

# Home work 4

A.

- 

```
intersection@i108588154:~$ nslookup z.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   z.com
Address: 163.44.130.37
```

- 

```
intersection@i108588154:~$ nslookup -type=NS ethz.ch
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
ethz.ch nameserver = ns1.ethz.ch.
ethz.ch nameserver = ns2.ethz.ch.

Authoritative answers can be found from:
```

- 

```
intersection@i108588154:~$ nslookup www.ox.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.ox.ac.uk
Address: 151.101.194.216
Name:   www.ox.ac.uk
Address: 151.101.66.216
Name:   www.ox.ac.uk
Address: 151.101.130.216
Name:   www.ox.ac.uk
Address: 151.101.2.216
```

Один:

```
intersection@i108588154:~$ nslookup spbu.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   spbu.ru
Address: 178.177.3.9
```

Б.

- Protocol: UDP (17)

66 1.674737337 192.168.1.4 192.168.1.1 DNS 72 Standard query response 0xfa8a A www.ietf.org

67 1.697826026 192.168.1.1 192.168.1.4 DNS 149 Standard query response 0xfa8a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99

173 1.897812941 192.168.1.4 192.168.1.1 DNS 78 Standard query 0x210d A analytics.ietf.org

277 2.237872819 192.168.1.1 192.168.1.4 DNS 94 Standard query response 0x210d A analytics.ietf.org A 4.31.198.45

354 3.045351977 192.168.1.4 192.168.1.1 DNS 81 Standard query 0xcb98 AAAA salt.baldr.yandex.net

371 3.054225610 192.168.1.1 192.168.1.4 DNS 109 Standard query response 0xcb98 AAAA salt.baldr.yandex.net AAAA 2a02:6b8:c01:d22:0:460a:0:b501

55 1.222123652 192.168.1.4 213.180.193.2 HTTP 403 GET /generate\_204 HTTP/1.1

57 1.253378886 213.180.193.2 192.168.1.4 HTTP 219 HTTP/1.1 204 No content

2 0.000020046 192.168.1.4 77.88.6.67 ICMP 166 Destination unreachable (Port unreachable)

51 1.077054122 192.168.1.4 77.88.6.67 ICMP 166 Destination unreachable (Port unreachable)

178 1.913879377 192.168.1.4 77.88.6.67 ICMP 166 Destination unreachable (Port unreachable)

402 2.514459950 192.168.1.4 77.88.6.67 ICMP 223 Destination unreachable (Port unreachable)

46 0.987446623 149.154.167.41 192.168.1.4 SSL 171 Continuation Data

407 3.660499626 4.31.198.45 192.168.1.4 SSLv2 5666 Encrypted Data, Continuation Data

6 0.194715436 213.180.193.24 192.168.1.4 TCP 66 443 → 55922 [ACK] Seq=1 Ack=2152 Win=1307 Len=0 TSval=317237133 TSecr=2519303952

7 0.199391681 213.180.193.24 192.168.1.4 TCP 1416 443 → 55922 [ACK] Seq=1 Ack=2292 Win=1307 Len=1350 TSval=317237141 TSecr=2519303958 [TCP segment of a reassembled PDU]

8 0.199418705 192.168.1.4 213.180.193.24 TCP 66 55922 → 443 [ACK] Seq=2292 Ack=1351 Win=493 Len=0 TSval=2519303986 TSecr=317237141

10 0.204769547 192.168.1.4 213.180.193.24 TCP 66 55922 → 443 [ACK] Seq=2292 Ack=2199 Win=493 Len=0 TSval=2519303992 TSecr=317237141

15 0.323066199 192.168.1.4 104.208.16.88 TCP 74 52458 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 TSval=1833059426 TSecr=0 WS=128

17 0.511862913 104.208.16.88 192.168.1.4 TCP 66 443 → 52458 [ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256 SACK\_PERM=1

▶ Frame 66: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface wlo1, id 0

▶ Ethernet II, Src: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89), Dst: Netgear\_0a:c2:48 (c4:04:15:0a:c2:48)

▼ Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1

0100 .... = Version: 4

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

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

Total Length: 58

Identification: 0xc85 (31877)

▶ Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0x3ad8 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.4

Destination: 192.168.1.1

▼ User Datagram Protocol, Src Port: 47978, Dst Port: 53

Source Port: 47978

Destination Port: 53

Length: 38

Checksum: 0x838d [unverified]

