



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-77
Нерубенко А.А.
Прийняв: Кухарєв С.О.

Київ 2020

3.2.1

```
No.      Time      Source      Destination      Protocol Length Info
 25 1.583324 192.168.31.207 192.168.31.1      DNS           76      Standard query 0x207a A storage.live.com
Frame 25: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-19508CF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 62280, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x207a
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
[Response In: 26]
No.      Time      Source      Destination      Protocol Length Info
 26 1.585216 192.168.31.1 192.168.31.207      DNS           144     Standard query response 0x207a A storage.live.com CNAME
odc-common-us-meta.onedrive.akadns.net A 104.44.88.28
Frame 26: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-19508CF276D4}, id 0
Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 62280
Domain Name System (response)
  Transaction ID: 0x207a
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
[Request In: 25]
[Time: 0.001892000 seconds]
No.      Time      Source      Destination      Protocol Length Info
 69 1.777197 192.168.31.207 192.168.31.1      DNS           79      Standard query 0xf9ae A logincdn.msauth.net
Frame 69: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-19508CF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 60566, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0xf9ae
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
[Response In: 74]
```

No.	Time	Source	Destination	Protocol	Length	Info
71	1.822200	192.168.31.207	192.168.31.1	DNS	89	Standard query 0x0458 A web.vortex.data.microsoft.com
<p>Frame 71: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0 Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de) Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1 User Datagram Protocol, Src Port: 49224, Dst Port: 53 Domain Name System (query) Transaction ID: 0x0458 Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries [Response In: 72]</p>						
72	1.825251	192.168.31.1	192.168.31.207	DNS	267	Standard query response 0x0458 A
<p>web.vortex.data.microsoft.com CNAME web.vortex.data.microsoft.com.akadns.net CNAME geo.vortex.data.microsoft.com.akadns.net CNAME db5.vortex.data.microsoft.com.akadns.net A 40.77.226.250 Frame 72: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0 Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64) Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207 User Datagram Protocol, Src Port: 53, Dst Port: 49224 Domain Name System (response) Transaction ID: 0x0458 Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 4 Authority RRs: 0 Additional RRs: 0 Queries Answers [Request In: 71] [Time: 0.003051000 seconds]</p>						
74	1.834375	192.168.31.1	192.168.31.207	DNS	235	Standard query response 0xf9ae A logincdn.msauth.net CNAME
<p>logincdn.trafficmanager.net CNAME logincdnvzeuno.azureedge.net CNAME logincdnvzeuno.ec.azureedge.net CNAME cs1227.wpc.alphacdn.net A 192.229.221.185 Frame 74: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0 Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64) Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207 User Datagram Protocol, Src Port: 53, Dst Port: 60566 Domain Name System (response) Transaction ID: 0xf9ae</p>						
<p>Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 5 Authority RRs: 0 Additional RRs: 0 Queries Answers [Request In: 69] [Time: 0.057178000 seconds]</p>						
253	2.472660	192.168.31.207	192.168.31.1	DNS	72	Standard query 0xd9f5 A api.bing.com
<p>Frame 253: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0 Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de) Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1 User Datagram Protocol, Src Port: 56958, Dst Port: 53 Domain Name System (query) Transaction ID: 0xd9f5 Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries [Response In: 281]</p>						
281	2.505656	192.168.31.1	192.168.31.207	DNS	183	Standard query response 0xd9f5 A api.bing.com CNAME api-
<p>bing.com.e-0001.e-msedge.net CNAME afd.e-0001.dc-msedge.net CNAME e-0001.dc-msedge.net A 13.107.13.80 Frame 281: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0 Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64) Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207 User Datagram Protocol, Src Port: 53, Dst Port: 56958 Domain Name System (response) Transaction ID: 0xd9f5 Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 4 Authority RRs: 0 Additional RRs: 0 Queries Answers [Request In: 253] [Time: 0.032996000 seconds]</p>						
297	2.563639	192.168.31.207	192.168.31.1	DNS	79	Standard query 0x639d A img.img-taboola.com
<p>Frame 297: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0 Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de) Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1 User Datagram Protocol, Src Port: 58320, Dst Port: 53 Domain Name System (query) Transaction ID: 0x639d Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries [Response In: 427]</p>						

```
No.      Time      Source      Destination      Protocol Length Info
 426 3.566852 192.168.31.207 192.168.31.1      DNS          79      Standard query 0x639d A img.img-taboola.com
Frame 426: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 58320, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x639d
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    [Retransmitted request. Original request in: 297]
    [Retransmission: True]
No.      Time      Source      Destination      Protocol Length Info
 427 3.609672 192.168.31.1 192.168.31.207  DNS          183      Standard query response 0x639d A img.img-taboola.com CNAME
trc.taboola.map.fastly.net A 151.101.2.49 A 151.101.66.49 A 151.101.130.49 A 151.101.194.49
Frame 427: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 58320
Domain Name System (response)
  Transaction ID: 0x639d
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 5
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    [Request In: 297]

[Time: 1.046033000 seconds]
No.      Time      Source      Destination      Protocol Length Info
 434 4.436189 192.168.31.207 192.168.31.1      DNS          72      Standard query 0x3b13 A www.ietf.org
Frame 434: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 64919, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x3b13
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    [Response In: 435]
No.      Time      Source      Destination      Protocol Length Info
 435 4.468788 192.168.31.1 192.168.31.207  DNS          149      Standard query response 0x3b13 A www.ietf.org CNAME
www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
Frame 435: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 64919
Domain Name System (response)
  Transaction ID: 0x3b13
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    [Request In: 434]
    [Time: 0.032599000 seconds]
No.      Time      Source      Destination      Protocol Length Info
1087 5.185467 192.168.31.207 192.168.31.1      DNS          78      Standard query 0x2736 A analytics.ietf.org
Frame 1087: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 60516, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x2736
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    [Response In: 1088]
No.      Time      Source      Destination      Protocol Length Info
1088 5.186573 192.168.31.1 192.168.31.207  DNS          116      Standard query response 0x2736 A analytics.ietf.org CNAME
ietf.org A 4.31.198.44
Frame 1088: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 60516
Domain Name System (response)
  Transaction ID: 0x2736
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    [Request In: 1087]
    [Time: 0.001106000 seconds]
```

