



Лабораториска вежба бр. 2	DNS протокол		
Име и презиме	Индекс	Група	Датум
Тодор Јовановски	213133	10	13.11.2022

01. За ова прашање ја извршив nslookup командата за страната на музејот на Studio Ghibli во Јапонија. IP адресата на тој сервер е: 52.222.214.12.

02. Овој пат nslookup ја извршив за универзитетот Оксфорд во Англија. Авторитативниот сервер е raptor.dns.ox.ac.uk.

03. По испраќање на барањето за !Yahoo mail серверите до raptor.dns.ox.ac.uk е добиена IP адресата 212.82.116.206.

04. DNS пораките за барањето и одговорите се испраќаат преку UDP.

Internet Protocol Version 4, Src: 192.168.0.113, Dst: 192.168.0.1

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 58

Identification: 0x6a0f (27151)

000. = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: UDP (17)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.0.113

Destination Address: 192.168.0.1

05. Дестинациската порта на порака за DNS барање е 53. Изворната порта на пораката за DNS одговор е исто така 53.

Барање: User Datagram Protocol, Src Port: 65129, Dst Port: 53

Одговор: User Datagram Protocol, Src Port: 53, Dst Port: 65129

06. Пораката за DNS барањето се испраќа на адреса 192.168.0.1. Истата се совпаѓа со адресата на мојот локален DNS сервер.

Internet Protocol Version 4, Src: 192.168.0.113, Dst: 192.168.0.1

DNS Servers : 192.168.0.1

07. DNS пораката за барање е од тип А. Пораката не содржи никакви одговори.

Domain Name System (query)

Transaction ID: 0x942f

Flags: 0x0100 Standard query

Questions: 1



Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.ietf.org: type A, class IN

08. Во пораката за DNS одговор се дадени 3 одговори.

Answer RRs: 3

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 104.16.45.99

www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99

09. IP адресата за дестинација на последователниот TCP SYN пакет одговара на IP адресата наведена во втората порака од DNS одговорот.

SYN: Internet Protocol Version 4, Src: 192.168.0.113, Dst: 104.16.45.99

Answer: www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99

10. Домаќинот не издава нови DNS барања.

11. Дестинациската порта на пораката за DNS барање е 53. Изворната порта на пораката за DNS одговор е исто така 53.

Барање: User Datagram Protocol, Src Port: 54195, Dst Port: 53

Одговор: User Datagram Protocol, Src Port: 53, Dst Port: 54195

12. Пораката за DNS барањето се испраќа на адреса 192.168.0.1. Истата се совпаѓа со адресата на мојот локален DNS сервер.

Internet Protocol Version 4, Src: 192.168.0.113, Dst: 192.168.0.1

DNS Servers : 192.168.0.1

13. DNS пораката за барање е од тип A. Пораката не содржи никакви одговори.

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



14. Во DNS пораката за одговор се дадени 3 одговори:

Answer RRs: 3

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 104.103.85.139

15.

Wireshark packet capture showing a DNS response from 192.168.0.113 to 192.168.0.1. The packet is a Standard query response (0x0002) for the domain www.mit.edu. The response contains three Answer RRs: www.mit.edu (CNAME), www.mit.edu.edgekey.net (CNAME), and e9566.dscb.akamaiedge.net (A). The packet is captured on interface \Device\NPF_{50FFA852-1140-49AB-8EA0-CC543E22BF}.

16. Пораката за DNS барањето се испраќа на адреса 192.168.0.1. Истата се совпаѓа со адресата на мојот локален DNS сервер.

Internet Protocol Version 4, Src: 192.168.0.113, Dst: 192.168.0.1

DNS Servers : 192.168.0.1

17. DNS пораката за барање е од тип NS. Пораката не содржи никакви одговори.

Domain Name System (query)

Transaction ID: 0x0002

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

mit.edu: type NS, class IN



18. DNS пораката за одговор ги содржи имињата на следните name сервери:

Answers

mit.edu: type NS, class IN, ns usw2.akam.net
mit.edu: type NS, class IN, ns asia2.akam.net
mit.edu: type NS, class IN, ns ns1-37.akam.net
mit.edu: type NS, class IN, ns ns1-173.akam.net
mit.edu: type NS, class IN, ns use2.akam.net
mit.edu: type NS, class IN, ns asia1.akam.net
mit.edu: type NS, class IN, ns eur5.akam.net
mit.edu: type NS, class IN, ns use5.akam.net

- IP адресите на name серверите се содржат во заглавјето Additional records:

Additional records

ns1-37.akam.net: type A, class IN, addr 193.108.91.37
ns1-173.akam.net: type A, class IN, addr 193.108.91.173
ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
asia1.akam.net: type A, class IN, addr 95.100.175.64
use5.akam.net: type A, class IN, addr 2.16.40.64
use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
asia2.akam.net: type A, class IN, addr 95.101.36.64
use2.akam.net: type A, class IN, addr 96.7.49.64
eur5.akam.net: type A, class IN, addr 23.74.25.64
usw2.akam.net: type A, class IN, addr 184.26.161.64

19.

