

Міністерство освіти і науки України Національний
технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Кафедра математичних методів системного аналізу

ЗВІТ

Про виконання лабораторних робіт з
дисципліни «Комп'ютерні мережі»

Виконав: ст. гр. ІС-ЗП93

Шаповалова О.І.

Прийняв: Кухарєв С.О.

Київ - 2020

Лабораторна робота 3.1

Хід роботи

Необхідно виконати наступні дії:

1. Очистіть кеш DNS-записів, для Windows-систем виконайте в терміналі
`ipconfig /flushdns`

1. Запустіть веб-браузер, очистіть кеш браузера:

2. Запустіть Wireshark, почніть захоплення пакетів.

3. Відкрийте за допомогою браузера одну із зазначених нижче адрес:

<http://www.ietf.org>

4. Зупиніть захоплення пакетів.

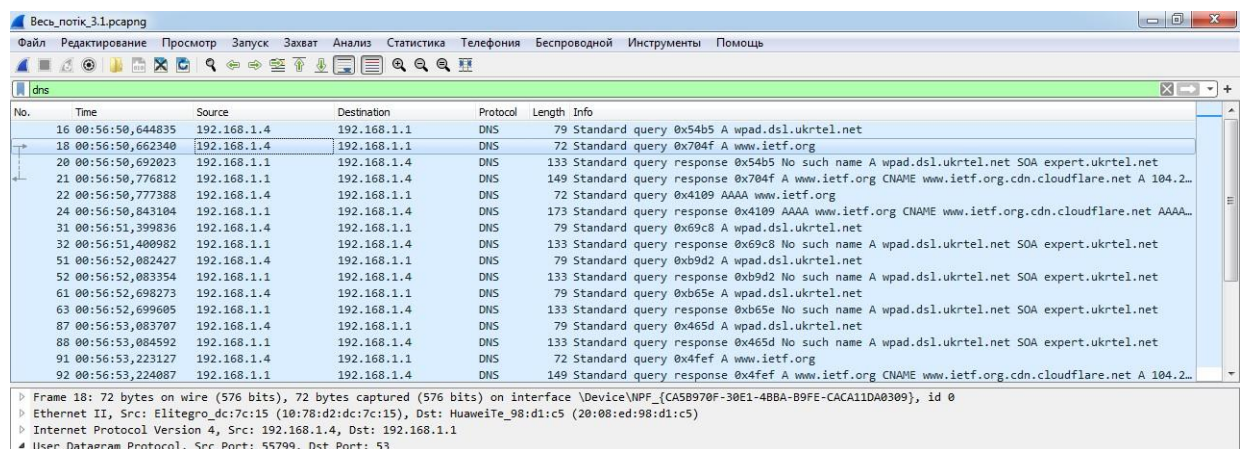
5. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/-).

6. Приготуйте відповіді на контрольні запитання 1-6, роздрукуйте необхідні для цього пакети.

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?

Запити і відповіді типу DNS використовують UDP протоколи. Номер цільового порта запиту – 53, номер вихідного порта відповіді DNS – 53



No.	Time	Source	Destination	Protocol	Length	Info
16	00:56:50,644835	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x54b5 A wpad.dsl.ukrtel.net
18	00:56:50,662340	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x704f A www.ietf.org
20	00:56:50,692023	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x54b5 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
21	00:56:50,776812	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0x704f A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.2...
22	00:56:50,777388	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4109 AAAA www.ietf.org
24	00:56:50,843104	192.168.1.1	192.168.1.4	DNS	173	Standard query response 0x4109 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA...
31	00:56:51,399836	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb65e A wpad.dsl.ukrtel.net
32	00:56:51,400982	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb65e No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
51	00:56:52,082427	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb9d2 A wpad.dsl.ukrtel.net
52	00:56:52,083354	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb9d2 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
61	00:56:52,698273	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb65e A wpad.dsl.ukrtel.net
63	00:56:52,699685	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb65e No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
87	00:56:53,083707	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x465d A wpad.dsl.ukrtel.net
88	00:56:53,084592	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x465d No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
91	00:56:53,223127	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4fef A www.ietf.org
92	00:56:53,224087	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0x4fef A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.2...

Frame 18: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{CA58970F-30E1-4BBA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 55799, Dst Port: 53

No.	Time	Source	Destination	Protocol	Length	Info
16	00:56:50,644835	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x54b5 A wpad.dsl.ukrtel.net
18	00:56:50,662340	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x704f A www.ietf.org
20	00:56:50,692023	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x54b5 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
21	00:56:50,776812	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0x704f A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.2...
22	00:56:50,777388	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4109 AAAA www.ietf.org
24	00:56:50,843104	192.168.1.1	192.168.1.4	DNS	173	Standard query response 0x4109 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA...
31	00:56:51,399836	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb69c8 A wpad.dsl.ukrtel.net
32	00:56:51,400982	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb69c8 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
51	00:56:52,082427	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb9d2 A wpad.dsl.ukrtel.net
52	00:56:52,083354	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb9d2 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
61	00:56:52,698273	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb65e A wpad.dsl.ukrtel.net
63	00:56:52,699605	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb65e No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
87	00:56:53,083707	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x465d A wpad.dsl.ukrtel.net
88	00:56:53,084592	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x465d No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
91	00:56:53,223127	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4fef A www.ietf.org
92	00:56:53,224087	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0x4fef A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.2...