[Checksum Status: Unverified]

[Stream index: 4]

▶ [Timestamps]

▶ Domain Name System (query)

- Destination Port: 53
- Destination: 192.168.1.1, совпадает
- www.ietf.org: type A, class IN, ответов не видно

66	1.674737337	192.168.1.4	192.168.1.1	DNS	72	Standard query 0xfa0a A www.ietf.org
67	1.697826026	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0xfa0a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
173	1.897812941	192.168.1.4	192.168.1.1	DNS	78	Standard query 0x210d A analytics.ietf.org
277	2.237872819	192.168.1.1	192.168.1.4	DNS	94	Standard query response 0x210d A analytics.ietf.org A 4.31.198.45
354	3.045351977	192.168.1.4	192.168.1.1	DNS	81	Standard query 0xcb98 AAAA salt.baldr.yandex.net
371	3.054225610	192.168.1.1	192.168.1.4	DNS	109	Standard query response 0xcb98 AAAA salt.baldr.yandex.net AAAA 2a02:6b8:c01:d22:0:460a:0:b501
55	1.222123652	192.168.1.4	213.180.193.2...	HTTP	403	GET /generate_204 HTTP/1.1
57	1.253378886	213.180.193.2...	192.168.1.4	HTTP	219	HTTP/1.1 204 No content
2	0.000020046	192.168.1.4	77.88.6.67	ICMP	166	Destination unreachable (Port unreachable)
51	1.077054122	192.168.1.4	77.88.6.67	ICMP	166	Destination unreachable (Port unreachable)
178	1.913979377	192.168.1.4	77.88.6.67	ICMP	166	Destination unreachable (Port unreachable)
402	3.514455950	192.168.1.4	77.88.6.67	ICMP	223	Destination unreachable (Port unreachable)
46	0.987446623	149.154.167.41	192.168.1.4	SSL	171	Continuation Data
407	3.660499626	4.31.198.45	192.168.1.4	SSLv2	5666	Encrypted Data, Continuation Data
6	0.194715436	213.180.193.24	192.168.1.4	TCP	66	443 → 55922 [ACK] Seq=1 Ack=2152 Win=1307 Len=0 TSval=317237133 TSecr=2519303952
7	0.199391681	213.180.193.24	192.168.1.4	TCP	1416	443 → 55922 [ACK] Seq=1 Ack=2292 Win=1307 Len=1350 TSval=317237141 TSecr=2519303958 [TCP segment of a reassembled PDU]
8	0.199418705	192.168.1.4	213.180.193.24	TCP	66	55922 → 443 [ACK] Seq=2292 Ack=1351 Win=493 Len=0 TSval=2519303986 TSecr=317237141
10	0.204769547	192.168.1.4	213.180.193.24	TCP	66	55922 → 443 [ACK] Seq=2292 Ack=2199 Win=493 Len=0 TSval=2519303992 TSecr=317237141
15	0.323066199	192.168.1.4	104.208.16.88	TCP	74	52458 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1833059426 TSecr=0 WS=128
17	0.511862913	104.208.16.88	192.168.1.4	TCP	66	443 → 52458 [SYN. ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM=1
Total Length: 58						
Identification: 0x7c85 (31877)						
Flags: 0x4000, Don't fragment						
Fragment offset: 0						
Time to live: 64						
Protocol: UDP (17)						
Header checksum: 0x3ad8 [validation disabled]						
[Header checksum status: Unverified]						
Source: 192.168.1.4						
Destination: 192.168.1.1						
User Datagram Protocol, Src Port: 47978, Dst Port: 53						
Source Port: 47978						
Destination Port: 53						
Length: 38						
Checksum: 0x838d [unverified]						
[Checksum Status: Unverified]						
[Stream index: 4]						
[Timestamps]						
Domain Name System (query)						
Transaction ID: 0xfa0a						
Flags: 0x0100 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 0						
Queries						
www.ietf.org: type A, class IN						
[Response In: 67]						

- три ответа, в каждом — домен, тип, класс и в зависимости от типа либо еще домен, либо адрес

