



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»**  
**КАФЕДРА ММСА**

**Практична робота № 3**  
**З курсу: «Комп'ютерні мережі»**

**Виконала:**  
**Студентка III курсу**  
**Групи КА-73**  
**Колесник М.М.**  
**Прийняв: Кухарев С.О.**

**Київ 2020**

### 3.2.1

No. Time Source Destination Protocol Length Info  
60 20.589855 192.168.0.106 192.168.0.1 DNS 72 Standard

query 0x5ee0 A www.ietf.org  
Frame 60: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0

Ethernet II, Src: Apple\_78:53:31 (f0:18:98:78:53:31), Internet Protocol Version 4, Src: 192.168.0.106,  
Dst: User Datagram Protocol, Src Port: 52943, Dst Port: 53 Domain Name System (query)

Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) 192.168.0.1

No.

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries

www.ietf.org: type A, class IN Name: www.ietf.org  
[Name Length: 12]  
[Label Count: 3]

Type: A (Host Address) (1)  
Class: IN (0x0001)  
[Response In: 62]

Time Source  
61 21.593510 192.168.0.106

Destination 192.168.0.1

Protocol Length Info  
DNS 72 Standard  
Transaction ID: 0x5ee0  
Flags: 0x0100 Standard query

0... ..000 0... ..0. ....1 .... ..

.... = Response: Message is a query  
.... = Opcode: Standard query (0)  
.... = Truncated: Message is not truncated .... = Recursion desired: Do query recursively .0. ....  
= Z: reserved (0)  
...0 .... = Non-authenticated data: Unacceptable

query 0x5ee0 A www.ietf.org  
Frame 61: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0

Ethernet II, Src: Apple\_78:53:31 (f0:18:98:78:53:31), Internet Protocol Version 4, Src: 192.168.0.106,  
Dst: User Datagram Protocol, Src Port: 52943, Dst Port: 53 Domain Name System (query)

Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) 192.168.0.1

No.

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries

www.ietf.org: type A, class IN Name: www.ietf.org  
[Name Length: 12]  
[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)  
[Retransmitted request. Original request in: 60] [Retransmission: True]

Time Source Destination 62 21.670330 192.168.0.1 192.168.0.106

Protocol Length Info  
Transaction ID: 0x5ee0  
Flags: 0x0100 Standard query

0... .... .000 0... .... ..0. .... ...1 .... .... ....

.... .... = Response: Message is a query  
.... .... = Opcode: Standard query (0)  
.... .... = Truncated: Message is not truncated .... .... = Recursion desired: Do query recursively .0.. ....  
= Z: reserved (0)  
...0 .... = Non-authenticated data: Unacceptable

DNS 459 Standard query response 0x5ee0 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A  
104.20.0.85 A

104.20.1.85 NS ns1.cloudflare.net NS ns4.cloudflare.net NS ns2.cloudflare.net NS ns3.cloudflare.net  
NS ns5.cloudflare.net A 173.245.59.31 AAAA 2400:cb00:2049:1::adf5:3b1f A 198.41.222.131 AAAA  
2400:cb00:2049:1::c629:de83 A 198.41.222.31 AAAA 2400:cb00:2049:1::c629:de1f A  
198.41.223.131 AAAA 2400:cb00:2049:1::c629:df83 A 198.41.223.31 AAAA  
2400:cb00:2049:1::c629:df1f  
Frame 62: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface en0, id 0  
Ethernet II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31)

/Users/mariia/Desktop/dump1.pcapng 6667 total packets, 7 shown

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106 User Datagram Protocol, Src Port:  
53, Dst Port: 52943  
Domain Name System (response)

Transaction ID: 0x5ee0  
Flags: 0x8180 Standard query response, No error

1... .... .... .000 0... .... .... .0.. .... .... .0. .... .... .... 1... .... .... 1... .... .... .0.. .... ....  
..0. ....

authenticated by the server .... .... ..0 ....

