МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №3

з курсу «Комп'ютерні мережі»

тема: «Протокол DNS»

Виконав: студент 3 курсу

групи КА-77

Буханевич Родион

Прийняв: Кухарєв С.О.

Київ – 2020р.

Пакети для відповідей 1-6

No.   Time   Source   Destination   Protocol Length Info

   33 2.156526   192.168.0.101   192.168.0.1   DNS   72   Standard query 0x00f6 A www.ietf.org

Frame 33: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 12:b3:18:08:af:dd (12:b3:18:08:af:dd), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 6858, Dst Port: 53

Domain Name System (query)

  Transaction ID: 0x00f6

  Flags: 0x0100 Standard query

    0... .... = Response: Message is a query

    .000 0... .... = Opcode: Standard query (0)

    .... ..0. .... = Truncated: Message is not truncated

    ....1 .... = 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

    www.ietf.org: type A, class IN

  [Response In: 37]

No.   Time   Source   Destination   Protocol Length Info

   34 2.182159   192.168.0.101   192.168.0.1   DNS   72   Standard query 0x00f6 A www.ietf.org

Frame 34: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 12:b3:18:08:af:dd (12:b3:18:08:af:dd), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 6858, Dst Port: 53

Domain Name System (query)

  Transaction ID: 0x00f6

    [Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 33]

  Flags: 0x0100 Standard query

    0... .... = Response: Message is a query

    .000 0... .... = Opcode: Standard query (0)

    .... ..0. .... = Truncated: Message is not truncated

    ....1 .... = 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

    www.ietf.org: type A, class IN

  [Retransmitted request. Original request in: 33]

  [Retransmission: True]

No.	Time	Source	Destination	Protocol	Length	Info
37	2.389594	192.168.0.1	192.168.0.101	DNS	149	Standard query response 0x00f6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85

Frame 37: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 12:b3:18:08:af:dd (12:b3:18:08:af:dd)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101

User Datagram Protocol, Src Port: 53, Dst Port: 6858

Domain Name System (response)

Transaction ID: 0x00f6

Flags: 0x8180 Standard query response, No error

   1... .... = Response: Message is a response

   .000 0... .... = Opcode: Standard query (0)

   .... .0.. .... = Authoritative: Server is not an authority for domain

   .... ..0. .... = Truncated: Message is not truncated

   ....1 .... = Recursion desired: Do query recursively

   .... 1... .... = Recursion available: Server can do recursive queries

   .... .0.. .... = Z: reserved (0)

   ....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server

   ....0 .... = Non-authenticated data: Unacceptable

   .... 0000 = Reply code: No error (0)

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 104.20.1.85

   www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85

[Request In: 33]

[Time: 0.233068000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
38	2.389595	192.168.0.1	192.168.0.101	DNS	149	Standard query response 0x00f6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85

Frame 38: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 12:b3:18:08:af:dd (12:b3:18:08:af:dd)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101

User Datagram Protocol, Src Port: 53, Dst Port: 6858

Domain Name System (response)

  Transaction ID: 0x00f6

    [Expert Info (Warning/Protocol): DNS response retransmission. Original response in frame 37]

  Flags: 0x8180 Standard query response, No error

    1... .... = Response: Message is a response

    .000 0... .... = Opcode: Standard query (0)

    .... .0.. .... = Authoritative: Server is not an authority for domain

    .... ..0. .... = Truncated: Message is not truncated

    ....1 .... = Recursion desired: Do query recursively

    .... 1... .... = Recursion available: Server can do recursive queries

    .... .0.. .... = Z: reserved (0)

    ....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server

    ....0 .... = Non-authenticated data: Unacceptable

    .... 0000 = Reply code: No error (0)

  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 104.20.1.85

    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85

  [Retransmitted response. Original response in: 37]

  [Retransmission: True]

Пакети для відповідей 7-10

No.	Time	Source	Destination	Protocol	Length	Info
36	7.576368	192.168.0.103	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa

Frame 36: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 1033, 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

      1.0.168.192.in-addr.arpa: type PTR, class IN

         Name: 1.0.168.192.in-addr.arpa

         [Name Length: 24]

         [Label Count: 6]

         Type: PTR (domain name PoinTeR) (12)

         Class: IN (0x0001)

   [Response In: 37]

No.	Time	Source	Destination	Protocol	Length	Info
37	7.578342	192.168.0.1	192.168.0.103	DNS	133	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA localhost

Frame 37: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 1033

Domain Name System (response)

