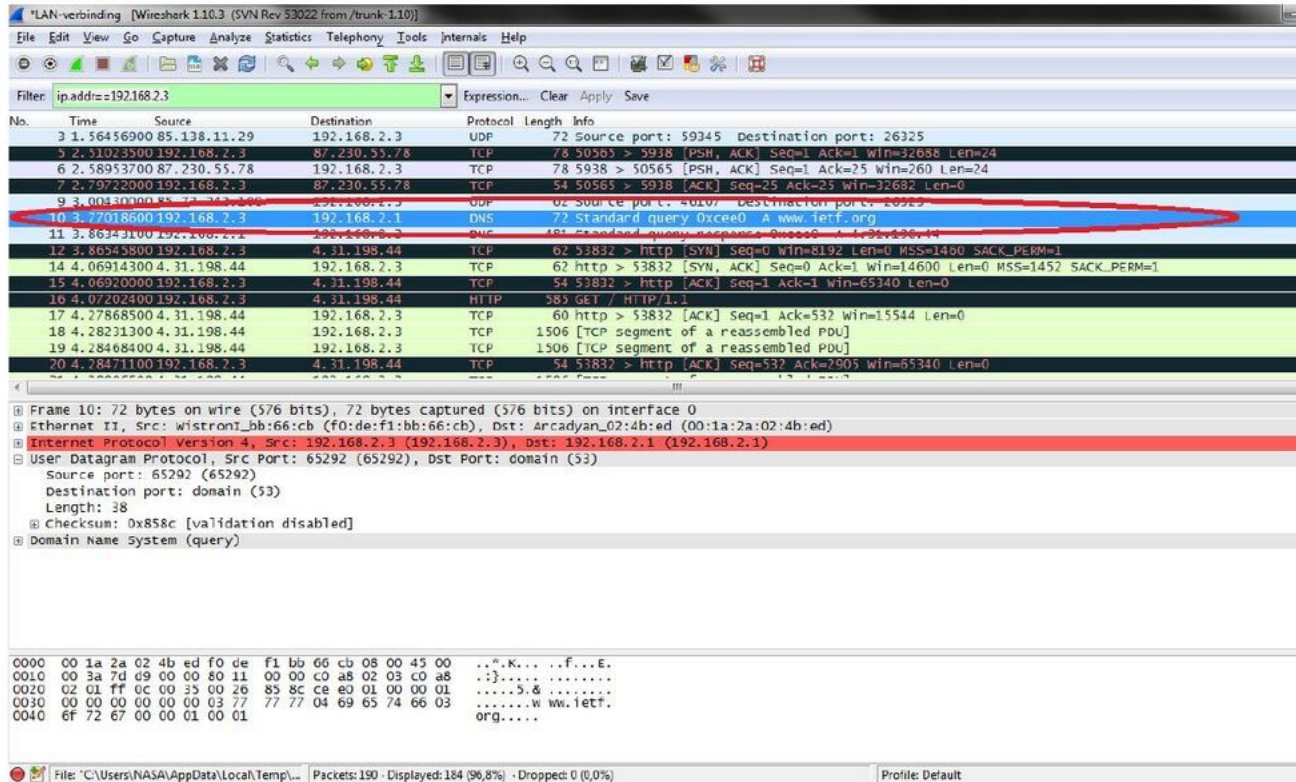
> nslookup mail.yahoo.com
Sunucu: login.lga1.b.yahoo.com
Address: 98.139.237.162
Aliases: mail.yahoo.com
login.yahoo.com
login-global.lga1.b.yahoo.com

DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** mail.yahoo.com yapilmasi istegi zaman asimina ugradi
>
```

3. Kısım ilk işlemi;

4)

www.ietf.com için wireshark ta bakıldığında aşağıda kırmızıyla belirttiğim gibi User Datagram Protocol yani UDP kullanılmıştır.