= Response: Message is a response  
= Opcode: Standard query (0)  
= Authoritative: Server is not an authority for domain

= Truncated: Message is not truncated  
= Recursion desired: Do query recursively  
= Recursion available: Server can do recursive queries  
= Z: reserved (0)  
= Answer authenticated: Answer/authority portion was not  
  
= Non-authenticated data: Unacceptable = Reply code: No error (0)

.... .... 0000 Questions: 1

Answer RRs: 3  
Authority RRs: 5  
Additional RRs: 10  
Queries

www.ietf.org: type A, class IN Name: www.ietf.org  
[Name Length: 12]  
[Label Count: 3]

Type: A (Host Address) (1)  
Class: IN (0x0001)  
Answers

Authoritative nameservers Additional records [Request In: 60]  
[Time: 1.080475000

Ethernet II, Src: Apple\_78:53:31 (f0:18:98:78:53:31), Internet Protocol Version 4, Src: 192.168.0.106,  
Dst: User Datagram Protocol, Src Port: 55217, Dst Port: 53 Domain Name System (query)

No.

seconds]  
Source  
192.168.0.106 192.168.0.1 DNS 78 Standard

Destination  
Frame 346: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0

Time  
346 22.780675

Protocol Length Info

query 0xc3f6 A analytics.ietf.org

No.

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries

analytics.ietf.org: type A, class IN Name: analytics.ietf.org  
[Name Length: 18]  
[Label Count: 3]

Type: A (Host Address) (1)  
Class: IN (0x0001)  
[Response In: 545]

Time Source  
545 23.016499 192.168.0.1

Destination

Protocol Length Info  
Transaction ID: 0xc3f6  
Flags: 0x0100 Standard query

0... .. .000 0... .. .0. .... 1 ... .. .

.... .. = Response: Message is a query  
.... .. = Opcode: Standard query (0)  
.... .. = Truncated: Message is not truncated .... .. = Recursion desired: Do query recursively .0.. ....  
= Z: reserved (0)  
...0 .... = Non-authenticated data: Unacceptable

192.168.0.106  
query response 0xc3f6 A analytics.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.ams1.afili-

nst.info NS ns1.mia1.afiliast-nst.info NS ns0.amsl.com NS ns1.yyz1.afiliast-nst.info NS  
ns1.sea1.afiliast-nst.info NS ns1.hkg1.afiliast-nst.info A 4.31.198.40 AAAA 2001:1900:3001:11::28 A  
65.22.6.79 AAAA 2001:500:6::79 A 65.22.6.1 AAAA 2a01:8840:6::1 A 65.22.7.1 AAAA  
2a01:8840:7::1 A 65.22.8.1 AAAA 2a01:8840:8::1 A 65.22.9.1 AAAA 2a01:8840:9::1

Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) 192.168.0.1

DNS 529 Standard

/Users/mariia/Desktop/dump1.pcapng 6667 total packets, 7 shown

Frame 545: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface en0, id 0  
Ethernet II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31)  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106  
User Datagram Protocol, Src Port: 53, Dst Port: 55217

Domain Name System (response)  
Transaction ID: 0xc3f6  
Flags: 0x8180 Standard query response, No error

1... .. .000 0... .. .0. .... .0. .... .... 1 ... .. . 1... .. . .0. .... ....  
..0. ....

authenticated by the server

- .... ..0 ....
- .... .. 0000 Questions: 1
- Answer RRs: 2
- Authority RRs: 6
- Additional RRs: 12
- Queries

analytics.ietf.org:  
Name: analytics.ietf.org [Name Length: 18]  
[Label Count: 3]  
Type: A (Host Address) (1) Class: IN (0x0001)

Answers  
Authoritative nameservers Additional records [Request In: 346]  
[Time: 0.235824000

= Response: Message is a response  
= Opcode: Standard query (0)  
= Authoritative: Server is not an authority for domain  
= Truncated: Message is not truncated  
= Recursion desired: Do query recursively  
= Recursion available: Server can do recursive queries  
= Z: reserved (0)  
= Answer authenticated: Answer/authority portion was not  
  
= Non-authenticated data: Unacceptable = Reply code: No error (0)

type A, class IN

seconds]  
Source  
192.168.0.106 192.168.0.1 DNS 96 Standard

Protocol Length Info  
Frame 3167: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface en0, id 0

No. Time 3167 25.322207

Destination

query 0x40ba A ss-prod-ew1-notif-26.aws.adobess.com

Ethernet II, Src: Apple\_78:53:31 (f0:18:98:78:53:31), Internet Protocol Version 4, Src: 192.168.0.106,  
Dst: User Datagram Protocol, Src Port: 61123, Dst Port: 53 Domain Name System (query)

Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) 192.168.0.1

No.

Type: A (Host Address) (1)  
Class: IN (0x0001)  
[Response In: 3169]

Time Source 3169 25.331050 192.168.0.1

Destination

Protocol Length Info  
Transaction ID: 0x40ba  
Flags: 0x0100 Standard query

0... ..000 0... ..0. ....1 .... .....