Frame 21: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{CASB970F-30E1-4BBA-B9FE-CACA11DA0309}, id 0
 Ethernet II, Src: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5), Dst: Elitegro_dc7c:15 (10:78:d2:dc:7c:15)
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4
 User Datagram Protocol, Src Port: 53, Dst Port: 55799
 Domain Name System (response)

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

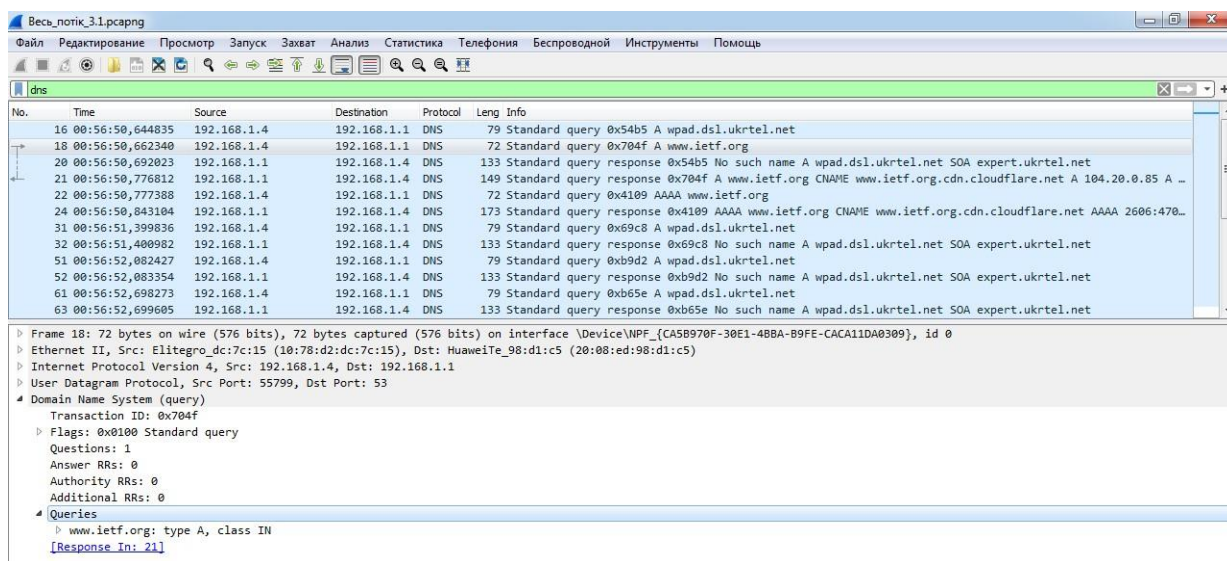
Запит DNS був відправлений за IP-адресою 192.168.1.4, який є адресою локального сервера DNS

No.	Time	Source	Destination	Protocol	Length	Info
16	00:56:50,644835	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x54b5 A wpad.dsl.ukrtel.net
18	00:56:50,662340	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x704f A www.ietf.org
20	00:56:50,692023	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x54b5 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
21	00:56:50,776812	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0x704f A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.2...
22	00:56:50,777388	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4109 AAAA www.ietf.org
24	00:56:50,843104	192.168.1.1	192.168.1.4	DNS	173	Standard query response 0x4109 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA...
31	00:56:51,399836	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb69c8 A wpad.dsl.ukrtel.net
32	00:56:51,400982	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb69c8 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
51	00:56:52,082427	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb9d2 A wpad.dsl.ukrtel.net
52	00:56:52,083354	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb9d2 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
61	00:56:52,698273	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb65e A wpad.dsl.ukrtel.net
63	00:56:52,699605	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb65e No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
87	00:56:53,083707	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x465d A wpad.dsl.ukrtel.net
88	00:56:53,084592	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x465d No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
91	00:56:53,223127	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4fef A www.ietf.org
92	00:56:53,224087	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0x4fef A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.2...

Frame 18: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{CASB970F-30E1-4BBA-B9FE-CACA11DA0309}, id 0
 Ethernet II, Src: Elitegro_dc7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
 Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
 User Datagram Protocol, Src Port: 55799, Dst Port: 53

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

Запит DNS визначається як 0x0100 «standard query», тобто стандартний запит. Запит і відповідь об'єднує спільний transaction ID, який для досліджуваного запиту складає 0x704f. Число записане у шістнадцятковій системі числення, у десятковій системі числення число має таке значення – 28751. Запит просить сервер надати таку інформацію про сайт www.ietf.org: type A, class IN



The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets, with packet 18 selected. The middle pane shows the details of packet 18, which is a DNS Standard query (type A, class IN) for the domain www.ietf.org. The bottom pane shows the raw packet data in hexadecimal and ASCII.