   Transaction ID: 0x0001

Flags: 0x8183 Standard query response, No such name

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 0

Queries

    1.0.168.192.in-addr.arpa: type PTR, class IN

        Name: 1.0.168.192.in-addr.arpa

        [Name Length: 24]

        [Label Count: 6]

        Type: PTR (domain name PoinTeR) (12)

        Class: IN (0x0001)

Authoritative nameservers

    168.192.in-addr.arpa: type SOA, class IN, mname localhost

        Name: 168.192.in-addr.arpa

        Type: SOA (Start Of a zone of Authority) (6)

        Class: IN (0x0001)

        Time to live: 5 (5 seconds)

        Data length: 37

        Primary name server: localhost

        Responsible authority's mailbox: root

        Serial Number: 1

        Refresh Interval: 604800 (7 days)

        Retry Interval: 86400 (1 day)

        Expire limit: 2419200 (28 days)

        Minimum TTL: 604800 (7 days)

  [Request In: 36]

  [Time: 0.001974000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
38	7.579268	192.168.0.103	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu

Frame 38: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 1044, 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

      www.mit.edu: type A, class IN

         Name: www.mit.edu

         [Name Length: 11]

         [Label Count: 3]

         Type: A (Host Address) (1)

         Class: IN (0x0001)

   [Response In: 39]

No.	Time	Source	Destination	Protocol	Length	Info
39	7.626000	192.168.0.1	192.168.0.103	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.9.14.138

Frame 39: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 1044

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

www.mit.edu: type A, class IN

Name: www.mit.edu

[Name Length: 11]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

Name: www.mit.edu

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 25

CNAME: www.mit.edu.edgekey.net

www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

Name: www.mit.edu.edgekey.net

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 35 (35 seconds)

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 23.9.14.138

Name: e9566.dscb.akamaiedge.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20 (20 seconds)

Data length: 4

Address: 23.9.14.138

[Request In: 38]

[Time: 0.046732000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info

40 7.629161   192.168.0.103   192.168.0.1   DNS   71   Standard query 0x0003 AAAA www.mit.edu

Frame 40: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 1045, 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

      www.mit.edu: type AAAA, class IN

         Name: www.mit.edu

         [Name Length: 11]

         [Label Count: 3]

         Type: AAAA (IPv6 Address) (28)

         Class: IN (0x0001)

   [Response In: 41]

No.	Time	Source	Destination	Protocol	Length	Info
41	7.645581	192.168.0.1	192.168.0.103	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 41: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 1045

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

    Name: www.mit.edu

    [Name Length: 11]

    [Label Count: 3]

    Type: AAAA (IPv6 Address) (28)

    Class: IN (0x0001)

Answers

  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

    Name: www.mit.edu

    Type: CNAME (Canonical NAME for an alias) (5)

    Class: IN (0x0001)

    Time to live: 1800 (30 minutes)

    Data length: 25

    CNAME: www.mit.edu.edgekey.net

  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

    Name: www.mit.edu.edgekey.net

    Type: CNAME (Canonical NAME for an alias) (5)

    Class: IN (0x0001)

    Time to live: 35 (35 seconds)

    Data length: 24

    CNAME: e9566.dscb.akamaiedge.net

  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:191::255e

    Name: e9566.dscb.akamaiedge.net

    Type: AAAA (IPv6 Address) (28)

    Class: IN (0x0001)

    Time to live: 20 (20 seconds)

    Data length: 16

    AAAA Address: 2a02:26f0:d200:191::255e

e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:19e::255e

    Name: e9566.dscb.akamaiedge.net

    Type: AAAA (IPv6 Address) (28)

    Class: IN (0x0001)

    Time to live: 20 (20 seconds)

    Data length: 16

    AAAA Address: 2a02:26f0:d200:19e::255e

[Request In: 40]

[Time: 0.016420000 seconds]

Пакети для відповідей 11-13

No.   Time   Source   Destination   Protocol Length Info

   11 3.053804   192.168.0.103   192.168.0.1   DNS   84   Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa

Frame 11: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 1046, 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

    1.0.168.192.in-addr.arpa: type PTR, class IN

      Name: 1.0.168.192.in-addr.arpa

      [Name Length: 24]

      [Label Count: 6]

      Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

[Response In: 12]

No.   Time   Source   Destination   Protocol Length Info

   12 3.058470   192.168.0.1   192.168.0.103   DNS   133   Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA localhost

Frame 12: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 1046

Domain Name System (response)

