



Лабораториска вежба бр. 2	DNS протокол		
Име и презиме	Индекс	Група	Датум
Стефан Милев	206055	4 – КН	07.11.2021

01. Извршете ја nslookup командата за да добиете IP адреса на веб-сервер во Азија.
Која е IP адресата на тој сервер?

Серверот има:

- IPv4: 166.111.4.100
- IPv6: 2402:f000:1:404:166:111:4:100

λ nslookup www.tsinghua.edu.cn

Server: one.one.one.one

Address: 1.1.1.1

Non-authoritative answer:

Name: www.tsinghua.edu.cn

Addresses: 2402:f000:1:404:166:111:4:100
166.111.4.100

02. Извршете ја nslookup командата за да ги одредите авторитетните DNS сервери
за универзитет во Европа.

Name servers за finki.ukim.mk:

- ns1.finki.ukim.mk
- ns2.finki.ukim.mk
- ns3.finki.ukim.mk
- ns4.finki.ukim.mk
- ns1.io.mk
- ns2.io.mk

λ nslookup -type=NS finki.ukim.mk

Server: one.one.one.one

Address: 1.1.1.1

Non-authoritative answer:

finki.ukim.mk nameserver = ns2.finki.ukim.mk
finki.ukim.mk nameserver = ns4.finki.ukim.mk
finki.ukim.mk nameserver = ns1.io.mk
finki.ukim.mk nameserver = ns1.finki.ukim.mk
finki.ukim.mk nameserver = ns2.io.mk
finki.ukim.mk nameserver = ns3.finki.ukim.mk



03. Извршете ја nslookup командата така што на еден од DNS серверите добиен од Прашањето 2 се испрати барање за mail серверите на Yahoo! mail. Која е неговата IP адреса?

Серверот mail.yahoo.com има:

- IPv6: 2a00:1288:80:800::7001, 2a00:1288:80:800::7000

- IPv4: 87.248.118.22, 87.248.118.23

λ nslookup mail.yahoo.com 1.1.1.1

Server: one.one.one.one

Address: 1.1.1.1

Non-authoritative answer:

Name: edge.gycpi.b.yahoodns.net

Addresses: 2a00:1288:80:800::7001

2a00:1288:80:800::7000

87.248.118.22

87.248.118.23

Aliases: mail.yahoo.com

04. Пронајдете ги DNS пораките за барањето и одговорите. Дали се испраќаат преку UDP или TCP?

Се испраќаат преку UDP.

Request:

The screenshot shows a Wireshark capture of network traffic on the 'Ethernet' interface. The packet list pane shows a DNS query (packet 1) and a response (packet 2) between 192.168.1.150 and 1.1.1.1. The packet details pane for packet 1 shows the User Datagram Protocol (UDP) header and the Domain Name System (query) section. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.150	1.1.1.1	DNS	72	Standard query 0x34c7 A www.ietf.org
2	0.053912	1.1.1.1	192.168.1.150	DNS	149	Standard query response 0x34c7 A www.ietf.org CNAME www.ietf.o...
3	0.054284	192.168.1.150	104.16.44.99	TCP	66	55937 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE...
4	0.092886	104.16.44.99	192.168.1.150	TCP	66	80 → 55937 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SA...
5	0.092929	192.168.1.150	104.16.44.99	TCP	54	55937 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
6	0.093076	192.168.1.150	104.16.44.99	HTTP	484	GET / HTTP/1.1
7	0.133630	104.16.44.99	192.168.1.150	TCP	60	80 → 55937 [ACK] Seq=1 Ack=431 Win=67584 Len=0
8	0.168629	104.16.44.99	192.168.1.150	HTTP	357	HTTP/1.1 301 Moved Permanently
9	0.170264	192.168.1.150	104.16.44.99	TCP	66	55938 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
10	0.210230	104.16.44.99	192.168.1.150	TCP	66	443 → 55938 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SA...