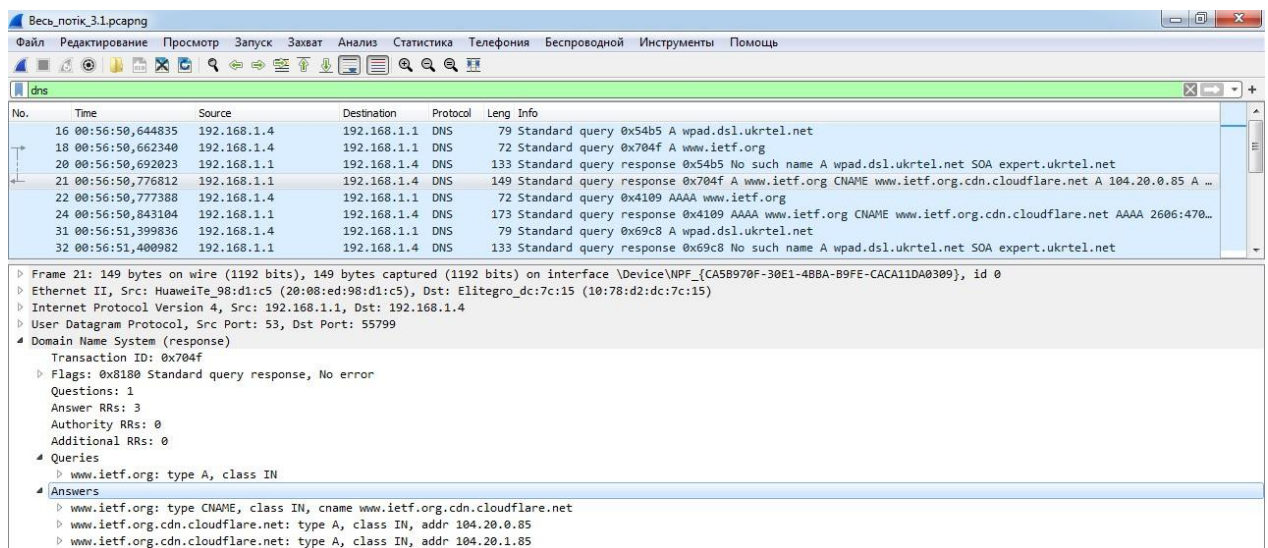
No.	Time	Source	Destination	Protocol	Leng	Info
16	00:56:50,644835	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x54b5 A wpad.dsl.ukrtel.net
18	00:56:50,662340	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x704f A www.ietf.org
20	00:56:50,692023	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x54b5 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
21	00:56:50,776812	192.168.1.4	192.168.1.4	DNS	149	Standard query response 0x704f A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A ...
22	00:56:50,777388	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4109 AAAA www.ietf.org
24	00:56:50,843104	192.168.1.1	192.168.1.4	DNS	173	Standard query response 0x4109 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:470...
31	00:56:51,399836	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x69c8 A wpad.dsl.ukrtel.net
32	00:56:51,400982	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x69c8 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
51	00:56:52,082427	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb9d2 A wpad.dsl.ukrtel.net
52	00:56:52,083354	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb9d2 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
61	00:56:52,698273	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb65e A wpad.dsl.ukrtel.net
63	00:56:52,699605	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb65e No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net

Frame 18: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{CA5B970F-30E1-4BBA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 55799, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x704f
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
[Response In: 21]

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

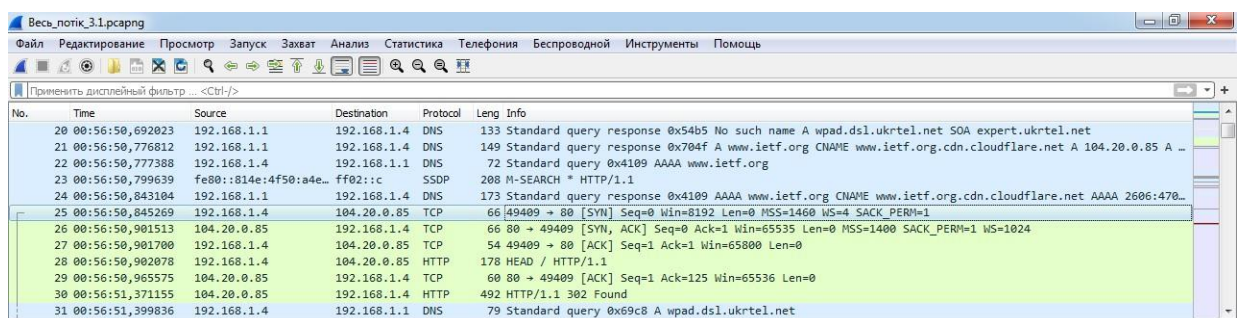
Сервер надає 3 відповіді. Відповідь містить характеристику адреси www.ietf.org та канонічного ім'я цієї адреси - www.ietf.org.cdn.cloudflare.net. Під час опису вказуються тип, клас і канонічне ім'я, адреси канонічного ім'я. У досліджуваній відповіді опис виконаний таким чином:

- 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 104.20.0.85
- www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85



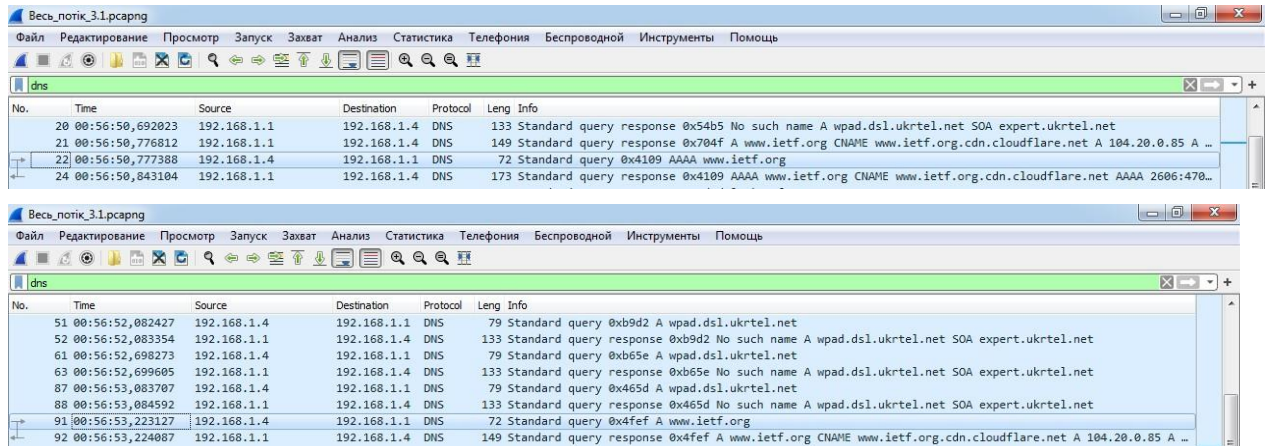
5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