  Transaction ID: 0x0001

  Flags: 0x8183 Standard query response, No such name

  Questions: 1

  Answer RRs: 0

  Authority RRs: 1

  Additional RRs: 0

  Queries

    1.0.168.192.in-addr.arpa: type PTR, class IN

      Name: 1.0.168.192.in-addr.arpa

      [Name Length: 24]

      [Label Count: 6]

      Type: PTR (domain name PoinTeR) (12)

      Class: IN (0x0001)

  Authoritative nameservers

    168.192.in-addr.arpa: type SOA, class IN, mname localhost

      Name: 168.192.in-addr.arpa

      Type: SOA (Start Of a zone of Authority) (6)

      Class: IN (0x0001)

Time to live: 30 (30 seconds)

Data length: 37

Primary name server: localhost

Responsible authority's mailbox: root

Serial Number: 1

Refresh Interval: 604800 (7 days)

Retry Interval: 86400 (1 day)

Expire limit: 2419200 (28 days)

Minimum TTL: 604800 (7 days)

[Request In: 11]

[Time: 0.004666000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
13	3.059366	192.168.0.103	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu

Frame 13: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 1047, 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

mit.edu: type NS, class IN

Name: mit.edu

[Name Length: 7]

[Label Count: 2]

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

[Response In: 14]

No.   Time   Source   Destination   Protocol Length Info

   14 3.061287   192.168.0.1   192.168.0.103   DNS   234   Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS asia2.akam.net NS asia1.akam.net NS eur5.akam.net NS usw2.akam.net NS use2.akam.net NS ns1-173.akam.net NS use5.akam.net

Frame 14: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 1047

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

    mit.edu: type NS, class IN

      Name: mit.edu

      [Name Length: 7]

      [Label Count: 2]

      Type: NS (authoritative Name Server) (2)

      Class: IN (0x0001)

  Answers

mit.edu: type NS, class IN, ns ns1-37.akam.net

    Name: mit.edu

    Type: NS (authoritative Name Server) (2)

    Class: IN (0x0001)

    Time to live: 902 (15 minutes, 2 seconds)

    Data length: 17

    Name Server: ns1-37.akam.net

mit.edu: type NS, class IN, ns asia2.akam.net

    Name: mit.edu

    Type: NS (authoritative Name Server) (2)

    Class: IN (0x0001)

    Time to live: 902 (15 minutes, 2 seconds)

    Data length: 8

    Name Server: asia2.akam.net

mit.edu: type NS, class IN, ns asia1.akam.net

    Name: mit.edu

    Type: NS (authoritative Name Server) (2)

    Class: IN (0x0001)

    Time to live: 902 (15 minutes, 2 seconds)

    Data length: 8

    Name Server: asia1.akam.net

mit.edu: type NS, class IN, ns eur5.akam.net

    Name: mit.edu

    Type: NS (authoritative Name Server) (2)

    Class: IN (0x0001)

    Time to live: 902 (15 minutes, 2 seconds)

    Data length: 7

    Name Server: eur5.akam.net

mit.edu: type NS, class IN, ns usw2.akam.net

    Name: mit.edu

    Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 902 (15 minutes, 2 seconds)

Data length: 7

Name Server: usw2.akam.net

mit.edu: type NS, class IN, ns use2.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 902 (15 minutes, 2 seconds)

Data length: 7

Name Server: use2.akam.net

mit.edu: type NS, class IN, ns ns1-173.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 902 (15 minutes, 2 seconds)

Data length: 10

Name Server: ns1-173.akam.net

mit.edu: type NS, class IN, ns use5.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 902 (15 minutes, 2 seconds)

Data length: 7

Name Server: use5.akam.net

[Request In: 13]

[Time: 0.001921000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
15	3.317423	192.168.0.103	192.168.0.1	DNS	79	Standard query 0xa536 A clients6.google.com

Frame 15: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 31720, Dst Port: 53

Domain Name System (query)

   Transaction ID: 0xa536

   Flags: 0x0100 Standard query

   Questions: 1

   Answer RRs: 0

   Authority RRs: 0

   Additional RRs: 0

   Queries

      clients6.google.com: type A, class IN

         Name: clients6.google.com

         [Name Length: 19]

         [Label Count: 3]

         Type: A (Host Address) (1)

         Class: IN (0x0001)

   [Response In: 16]