66	1.674737337	192.168.1.4	192.168.1.1	DNS	72	Standard query 0xfa0a A www.ietf.org
67	1.697826026	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0xfa0a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
173	1.897812941	192.168.1.4	192.168.1.1	DNS	78	Standard query 0x210d A analytics.ietf.org
277	2.237872819	192.168.1.1	192.168.1.4	DNS	94	Standard query response 0x210d A analytics.ietf.org A 4.31.198.45
354	3.045351977	192.168.1.4	192.168.1.1	DNS	81	Standard query 0xcb98 AAAA salt.baldr.yandex.net
371	3.054225610	192.168.1.1	192.168.1.4	DNS	109	Standard query response 0xcb98 AAAA salt.baldr.yandex.net AAAA 2a02:6b8:c01:d22:0:460a:0:b501
55	1.222123652	192.168.1.4	213.180.193.2...	HTTP	403	GET /generate_204 HTTP/1.1
57	1.253378886	213.180.193.2...	192.168.1.4	HTTP	219	HTTP/1.1 204 No content
2	0.000020046	192.168.1.4	77.88.6.67	ICMP	166	Destination unreachable (Port unreachable)
51	1.077054122	192.168.1.4	77.88.6.67	ICMP	166	Destination unreachable (Port unreachable)
178	1.913979377	192.168.1.4	77.88.6.67	ICMP	166	Destination unreachable (Port unreachable)
402	3.514455950	192.168.1.4	77.88.6.67	ICMP	223	Destination unreachable (Port unreachable)
46	0.987446623	149.154.167.41	192.168.1.4	SSL	171	Continuation Data
407	3.660499626	4.31.198.45	192.168.1.4	SSLv2	5666	Encrypted Data, Continuation Data
6	0.194715436	213.180.193.24	192.168.1.4	TCP	66	443 → 55922 [ACK] Seq=1 Ack=2152 Win=1307 Len=0 TSval=317237133 TSecr=2519303952
7	0.199391681	213.180.193.24	192.168.1.4	TCP	1416	443 → 55922 [ACK] Seq=1 Ack=2292 Win=1307 Len=1350 TSval=317237141 TSecr=2519303958 [TCP segment of a reassembled PDU]
8	0.199418705	192.168.1.4	213.180.193.24	TCP	66	55922 → 443 [ACK] Seq=2292 Ack=1351 Win=493 Len=0 TSval=2519303986 TSecr=317237141
10	0.204769547	192.168.1.4	213.180.193.24	TCP	66	55922 → 443 [ACK] Seq=2292 Ack=2199 Win=493 Len=0 TSval=2519303992 TSecr=317237141
15	0.323066199	192.168.1.4	104.208.16.88	TCP	74	52458 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1833059426 TSecr=0 WS=128
17	0.511862913	104.208.16.88	192.168.1.4	TCP	66	443 → 52458 [SYN. ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM=1
Protocol: UDP (17)						
Header checksum: 0xb710 [validation disabled]						
[Header checksum status: Unverified]						
Source: 192.168.1.1						
Destination: 192.168.1.4						
User Datagram Protocol, Src Port: 53, Dst Port: 47978						
Source Port: 53						
Destination Port: 47978						
Length: 115						
Checksum: 0x4db2 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 4]						
[Timestamps]						
Domain Name System (response)						
Transaction ID: 0xfa0a						
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 104.16.45.99						
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99						
[Request In: 66]						
[Time: 0.023088689 seconds]						

- Да, соответствует

66	1.674737337	192.168.1.4	192.168.1.1	DNS	72	Standard query 0xfa0a A www.ietf.org
67	1.697826026	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0xfa0a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
68	1.698424318	192.168.1.4	104.16.44.99	TCP	74	51490 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1177109088 TSecr=0 WS=128

- Единственное, что видно — доп запрос в analytics.ietf.org, но я не нашел прямой связи этого с изображениями.

## В.

- Destination Port: 53

4 0.795144721 192.168.1.1 192.168.1.1 DNS 67 Standard query 0x735a AAAA spbu.ru

5 0.799642599 192.168.1.1 192.168.1.4 DNS 129 Standard query response 0x735a AAAA spbu.ru SOA ns.pu.ru

6 0.845676526 213.180.193.24 192.168.1.4 TLSv1.2 97 Encrypted Alert

7 0.845706570 192.168.1.4 213.180.193.24 TCP 66 56708 - 443 [ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=2521553036 TSecr=3851010990

8 0.847236947 213.180.193.24 192.168.1.4 TCP 66 443 - 56708 [FIN, ACK] Seq=32 Ack=1 Win=587 Len=0 TSval=3851010990 TSecr=2521548036