.... .... = Response: Message is a query  
.... .... = Opcode: Standard query (0)  
.... .... = Truncated: Message is not truncated .... .... = Recursion desired: Do query recursively .0.. ....  
= Z: reserved (0)  
...0 .... = Non-authenticated data: Unacceptable

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries

ss-prod-ew1-notif-26.aws.adobess.com: type A, class IN Name: ss-prod-ew1-notif-  
26.aws.adobess.com  
[Name Length: 36]  
[Label Count: 4]

192.168.0.106  
query response 0x40ba A ss-prod-ew1-notif-26.aws.adobess.com A 52.31.117.171 A 18.202.149.73  
A

18.203.76.53 NS ns-1000.awsdns-61.net NS ns-1676.awsdns-17.co.uk NS ns-445.awsdns-55.com  
NS ns-1326.awsdns-37.org A 205.251.193.189 A 205.251.195.232

DNS 314 Standard

/Users/mariia/Desktop/dump1.pcapng 6667 total packets, 7 shown

Frame 3169: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface en0, id 0  
Ethernet II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31)  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106  
User Datagram Protocol, Src Port: 53, Dst Port: 61123

Domain Name System (response)  
Transaction ID: 0x40ba  
Flags: 0x8180 Standard query response, No error

1... .... .000 0... .... .0.. .... .0. .... ...1 ... 1... .... .0.. ....  
..0. ....

authenticated by the server .... ...0 ....

.... .... 0000 Questions: 1

Answer RRs: 3  
Authority RRs: 4  
Additional RRs: 2  
Queries  
= Response: Message is a response  
= Opcode: Standard query (0)  
= Authoritative: Server is not an authority for domain  
= Truncated: Message is not truncated  
= Recursion desired: Do query recursively  
= Recursion available: Server can do recursive queries  
= Z: reserved (0)  
= Answer authenticated: Answer/authority portion was not

= Non-authenticated data: Unacceptable = Reply code: No error (0)

ss-prod-ew1-notif-26.aws.adobess.com: type A, class IN Name: ss-prod-ew1-notif-26.aws.adobess.com  
[Name Length: 36]  
[Label Count: 4]

Type: A (Host Address) (1)  
Class: IN (0x0001)

Answers

Authoritative nameservers Additional records [Request In: 3167]  
[Time: 0.008843000 seconds]

## 3.2.2

No. Time Source Destination Protocol Length Info  
9 0.622283 192.168.0.106 192.168.0.1 DNS 77 Standard

query 0x3691 A polka.typekit.com  
Frame 9: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1  
User Datagram Protocol, Src Port: 61610, Dst Port: 53  
Domain Name System (query)

No.

Transaction ID: 0x3691  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
[Response In: 11]

Source

Destination

Protocol

Length Info 390 Standard 34.199.93.198 A

No.

Time Source  
69 12.965187 192.168.0.106

Destination 192.168.0.1

Protocol Length Info  
DNS 71 Standard

No.



Transaction ID: 0x075a  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
[Response In: 70]

Source

Destination

Protocol Length Info

Time  
11 0.660230

192.168.0.1  
query response 0x3691 A polka.typekit.com A 34.195.21.71 A 34.225.200.117 A

Transaction ID: 0x3691  
Flags: 0x8180 Standard query response, No error Questions: 1  
Answer RRs: 8  
Authority RRs: 4  
Additional RRs: 3  
Queries  
Answers  
Authoritative nameservers  
Additional records  
[Request In: 9]  
[Time: 0.037947000 seconds]

192.168.0.106

DNS

34.199.238.234 A 34.195.121.224 A 34.203.172.63 A 34.202.173.107 A 34.206.199.72 NS ns-964.awsdns-56.net NS ns-342.awsdns-42.com NS ns-1561.awsdns-03.co.uk NS ns-1260.awsdns-29.org A 205.251.193.86 A 205.251.195.196 A 205.251.196.236  
Frame 11: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) on interface en0, id 0  
Ethernet II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31)  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106  
User Datagram Protocol, Src Port: 53, Dst Port: 61610  
Domain Name System (response)

query 0x075a A www.mit.edu  
Frame 69: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1  
User Datagram Protocol, Src Port: 65377, Dst Port: 53  
Domain Name System (query)