Filter: ip.addr==192.168.2.3

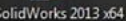
No.	Time	Source	Destination	Protocol	Length	Info
3	1.56456900	85.138.11.29	192.168.2.3	UDP	72	Source port: 59345 Destination port: 26325
5	2.51023500	192.168.2.3	87.230.55.78	TCP	78	50585 > 5938 [PSH, ACK] Seq=1 Ack=1 Win=32688 Len=24
6	2.58953700	87.230.55.78	192.168.2.3	TCP	78	5938 > 50565 [PSH, ACK] Seq=1 Ack=25 Win=260 Len=24
7	2.79722000	192.168.2.3	87.230.55.78	TCP	54	50565 > 5938 [ACK] Seq=25 Ack=25 Win=32682 Len=0
9	3.00430000	85.138.11.29	192.168.2.3	UDP	62	Source port: 50107 Destination port: 26325
10	3.77018600	192.168.2.3	192.168.2.1	DNS	72	Standard query 0xc000 A www.ietf.org
11	3.86343100	192.168.2.1	192.168.2.3	DNS	151	Standard query response 0xc000 A 192.168.2.1
12	3.86545800	192.168.2.3	4.31.198.44	TCP	62	53832 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
14	4.06914300	4.31.198.44	192.168.2.3	TCP	62	http > 53832 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_PERM=1
15	4.06920000	192.168.2.3	4.31.198.44	TCP	54	53832 > http [ACK] Seq=1 Ack=1 Win=65340 Len=0
16	4.07202400	192.168.2.3	4.31.198.44	HTTP	583	GET / HTTP/1.1
17	4.27868500	4.31.198.44	192.168.2.3	TCP	60	http > 53832 [ACK] Seq=1 Ack=532 Win=15544 Len=0
18	4.28231300	4.31.198.44	192.168.2.3	TCP	1506	[TCP segment of a reassembled PDU]
19	4.28468400	4.31.198.44	192.168.2.3	TCP	1506	[TCP segment of a reassembled PDU]
20	4.28471100	192.168.2.3	4.31.198.44	TCP	54	53832 > http [ACK] Seq=532 Ack=2903 Win=65340 Len=0

Frame 10: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
Ethernet II, Src: WistronI_b6:66:cb (f0:de:f1:bb:66:cb), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)
Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3), Dst: 192.168.2.1 (192.168.2.1)
User Datagram Protocol, Src Port: 65292 (65292), Dst Port: domain (53)
Source port: 65292 (65292)
Destination port: domain (53)
Length: 38
Checksum: 0x858c [validation disabled]
Domain Name System (query)

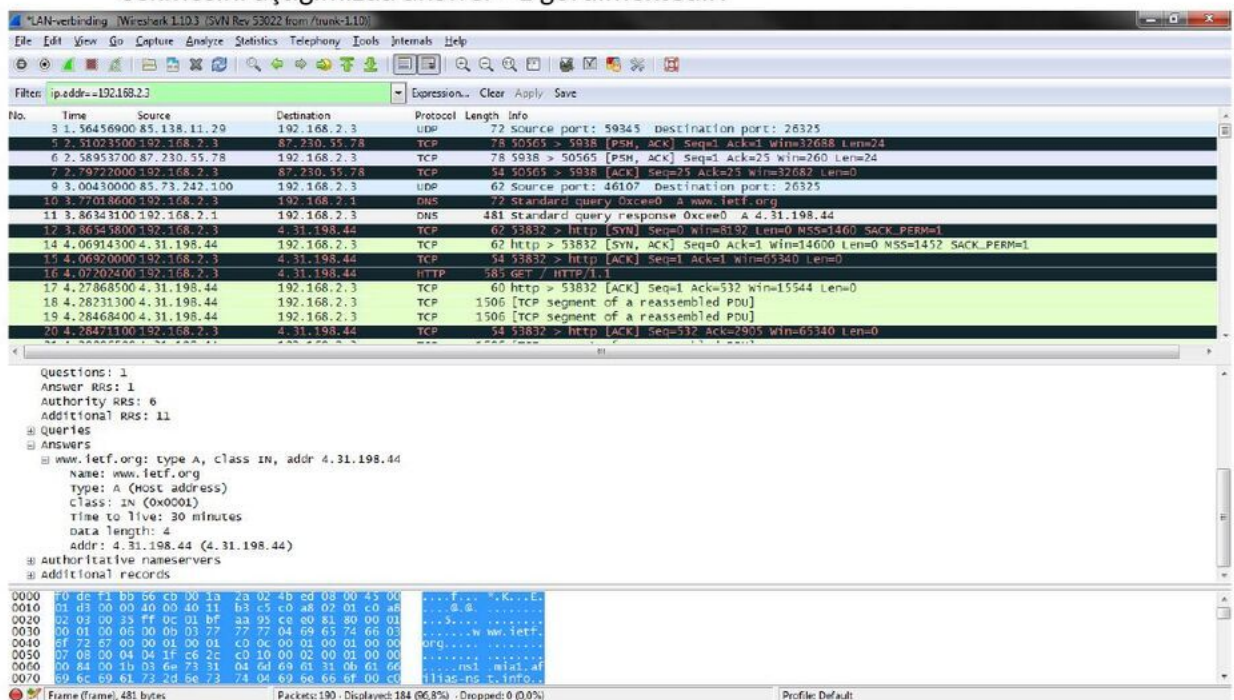
0000 00 1a 2a 02 4b ed f0 de f1 bb 66 cb 08 00 45 00 ..*.K... ..f...E.