Аналізуючи пакет 25, який є пакетом TCP [SYN] можна побачити, що цільова адреса пакету (104.20.0.85) була записано у другому рядку відповідей пакету відповіді сервера 21, який досліджувався в питанні №4



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

Так, крім запиту на адресу www.ietf.org, який був закладений у пакет №18, на цю адресу також були виконані запити, закладені в пакетах 22 і 91.



Весь_потік_3.1.pcapng

No.	Time	Source	Destination	Protocol	Leng	Info
20	00:56:50,692823	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x54b5 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
21	00:56:50,776812	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0x704f A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A ...
22	00:56:50,777388	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4109 AAAA www.ietf.org
24	00:56:50,843104	192.168.1.1	192.168.1.4	DNS	173	Standard query response 0x4109 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:470...

Весь_потік_3.1.pcapng

No.	Time	Source	Destination	Protocol	Leng	Info
51	00:56:52,082427	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb9d2 A wpad.dsl.ukrtel.net
52	00:56:52,083354	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb9d2 No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
61	00:56:52,698273	192.168.1.4	192.168.1.1	DNS	79	Standard query 0xb65e A wpad.dsl.ukrtel.net
63	00:56:52,699605	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0xb65e No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
87	00:56:53,083707	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x465d A wpad.dsl.ukrtel.net
88	00:56:53,084592	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x465d No such name A wpad.dsl.ukrtel.net SOA expert.ukrtel.net
91	00:56:53,223127	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4fef A www.ietf.org
92	00:56:53,224087	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0x4fef A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A ...

Запит на сайт www.ietf.org і відповідь з transaction ID
0x704f

No.	Time	Source	Destination	
	Protocol Length Info			
18	00:56:50,662340	192.168.1.4	192.168.1.1	DNS
72	Standard query 0x704f A www.ietf.org			

Frame 18: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{CA5B970F-30E1-4BBA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 55799, Dst Port: 53
Domain Name System (query)

No.	Time	Source	Destination	
	Protocol Length Info			
21	00:56:50,776812	192.168.1.1	192.168.1.4	DNS
149	Standard query response 0x704f A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85			

Frame 21: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{CA5B970F-30E1-4BBA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5), Dst: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4
User Datagram Protocol, Src Port: 53, Dst Port: 55799
Domain Name System (response)