Time  
70 13.002524

192.168.0.1  
query response 0x075a A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME

e9566.dscb.akamaiedge.net A 92.123.2.59 NS n3dscb.akamaiedge.net NS n5dscb.akamaiedge.net  
NS n6dscb.akamaiedge.net NS n7dscb.akamaiedge.net NS n0dscb.akamaiedge.net NS  
n4dscb.akamaiedge.net NS n2dscb.akamaiedge.net NS n1dscb.akamaiedge.net A 88.221.81.192  
AAAA 2600:1480:e800::c0 A 104.94.100.70 A 104.94.100.94 A 104.94.100.29 A 104.94.100.93 A  
104.94.100.132 A 95.101.23.214 A 2.16.10.190  
Frame 70: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface en0, id 0  
Ethernet II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31)  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106  
User Datagram Protocol, Src Port: 53, Dst Port: 65377

192.168.0.106

DNS 484 Standard

/Users/mariia/Desktop/dump2.pcapng 164 total packets, 8 shown

Domain Name System (response)  
Transaction ID: 0x075a  
Flags: 0x8180 Standard query response, No error Questions: 1  
Answer RRs: 3  
Authority RRs: 8  
Additional RRs: 9  
Queries  
Answers  
Authoritative nameservers  
Additional records  
[Request In: 69]  
[Time: 0.037337000

No. Time  
72 13.364475

query 0x6e6b A mail.ukr.net  
Frame 72: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1  
User Datagram Protocol, Src Port: 57339, Dst Port: 53  
Domain Name System (query)

No.

Transaction ID: 0x6e6b  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
[Response In: 74]

Source

Destination

Protocol Length Info

Time  
74 13.591777

seconds]  
Source  
192.168.0.106 192.168.0.1 DNS 72 Standard

Destination

Protocol Length Info

192.168.0.1  
query response 0x6e6b A mail.ukr.net A 212.42.75.249 NS ns2.fwdcdn.net NS ns1.fwdcdn.net A

212.42.82.100 A 212.42.77.100  
Frame 74: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface en0, id 0  
Ethernet II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31)  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106  
User Datagram Protocol, Src Port: 53, Dst Port: 57339  
Domain Name System (response)

No.

seconds]  
Source  
192.168.0.106 192.168.0.1 DNS 96 Standard

Transaction ID: 0x6e6b  
Flags: 0x8180 Standard query response, No error Questions: 1  
Answer RRs: 1  
Authority RRs: 2  
Additional RRs: 2  
Queries  
Answers  
Authoritative nameservers  
Additional records  
[Request In: 72]  
[Time: 0.227302000

Time  
125 17.439749

192.168.0.106

DNS 163 Standard

Destination

Protocol Length Info

query 0x090d A ss-prod-ew1-notif-26.aws.adobess.com  
Frame 125: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1  
User Datagram Protocol, Src Port: 52409, Dst Port: 53  
Domain Name System (query)

Transaction ID: 0x090d  
Flags: 0x0100 Standard query  
Questions: 1

Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
[Response In: 127]

No. Time

Source

Destination

Protocol Length Info

/Users/mariia/Desktop/dump2.pcapng 164 total packets, 8 shown

127 17.450149 192.168.0.1 192.168.0.106 DNS 314 Standard query response 0x090d A ss-prod-ew1-notif-26.aws.adobess.com A 18.202.149.73 A 52.31.117.171 A 18.203.76.53 NS ns-445.awsdns-55.com NS ns-1326.awsdns-37.org NS ns-1000.awsdns-61.net NS ns-1676.awsdns-17.co.uk A 205.251.193.189 A 205.251.195.232  
Frame 127: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface en0, id 0 Ethernet II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31) Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106 User Datagram Protocol, Src Port: 53, Dst Port: 52409 Domain Name System (response)

Transaction ID: 0x090d  
Flags: 0x8180 Standard query response, No error Questions: 1  
Answer RRs: 3  
Authority RRs: 4  
Additional RRs: 2  
Queries  
Answers  
Authoritative nameservers  
Additional records  
[Request In: 125]  
[Time: 0.010400000 seconds]

### 3.2.3

No. Time Source Destination Protocol Length Info  
35 4.744495 192.168.0.106 192.168.0.1 DNS 67 Standard

query 0x631a A mit.edu  
Frame 35: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface en0, id 0 Ethernet II, Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1 User Datagram Protocol, Src Port: 51297, Dst Port: 53 Domain Name System (query)

No.