3.2.2

```

No.      Time           Source           Destination      Protocol Length Info
 6 1.977562      192.168.31.207  192.168.31.1    DNS              85      Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
Frame 6: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEL_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 50509, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x0001
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
  [Request In: 7]

No.      Time           Source           Destination      Protocol Length Info
 7 1.978992      192.168.31.1    192.168.31.207  DNS              108     Standard query response 0x0001 PTR 1.31.168.192.in-
addr.arpa PTR XiaoQiang
Frame 7: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 50509
Domain Name System (response)
  Transaction ID: 0x0001
  Flags: 0x8580 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
  [Request In: 6]
  [Time: 0.001430000 seconds]

No.      Time           Source           Destination      Protocol Length Info
 8 1.981158      192.168.31.207  192.168.31.1    DNS              71      Standard query 0x0002 A www.mit.edu
Frame 8: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEL_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 50510, 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
  Answers
  [Request In: 9]

No.      Time           Source           Destination      Protocol Length Info
 9 2.022886      192.168.31.1    192.168.31.207  DNS              160     Standard query response 0x0002 A www.mit.edu CNAME
www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.109.79.114
Frame 9: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 50510
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
  Answers
  [Request In: 8]
  [Time: 0.041728000 seconds]

No.      Time           Source           Destination      Protocol Length Info
10 2.022957      192.168.31.207  192.168.31.1    DNS              71      Standard query 0x0003 AAAA www.mit.edu
Frame 10: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEL_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 50511, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x0003
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
  [Request In: 12]

No.      Time           Source           Destination      Protocol Length Info
12 2.184693      192.168.31.1    192.168.31.207  DNS              200     Standard query response 0x0003 AAAA www.mit.edu CNAME
www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:d200:191::255e AAAA 2a02:26f0:d200:19e::255e
Frame 12: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 50511
Domain Name System (response)
  Transaction ID: 0x0003
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
  [Request In: 10]
  [Time: 0.155116000 seconds]