Лабораторна робота 3.2

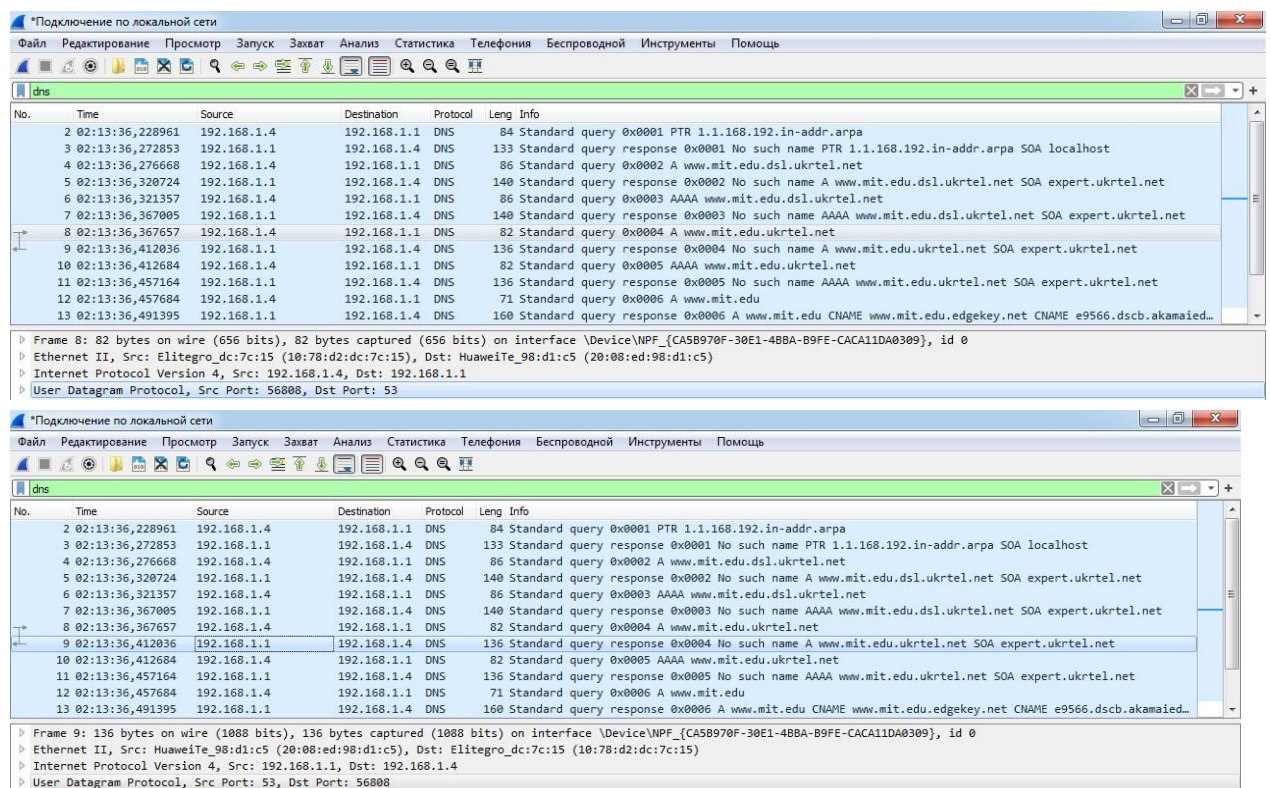
Хід роботи

1. Почніть захоплення пакетів.
2. Виконайте nslookup для домену www.mit.edu за допомогою команди nslookup www.mit.edu
3. Зупиніть захоплення пакетів.
4. Приготуйте відповіді на контрольні запитання 7-10, роздрукуйте необхідні для цього пакети. Утиліта nslookup відправляє три запити та отримує три відповіді, така поведінка є специфічною, тому слід ігнорувати перші два запити та перші дві відповіді.

Контрольні запитання

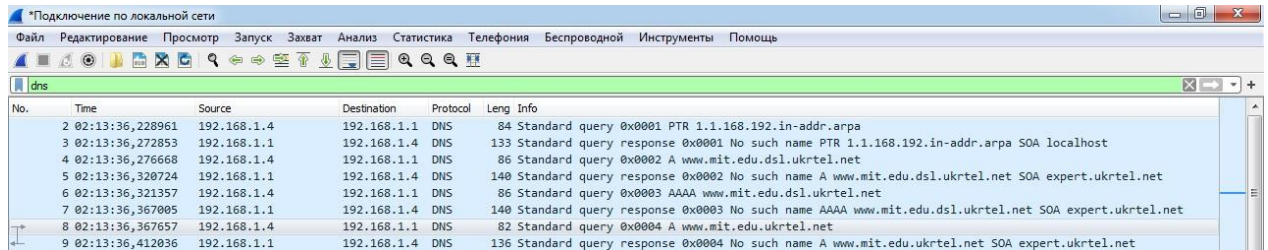
7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

Номер цільового порта із запитом – 53, номер вихідного порта відповіді – 53



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

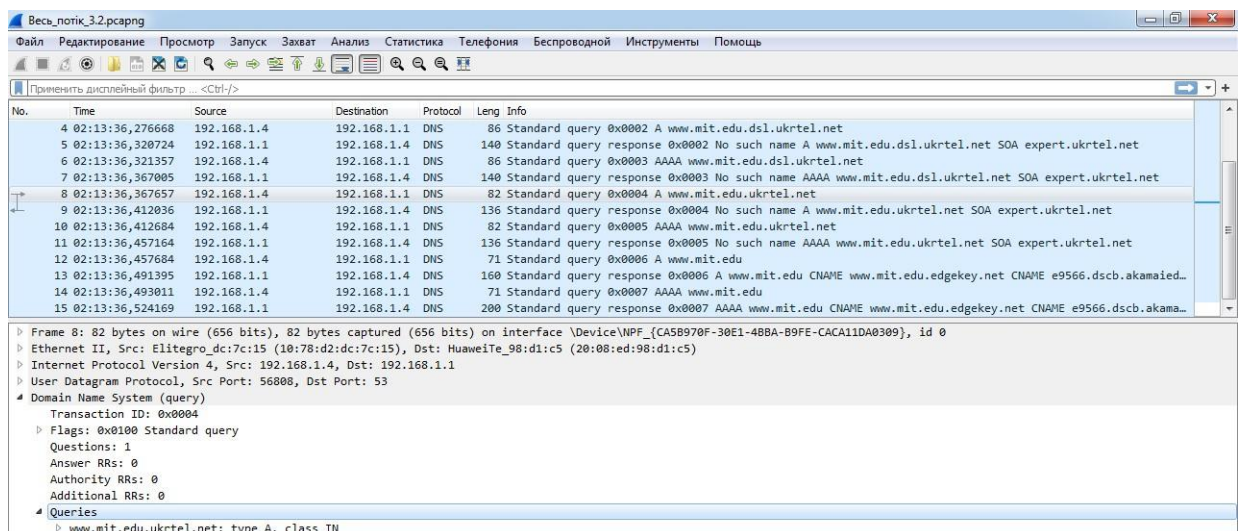
Запит DNS був направлений на адресу 192.168.1.1, яка є адресою локального DNS серверу за замовчанням