Transaction ID: 0x631a  
Flags: 0x0100 Standard query  
Questions: 1

Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
[Response In: 36]

Source

Destination

Protocol Length Info

No.

Destination

Protocol Length Info  
DNS 70 Standard

Time  
36 4.801817

192.168.0.1  
query response 0x631a A mit.edu A 23.37.44.254 NS eur5.akam.net NS ns1-173.akam.net NS

ns1-37.akam.net NS use2.akam.net NS use5.akam.net NS asia1.akam.net NS usw2.akam.net NS  
asia2.akam.net A 23.74.25.64 A 96.7.49.64 A 184.26.161.64 A 95.100.175.64 A 95.101.36.64  
Frame 36: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface en0, id 0  
Ethernet II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31)  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106  
User Datagram Protocol, Src Port: 53, Dst Port: 51297  
Domain Name System (response)

Transaction ID: 0x631a  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 1  
Authority RRs: 8  
Additional RRs: 5  
Queries  
Answers

mit.edu: type A, class IN, addr 23.37.44.254 Authoritative nameservers

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

Additional records eur5.akam.net: use2.akam.net: usw2.akam.net:

type A, class IN, addr 23.74.25.64 type A, class IN, addr 96.7.49.64 type A, class IN, addr  
184.26.161.64

asia1.akam.net: type A,

asia2.akam.net: type A, [Request In: 35]  
[Time: 0.057322000 seconds]

Time Source  
37 4.804571 192.168.0.106 23.37.44.254

192.168.0.106

DNS 330 Standard

class IN, addr 95.100.175.64 class IN, addr 95.101.36.64

query 0xb0c5 A -type=NS

Frame 37: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 23.37.44.254  
User Datagram Protocol, Src Port: 59228, Dst Port: 53  
Domain Name System (query)

Transaction ID: 0xb0c5  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries

/Users/mariia/Desktop/dump3.pcapng 133 total packets, 5 shown

No. Time Source Destination Protocol Length Info  
52 9.809429 192.168.0.106 23.37.44.254 DNS 70 Standard

query 0xb0c5 A -type=NS

Frame 52: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 23.37.44.254  
User Datagram Protocol, Src Port: 59228, Dst Port: 53  
Domain Name System (query)

No.

Time  
85 14.811855

Source

Destination 23.37.44.254

Protocol Length Info  
DNS 70 Standard  
Transaction ID: 0xb0c5  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries

192.168.0.106 query 0xb0c5 A -type=NS

Frame 85: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 23.37.44.254  
User Datagram Protocol, Src Port: 59228, Dst Port: 53  
Domain Name System (query)

Transaction ID: 0xb0c5  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries

### 3.2.4

No. Time Source Destination Protocol Length Info  
5 2.042217 192.168.0.106 192.168.0.1 DNS 90 Standard

query 0xc45e A nexusrules.officeapps.live.com  
Frame 5: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1  
User Datagram Protocol, Src Port: 61102, Dst Port: 53  
Domain Name System (query)

No.

Transaction ID: 0xc45e  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
[Response In: 7]

Time  
7 2.084037

Transaction ID: 0xc45e  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 2  
Authority RRs: 10  
Additional RRs: 5  
Queries  
Answers

nexusrules.officeapps.live.com: type CNAME, class IN, cname prod.nexusrules.live.com.akadns.net

Source

Destination

## Protocol Length Info

192.168.0.1

query response 0xc45e A nexusrules.officeapps.live.com CNAME  
prod.nexusrules.live.com.akadns.net A 52.109.120.17 NS a5-130.akagtm.org NS a11-129.akadns.net  
NS a3-129.akadns.net NS a28-129.akagtm.org NS a1-128.akadns.net NS a7-131.akadns.net NS  
a13-130.akagtm.org NS a9-128.akadns.net NS a12-131.akagtm.org NS a18-128.akagtm.org A  
193.108.88.128 A 96.7.49.129 A 23.61.199.131 A 184.85.248.128 A 84.53.139.129  
Frame 7: 460 bytes on wire (3680 bits), 460 bytes captured (3680 bits) on interface en0, id 0 Ethernet  
II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31) Internet  
Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106  
User Datagram Protocol, Src Port: 53, Dst Port: 61102  
Domain Name System (response)

No.