0010 00 3a 7d 09 00 00 80 11 00 00 c0 a8 02 03 c0 a8 .:}.....
0020 02 01 ff 0c 00 35 00 26 85 8c ce e0 01 00 00 01 S&.....
0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03 W ww.ietf.
0040 6f 72 67 00 00 01 00 01 org.....

File: C:\Users\NASA\AppData\Local\Temp\... Packets: 190 - Displayed: 184 (96.8%) - Dropped: 0 (0.0%) Profile: Default

6) Aşağıda da gösterdiğim gibi Varsayılan ağ geçidi ve DHCP sunucusu IP si 192.168.2.1 dir.Wire shar ta da görülmektedir. Benim Ip adresimde 192.168.2.3 dür.



8) Aşağıda da gösterildiği gibi TYPE A class IN adres 4.31.198.44 ve DNS sekmesini açtığımızda answer =1 görülmektedir.



9) ilk SYN paketinde 4.31.198.44 IP adresinden cevap gönderilmiştir.

The image shows a Wireshark packet capture of a network traffic. The filter is set to 'ip.addr==192.168.2.3'. The packet list shows a SYN packet (No. 62) from 192.168.2.3 to 4.31.198.44. The packet details show the following information:

- Frame 62: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
- Ethernet II, Src: Wistron1_bb:66:cb (f0:de:f1:bb:66:cb), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)
- Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3), Dst: 4.31.198.44 (4.31.198.44)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 48
- Identification: 0x7dda (32218)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 128
- Protocol: TCP (6)

10) Aşağıda da görüldüğü gibi web sitesindeki resimler için yeni bir DNS query oluşturulmamıştır.

The image shows a Wireshark packet capture of a network traffic. The filter is set to 'ip.addr==192.168.2.3'. The packet list shows a GET request (No. 53) from 192.168.2.3 to 4.31.198.44. The packet details show the following information:

- Frame 53: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface 0
- Ethernet II, Src: Wistron1_bb:66:cb (f0:de:f1:bb:66:cb), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)
- Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3), Dst: 4.31.198.44 (4.31.198.44)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 443
- Identification: 0x7df9 (32249)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0x0000 [incorrect, should be 0xee4c (may be caused by "IP checksum offload?")]

The packet bytes are displayed in hexadecimal and ASCII format at the bottom of the packet details pane.

** nslookup cmd kısmından www.mit.edu yaptığımızda aşağıdaki çıktıyı görmekteyiz.

The screenshot shows a Wireshark capture of network traffic on the interface 0. The filter is set to 'ip.addr == 192.168.2.3'. The packet list shows several packets, with packet 11 being a DNS query from 192.168.2.1 to 192.168.2.3. The packet details pane shows the following information:

- Frame 13: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
- Ethernet II, Src: WistronIb:66:cb (f0:de:f1:bb:66:cb), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)
- Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3), Dst: 192.168.2.1 (192.168.2.1)
- User Datagram Protocol, Src Port: 55516 (55516), Dst Port: domain (53)
- Domain Name System (query)
 - Transaction ID: 0x0002
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.mit.edu: type A, class IN
 - Name: www.mit.edu
 - Type: A (Host address)
 - Class: IN (0x0001)

The packet bytes pane shows the raw data of the DNS query, including the transaction ID 0002 and the query for www.mit.edu.

11) Source port 55516 ve Destination Port ta 53 dür. Yukarıdaki screen shottada görülmektedir.

12) Daha önce ipconfig / all yaptığımızda da gördüğümüz gibi 192.168.2.1 IP adresi benim local default DNS server IP adresimdir.