No.	Time	Source	Destination	Protocol	Length	Info
16	3.319421	192.168.0.1	192.168.0.103	DNS	119	Standard query response 0xa536 A clients6.google.com CNAME clients.l.google.com A 216.58.215.78

Frame 16: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 31720

Domain Name System (response)

Transaction ID: 0xa536

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

Queries

clients6.google.com: type A, class IN

Name: clients6.google.com

[Name Length: 19]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

clients6.google.com: type CNAME, class IN, cname clients.l.google.com

Name: clients6.google.com

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 165 (2 minutes, 45 seconds)

Data length: 12

CNAME: clients.l.google.com

clients.l.google.com: type A, class IN, addr 216.58.215.78

Name: clients.l.google.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 165 (2 minutes, 45 seconds)

Data length: 4

Address: 216.58.215.78

[Request In: 15]

[Time: 0.001998000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
39	5.314430	192.168.0.103	192.168.0.1	DNS	106	Standard query 0xa9a9 A catalog-public-service-prod06.ol.epicgames.com

Frame 39: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 28191, Dst Port: 53

Domain Name System (query)

   Transaction ID: 0xa9a9

   Flags: 0x0100 Standard query

   Questions: 1

   Answer RRs: 0

   Authority RRs: 0

   Additional RRs: 0

   Queries

     catalog-public-service-prod06.ol.epicgames.com: type A, class IN

       Name: catalog-public-service-prod06.ol.epicgames.com

       [Name Length: 46]

       [Label Count: 4]

       Type: A (Host Address) (1)

       Class: IN (0x0001)

   [Response In: 40]

No.	Time	Source	Destination	Protocol	Length	Info
40	5.316622	192.168.0.1	192.168.0.103	DNS	307	Standard query response 0xa9a9 A catalog-public-service-prod06.ol.epicgames.com CNAME catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com A 54.158.230.97 A 52.20.3.255 A 35.174.163.193 A 35.171.214.220 A 54.82.245.68 A 52.54.29.61 A 52.5.166.101 A 18.211.165.162

Frame 40: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 28191

Domain Name System (response)

   Transaction ID: 0xa9a9

   Flags: 0x8180 Standard query response, No error

   Questions: 1

   Answer RRs: 9

   Authority RRs: 0

   Additional RRs: 0

   Queries

      catalog-public-service-prod06.ol.epicgames.com: type A, class IN

         Name: catalog-public-service-prod06.ol.epicgames.com

         [Name Length: 46]

         [Label Count: 4]

         Type: A (Host Address) (1)

         Class: IN (0x0001)

   Answers

      catalog-public-service-prod06.ol.epicgames.com: type CNAME, class IN, cname catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

         Name: catalog-public-service-prod06.ol.epicgames.com

         Type: CNAME (Canonical NAME for an alias) (5)

         Class: IN (0x0001)

         Time to live: 121 (2 minutes, 1 second)

         Data length: 61

         CNAME: catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

      catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com: type A, class IN, addr 54.158.230.97

Name: catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5 (5 seconds)

Data length: 4

Address: 54.158.230.97

catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com: type A, class IN, addr 52.20.3.255

Name: catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5 (5 seconds)

Data length: 4

Address: 52.20.3.255

catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com: type A, class IN, addr 35.174.163.193

Name: catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5 (5 seconds)

Data length: 4

Address: 35.174.163.193

catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com: type A, class IN, addr 35.171.214.220

Name: catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5 (5 seconds)

Data length: 4

Address: 35.171.214.220

catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com: type A, class IN, addr 54.82.245.68

Name: catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5 (5 seconds)

Data length: 4

Address: 54.82.245.68

catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com: type A, class IN, addr 52.54.29.61

Name: catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5 (5 seconds)

Data length: 4

Address: 52.54.29.61

catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com: type A, class IN, addr 52.5.166.101

Name: catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5 (5 seconds)

Data length: 4

Address: 52.5.166.101

catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com: type A, class IN, addr 18.211.165.162

Name: catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5 (5 seconds)

Data length: 4

Address: 18.211.165.162

[Request In: 39]

[Time: 0.002192000 seconds]]

Пакети для відповідей 14-16

No.	Time	Source	Destination	Protocol	Length	Info
11	1.988600	192.168.0.103	192.168.0.1	DNS	73	Standard query 0xc7b3 A bitsy.mit.edu

Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 1025, Dst Port: 53

Domain Name System (query)