akadns.net: type NS, class IN, ns a5-130.akagtm.org akadns.net: type NS, class IN, ns a11-  
129.akadns.net akadns.net: type NS, class IN, ns a3-129.akadns.net akadns.net: type NS, class IN,  
ns a28-129.akagtm.org akadns.net: type NS, class IN, ns a1-128.akadns.net akadns.net: type NS,  
class IN, ns a7-131.akadns.net akadns.net: type NS, class IN, ns a13-130.akagtm.org akadns.net:  
type NS, class IN, ns a9-128.akadns.net akadns.net: type NS, class IN, ns a12-131.akagtm.org  
akadns.net: type NS, class IN, ns a18-128.akagtm.org

## Additional records

a1-128.akadns.net: type A, class IN, addr 193.108.88.128 a3-129.akadns.net: type A, class IN, addr  
96.7.49.129 a7-131.akadns.net: type A, class IN, addr 23.61.199.131 a9-128.akadns.net: type A,  
class IN, addr 184.85.248.128 a11-129.akadns.net: type A, class IN, addr 84.53.139.129

[Request In: 5]

[Time: 0.041820000 seconds]

Time Source Destination 407 6.754482 192.168.0.106 18.0.72.3

## Protocol Length Info

DNS 74 Standard

prod.nexusrules.live.com.akadns.net: type A, class IN, addr 52.109.120.17 Authoritative nameservers

192.168.0.106

DNS 460 Standard

query 0x88a8 A www.aiit.or.kr

Frame 407: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 18.0.72.3  
User Datagram Protocol, Src Port: 55695, Dst Port: 53  
Domain Name System (query)

Transaction ID: 0x88a8

/Users/mariia/Desktop/dump4.pcapng 551 total packets, 7 shown

No.

Additional RRs: 0  
Queries



Time  
442 11.676320

Source

Destination 192.168.0.1

Protocol Length Info  
DNS 84 Standard

No.

Time  
444 11.691426

Transaction ID: 0xae8d  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 8  
Authority RRs: 4  
Additional RRs: 2  
Queries  
Answers

gateway.fe.apple-dns.net: type A, class IN, gateway.fe.apple-dns.net: type A, class IN,  
gateway.fe.apple-dns.net: type A, class IN, gateway.fe.apple-dns.net: type A, class IN,  
gateway.fe.apple-dns.net: type A, class IN, gateway.fe.apple-dns.net: type A, class IN,  
gateway.fe.apple-dns.net: type A, class IN, gateway.fe.apple-dns.net: type A, class IN,

No.

Authoritative nameservers  
fe.apple-dns.net: type NS, class IN, ns ns-287.awsdns-35.com fe.apple-dns.net: type NS, class IN, ns  
ns-748.awsdns-29.net fe.apple-dns.net: type NS, class IN, ns ns-1572.awsdns-04.co.uk fe.apple-  
dns.net: type NS, class IN, ns ns-1124.awsdns-12.org

Additional records  
ns-287.awsdns-35.com: type A, class IN, addr 205.251.193.31 ns-1124.awsdns-12.org: type A, class  
IN, addr 205.251.196.100

[Request In: 442]  
[Time: 0.015106000 seconds]

Time Source Destination Protocol Length Info 445 11.755899 192.168.0.106 18.0.72.3 DNS 74  
Standard

Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0

192.168.0.106 query 0xae8d A gateway.fe.apple-dns.net

Frame 442: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface en0, id 0

Ethernet II, Src: Apple\_78:53:31 (f0:18:98:78:53:31), Internet Protocol Version 4, Src: 192.168.0.106,  
Dst: User Datagram Protocol, Src Port: 59758, Dst Port: 53 Domain Name System (query)

Transaction ID: 0xae8d  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
[Response In: 444]

Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) 192.168.0.1

Source

Destination

Protocol Length Info

192.168.0.1

query response 0xae8d A gateway.fe.apple-dns.net A 17.248.147.51 A 17.248.147.53 A  
17.248.147.15 A 17.248.147.176 A 17.248.147.168 A 17.248.147.76 A 17.248.147.181 A  
17.248.147.147 NS ns-287.awsdns-35.com NS ns-748.awsdns-29.net NS ns-1572.awsdns-04.co.uk  
NS ns-1124.awsdns-12.org A 205.251.193.31 A 205.251.196.100  
Frame 444: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interface en0, id 0  
Ethernet II, Src: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple\_78:53:31 (f0:18:98:78:53:31)  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106  
User Datagram Protocol, Src Port: 53, Dst Port: 59758  
Domain Name System (response)

192.168.0.106

DNS 381 Standard

query 0x88a8 A www.aiit.or.kr  
Frame 445: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0 Ethernet II,  
Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet  
Protocol Version 4, Src: 192.168.0.106, Dst: 18.0.72.3  
User Datagram Protocol, Src Port: 55695, Dst Port: 53  
Domain Name System (query)

addr 17.248.147.51 addr 17.248.147.53 addr 17.248.147.15 addr 17.248.147.176 addr  
17.248.147.168 addr 17.248.147.76 addr 17.248.147.181 addr 17.248.147.147

/Users/mariia/Desktop/dump4.pcapng 551 total packets, 7 shown

No.