13) Yukarıdaki screenshottada görüldüğü gibi TYPE A DNS türüdür. Ve Answer veya bi içerik içermez.

14) Aşağıdaki screenshottada görüldüğü gibi 1 cevap gelmiş ve içeriğinde aşağıda belirtilmiştir.

Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr == 192.168.2.3` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
12	10.6761540	192.168.2.1	192.168.2.3	DNS	100	Standard
13	10.6766520	192.168.2.3	192.168.2.1	DNS	71	Standard
14	10.7565680	192.168.2.1	192.168.2.3	DNS	429	Standard
15	10.7573440	192.168.2.3	192.168.2.1	DNS	71	Standard
16	10.7801400	192.168.2.1	192.168.2.3	DNS	202	Standard

Packet 13 details:

- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 0
- Queries
 - 1.2.168.192.in-addr.arpa: type PTR, class IN
 - Name: 1.2.168.192.in-addr.arpa
 - Type: PTR (Domain name pointer)
 - Class: IN (0x0001)
- Answers
 - 1.2.168.192.in-addr.arpa: type PTR, class IN, RT
 - Name: 1.2.168.192.in-addr.arpa
 - Type: PTR (Domain name pointer)
 - Class: IN (0x0001)
 - Time to live: 2 hours, 46 minutes, 40 seconds
 - Data length: 4
 - Domain Name: RT

16) Kendi bilgisayarımdan ve farklı bir bilgisayardan denememe rağmen nslookup-type=NS mit.edu DNS için timeout vermektedir. Bundan dolayı lab füyünden trace indirme kısmından edindiğim tracelerle devam etmekte dolayısıyla IP adreslerinde farklılıklar bulunmaktadır. **

Aşağıdaki screenshot a göre DNS query mesajının IP adresi 128.238.29.22 dir.

Wireshark 1.10.3 (SVN Rev 53022 from /trunk-110)

Filter: Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
493.30.918636	128.238.29.22	128.238.38.160	DNS	176	Standard query response 0x0003 NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu
492.30.918275	128.238.38.160	128.238.29.22	DNS	67	Standard query 0x0003 NS mit.edu
491.30.918044	128.238.29.22	128.238.38.160	DNS	135	Standard query response 0x0002 No such name
490.30.917700	128.238.38.160	128.238.29.22	DNS	76	Standard query 0x0002 NS mit.edu.poly.edu
489.80.916359	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR dns-prime.poly.edu
488.30.916492	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
389.25.565667	128.238.38.154	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x7e7caa5e
325.21.564095	128.238.38.154	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x7e7caa5e
8.0.514535	CISCO_fc:F0:de		CDP/VTP/DTP/PAGP/UDCDP	371	Device ID: D8221C Port ID: FastEthernet0/30
553.34.289153	128.238.38.252	128.238.38.255	BROWSER	243	Host Announcement POLYME, Workstation, Server, NT Workstation, Potential Browser
578.32.914447	128.238.38.255	128.238.38.255	BROWSER	248	Host Announcement WINXP-17004 Workstation Server NT Workstation Potential Browser

[Request In: 488]
[Time: 0.000367000 seconds]
Transaction ID: 0x0001
Flags: 0x8580 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
ANSWERS
22.29.238.128.in-addr.arpa: type PTR, class IN, dns-prime.poly.edu
Name: 22.29.238.128.in-addr.arpa
Type: PTR (Domain name pointer)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 20
Domain Name: dns-prime.poly.edu

0000 00 09 6b 10 60 99 00 b0 8e 83 e4 54 08 00 45 00 .k. . . .T..E.
0010 00 68 00 55 00 00 7e 11 f6 9d 80 ee 1d 16 80 ee .h.U.. . . .
0020 26 a0 00 35 0e a0 00 54 25 35 00 01 85 80 00 01 6..5...T %5.....
0030 00 01 00 00 00 00 02 32 32 02 32 39 03 32 33 38 2 2.29.238
0040 03 31 32 38 07 69 6e 7d e1 64 84 72 04 61 72 70 .128.in-addr.arp
0050 61 00 00 0c 00 01 0c 0c 00 0c 00 01 00 00 0e 10 a.....
0060 00 14 09 64 6e 73 2d 70 72 69 6d 65 04 70 6f 6c ...dns-p rime.pol
0070 79 03 65 64 75 00 y.edu.