No.	Time	Source	Destination	Protocol	Length	Info
2	02:13:36,228961	192.168.1.4	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
3	02:13:36,272853	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
4	02:13:36,276668	192.168.1.4	192.168.1.1	DNS	86	Standard query 0x0002 A www.mit.edu.dsl.ukrtel.net
5	02:13:36,320724	192.168.1.1	192.168.1.4	DNS	140	Standard query response 0x0002 No such name A www.mit.edu.dsl.ukrtel.net SOA expert.ukrtel.net
6	02:13:36,321357	192.168.1.4	192.168.1.1	DNS	86	Standard query 0x0003 AAAA www.mit.edu.dsl.ukrtel.net
7	02:13:36,367005	192.168.1.1	192.168.1.4	DNS	140	Standard query response 0x0003 No such name AAAA www.mit.edu.dsl.ukrtel.net SOA expert.ukrtel.net
8	02:13:36,367657	192.168.1.4	192.168.1.1	DNS	82	Standard query 0x0004 A www.mit.edu.ukrtel.net
9	02:13:36,412036	192.168.1.1	192.168.1.4	DNS	136	Standard query response 0x0004 No such name A www.mit.edu.ukrtel.net SOA expert.ukrtel.net

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

Запит DNS визначається як 0x0100 «standard query», тобто стандартний запит. Запит і відповідь об'єднує спільний transaction ID, який для досліджуваного запиту складає 0x0004. Число записане у шістнадцятковій системі числення, у десятковій системі числення число має значення 4. Запит просить сервер надати таку інформацію про сайт www.mit.edu: type A, class IN



No.	Time	Source	Destination	Protocol	Length	Info
4	02:13:36,276668	192.168.1.4	192.168.1.1	DNS	86	Standard query 0x0002 A www.mit.edu.dsl.ukrtel.net
5	02:13:36,320724	192.168.1.1	192.168.1.4	DNS	140	Standard query response 0x0002 No such name A www.mit.edu.dsl.ukrtel.net SOA expert.ukrtel.net
6	02:13:36,321357	192.168.1.4	192.168.1.1	DNS	86	Standard query 0x0003 AAAA www.mit.edu.dsl.ukrtel.net
7	02:13:36,367005	192.168.1.1	192.168.1.4	DNS	140	Standard query response 0x0003 No such name AAAA www.mit.edu.dsl.ukrtel.net SOA expert.ukrtel.net
8	02:13:36,367657	192.168.1.4	192.168.1.1	DNS	82	Standard query 0x0004 A www.mit.edu.ukrtel.net
9	02:13:36,412036	192.168.1.1	192.168.1.4	DNS	136	Standard query response 0x0004 No such name A www.mit.edu.ukrtel.net SOA expert.ukrtel.net
10	02:13:36,412684	192.168.1.4	192.168.1.1	DNS	82	Standard query 0x0005 AAAA www.mit.edu.ukrtel.net
11	02:13:36,457164	192.168.1.1	192.168.1.4	DNS	136	Standard query response 0x0005 No such name AAAA www.mit.edu.ukrtel.net SOA expert.ukrtel.net
12	02:13:36,457684	192.168.1.4	192.168.1.1	DNS	71	Standard query 0x0006 A www.mit.edu
13	02:13:36,491395	192.168.1.1	192.168.1.4	DNS	160	Standard query response 0x0006 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaied...
14	02:13:36,493011	192.168.1.4	192.168.1.1	DNS	71	Standard query 0x0007 AAAA www.mit.edu
15	02:13:36,524169	192.168.1.1	192.168.1.4	DNS	200	Standard query response 0x0007 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaied...

Frame 8: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{C45B970F-30E1-4BBA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 56808, 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.mit.edu.ukrtel.net: type A, class IN

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

Для розкриття цього питання розглянемо запит, закладений в пакет 12, і відповідь, закладену в пакет 13. Було надано 3 відповіді. Відповідь містить характеристику адреси www.mit.edu та канонічного ім'я цієї адреси - www.mit.edu.edgekey.net. Під час опису вказуються тип, клас, канонічне ім'я та деякі інші адреси. У досліджуваній відповіді опис виконаний таким чином:

- 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 A, class IN, addr 104.104.191.7

12	02:13:36,457684	192.168.1.4	192.168.1.1	DNS	71 Standard query 0x0006 A www.mit.edu
13	02:13:36,491395	192.168.1.1	192.168.1.4	DNS	160 Standard query response 0x0006 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net
14	02:13:36,493011	192.168.1.4	192.168.1.1	DNS	71 Standard query 0x0007 AAAA www.mit.edu
15	02:13:36,524169	192.168.1.1	192.168.1.4	DNS	200 Standard query response 0x0007 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net

Frame 13:	160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{C45B970F-30E1-4BBA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src:	HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5), Dst: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15)
Internet Protocol Version 4, Src:	192.168.1.1, Dst: 192.168.1.4
User Datagram Protocol, Src Port:	53, Dst Port: 56810
Domain Name System (response)	
Transaction ID:	0x0006
Flags:	0x0100 Standard query response, No error
Questions:	1
Answer RRs:	3
Authority RRs:	0
Additional RRs:	0
Queries	
Answers	
www.mit.edu:	type A, class IN
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 A, class IN, addr 104.104.191.7
[Request in: 12]	
[Time: 0.033711000 seconds]	

Лабораторна робота 3.3

Хід роботи

1. Почніть захоплення пакетів.
2. Виконайте nslookup для домену www.mit.edu за допомогою команди nslookup -type=NS mit.edu