```

3.2.3

```
No.      Time      Source      Destination  Protocol Length Info
 1 0.000000    192.168.31.207 192.168.31.1  DNS        85    Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 62972, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x0001
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
[Response In: 2]
No.      Time      Source      Destination  Protocol Length Info
 2 0.002462    192.168.31.1    192.168.31.207  DNS       108    Standard query response 0x0001 PTR 1.31.168.192.in-
addr.arpa PTR XiaoQiang
Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 62972
Domain Name System (response)
  Transaction ID: 0x0001
  Flags: 0x8580 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    1.31.168.192.in-addr.arpa: type PTR, class IN, XiaoQiang
[Request In: 1]
[Time: 0.002462000 seconds]
No.      Time      Source      Destination  Protocol Length Info
 3 0.005835    192.168.31.207 192.168.31.1  DNS        67    Standard query 0x0002 NS mit.edu
Frame 3: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 62973, 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
[Response In: 4]
No.      Time      Source      Destination  Protocol Length Info
 4 0.038240    192.168.31.1    192.168.31.207  DNS       234    Standard query response 0x0002 NS mit.edu NS eur5.akam.net
NS use2.akam.net NS asia2.akam.net NS use5.akam.net NS ns1-37.akam.net NS asia1.akam.net NS usw2.akam.net NS ns1-173.akam.net
Frame 4: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 62973
Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    mit.edu: type NS, class IN, ns eur5.akam.net
    mit.edu: type NS, class IN, ns use2.akam.net
    mit.edu: type NS, class IN, ns asia2.akam.net
    mit.edu: type NS, class IN, ns use5.akam.net
    mit.edu: type NS, class IN, ns ns1-37.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 ns1-173.akam.net
[Request In: 3]
[Time: 0.032405000 seconds]
```

3.2.4

```
No.      Time      Source      Destination      Protocol Length Info
3 1.646917 192.168.31.207 192.168.31.1      DNS      73      Standard query 0xbc1c A bitsy.mit.edu
Frame 3: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEL_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
User Datagram Protocol, Src Port: 58296, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0xbc1c
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    [Response In: 4]
No.      Time      Source      Destination      Protocol Length Info
4 1.679853 192.168.31.1 192.168.31.207      DNS      89      Standard query response 0xbc1c A bitsy.mit.edu A 18.0.72.3
Frame 4: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: XIAOMIEL_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
User Datagram Protocol, Src Port: 53, Dst Port: 58296
Domain Name System (response)
  Transaction ID: 0xbc1c
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    Answers
      [Request In: 3]
      [Time: 0.032936000 seconds]
No.      Time      Source      Destination      Protocol Length Info
5 1.688786 192.168.31.207 18.0.72.3          DNS      82      Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
Frame 5: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEL_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 18.0.72.3
User Datagram Protocol, Src Port: 58297, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x0001
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
No.      Time      Source      Destination      Protocol Length Info
6 3.722261 192.168.31.207 18.0.72.3          DNS      74      Standard query 0x0002 A www.aiit.or.kr
Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEL_ce:26:de (50:64:2b:ce:26:de)
Internet Protocol Version 4, Src: 192.168.31.207, Dst: 18.0.72.3
User Datagram Protocol, Src Port: 58298, 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
```

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 25: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{2F19C457-96E0-430A-8089-1950BCF276D4}, id 0
> Ethernet II, Src: IntelCor_73:73:64 (7c:b0:c2:73:73:64), Dst: XIAOMIEL_ce:26:de (50:64:2b:ce:26:de)
> Internet Protocol Version 4, Src: 192.168.31.207, Dst: 192.168.31.1
> User Datagram Protocol, Src Port: 62280, Dst Port: 53
```

Цільовий порт: 53

Вихідний порт: 62280

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

IP: 192.168.31.1, 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.

[\[Response In: 26\]](#)

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: 2
Authority RRs: 0
Additional RRs: 0
> Queries
▼ Answers
  > storage.live.com: type CNAME, class IN, cname odc-common-us-meta.onedrive.akadns.net
  > odc-common-us-meta.onedrive.akadns.net: type A, class IN, addr 104.44.88.28
```