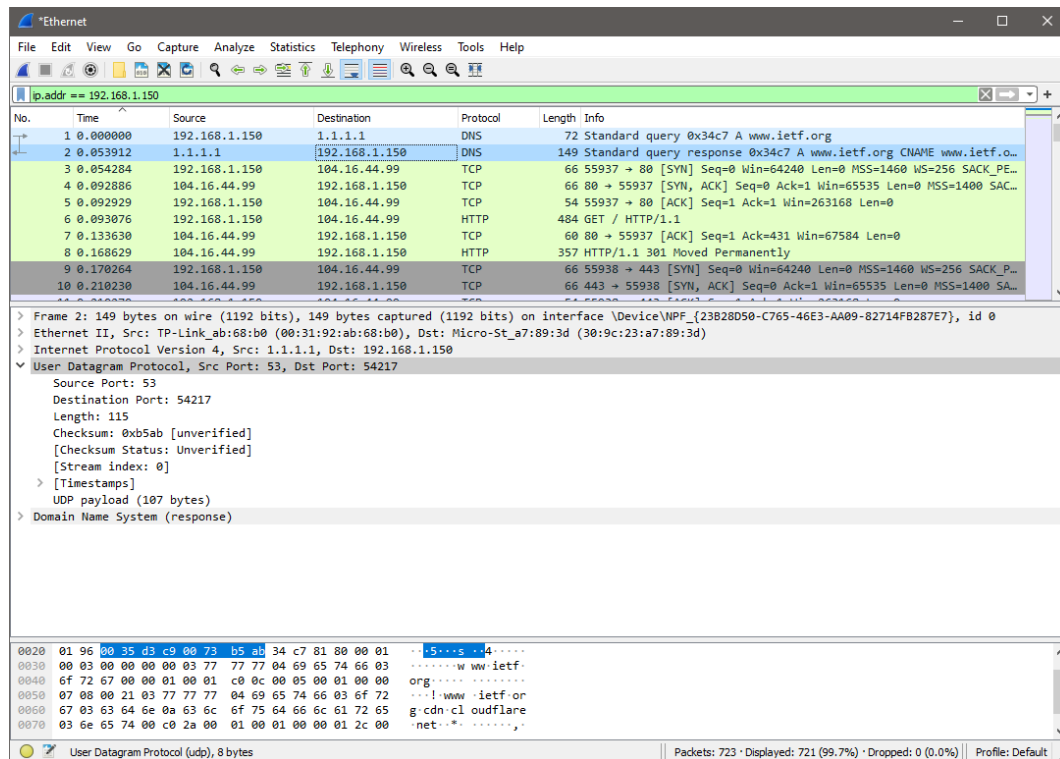
Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{23B28D50-C765-46E3-AA09-82714FB287E7}, id 0
> Ethernet II, Src: Micro-St_a7:89:3d (30:9c:23:a7:89:3d), Dst: TP-Link_ab:68:b0 (00:31:92:ab:68:b0)
> Internet Protocol Version 4, Src: 192.168.1.150, Dst: 1.1.1.1
User Datagram Protocol, Src Port: 54217, Dst Port: 53
Source Port: 54217
Destination Port: 53
Length: 38
Checksum: 0xc477 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
> [Timestamps]
> UDP payload (30 bytes)
> Domain Name System (query)

0000 00 31 92 ab 68 b0 30 9c 23 a7 89 3d 00 00 45 00 .1.h.0.#.....E
0010 00 3a 6e 64 00 00 00 11 00 00 c0 a8 01 95 01 01 .:nd.....
0020 01 01 55 c3 00 25 00 26 c4 77 34 c7 01 00 00 01 ..P.5.8.4.....
0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03Www.ietf-
0040 6f 72 67 00 00 01 00 01 org.....

User Datagram Protocol (udp), 8 bytes | Packets: 723 · Displayed: 721 (99.7%) · Dropped: 0 (0.0%) | Profile: Default



Response:



05. Која е дестинациската порта на пораката за DNS барање? Која е изворната порта на пораката за DNS одговор?

Изворната порта: 54217

Дестинациска порта: 53

06. На која IP адреса се испраќа пораката за DNS барање? Користете ipconfig за да ја одредите IP адресата на вашиот локален DNS сервер. Дали се овие две IP адреси исти?

Пораката се испраќа на локалниот DNS сервер 1.1.1.1 кој исто така може да се добие со ipconfig.

Ethernet adapter Ethernet:

DNS Servers : 1.1.1.1
1.0.0.1



07. Разгледајте ја пораката за DNS барање. Кој "Туре" на DNS барањето е тоа? Дали пораката за барање содржи некои „одговори“?

Типот на DNS барањето е А.

DNS барањето не содржи одговори.