Time  
517.16756563

Source

Destination 18.0.72.3

Protocol Length Info  
DNS 74 Standard  
Transaction ID: 0x88a8  
Flags: 0x0100 Standard query

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries

192.168.0.106 query 0x88a8 A www.aiit.or.kr

Frame 517: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0 Ethernet II, Src: Apple\_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT\_66:88:6a (ac:84:c6:66:88:6a) Internet Protocol Version 4, Src: 192.168.0.106, Dst: 18.0.72.3 User Datagram Protocol, Src Port: 55695, Dst Port: 53 Domain Name System (query)

Transaction ID: 0x88a8  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries

## Контрольні запитання

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?

```
► Frame 60: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0  
► Ethernet II, Src: Apple_78:53:31 (f0:18:98:78:53:31), Dst: Tp-LinkT_66:88:6a (ac:84:c6:66:88:6a)  
► Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1  
► User Datagram Protocol, Src Port: 52943, Dst Port: 53
```

Цільовий порт: 53

Вихідний порт: 52943

2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?

IP: 192.168.0.1, є адресом локального порта.

3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Цей запит – є запитом стандартного типу. Вміщує.

[\[Response In: 62\]](#)

4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?

```
► Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 4
Additional RRs: 1
► Queries
▼ Answers
  ► ss-prod-ew1-notif-26.aws.adobess.com: type A, class IN, addr 18.202.149.73
  ► ss-prod-ew1-notif-26.aws.adobess.com: type A, class IN, addr 52.31.117.171
  ► ss-prod-ew1-notif-26.aws.adobess.com: type A, class IN, addr 18.203.76.53
► Authoritative nameservers
► Additional records
[Request In: 497]
[Time: 0.012898000 seconds]
```

5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

Так, співпадає

64	11.561363	192.168.0.106	104.20.0.85	TLSv1...	172	Application Data
65	11.574634	192.168.0.106	104.20.0.85	TLSv1...	170	Application Data
66	11.614400	192.168.0.106	192.168.0.1	DNS	86	Standard query 0xa018 A e17437.dscb.akamaiedge.net
67	11.614718	192.168.0.106	2.18.68.80	TCP	78	49997 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64

6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?

86	Standard query 0xa018 A e17437.dscb.akamaiedge.net
426	Standard query response 0xa018 A e17437.dscb.akamaiedge.net A 2.18.68.80 NS n3dscb.akamaiedge.net NS n...
85	Standard query 0xc29d A e673.dsce9.akamaiedge.net
433	Standard query response 0xc29d A e673.dsce9.akamaiedge.net A 92.122.156.104 NS n6dsce9.akamaiedge.net ...
96	Standard query 0xb2b8 A ss-prod-ew1-notif-26.aws.adobess.com
298	Standard query response 0xb2b8 A ss-prod-ew1-notif-26.aws.adobess.com A 18.202.149.73 A 52.31.117.171 ...

7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

Цільовий: 192.168.0.1  
Вихідний: 192.168.0.106

8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

192.168.0.1, є адресою локального сервера

9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Цей запит - є запитом стандартного типу. Вміщує.

► **Flags: 0x0100 Standard query**

**Questions: 1**

**Answer RRs: 0**

**Authority RRs: 0**

**Additional RRs: 0**

► **Queries**

[\[Response In: 11\]](#)