  Transaction ID: 0xc7b3

  Flags: 0x0100 Standard query

  Questions: 1

  Answer RRs: 0

  Authority RRs: 0

  Additional RRs: 0

  Queries

    bitsy.mit.edu: type A, class IN

      Name: bitsy.mit.edu

      [Name Length: 13]

      [Label Count: 3]

      Type: A (Host Address) (1)

      Class: IN (0x0001)

  [Response In: 13]

No.	Time	Source	Destination	Protocol	Length	Info
12	2.014317	192.168.0.103	192.168.0.1	DNS	73	Standard query 0xc7b3 A bitsy.mit.edu

Frame 12: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 1025, Dst Port: 53

Domain Name System (query)

   Transaction ID: 0xc7b3

     [Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 11]

   Flags: 0x0100 Standard query

   Questions: 1

   Answer RRs: 0

   Authority RRs: 0

   Additional RRs: 0

   Queries

     bitsy.mit.edu: type A, class IN

       Name: bitsy.mit.edu

       [Name Length: 13]

       [Label Count: 3]

       Type: A (Host Address) (1)

       Class: IN (0x0001)

   [Retransmitted request. Original request in: 11]

   [Retransmission: True]

No.	Time	Source	Destination	Protocol	Length	Info
13	2.022430	192.168.0.1	192.168.0.103	DNS	89	Standard query response 0xc7b3 A bitsy.mit.edu A 18.0.72.3

Frame 13: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 1025

Domain Name System (response)

   Transaction ID: 0xc7b3

   Flags: 0x8180 Standard query response, No error

   Questions: 1

   Answer RRs: 1

   Authority RRs: 0

   Additional RRs: 0

   Queries

      bitsy.mit.edu: type A, class IN

         Name: bitsy.mit.edu

         [Name Length: 13]

         [Label Count: 3]

         Type: A (Host Address) (1)

         Class: IN (0x0001)

   Answers

      bitsy.mit.edu: type A, class IN, addr 18.0.72.3

         Name: bitsy.mit.edu

         Type: A (Host Address) (1)

         Class: IN (0x0001)

         Time to live: 1800 (30 minutes)

         Data length: 4

         Address: 18.0.72.3

   [Request In: 11]

   [Time: 0.033830000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
14	2.024212	192.168.0.103	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa

Frame 14: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 18.0.72.3

User Datagram Protocol, Src Port: 1033, 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

      3.72.0.18.in-addr.arpa: type PTR, class IN

         Name: 3.72.0.18.in-addr.arpa

         [Name Length: 22]

         [Label Count: 6]

         Type: PTR (domain name PoinTeR) (12)

         Class: IN (0x0001)

No.   Time   Source   Destination   Protocol Length Info

    16 2.048388   192.168.0.1   192.168.0.103   DNS   89   Standard query response 0xc7b3 A bitsy.mit.edu A 18.0.72.3

Frame 16: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 1025

Domain Name System (response)

   Transaction ID: 0xc7b3

[Expert Info (Warning/Protocol): DNS response retransmission. Original response in frame 13]

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

　bitsy.mit.edu: type A, class IN

　　Name: bitsy.mit.edu

　　[Name Length: 13]

　　[Label Count: 3]

　　Type: A (Host Address) (1)

　　Class: IN (0x0001)

Answers

　bitsy.mit.edu: type A, class IN, addr 18.0.72.3

　　Name: bitsy.mit.edu

　　Type: A (Host Address) (1)

　　Class: IN (0x0001)

　　Time to live: 1800 (30 minutes)

　　Data length: 4

　　Address: 18.0.72.3

[Retransmitted response. Original response in: 13]

[Retransmission: True]

No.	Time	Source	Destination	Protocol	Length	Info
36	4.029887	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr

Frame 36: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 18.0.72.3

User Datagram Protocol, Src Port: 1044, 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

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

      Name: www.aiit.or.kr

      [Name Length: 14]

      [Label Count: 4]

      Type: A (Host Address) (1)

      Class: IN (0x0001)

No.	Time	Source	Destination	Protocol	Length	Info
43	5.858289	192.168.0.103	192.168.0.1	DNS	79	Standard query 0xe086 A clients6.google.com

Frame 43: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 32930, Dst Port: 53

Domain Name System (query)

   Transaction ID: 0xe086

   Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

   clients6.google.com: type A, class IN

     Name: clients6.google.com

     [Name Length: 19]

     [Label Count: 3]

     Type: A (Host Address) (1)

     Class: IN (0x0001)

  [Response In: 44]