Response:

The screenshot shows a Wireshark packet capture of a DNS query and response. The packet list at the top shows a query (packet 2) and a response (packet 3). The packet details pane for packet 3 shows the response structure, including the transaction ID, flags, and the list of answers. The packet bytes pane shows the raw data of the response packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.150	1.1.1.1	DNS	72	Standard query 0x34c7 A www.ietf.org
2	0.053912	1.1.1.1	192.168.1.150	DNS	149	Standard query response 0x34c7 A www.ietf.org CNAME www.ietf.org
3	0.054284	192.168.1.150	104.16.44.99	TCP	66	55937 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
4	0.092886	104.16.44.99	192.168.1.150	TCP	66	80 → 55937 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SAC...
5	0.092929	192.168.1.150	104.16.44.99	TCP	54	55937 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
6	0.093076	192.168.1.150	104.16.44.99	HTTP	484	GET / HTTP/1.1
7	0.133630	104.16.44.99	192.168.1.150	TCP	60	80 → 55937 [ACK] Seq=1 Ack=431 Win=67584 Len=0
8	0.168629	104.16.44.99	192.168.1.150	HTTP	357	HTTP/1.1 301 Moved Permanently
9	0.170264	192.168.1.150	104.16.44.99	TCP	66	55938 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
10	0.210230	104.16.44.99	192.168.1.150	TCP	66	443 → 55938 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SA...

Packet 3 details:

- [Checksum Status: Unverified]
- [Stream index: 0]
- [Timestamps]
- UDP payload (107 bytes)
- Domain Name System (response)
 - Transaction ID: 0x34c7
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.ietf.org: type A, class IN
 - Answers
 - www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
 - www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
 - www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99

Packet 3 bytes:

```
0030 00 03 00 00 00 00 77 77 77 04 69 65 74 66 03 .....w ww.ietf
0040 6f 72 67 06 00 01 00 01 c0 0c 00 05 00 01 00 00 ogse...
0050 07 08 00 21 03 77 77 77 04 69 65 74 66 03 6f 72 ...l www .ietf.or
0060 67 03 63 64 6e 0a 63 6c 6f 75 64 66 6c 61 72 65 g:cdn:cl oudflare
0070 03 6e 65 74 00 c0 2a 00 01 00 01 00 00 01 2c 00 net...:
0080 04 68 10 2c 63 c0 2a 00 01 00 01 00 00 01 2c 00 h,c*: .....
```

08. Разгледајте ја пораката за DNS одговор. Колку „одговори“ се дадени? Што содржат секој од овие одговори?

Дадени се 3 одговори:

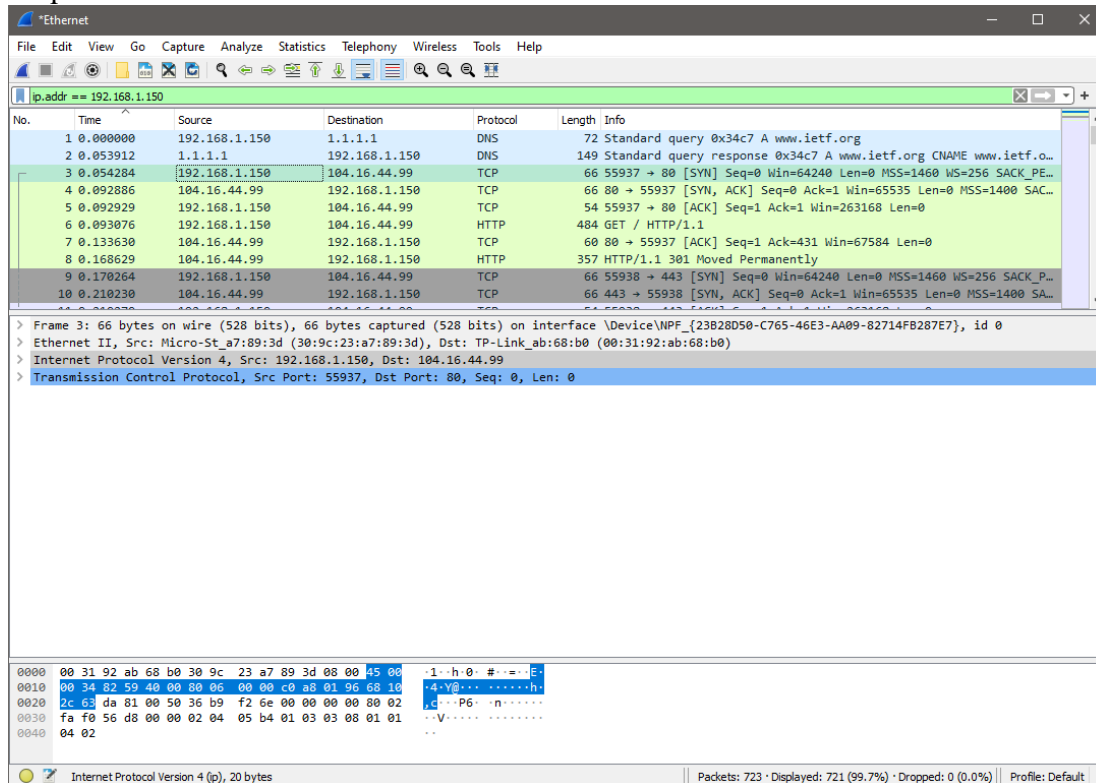
- 1 CNAME, кој враќа алиас на доменот
- 2 А, кои враќаат IP адреси