9 0.887959230 192.168.1.4 213.180.193.24 TCP 66 56708 - 443 [ACK] Seq=1 Ack=33 Win=501 Len=0 TSval=2521553079 TSecr=3851010990

10 1.560167867 192.168.1.4 3.68.18.70 TLSv1.2 120 Application Data

11 1.611998121 3.68.18.70 192.168.1.4 TCP 66 443 - 59690 [ACK] Seq=1 Ack=55 Win=8 Len=0 TSval=485776341 TSecr=1335416640

12 1.612716143 3.68.18.70 192.168.1.4 TLSv1.2 122 Application Data

13 1.612741336 192.168.1.4 3.68.18.70 TCP 66 59690 - 443 [ACK] Seq=55 Ack=57 Win=501 Len=0 TSval=1335416693 TSecr=485776342

14 1.763697770 192.168.1.1 213.180.193.24 TCP 66 56708 - 443 [RST, ACK] Seq=1 Ack=33 Win=501 Len=0 TSval=2521553954 TSecr=3851010990

15 1.763303900 192.168.1.4 213.180.193.24 TCP 74 56710 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 TSval=2521553954 TSecr=0 WS=128

16 1.763561732 192.168.1.4 185.5.137.248 TLSv1.2 210 Application Data

17 1.763656017 192.168.1.4 185.5.137.248 TLSv1.2 1510 Application Data, Application Data

Frame 4: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface wlo1, id 0

Ethernet II, Src: 64:6e:c0:e0:a2:6f:89 (64:6e:c0:e0:a2:6f:89), Dst: Netgear\_0a:c2:48 (c4:04:15:0a:c2:48)

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1

0100 .... = Version: 4

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

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

Total Length: 53

Identification: 0x7a21 (31265)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0x3d41 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.4

Destination: 192.168.1.1

User Datagram Protocol, Src Port: 33208, Dst Port: 53

Source Port: 33208

Destination Port: 53

Length: 33

Checksum: 0x8388 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Timestamps]

Domain Name System (query)

Transaction ID: 0x735a

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

0000 c4 04 15 0a c2 48 64 6e e0 a2 6f 89 08 00 45 00 .....Hdn...o...E

0010 00 35 7a 21 40 00 40 11 3d 41 c0 a8 01 04 c0 a8 5210@=A.....

0020 01 01 01 b8 00 00 00 21 83 88 73 5a 01 00 00 01 .....s!...sZ....

0030 00 00 00 00 00 00 04 73 70 62 75 02 72 75 00 00 .....s pbu.ru...

0040 1c 00 01 .....

- Destination: 192.168.1.1, совпадает
- spbu.ru: type AAAA, class IN, ответов не видно

4 0.795144721 192.168.1.4 192.168.1.1 DNS 67 Standard query 0x735a AAAA spbu.ru

5 0.799642599 192.168.1.1 192.168.1.4 DNS 129 Standard query response 0x735a AAAA spbu.ru SOA ns.pu.ru

6 0.845676526 213.180.193.24 192.168.1.4 TLSv1.2 97 Encrypted Alert

7 0.845706570 192.168.1.4 213.180.193.24 TCP 66 56708 - 443 [ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=2521553036 TSecr=3851010990

8 0.847236947 213.180.193.24 192.168.1.4 TCP 66 443 - 56708 [FIN, ACK] Seq=32 Ack=1 Win=587 Len=0 TSval=3851010990 TSecr=2521548036

9 0.887959230 192.168.1.4 213.180.193.24 TCP 66 56708 - 443 [ACK] Seq=1 Ack=33 Win=501 Len=0 TSval=2521553079 TSecr=3851010990

10 1.560167867 192.168.1.4 3.68.18.70 TLSv1.2 120 Application Data

11 1.611998121 3.68.18.70 192.168.1.4 TCP 66 443 - 59690 [ACK] Seq=1 Ack=55 Win=8 Len=0 TSval=485776341 TSecr=1335416640

12 1.612716143 3.68.18.70 192.168.1.4 TLSv1.2 122 Application Data

13 1.612741336 192.168.1.4 3.68.18.70 TCP 66 59690 - 443 [ACK] Seq=55 Ack=57 Win=501 Len=0 TSval=1335416693 TSecr=485776342