[\[Request In: 25\]](#)

[Time: 0.001892000 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

434	4.436189	192.168.31.207	192.168.31.1	DNS	72 Standard query 0x3b13 A www.ietf.org
435	4.468788	192.168.31.1	192.168.31.207	DNS	149 Standard query response 0x3b13 A www.ietf.org Cl
436	4.470098	192.168.31.207	104.20.1.85	TCP	66 64070 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=146

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

```
76 Standard query 0x207a A storage.live.com
144 Standard query response 0x207a A storage.live.com CNAME odc-common-us-meta.onedrive.akadns.net A 104.44.88.28
79 Standard query 0xf9ae A logincdn.msauth.net
89 Standard query 0x0458 A web.vortex.data.microsoft.com
267 Standard query response 0x0458 A web.vortex.data.microsoft.com CNAME web.vortex.data.microsoft.com.akadns.net CNAME geo.vortex.data...
235 Standard query response 0xf9ae A logincdn.msauth.net CNAME lgincdn.trafficmanager.net CNAME lgincdnvzeuno.azureedge.net CNAME lgincd...
72 Standard query 0xd9f5 A api.bing.com
183 Standard query response 0xd9f5 A api.bing.com CNAME api-bing-com.e-0001.e-msedge.net CNAME afd.e-0001.dc-msedge.net CNAME e-0001.dc-...
79 Standard query 0x639d A img.img-taboola.com
79 Standard query 0x639d A img.img-taboola.com
183 Standard query response 0x639d A img.img-taboola.com CNAME trc.taboola.map.fastly.net A 151.101.2.49 A 151.101.66.49 A 151.101.130.4...
72 Standard query 0x3b13 A www.ietf.org
149 Standard query response 0x3b13 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
78 Standard query 0x2736 A analytics.ietf.org
116 Standard query response 0x2736 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
```

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

Цільовий: 192.168.31.1

Вихідний: 192.168.31.1

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

192.168.31.1, 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

[\[Response In: 12\]](#)

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

```

> Frame 12: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: XIAOMI_E1_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2:73:73:64)
> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
> User Datagram Protocol, Src Port: 53, Dst Port: 50511
▼ Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 0
  Additional RRs: 0
▼ Queries
  > www.mit.edu: type AAAA, class IN
▼ 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 AAAA, class IN, addr 2a02:26f0:d200:191::255e
  > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:19e::255e
  [Request In: 10]
  [Time: 0.155116000 seconds]

```

0030	00 04 00 00 00 00 03 77 77 77 03 6d 69 74 03 65-w ww-mit-e
0040	64 75 00 00 1c 00 01 c0 0c 00 05 00 01 00 00 03	du-.....

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

IP: 192.168.31.1. 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: 4]

```

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 4: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface
> Ethernet II, Src: XIAOMIEI_ce:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:
> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
> User Datagram Protocol, Src Port: 53, Dst Port: 62973
▼ Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  ▼ Answers
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.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 ns1-173.akam.net
  [Request In: 3]
  [Time: 0.032405000 seconds]
```

0000	7c b0 c2 73 73 64 50 64 2b ce 26 de 08 00 45 00	..ssdPd+.&...E.
0010	00 dc 00 00 40 00 40 11 79 f0 c0 a8 1f 01 c0 a8@.@.y.....

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: 0xbc1c
  > 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: 0xbc1c
  > 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 була отримана 1.

```
> Frame 4: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\N
> Ethernet II, Src: XIAOMI_E1_08:00:26:de (50:64:2b:ce:26:de), Dst: IntelCor_73:73:64 (7c:b0:c2
> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.207
> User Datagram Protocol, Src Port: 53, Dst Port: 58296
▼ Domain Name System (response)
  Transaction ID: 0xbc1c
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  > Answers
    [Request In: 3]
    [Time: 0.032936000 seconds]
```

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.