09. Разгледајте го последователниот TCP SYN пакет испратен од вашиот домаќин. Дали IP адресата за дестинација на SYN пакетот одговара на која било IP адреса дадена во пораката за DNS одговор?

Да, дестинациската IP адреса е 104.16.44.99, која се содржи во првиот А одговор на DNS барањето.

Request:



10. Оваа Веб страница содржи слики. Пред да ја прегледате секоја слика, дали вашиот домаќин издава нови DNS барања?

Не се издадени нови DNS барања затоа што сите слики се наоѓаат на истиот хост за кој веќе имаме кеширано DNS барање.

11. Која е дестинациската порта на пораката за DNS барање? Која е изворната порта на пораката за DNS одговор?

Изворна порта: 49703

Дестинациска порта: 53



Request:

Wireshark packet capture showing a DNS query from 192.168.1.150 to 1.1.1.1. The packet list shows a standard query for PTR 1.1.1.1.in-addr.arpa. The packet details show the User Datagram Protocol (UDP) and Domain Name System (DNS) fields. The packet bytes show the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.150	1.1.1.1	DNS	80	Standard query 0x0001 PTR 1.1.1.1.in-addr.arpa
2	0.039171	1.1.1.1	192.168.1.150	DNS	109	Standard query response 0x0001 PTR 1.1.1.1.in-addr.arpa PTR on...
3	0.040150	192.168.1.150	1.1.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
4	0.126029	146.66.155.38	192.168.1.150	TLSv1.2	576	Application Data
5	0.175518	146.66.155.38	192.168.1.150	TLSv1.2	541	Application Data
6	0.175550	192.168.1.150	146.66.155.38	TCP	54	54094 → 27038 [ACK] Seq=1 Ack=1010 Win=1026 Len=0
7	0.225496	146.66.155.38	192.168.1.150	TLSv1.2	154	Application Data
8	0.245754	1.1.1.1	192.168.1.150	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu...
9	0.247722	192.168.1.150	1.1.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
10	0.274657	192.168.1.150	146.66.155.38	TCP	54	54094 → 27038 [ACK] Seq=1 Ack=1110 Win=1026 Len=0

Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{23B28D50-C765-46E3-AA09-82714FB287E7}, id 0

Ethernet II, Src: Micro-St_a7:89:3d (30:9c:23:a7:89:3d), Dst: TP-Link_ab:68:b0 (00:31:92:ab:68:b0)

Internet Protocol Version 4, Src: 192.168.1.150, Dst: 1.1.1.1

User Datagram Protocol, Src Port: 49703, Dst Port: 53

Source Port: 49703
Destination Port: 53
Length: 46
Checksum: 0xc47f [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (38 bytes)

Domain Name System (query)

Transaction ID: 0x0001

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

0000 00 31 92 ab 68 b0 30 9c 23 a7 89 3d 08 00 45 00 1·h·0·#····E·
0010 00 42 6e f8 00 00 80 11 00 00 c0 a8 01 96 01 01 ·8n·····
0020 01 01 c2 2f 00 35 00 2e c4 7f 00 01 01 00 00 01 ·5·
0030 00 00 00 00 00 01 31 01 31 01 31 01 31 07 69 ····1·1·1·i·
0040 6e 2d 61 64 64 72 04 61 72 70 61 00 00 0c 00 01 n-addr:a rpa·

12. На која IP адреса се испраќа пораката за DNS барање? Дали е ова IP адресата на вашиот основен локален DNS сервер?