14 1.763697770 192.168.1.1 213.180.193.24 TCP 66 56708 - 443 [RST, ACK] Seq=1 Ack=33 Win=501 Len=0 TSval=2521553954 TSecr=3851010990

15 1.763303900 192.168.1.4 213.180.193.24 TCP 74 56710 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 TSval=2521553954 TSecr=0 WS=128

16 1.763561732 192.168.1.4 185.5.137.248 TLSv1.2 210 Application Data

17 1.763656017 192.168.1.4 185.5.137.248 TLSv1.2 1510 Application Data, Application Data

Total Length: 53

Identification: 0x7a21 (31265)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0x3d41 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.4

Destination: 192.168.1.1

User Datagram Protocol, Src Port: 33208, Dst Port: 53

Source Port: 33208

Destination Port: 53

Length: 33

Checksum: 0x8388 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Timestamps]

Domain Name System (query)

Transaction ID: 0x735a

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

spbu.ru: type AAAA, class IN

Response In: 5

0000 c4 04 15 0a c2 48 64 6e e0 a2 6f 89 08 00 45 00 .....Hdn...o...E

0010 00 35 7a 21 40 00 40 11 3d 41 c0 a8 01 04 c0 a8 5210@=A.....

- в последней паре запросов DNS нет ответов:

4 0.795144721 192.168.1.4 192.168.1.1 DNS 67 Standard query 0x735a AAAA spbu.ru

5 0.799642599 192.168.1.1 192.168.1.4 DNS 129 Standard query response 0x735a AAAA spbu.ru SOA ns.pu.ru

6 0.845676526 213.180.193.24 192.168.1.4 TLSv1.2 97 Encrypted Alert

7 0.845706570 192.168.1.4 213.180.193.24 TCP 66 56708 - 443 [ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=2521553036 TSecr=3851010990

8 0.847236947 213.180.193.24 192.168.1.4 TCP 66 443 - 56708 [FIN, ACK] Seq=32 Ack=1 Win=587 Len=0 TSval=3851010990 TSecr=2521548036

9 0.887959230 192.168.1.4 213.180.193.24 TCP 66 56708 - 443 [ACK] Seq=1 Ack=33 Win=501 Len=0 TSval=2521553079 TSecr=3851010990

10 1.560167867 192.168.1.4 3.68.18.70 TLSv1.2 120 Application Data

11 1.611998121 3.68.18.70 192.168.1.4 TCP 66 443 - 59690 [ACK] Seq=1 Ack=55 Win=8 Len=0 TSval=485776341 TSecr=1335416640

12 1.612716143 3.68.18.70 192.168.1.4 TLSv1.2 122 Application Data

13 1.612741336 192.168.1.4 3.68.18.70 TCP 66 59690 - 443 [ACK] Seq=55 Ack=57 Win=501 Len=0 TSval=1335416693 TSecr=485776342

14 1.763697770 192.168.1.1 213.180.193.24 TCP 66 56708 - 443 [RST, ACK] Seq=1 Ack=33 Win=501 Len=0 TSval=2521553954 TSecr=3851010990

15 1.763303900 192.168.1.4 213.180.193.24 TCP 74 56710 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 TSval=2521553954 TSecr=0 WS=128

16 1.763561732 192.168.1.4 185.5.137.248 TLSv1.2 210 Application Data

17 1.763656017 192.168.1.4 185.5.137.248 TLSv1.2 1510 Application Data, Application Data

Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0xb72d [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.1

Destination: 192.168.1.4

User Datagram Protocol, Src Port: 53, Dst Port: 33208

Source Port: 53

Destination Port: 33208

Length: 86

Checksum: 0x6c37 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Timestamps]

Domain Name System (response)

Transaction ID: 0x735a

Flags: 0x0180 Standard query response, No error

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 0

Queries

spbu.ru: type AAAA, class IN

Authoritative nameservers

spbu.ru: type SOA, class IN, mname ns.pu.ru

Request In: 4

[Time: 0.004497788 seconds]

0000 64 6e c0 e0 a2 6f 89 08 00 45 00 .....Hdn...o...E



17.763656017 192.168.1.4 185.5.137.248 TLSv1.2 1510 Application Data, Application Data
7/1 Standard query xea9a A www.spbu.ru 82.282.190.112