No.	Time	Source	Destination	Protocol	Length	Info
44	5.861086	192.168.0.1	192.168.0.103	DNS	119	Standard query response 0xe086 A clients6.google.com CNAME clients.l.google.com A 216.58.215.78

Frame 44: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2), Dst: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 32930

Domain Name System (response)

  Transaction ID: 0xe086

  Flags: 0x8180 Standard query response, No error

  Questions: 1

  Answer RRs: 2

  Authority RRs: 0

  Additional RRs: 0

  Queries

    clients6.google.com: type A, class IN

Name: clients6.google.com

[Name Length: 19]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

clients6.google.com: type CNAME, class IN, cname clients.l.google.com

Name: clients6.google.com

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 129 (2 minutes, 9 seconds)

Data length: 12

CNAME: clients.l.google.com

clients.l.google.com: type A, class IN, addr 216.58.215.78

Name: clients.l.google.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 129 (2 minutes, 9 seconds)

Data length: 4

Address: 216.58.215.78

[Request In: 43]

[Time: 0.002797000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
56	6.031348	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr

Frame 56: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 18.0.72.3

User Datagram Protocol, Src Port: 32932, 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

    www.aiit.or.kr: type AAAA, class IN

      Name: www.aiit.or.kr

      [Name Length: 14]

      [Label Count: 4]

      Type: AAAA (IPv6 Address) (28)

      Class: IN (0x0001)

No.	Time	Source	Destination	Protocol	Length	Info
61	8.033270	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr

Frame 61: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 18.0.72.3

User Datagram Protocol, Src Port: 32933, Dst Port: 53

Domain Name System (query)

  Transaction ID: 0x0004

  Flags: 0x0100 Standard query

  Questions: 1

  Answer RRs: 0

  Authority RRs: 0

Additional RRs: 0

Queries

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

    Name: www.aiit.or.kr

    [Name Length: 14]

    [Label Count: 4]

    Type: A (Host Address) (1)

    Class: IN (0x0001)

No.	Time	Source	Destination	Protocol	Length	Info
65	10.034574	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

Frame 65: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B00D5FF3-E366-47DF-A1CA-F139AE16F5AE}, id 0

Ethernet II, Src: 92:a8:43:5f:64:b6 (92:a8:43:5f:64:b6), Dst: Tp-LinkT_34:cf:c2 (c0:4a:00:34:cf:c2)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 18.0.72.3

User Datagram Protocol, Src Port: 32934, Dst Port: 53

Domain Name System (query)

  Transaction ID: 0x0005

  Flags: 0x0100 Standard query

  Questions: 1

  Answer RRs: 0

  Authority RRs: 0

  Additional RRs: 0

  Queries

    www.aiit.or.kr: type AAAA, class IN

      Name: www.aiit.or.kr

      [Name Length: 14]

      [Label Count: 4]

      Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Контрольні питання

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?

UPD (17), номер цільового порту запиту DNS – domain (53), номер вихідного порту відповіді DNS – 6858.

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

На 192.168.0.1. Так, є.

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

Типу «А» (Host Address), ні.

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

3 відповіді. Name, Type, Class, Time to live, Data length, Adress.

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.

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

Так.

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

Номер цільового порту запиту DNS – domain (53), номер вихідного порту відповіді DNS – 1045).

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

192.168.0.1, так, є.

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

Типу «А» (Host address), ні.

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

3 записи із відповідями. Кожна відповідь складається з: Name, Type, Class, Time to live, Data length, CNAME/Adress.

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

192.168.0.1, так.

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

Типу «A» (Host Address), ні.

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?

18 записів із відповідями: eur5.akam.net, use2.akam.net, use5.akam.net, usw2.akam.net, asia1.akam.net, asia2.akam.net, ns1-37.akam.net, ns1-173.akam.net, clients.l.google.com , clients6.google.com, catalog-public-service-prod06.ol.epicgames.com, catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com, catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com, catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com, catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com, catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com, catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com, catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com,, catalogv2-svc-prod06-pub-772318179.us-east-1.elb.amazonaws.com. Сервери були запропоновані за домогою адреси IP.

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?

192.168.0.1 – локальний сервер, 18.0.72.3- bitsy.mit.edu.

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

Типу PTR, ні.

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

Одна відповідь від першого сервера, жодної від другого. Відповідь складається з Name, Type, Class, Time to live, Data length, CNAME/Adress.

Висновки

Проаналізували деталі роботи протоколу DNS.