Пораката се испраќа на локалниот DNS сервер 1.1.1.1.



13. Разгледајте ја пораката за DNS барање. Кој "Type" на DNS барање е тоа? Дали пораката за DNS барање содржи „одговори“?

Типот на DNS барање е A.

Пораката за DNS барањето не содржи одговори.

Request:

Wireshark packet capture showing a DNS query. The packet list shows a standard query from 192.168.1.150 to 1.1.1.1. The packet details show a standard query for www.mit.edu type A, class IN. The packet bytes show the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.150	1.1.1.1	DNS	80	Standard query 0x0001 PTR 1.1.1.1.in-addr.arpa
2	0.039171	1.1.1.1	192.168.1.150	DNS	109	Standard query response 0x0001 PTR 1.1.1.1.in-addr.arpa PTR on...
3	0.040150	192.168.1.150	1.1.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
4	0.126029	146.66.155.38	192.168.1.150	TLSv1.2	576	Application Data
5	0.175518	146.66.155.38	192.168.1.150	TLSv1.2	541	Application Data
6	0.175550	192.168.1.150	146.66.155.38	TCP	54	54094 → 27038 [ACK] Seq=1 Ack=1010 Win=1026 Len=0
7	0.225496	146.66.155.38	192.168.1.150	TLSv1.2	154	Application Data
8	0.245754	1.1.1.1	192.168.1.150	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu...
9	0.247722	192.168.1.150	1.1.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
10	0.274657	192.168.1.150	146.66.155.38	TCP	54	54094 → 27038 [ACK] Seq=1 Ack=1110 Win=1026 Len=0

[Checksum Status: Unverified]
[Stream index: 1]
> [Timestamps]
UDP payload (29 bytes)
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
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 8]

0000 00 31 92 ab 68 b0 30 9c 23 a7 89 3d 08 00 45 00 :1..h.0.#.....E
0010 00 39 6e f9 00 00 00 11 00 00 c0 a8 01 96 01 01 :9n.....
0020 01 01 c2 28 00 35 00 25 c4 76 00 02 01 00 00 01 :...(-5.%-v.....
0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65 :.....w ww-mit-e
0040 64 75 00 00 01 00 01 du.....



14. Разгледајте ја пораката за DNS одговор. Колку „одговори“ се дадени? Што содржи секој од овие одговори?

Одговори:

- 2 CNAME, кои враќаат алиас
- 1 A, кој враќа IP адреса

Response:

The screenshot shows a Wireshark capture of network traffic on the 'Ethernet' interface. The filter is set to 'ip.addr == 192.168.1.150'. The packet list shows a DNS response from 192.168.1.150 to 1.1.1.1. The packet details pane shows the following information:

- Transaction ID: 0x0002
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 3
- Authority RRs: 0
- Additional RRs: 0
- Queries
 - www.mit.edu: type A, class IN
 - Name: www.mit.edu
 - [Name Length: 11]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
- Answers
 - www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 - www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 - e9566.dscb.akamaiedge.net: type A, class IN, addr 96.16.142.195

The packet bytes pane shows the raw data of the DNS response, including the header and the three answer records.



15. Поставете screenshot.

The screenshot shows a Wireshark capture of network traffic on the Ethernet interface. The packet list pane displays 18 packets. Packet 8 is a DNS Standard query response from 1.1.1.1 to 192.168.1.150. The packet details pane for packet 8 shows the following information:

- Checksum: 0xc3c0 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 1]
- > [Timestamps]
- UDP payload (118 bytes)
- Domain Name System (response)
 - Transaction ID: 0x0002
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - www.mit.edu: type A, class IN
 - Name: www.mit.edu
 - [Name Length: 11]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
- Answers
 - www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 - www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 - e9566.dscb.akamaiedge.net: type A, class IN, addr 96.16.142.195
- [Request In: 3]
- [Time: 0.205604000 seconds]

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header.

16. На која IP адреса се испраќа пораката за DNS барање? Дали е ова IP адресата на вашиот основен локален DNS сервер?