3	0.785095293	192.168.1.4	192.168.1.4	UNS	7/1 Standard query xea9a A www.spbu.ru
4	0.795144721	192.168.1.4	192.168.1.4	DNS	161 Standard query response 0xa9a A www.spbu.ru CNAME spbu.ru A 82.282.190.112
5	0.798425569	192.168.1.1	192.168.1.4	DNS	67 Standard query 0x735a AAAA spbu.ru
6	0.845676526	212.180.193.24	192.168.1.4	TLSv1.2	129 Standard query response 0x735a AAAA spbu.ru SOA ns.pu.ru
7	0.845706570	192.168.1.4	212.180.193.24	TCP	97 Encrypted Alert
8	0.847236947	212.180.193.24	192.168.1.4	TCP	66 56708 → 443 [ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=2521553036 TSecr=3851010990
9	0.887059239	192.168.1.4	212.180.193.24	TCP	66 443 → 56708 [FIN, ACK] Seq=32 Ack=1 Win=587 Len=0 TSval=3851010990 TSecr=2521548036
10	1.580167867	192.168.1.4	3.68.18.70	TLSv1.2	66 56708 → 443 [ACK] Seq=1 Ack=33 Win=501 Len=0 TSval=2521553079 TSecr=3851010990
11	1.611998121	3.68.18.70	192.168.1.4	TCP	129 Application Data
12	1.612716143	3.68.18.70	192.168.1.4	TLSv1.2	66 443 → 59690 [ACK] Seq=1 Ack=55 Win=0 Len=0 TSval=485776341 TSecr=1335416640
13	1.612741336	192.168.1.4	3.68.18.70	TCP	122 Application Data
14	1.630377770	212.180.193.24	192.168.1.4	TCP	66 59690 → 443 [ACK] Seq=55 Ack=57 Win=501 Len=0 TSval=1335416693 TSecr=485776342
15	1.633039900	192.168.1.4	212.180.193.24	TCP	66 59690 → 443 [SYN, ACK] Seq=0 Win=64240 Len=0 TSval=2521553954 TSecr=3851010990
16	1.763561732	192.168.1.4	185.5.137.248	TLSv1.2	74 56710 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2521553954 TSecr=0 WS=128
17	1.763656017	192.168.1.4	185.5.137.248	TLSv1.2	210 Application Data

Time to live: 64  
Protocol: UDP (17)  
Header checksum: 0xb740 [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.168.1.1  
Destination: 192.168.1.4
▼ User Datagram Protocol, Src Port: 53, Dst Port: 42379

Source Port: 53  
Destination Port: 42379  
Length: 67  
Checksum: 0x068f [unverified]  
[Checksum status: Unverified]  
[Stream index: 0]  
[Timestamps]
▼ Domain Name System (response)  
Transaction ID: 0xea9a  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 2  
Authority RRs: 0  
Additional RRs: 0

▼ Queries  
www.spbu.ru: type A, class IN
▼ Answers  
www.spbu.ru: type CNAME, class IN, cname spbu.ru  
spbu.ru: type A, class IN, addr 82.282.190.112  
[Request ID: 2]  
[Time: 0.009495331 seconds]

0000 64 6e 00 a2 6f 89 c4 04 15 0a c2 48 08 00 45 00 dn--o--H-E

0010 00 57 00 00 40 00 40 11 b7 40 c0 a8 01 01 c0 a8 W--@-@-@-@-

0020 01 04 00 35 a5 80 00 43 06 8f ea 9a 81 00 00 01 ...5--C

0030 00 02 00 00 00 00 33 77 77 05 73 03 03 05 02 ...w www.spbu

0040 00 00 00 00 00 00 01 c0 ac 00 05 00 01 00 00 00 00 ...

0050 81 00 02 c0 10 c0 10 00 01 00 01 00 00 0d 92 00 ...

0060 04 52 ca be 70 -R--p

Packets: 17 · Displayed: 17 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

Г.