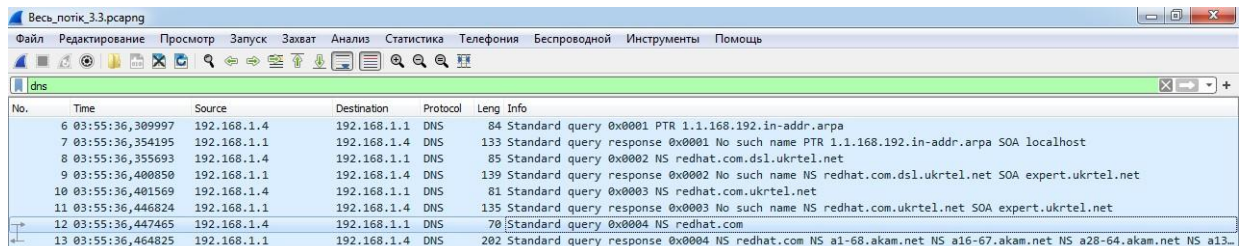
Посилання на адресу mit.edu викликає помилку типу DNS request timed out, замість неї використаємо адресу redhat.com, тобто команда для роботи буде виглядати таким чином: nslookup -type=NS redhat.com

3. Зупиніть захоплення пакетів.
4. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети.

Контрольні запитання

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

Запит DNS був направлений на адресу 192.168.1.1, яка є адресою локального DNS серверу за замовченням



The screenshot shows a Wireshark capture of network traffic on the 'dns' filter. The packet list shows several DNS queries and responses between 192.168.1.1 and 192.168.1.4. The details pane for the selected packet (No. 13) shows a 'Standard query response' for the PTR record 1.1.168.192.in-addr.arpa, indicating the local DNS server is responding.

No.	Time	Source	Destination	Protocol	Length	Info
6	03:55:36,309997	192.168.1.4	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
7	03:55:36,354195	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
8	03:55:36,355693	192.168.1.4	192.168.1.1	DNS	85	Standard query 0x0002 NS redhat.com.dsl.ukrtel.net
9	03:55:36,400850	192.168.1.1	192.168.1.4	DNS	139	Standard query response 0x0002 No such name NS redhat.com.dsl.ukrtel.net SOA expert.ukrtel.net
10	03:55:36,401569	192.168.1.4	192.168.1.1	DNS	81	Standard query 0x0003 NS redhat.com.ukrtel.net
11	03:55:36,446824	192.168.1.1	192.168.1.4	DNS	135	Standard query response 0x0003 No such name NS redhat.com.ukrtel.net SOA expert.ukrtel.net
12	03:55:36,447465	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x0004 NS redhat.com
13	03:55:36,464825	192.168.1.1	192.168.1.4	DNS	202	Standard query response 0x0004 NS redhat.com NS a1-68.akam.net NS a16-67.akam.net NS a28-64.akam.net NS a13-

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

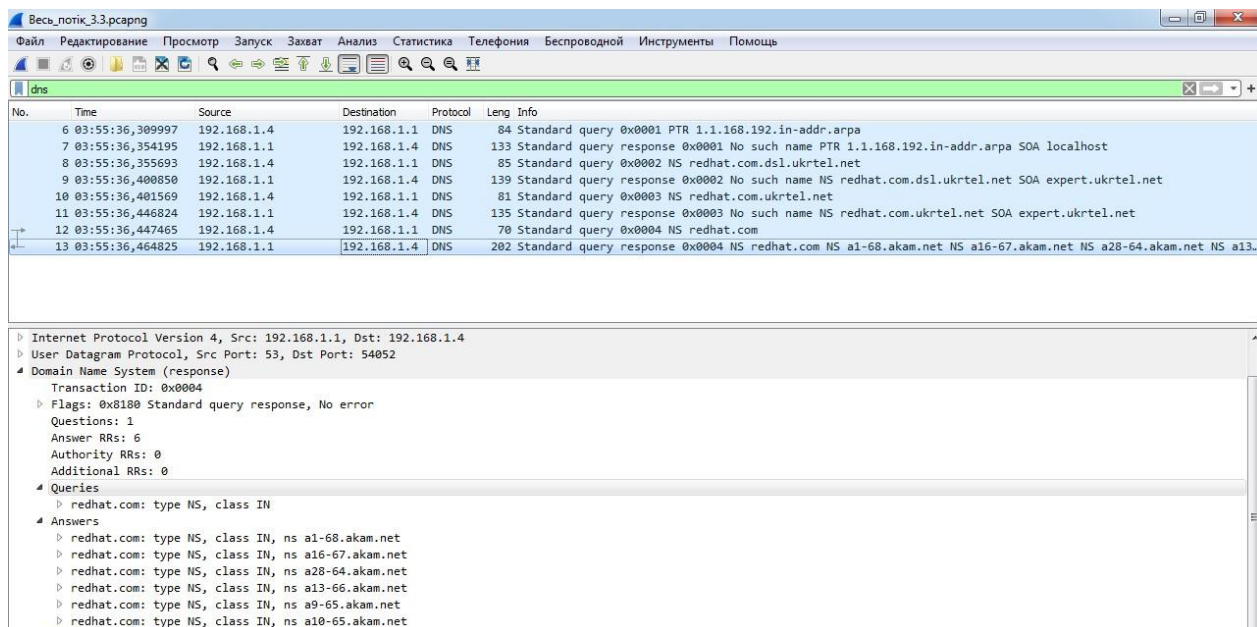
Запит DNS визначається як 0x0100 «standard query», тобто стандартний запит. Запит і відповідь об'єднує спільний transaction ID, який для досліджуваного запиту складає 0x0004. Число записане у шістнадцятковій системі числення, у десятковій системі числення число має значення 4. Запит вимагає від сервера надати такі данні сайту redhat.com: type NS, class IN

The screenshot shows the Wireshark interface with a packet list and packet details pane. The packet list shows a DNS query (packet 12) and its response (packet 13). The packet details pane for packet 13 shows the DNS response structure, including the transaction ID (0x0004), flags (0x0100), and the query details (redhat.com: type NS, class IN).

