



Лабораториска вежба бр. 2	DNS протокол		
Име и презиме	Индекс	Група	Датум
<i>Име и презиме</i>	<i>223311</i>	<i>ПИТ2</i>	<i>12.11.2023</i>

**Напомена:** Сите одговори треба да бидат напишани со црвена боја.

01. Резултатот од командата nslookup покажува дека IP адресата на доменот е 23.56.205.41 (www.alibaba.com)

02. Авторитетните сервери на www.ue-germany.com се:  
ue-germany.com nameserver = ns-1144.awsdns-15.org.  
ue-germany.com nameserver = ns-614.awsdns-12.net.  
ue-germany.com nameserver = ns-55.awsdns-06.com.  
ue-germany.com nameserver = ns-1766.awsdns-28.co.uk.

03. nslookup -type=MX yahoo.com ns-1144.awsdns-15.org

Server: ns-1144.awsdns-15.org

Address: 205.251.196.120#53

\*\* server can't find yahoo.com: REFUSED

04. 3 0.042749 192.168.100.88 192.168.100.1 DNS 81 Standard  
query 0xb087 HTTPS courses.finki.ukim.mk  
4 0.042895 192.168.100.88 192.168.100.1 DNS 81 Standard  
query 0x65b1 A courses.finki.ukim.mk  
5 0.048147 192.168.100.1 192.168.100.88 DNS 148 Standard  
query response 0xb087 HTTPS courses.finki.ukim.mk CNAME lb.finki.ukim.mk SOA  
ns3.finki.ukim.mk  
7 0.052036 192.168.100.1 192.168.100.88 DNS 241 Standard  
query response 0x65b1 A courses.finki.ukim.mk CNAME lb.finki.ukim.mk A  
194.149.137.199 NS ns3.finki.ukim.mk NS ns2.io.mk NS ns4.finki.ukim.mk NS  
ns1.io.mk NS ns1.finki.ukim.mk NS ns2.finki.ukim.mk A 194.149.137.129  
Според стандартите комуникацијата се извршува преку UDP на порта 53

05. Дестинациска порта е 53 а изворна порта е 62979

06. Адресата на мојот локален сервер е 192.168.100.1 и адресата на која што се праќа порака за барање на ДНС е 192.186.100.1, односно иста.



07. Тип на порака е standard query и дополнителни информации кои што ги содржи пораката се: HTTPS courses.finki.ukim.mk

08. Има 2 одговори (пораки).

5 0.048147 192.168.100.1 192.168.100.88 DNS 148 Standard query response 0xb087 HTTPS courses.finki.ukim.mk CNAME lb.finki.ukim.mk SOA ns3.finki.ukim.mk

7 0.052036 192.168.100.1 192.168.100.88 DNS 241 Standard query response 0x65b1 A courses.finki.ukim.mk CNAME lb.finki.ukim.mk A 194.149.137.199 NS ns3.finki.ukim.mk NS ns2.io.mk NS ns4.finki.ukim.mk NS ns1.io.mk NS ns1.finki.ukim.mk NS ns2.finki.ukim.mk A 194.149.137.129

09. IP адреса во пакетот TCP SYN (194.149.137.199) одговара на IP адресата добиена од одговорот на барањето DNS, што покажува дека хостот се обидува да се поврзе со веб-серверот

10. Да домаќинот често прави нови барања за имињата на домените за каде се архивирани сликите.

11. Дестинациска порта: 53 Изворна порта:57713

12. 192.168.100.1 е адресата на која што се праќа барањето и се совпаѓа со адресата на мојот локален сервер.

13. www.mit.edu:A(address)

14. Има само еден одговор. Non-authoritative answer:

www.mit.edu canonical name = www.mit.edu.edgekey.net.

www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.