Нет DNS запросов

**Задания В, но теперь для команды:**

```
nslookup -type=NS spbu.ru
server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
spbu.ru nameserver = ns2.pu.ru.
spbu.ru nameserver = ns.pu.ru.
spbu.ru nameserver = ns7.spbu.ru.

Authoritative answers can be found from:

nslookup -type=NS spbu.ru
server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
spbu.ru nameserver = ns2.pu.ru.
spbu.ru nameserver = ns.pu.ru.
spbu.ru nameserver = ns7.spbu.ru.

Authoritative answers can be found from:
```

Д

- Destination: 195.70.196.210, не совпадает, ns2.pu.ru

```
intersection@i108588154:~$ nslookup ns2.pu.ru
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   ns2.pu.ru
Address: 195.70.196.210
```

- Отвечаю сразу на два вопроса последующих: всё как в пункте В, в последней паре ничего интересного, а вот в предпоследней интереснее

ip.addr == 192.168.1.4						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.4	192.168.1.1	DNS	69	Standard query 0xb196 AAAA ns2.pu.ru
2	0.006755053	192.168.1.1	192.168.1.4	DNS	69	Standard query response 0xb196 AAAA ns2.pu.ru
3	0.008244669	192.168.1.4	195.70.196.210	DNS	71	Standard query 0x9c62 A www.spbu.ru
4	0.022100926	195.70.196.210	192.168.1.4	DNS	285	Standard query response 0x9c62 A www.spbu.ru CNAME spbu.ru A 82.202.190.112 NS ns2.pu.ru NS ns.pu.ru NS ns7.spbu.ru A 195.70.196.210 A 185...
5	0.022890711	192.168.1.4	195.70.196.210	DNS	67	Standard query 0x0040 AAAA spbu.ru
6	0.031166699	195.70.196.210	192.168.1.4	DNS	120	Standard query response 0x0040 AAAA spbu.ru SOA ns.pu.ru

Domain Name System (response)

Transaction ID: 0x9c62

Flags: 0x8500 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 3

Additional RRs: 3

Queries

www.spbu.ru: type A, class IN

Answers

www.spbu.ru: type CNAME, class IN, cname spbu.ru

spbu.ru: type A, class IN, addr 82.202.190.112

Authoritative nameservers

spbu.ru: type NS, class IN, ns ns2.pu.ru

spbu.ru: type NS, class IN, ns ns.pu.ru

spbu.ru: type NS, class IN, ns ns7.spbu.ru

Additional records

ns.pu.ru: type A, class IN, addr 195.70.196.210

ns2.pu.ru: type A, class IN, addr 195.70.196.210

ns7.spbu.ru: type A, class IN, addr 185.44.15.195

Request in: 31

Time: 0.013946257 seconds

0030 00 02 00 03 00 03 03 77 77 77 04 73 70 62 75 02 .....w ww.spbu-  
0040 72 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 0e ru.....  
0050 10 00 02 c0 10 c0 10 00 01 00 01 00 00 0e 10 00 .....  
0060 04 52 ca be 70 c0 10 00 02 00 01 00 00 0e 10 00 -R-p-.....  
0070 09 03 6e 73 32 02 70 75 c0 15 c0 10 00 02 00 01 --ns2-pu.....  
0080 00 00 0e 10 00 05 02 0e 73 c0 4b c0 10 00 02 00 .....n s-K.....  
0090 01 00 00 0e 10 00 06 03 0e 73 37 c0 10 c0 5c 00 .....ns7.....  
00a0 01 00 01 00 00 0e 4c 00 04 c3 46 c4 db c0 47 00 .....L--F---G-

Number of additional records in packet (dns.count.add\_rr), 2 bytesPackets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%)Profile: Default

E.

- WHOIS – это база данных, в которой хранятся сведения о доменах. В ней можно найти следующую информацию:
  - контактные данные регистранта, администратора и технических специалистов;
  - сведения о спонсирующем регистраторе;
  - дату создания и обновления домена, а также срок его регистрации;
  - DNS-серверы и статус домена.
- [ns1.vkontakte.ru](#), [ns2.vkontakte.ru](#); использовал [2domains.ru/whois](#)

```
intersection@i108588154:~$ nslookup 192.168.1.1
1.1.168.192.in-addr.arpa          name = _gateway.

Authoritative answers can be found from:

intersection@i108588154:~$ nslookup ns1.vkontakte.ru
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   ns1.vkontakte.ru
Address: 87.240.131.131
Name:   ns1.vkontakte.ru
Address: 2a00:bdc0:ff:1::2

intersection@i108588154:~$ nslookup ns2.vkontakte.ru
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   ns2.vkontakte.ru
Address: 95.213.21.21
Name:   ns2.vkontakte.ru
Address: 2a00:bdc0:ff:2::2
```

•