10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?

```

▶ Frame 11: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) on interface en0, id 0
▶ Ethernet II, Src: Tp-LinkT_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple_78:53:31 (f0:18:98:78:53:31)
▶ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106
▶ User Datagram Protocol, Src Port: 53, Dst Port: 61610
▼ Domain Name System (response)
  Transaction ID: 0x3691
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 4
  Additional RRs: 3
  ▶ Queries
  ▼ Answers
    ▶ polka.typekit.com: type A, class IN, addr 34.195.21.71
    ▶ polka.typekit.com: type A, class IN, addr 34.225.200.117
    ▶ polka.typekit.com: type A, class IN, addr 34.199.93.198
    ▶ polka.typekit.com: type A, class IN, addr 34.199.238.234
    ▶ polka.typekit.com: type A, class IN, addr 34.195.121.224
    ▶ polka.typekit.com: type A, class IN, addr 34.203.172.63
    ▶ polka.typekit.com: type A, class IN, addr 34.202.173.107
    ▶ polka.typekit.com: type A, class IN, addr 34.206.199.72
  ▶ Authoritative nameservers
  ▶ Additional records
  [Request In: 9]
  [Time: 0.037947000 seconds]
0030  00 08 00 04 00 03 05 70 6f 6c 6b 61 07 74 79 70  .....p olka·typ
0040  65 6b 69 74 03 63 6f 6d 00 00 01 00 01 c0 0c 00  ekit·com ·.....
0050  01 00 01 00 00 00 3c 00 04 22 c3 15 47 c0 0c 00  .....< "·G...
0060  01 00 01 00 00 00 3c 00 04 22 e1 c8 75 c0 0c 00  .....< "·u...

```

11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

IP: 192.168.0.1. Так є.

12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Стандартний тип запиту. Так вміщує.

```

▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
▶ Queries
  [Response In: 36]

```

13. Дослідіть повідомлення із відповіддю DNS. Скільки

записів із відповідями було запропоновано сервером?  
Які сервери DNS були запропоновані у відповіді?  
Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?

```
► Frame 36: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface en0, id 0
► Ethernet II, Src: Tp-LinkT_66:88:6a (ac:84:c6:66:88:6a), Dst: Apple_78:53:31 (f0:18:98:78:53:31)
► Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106
► User Datagram Protocol, Src Port: 53, Dst Port: 51297
▼ Domain Name System (response)
  Transaction ID: 0x631a
  ► Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 8
  Additional RRs: 5
  ► Queries
▼ Answers
  ► mit.edu: type A, class IN, addr 23.37.44.254
  ► Authoritative nameservers
  ► Additional records
  [Request In: 35]
  [Time: 0.057322000 seconds]
```

```
0040 01 00 01 c0 0c 00 01 00 01 00 00 00 14 00 04 17 .....
0050 25 2c fe c0 0c 00 02 00 01 00 02 84 01 00 0f 04 %,.....
0060 65 75 72 35 04 61 6b 61 6d 03 6e 65 74 00 c0 0c eur5-aka m-net...
0070 00 02 00 01 00 02 84 01 00 0a 07 6e 73 31 2d 31 .....ns1-1
0080 37 33 c0 3a c0 0c 00 02 00 01 00 02 84 01 00 09 73:.....
0090 06 6e 73 31 2d 33 37 c0 3a c0 0c 00 02 00 01 00 ns1-37:.....
00a0 02 84 01 00 07 04 75 73 65 32 c0 3a c0 0c 00 02 .....us e2:.....
00b0 00 01 00 02 84 01 00 07 04 75 73 65 35 c0 3a c0 .....use5:..
00c0 0c 00 02 00 01 00 02 84 01 00 08 05 61 73 69 61 .....asia
00d0 31 c0 3a c0 0c 00 02 00 01 00 02 84 01 00 07 04 1:.....
00e0 75 73 77 32 c0 3a c0 0c 00 02 00 01 00 02 84 01 usw2:.....
00f0 00 08 05 61 73 69 61 32 c0 3a c0 35 00 01 00 01 .....asia2 :5...
0100 00 02 44 1f 00 04 17 4a 19 40 c0 7b 00 01 00 01 ..D...J .@:{...
0110 00 02 42 9c 00 04 60 07 31 40 c0 b5 00 01 00 01 ..B...` 1@.....
0120 00 01 2d a1 00 04 b8 1a a1 40 c0 a1 00 01 00 01 ..-.....@.....
0130 00 02 3e ab 00 04 5f 64 af 40 c0 c8 00 01 00 01 ..>..._d .@.....
```

14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

IP: 18.0.72.3. Не є адресою локального сервера.

#### ▼ Domain Name System (query)

Transaction ID: 0x88a8

► Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

► Queries

15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Стандартний тип запиту. Ні не вміщує.

▼ Domain Name System (query)

Transaction ID: 0x88a8

► Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

► Queries

16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?

Відповідь не була отримана.

**Висновок:** В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи DNS та було проведено аналіз деталей роботи даних протоколів.