Name: e9566.dscb.akamaiedge.net

Address: 23.56.203.58

Одговорот е само IPv4 адреса за www.mit.edu: 23.56.203.58

15.

```
[eva@Evas-MacBook-Pro ~ % nslookup www.mit.edu
Server:      192.168.100.1
Address:     192.168.100.1#53

Non-authoritative answer:
www.mit.edu canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:       e9566.dscb.akamaiedge.net
Address: 23.56.203.58

eva@Evas-MacBook-Pro ~ %
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.88	192.168.100.88	TLSv1..	157	Application Data
2	0.000192	192.168.100.101	239.255.255.250	UDP	514	41797 → 8082 Len=472
3	0.000245	192.168.100.88	162.159.134.234	TCP	66	54865 → 443 [ACK] Seq=1 Ack=92 Win=2046 Len=0 TSval=3111225988 TSecr=1265518621
4	1.531951	192.168.100.88	17.250.82.9	UDP	83	64217 → 443 Len=41
5	1.576739	17.250.82.9	192.168.100.88	UDP	73	443 → 64217 Len=31
6	2.759866	192.168.100.88	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
7	2.951571	192.168.100.101	239.255.255.250	UDP	514	41797 → 8082 Len=472
8	3.859237	192.168.100.88	192.168.100.1	DNS	95	Standard query 0x32f5 HTTPS smoot-searchv2-aeucla.v.aapling.com
9	3.859374	192.168.100.88	192.168.100.1	DNS	95	Standard query 0xb2bb A smoot-searchv2-aeucla.v.aapling.com
10	3.868333	192.168.100.1	192.168.100.88	DNS	155	Standard query response 0x32f5 HTTPS smoot-searchv2-aeucla.v.aapling.com SOA a.gslb.aapling.com
11	3.868520	192.168.100.1	192.168.100.88	DNS	182	Standard query response 0xb2bb A smoot-searchv2-aeucla.v.aapling.com A 3.73.166.250 NS v1.gslb.aapling.com NS a.gslb.aapling.com
12	8.872171	192.168.100.88	3.73.166.250	TCP	78	51913 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1892112446 TSecr=0 SACK_PERM TF=0
13	3.111433	3.73.166.250	192.168.100.88	TCP	74	443 → 51913 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1412 SACK_PERM TSval=1879582629 TSecr=1892112446 WS=128
14	3.111713	192.168.100.88	3.73.166.250	TLSv1..	583	Client Hello
15	3.142597	192.168.100.88	192.168.100.1	DNS	71	Standard query 0xc8c8 HTTPS www.mit.edu
16	3.142835	192.168.100.88	192.168.100.1	DNS	71	Standard query 0xc7f9 A www.mit.edu
17	3.152976	3.73.166.250	192.168.100.88	TCP	66	443 → 51913 [ACK] Seq=1 Ack=518 Win=62080 Len=0 TSval=1879582668 TSecr=1892112486
18	3.153117	3.73.166.250	192.168.100.88	TLSv1..	1466	Server Hello, Change Cipher Spec, Application Data
19	3.153144	3.73.166.250	192.168.100.88	TCP	1466	443 → 51913 [PSH, ACK] Seq=1481 Ack=518 Win=62080 Len=1400 TSval=1879582671 TSecr=1892112486 [TCP segment of a reassembled PDU]
20	3.153150	3.73.166.250	192.168.100.88	TLSv1..	1007	Application Data, Application Data, Application Data, Application Data
21	3.153668	192.168.100.88	3.73.166.250	TCP	66	51913 → 443 [ACK] Seq=518 Ack=2801 Win=130176 Len=0 TSval=1892112528 TSecr=1879582671
22	3.154048	192.168.100.88	3.73.166.250	TCP	66	51913 → 443 [ACK] Seq=518 Ack=3802 Win=130048 Len=0 TSval=1892112528 TSecr=1879582671
23	3.158813	192.168.100.88	3.73.166.250	TLSv1..	130	Change Cipher Spec, Application Data
24	3.197095	3.73.166.250	192.168.100.88	TLSv1..	127	Application Data
25	3.197922	192.168.100.88	3.73.166.250	TLSv1..	146	Application Data
26	3.207933	192.168.100.1	192.168.100.88	DNS	500	Standard query response 0xc7f9 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.56.283.58 NS n2ds
27	3.210857	192.168.100.1	192.168.100.88	DNS	208	Standard query response 0xc8c8 HTTPS www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net SOA n0dscb.akamaiedge.net
28	3.211325	192.168.100.88	192.168.100.1	DNS	85	Standard query 0x4da3 HTTPS e9566.dscb.akamaiedge.net
29	3.211324	192.168.100.88	192.168.100.1	DNS	108	Standard query response 0x4da3 HTTPS e9566.dscb.akamaiedge.net SOA n0dscb.akamaiedge.net
30	3.220109	192.168.100.88	23.56.203.58	TCP	78	51914 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3793223452 TSecr=0 SACK_PERM
31	3.236374	3.73.166.250	192.168.100.88	TLSv1..	101	Application Data
32	3.236419	3.73.166.250	192.168.100.88	TLSv1..	97	Application Data
33	3.236657	192.168.100.88	3.73.166.250	TLSv1..	97	Application Data
34	3.236658	192.168.100.88	3.73.166.250	TCP	66	51913 → 443 [ACK] Seq=693 Ack=3929 Win=130944 Len=0 TSval=1892112611 TSecr=1879582754
35	3.260600	23.56.203.58	192.168.100.88	TCP	74	80 → 51914 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3793223452 TSecr=3793223452 WS=128
36	3.261408	192.168.100.88	23.56.203.58	TCP	66	51914 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=3793223492 TSecr=3873389960
37	3.322865	3.73.166.250	192.168.100.88	TCP	66	443 → 51913 [ACK] Seq=3929 Ack=693 Win=62080 Len=0 TSval=1879582835 TSecr=1892112611
38	3.397121	192.168.100.88	23.56.203.58	TCP	78	51915 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=682158613 TSecr=0 SACK_PERM
39	4.439158	23.56.203.58	192.168.100.88	TCP	74	80 → 51915 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=840049327 TSecr=682158613 WS=128
40	4.439727	192.168.100.88	23.56.203.58	TCP	66	51915 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=682158656 TSecr=840049327
41	4.463906	192.168.100.88	23.56.203.58	TCP	78	51916 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=192451318 TSecr=0 SACK_PERM
42	3.504657	23.56.203.58	192.168.100.88	TCP	74	443 → 51916 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3873390281 TSecr=192451318 WS=128
43	3.505496	192.168.100.88	23.56.203.58	TCP	66	51916 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=192451351 TSecr=3873390281
44	3.505896	192.168.100.88	23.56.203.58	TLSv1..	583	Client Hello
45	3.547781	23.56.203.58	192.168.100.88	TLSv1..	1466	Server Hello
46	3.548096	192.168.100.88	23.56.203.58	TCP	66	51916 → 443 [ACK] Seq=518 Ack=1481 Win=130176 Len=0 TSval=192451395 TSecr=3873390245
47	3.549139	23.56.203.58	192.168.100.88	TCP	1466	443 → 51916 [PSH, ACK] Seq=1481 Ack=518 Win=64768 Len=1400 TSval=3873390245 TSecr=192451351 [TCP segment of a reassembled PDU]
48	3.549253	192.168.100.88	23.56.203.58	TCP	66	51916 → 443 [ACK] Seq=518 Ack=2801 Win=129664 Len=0 TSval=192451396 TSecr=3873390245
49	3.549699	23.56.203.58	192.168.100.88	TLSv1..	1362	Certificate, Certificate Status
50	3.549970	192.168.100.88	23.56.203.58	TCP	66	51916 → 443 [ACK] Seq=518 Ack=4097 Win=129728 Len=0 TSval=192451396 TSecr=3873390245
51	3.550266	23.56.203.58	192.168.100.88	TLSv1..	387	Server Key Exchange, Server Hello Done

16. Дестинација: 192.168.100.1 Мојот локален сервер: 192.168.100.1

17. Не бидејќи оваа команда бара имиња на авторитетни сервери за www.mit.edu

18. mit.edu nameserver = ns1-37.akam.net.

mit.edu nameserver = ns1-173.akam.net.

mit.edu nameserver = usw2.akam.net.

mit.edu nameserver = use5.akam.net.

mit.edu nameserver = asia1.akam.net.

mit.edu nameserver = eur5.akam.net.

mit.edu nameserver = asia2.akam.net.

mit.edu nameserver = use2.akam.net. не ги дава одговорите директно

19.