File: C:\Users\NASA\Desktop\Yeni Klasör\d... Pack... Profile: Default

17)

Type NS ve answer yani bir içerik bulunmamaktadır.

18)

İsim serverı bitsy, strawb and w20ns.

Additional kısmına bakar isek Ip adresini buluruz

Answers

mit.edu: type NS, class inet, ns bitsy.mit.edu

mit.edu: type NS, class inet, ns strawb.mit.edu

mit.edu: type NS, class inet, ns w20ns.mit.edu

Additional records

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

strawb.mit.edu: type A, class inet, addr 18.71.0.151

w20ns.mit.edu: type A, class inet, addr 18.70.0.160

20)

belirtilen siteden indirerek yaptım. **

Aşağıdaki screenshotta da belirtildiği gibi IP = 18.72.0.3 dur. Hayır benim default local DNS serverım değil. Bu bitsy.mit.edu ya ait.

Wireshark network capture showing a DNS query and response. The query is for www.a1it.or.kr.poly.edu and the response returns 18.72.0.3. The packet list shows a standard query and response. The packet details show the query and response structure. The packet bytes show the raw data.

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
97	4.230878	128.238.38.177	128.238.38.255	BROWSER	216	Get Backup List Request
97	4.186743	128.238.38.207	128.238.38.255	BROWSER	254	Domain/workgroup Announcement MSHOME, NT Workstation, Domain Erum
113	4.480689	128.238.38.177	128.238.38.255	BROWSER	216	Get Backup List Request
100	4.265296	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	4.278516	18.72.0.3	128.238.38.160	DNS	83	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa
102	4.279410	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.a1it.or.kr.poly.edu
103	4.293283	18.72.0.3	128.238.38.160	DNS	83	Standard query response 0x0002 A www.a1it.or.kr.poly.edu
104	4.293517	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.a1it.or.kr
105	4.307859	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A 218.36.94.200
41	1.866140	128.238.38.2	224.0.0.2	HSRP	62	Hello (State Active)
115	4.408168	128.238.38.2	224.0.0.2	HSRP	62	Hello (State Active)

Frame 102: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)

Ethernet II, Src: Bm_10:60:99 (00:09:6b:10:60:99), Dst: All-HERP-routers_00 (00:00:0c:07:ac:00)

Internet Protocol Version 4, Src: 128.238.38.160 (128.238.38.160), Dst: 18.72.0.3 (18.72.0.3)

User Datagram Protocol, Src Port: v1pnmoteagent (3752), Dst Port: domain (53)

Domain Name System (query)

[Response in: 103]

Transaction ID: 0x0002

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- www.a1it.or.kr.poly.edu: type A, class IN
- Name: www.a1it.or.kr.poly.edu
- Type: A (Host address)
- Class: IN (0x0001)

0000 00 00 0c 07 ac 00 00 09 6b 10 60 99 08 00 45 00 K.....E..

0010 00 43 28 04 00 00 00 11 58 00 00 ee 28 a0 12 48 ..E.....X.....

0020 00 03 de a8 00 35 00 31 ae 72 00 02 01 00 00 01 S.I..f.....

0030 00 00 00 00 00 00 03 77 77 77 d4 61 69 69 74 02 www.a1it..

0040 6f 72 02 6b 72 04 70 6f 6c 79 03 65 64 75 00 00 ..or.kr.poly.edu..

0050 01 00 01

Frame (frame), 83 bytes

Profile: Default

22-23) Aşağıdaki screenshot tada görüldüğü gibi 1 answer var ve içeriğinde screenthotta gösterilmiştir.

The screenshot displays the Wireshark network protocol analyzer interface. At the top, the title bar reads "dns-ethereal-trace-4 [Wireshark 1.6.0] (SVN Rev 93022 from /trunk-1.10)". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations and analysis. A filter bar contains the text "Expression..." followed by "Clear", "Apply", and "Save". The main packet list pane shows several entries, with the selected entry being a DNS query from source IP 128.238.38.177 to destination IP 218.36.94.200. The details pane below shows the structure of the selected packet, including Authority RRS, Queries, Answers, Authoritative nameservers, and Additional records. The packet bytes pane at the bottom shows the raw data of the selected packet, which is a DNS query for www.aikt.or.kr. The status bar at the bottom indicates "Frame (frame) 156 bytes" and "Profile Default".