Пораката се испраќа на локалниот DNS сервер 1.1.1.1.

17. Разгледајте ја пораката за DNS барање. Кој "Type" на DNS барање е тоа? Дали пораката за DNS барање содржи „одговори“?

Типот на DNS барањето е NS.
Не содржи одговори.



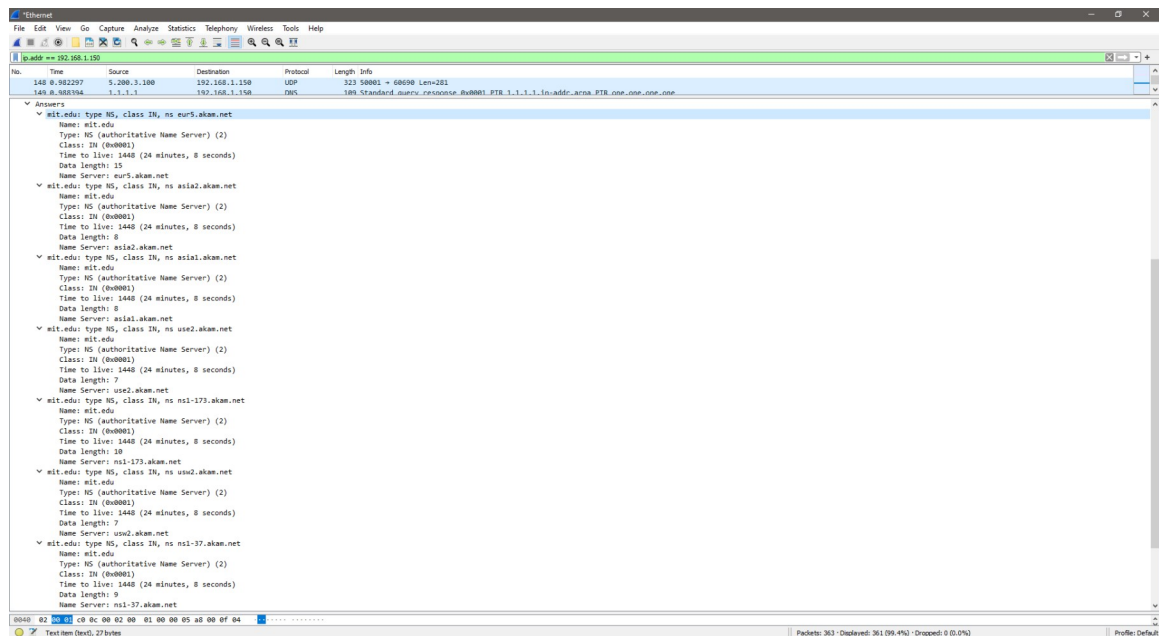
18. Разгледајте ја пораката за DNS одговор. Кои пате сервери на MIT се дадени во порака за одговор? Дали оваа порака за одговор дава и IP адреси на пате серверите на MIT?

Name servers:

- ns1-173.akam.net
- ns1-37.akam.net
- usw2.akam.net
- eur5.akam.net
- asia1.akam.net
- use2.akam.net
- use5.akam.net
- asia2.akam.net

Во полето Additional records се достапни IP адресите на пате серверите.

19. Поставете screenshot.





20. На која IP адреса е пратено DNS барањето? Дали е ова IP адресата на вашиот основен локален DNS сервер? Ако не, на што одговара оваа IP адреса?

Барањето се испраќа на локалниот DNS сервер 1.1.1.1 за да се добие адресата на dns.google, а потоа се испраќа барање на IP адресата 8.8.4.4. Оваа IP адреса одговара на dns.google.