```
eva@Evas-MacBook-Pro ~ % nslookup -type=NS mit.edu
Server:      192.168.100.1
Address:     192.168.100.1#53
```

Non-authoritative answer:

```
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = use2.akam.net.
```

Authoritative answers can be found from:

```
asia1.akam.net internet address = 95.100.175.64
asia2.akam.net internet address = 95.101.36.64
```



20. 8.8.8.8 (dns.google) не оваа адреса припаѓа google dns

21. A(Address)

22. Non-authoritative answer:

Name: www.aiit.or.kr

Address: 58.229.6.225

да ја содржи адресата 58.229.6.225

23.

```
use5.akam.net    internet address = 2.16.40.64
use5.akam.net    has AAAA address 2600:1403:a::40

[eva@Evas-MacBook-Pro ~ % nslookup www.mit.edu
Server:          192.168.100.1
Address:         192.168.100.1#53

Non-authoritative answer:
www.mit.edu      canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:           e9566.dscb.akamaiedge.net
Address: 23.56.203.58

[eva@Evas-MacBook-Pro ~ % nslookup www.aiit.or.kr dns.google
Server:          dns.google
Address:         8.8.8.8#53

Non-authoritative answer:
Name:           www.aiit.or.kr
Address: 58.229.6.225

eva@Evas-MacBook-Pro ~ %
```