The screenshot displays a Wireshark capture of a DNS response packet. The packet list on the left shows a 'Standard query response' from 192.168.0.1 to 192.168.0.113. The packet details pane on the right shows the 'Domain Name System (response)' section with transaction ID 0x0002. The packet bytes pane on the right shows the raw data of the DNS response, including the header and the list of answers and additional records.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.113	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
2	0.002584	192.168.0.1	192.168.0.113	DNS	161	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa 50A prisoner.iana.org
3	0.002932	192.168.0.113	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
4	0.027598	192.168.0.1	192.168.0.113	DNS	418	Standard query response 0x0002 NS mit.edu NS usw2.akam.net NS asia2.akam.net NS ns1-37.akam.net NS ns1-173.akam.net

Packet Details:

Frame 4: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface \Device\NPF_{50FFA852-1140-49A8-8EA9-CCF543E22BF9}

Ethernet II, Src: Tp-Link_t5:9d:f0 (f8:1a:67:e5:9d:f0), Dst: Giga-Byt_76:3a:fb (18:c0:4d:76:3a:fb)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.113

User Datagram Protocol, Src Port: 53, Dst Port: 52529

Domain Name System (response)

Transaction ID: 0x0002

Flags: 0x1800 Standard query response, No error

Questions: 1

Answer RRs: 8

Authority RRs: 0

Additional RRs: 10

Queries

Answers

- mit.edu: type NS, class IN, ns usw2.akam.net
- mit.edu: type NS, class IN, ns asia2.akam.net
- mit.edu: type NS, class IN, ns ns1-37.akam.net
- mit.edu: type NS, class IN, ns ns1-173.akam.net
- mit.edu: type NS, class IN, ns use2.akam.net
- mit.edu: type NS, class IN, ns asia1.akam.net
- mit.edu: type NS, class IN, ns eur5.akam.net
- mit.edu: type NS, class IN, ns use5.akam.net

Additional records

- ns1-37.akam.net: type A, class IN, addr 193.108.91.37
- ns1-173.akam.net: type A, class IN, addr 193.108.91.173
- ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
- asia1.akam.net: type A, class IN, addr 95.100.175.64
- use5.akam.net: type A, class IN, addr 2.16.40.64
- use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
- asia2.akam.net: type A, class IN, addr 95.101.36.64
- use2.akam.net: type A, class IN, addr 96.7.49.64
- eur5.akam.net: type A, class IN, addr 23.74.25.64
- usw2.akam.net: type A, class IN, addr 184.26.161.64

[Request In: 3]

[Time: 0.024666000 seconds]



20. Првото DNS до dns.google е испратено до локалниот DNS сервер со IP адреса 192.168.0.1. IP адресата во второто DNS барање изнесува 8.8.8.8 и истата соодветствува на www.aiit.or.kr.

21. DNS пораката за барање е од тип A. Пораката не содржи никакви одговори.

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

22. Во DNS пораката за одговор е даден еден одговор:

Answers

www.aiit.or.kr: type A, class IN, addr 58.229.6.225

23.

The screenshot displays a Wireshark capture of network traffic on the interface \Device\NPF_{50FFA852-1140-49A8-8EA9-CC543E22BF9}. The packet list shows several DNS queries and responses. The selected packet is a DNS Standard query response (Frame 9) from 192.168.0.113 to 8.8.8.8, containing an answer for www.aiit.or.kr with IP address 58.229.6.225.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.113	142.250.187.132	TCP	55	59279 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
2	0.005676	142.250.187.132	192.168.0.113	TCP	60	443 → 59279 [RST] Seq=1 Win=0 Len=0
3	0.159989	192.168.0.113	192.168.0.1	DNS	70	Standard query 0xa31e A dns.google
4	0.161454	192.168.0.1	192.168.0.113	DNS	355	Standard query response 0xa31e A dns.google A 8.8.8.8 A 8.8.4.4 NS ns4.zdns.google NS ns2.zdns.google NS ns3.zdns.google
5	0.162504	192.168.0.113	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
6	0.166945	192.168.0.113	146.66.155.38	TLSv1.2	105	Application Data
7	0.168018	8.8.8.8	192.168.0.113	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
8	0.168670	192.168.0.113	8.8.8.8	DNS	74	Standard query 0x0002 A www.aiit.or.kr
9	0.202566	8.8.8.8	192.168.0.113	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
10	0.204042	192.168.0.113	8.8.8.8	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
11	0.240636	146.66.155.38	192.168.0.113	TCP	60	27029 → 57367 [ACK] Seq=1 Ack=52 Win=1026 Len=0
12	0.788497	8.8.8.8	192.168.0.113	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszl.com

Frame 9: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{50FFA852-1140-49A8-8EA9-CC543E22BF9}, Id 00000000, Ethernet II, Src: Tp-LinkT_e5:9d:f0 (f8:1a:67:e5:9d:f0), Dst: Giga-Byt_76:3a:fb (18:c0:4d:76:3a:fb)

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.0.113

User Datagram Protocol, Src Port: 53, Dst Port: 64900

Domain Name System (response)

Transaction ID: 0x0002

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

Answers

> www.aiit.or.kr: type A, class IN, addr 58.229.6.225

[Request In: 8]

[Time: 0.033896000 seconds]