Request:

Wireshark packet capture showing a DNS query. The packet list shows a standard query from 192.168.1.150 to 8.8.4.4. The packet details show the query structure with transaction ID 0x0002 and flags for standard query. The packet bytes show the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
40	0.403401	8.8.4.4	192.168.1.150	DNS	104	Standard query response 0x0001 PTR 4.4.8.in-addr.arpa PTR dn...
41	0.403985	192.168.1.150	8.8.4.4	DNS	74	Standard query 0x0002 A www.aiit.or.kr
42	0.409986	192.168.1.150	162.159.138.234	TLSv1.2	140	Application Data
43	0.411191	192.168.1.100	192.168.1.150	TCP	414	42420 → 60582 [PSH, ACK] Seq=5028 Ack=173 Win=8209 Len=360
44	0.419922	5.200.3.100	192.168.1.150	UDP	85	50001 → 64228 Len=43
45	0.422330	192.168.1.150	5.200.3.100	UDP	305	64228 → 50001 Len=263
46	0.428009	192.168.1.150	192.168.1.100	TCP	97	60582 → 42420 [PSH, ACK] Seq=173 Ack=5388 Win=8211 Len=43
47	0.433654	8.8.4.4	192.168.1.150	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225

Frame 41: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{23B28D50-C765-46E3-AA09-82714FB287E7}, id 0
Ethernet II, Src: Micro-St_a7:89:3d (30:9c:23:a7:89:3d), Dst: TP-Link_ab:68:b0 (00:31:92:ab:68:b0)
Internet Protocol Version 4, Src: 192.168.1.150, Dst: 8.8.4.4
User Datagram Protocol, Src Port: 62403, Dst Port: 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.aiit.or.kr: type A, class IN
Name: www.aiit.or.kr
[Name Length: 14]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 47]

0000 00 31 92 ab 68 b0 30 9c 23 a7 89 3d 08 00 45 00 1..h.0. #...E.
0010 00 3c da b6 00 00 00 11 00 00 c0 a8 01 96 08 08 <.....
0020 04 04 f3 c3 00 35 00 28 ce 83 00 02 01 00 00 015(.....
0030 00 00 00 00 00 00 03 77 77 77 04 61 69 69 74 02w ww.aiit.
0040 6f 72 02 6b 72 00 00 01 00 01 or.kr....

21. Разгледајте ја пораката за DNS барање. Кој "Туре" на DNS барање е тоа? Дали пораката за DNS барање содржи „одговори“?

Типот на DNS барањето е А.
Не содржи одговори.

22. Разгледајте ја пораката за DNS одговор. Колку „одговори“ се дадени? Што содржи секој од овие одговори?

Има еден одговор од А тип кој ја содржи IP адресата.



23. Поставет screenshot.

The screenshot displays the Wireshark interface with a packet capture of network traffic. The filter bar at the top shows 'ip.addr == 192.168.1.150'. The packet list on the left shows several packets, with packet 47 selected. The packet details pane on the right shows the structure of the selected packet, which is a DNS Standard query response. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
43	0.411191	192.168.1.100	192.168.1.150	TCP	414	42420 → 60582 [PSH, ACK] Seq=5028 Ack=173 Win=8209 Len=360
44	0.419922	5.200.3.100	192.168.1.150	UDP	85	50001 → 64228 Len=43
45	0.422330	192.168.1.150	5.200.3.100	UDP	305	64228 → 50001 Len=263
46	0.428009	192.168.1.150	192.168.1.100	TCP	97	60582 → 42420 [PSH, ACK] Seq=173 Ack=5388 Win=8211 Len=43
47	0.433654	8.8.4.4	192.168.1.150	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
48	0.435610	192.168.1.150	8.8.4.4	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
49	0.437416	5.200.3.100	192.168.1.150	UDP	85	50001 → 64228 Len=43
50	0.439304	192.168.1.150	5.200.3.100	UDP	300	64228 → 50001 Len=258

Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0

Queries

- www.aiit.or.kr: type A, class IN
Name: www.aiit.or.kr
[Name Length: 14]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

- www.aiit.or.kr: type A, class IN, addr 58.229.6.225
Name: www.aiit.or.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 2423 (40 minutes, 23 seconds)
Data length: 4
Address: 58.229.6.225
[Request In: 41]
[Time: 0.029669000 seconds]

0010 00 4c b1 d8 00 00 7b 11 be fe 08 08 04 04 c0 a8 .L....{.....
0020 01 96 00 35 f3 c3 00 38 6f cb 00 02 81 80 00 01 ...5...8 o.....
0030 00 01 00 00 00 00 03 77 77 77 04 61 69 69 74 02w ww.aiit..
0040 6f 72 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01 or kn.....
0050 00 00 09 77 00 04 3a e5 06 e1W...i.....

Text item (text), 16 bytes | Packets: 142 · Displayed: 142 (100.0%) · Dropped: 0 (0.0%) | Profile: Default