No.	Time	Source	Destination	Protocol	Leng	Info
6	03:55:36,309997	192.168.1.4	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
7	03:55:36,354195	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
8	03:55:36,355693	192.168.1.4	192.168.1.1	DNS	85	Standard query 0x0002 NS redhat.com.dsl.ukrtel.net
9	03:55:36,400850	192.168.1.1	192.168.1.4	DNS	139	Standard query response 0x0002 No such name NS redhat.com.dsl.ukrtel.net SOA expert.ukrtel.net
10	03:55:36,401569	192.168.1.4	192.168.1.1	DNS	81	Standard query 0x0003 NS redhat.com.ukrtel.net
11	03:55:36,446824	192.168.1.1	192.168.1.4	DNS	135	Standard query response 0x0003 No such name NS redhat.com.ukrtel.net SOA expert.ukrtel.net
12	03:55:36,447465	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x0004 NS redhat.com
13	03:55:36,464825	192.168.1.1	192.168.1.4	DNS	202	Standard query response 0x0004 NS redhat.com NS a1-68.akam.net NS a16-67.akam.net NS a28-64.akam.net NS a13-

Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{CA5B970F-30E1-4B8A-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 54052, 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
redhat.com: type NS, class IN
[Response In: 13]

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?



No.	Time	Source	Destination	Protocol	Length	Info
6	03:55:36,309997	192.168.1.4	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
7	03:55:36,354195	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
8	03:55:36,355693	192.168.1.4	192.168.1.1	DNS	85	Standard query 0x0002 NS redhat.com.dsl.ukrtel.net
9	03:55:36,400850	192.168.1.1	192.168.1.4	DNS	139	Standard query response 0x0002 No such name NS redhat.com.dsl.ukrtel.net SOA expert.ukrtel.net
10	03:55:36,401569	192.168.1.4	192.168.1.1	DNS	81	Standard query 0x0003 NS redhat.com.ukrtel.net
11	03:55:36,446824	192.168.1.1	192.168.1.4	DNS	135	Standard query response 0x0003 No such name NS redhat.com.ukrtel.net SOA expert.ukrtel.net
12	03:55:36,447465	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x0004 NS redhat.com
13	03:55:36,464825	192.168.1.1	192.168.1.4	DNS	202	Standard query response 0x0004 NS redhat.com NS a1-68.akam.net NS a16-67.akam.net NS a28-64.akam.net NS a13-

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

User Datagram Protocol, Src Port: 53, Dst Port: 54052

Domain Name System (response)

Transaction ID: 0x0004

Flags: 0x8100 Standard query response, No error

Questions: 1

Answer RRs: 6

Authority RRs: 0

Additional RRs: 0

Queries

redhat.com: type NS, class IN

Answers

redhat.com: type NS, class IN, ns a1-68.akam.net

redhat.com: type NS, class IN, ns a16-67.akam.net

redhat.com: type NS, class IN, ns a28-64.akam.net

redhat.com: type NS, class IN, ns a13-66.akam.net

redhat.com: type NS, class IN, ns a9-65.akam.net

redhat.com: type NS, class IN, ns a10-65.akam.net

Відповідь містить характеристику адреси www.redhat.com та список адрес серверів сайту. На запит було надано 6 відповідей. У досліджуваній відповіді опис виконаний таким чином:

- redhat.com: type NS, class IN, ns a1-68.akam.net
- redhat.com: type NS, class IN, ns a16-67.akam.net
- redhat.com: type NS, class IN, ns a28-64.akam.net
- redhat.com: type NS, class IN, ns a13-66.akam.net
- redhat.com: type NS, class IN, ns a9-65.akam.net
- redhat.com: type NS, class IN, ns a10-65.akam.net

Сервери були запропоновані лише з використанням доменних імен

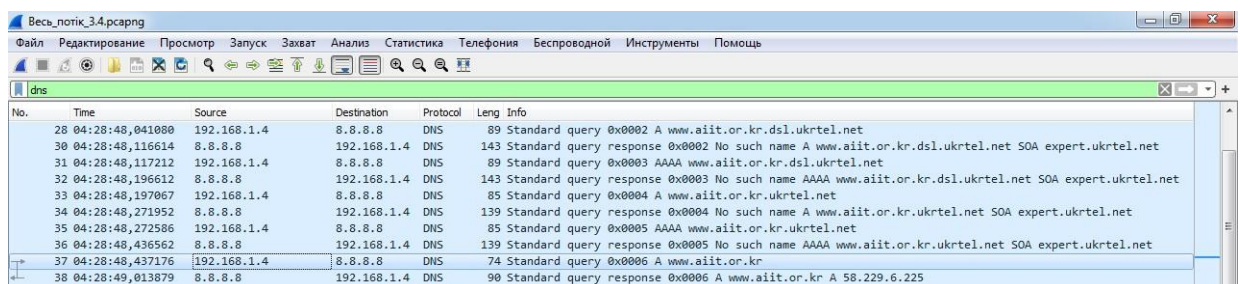
Лабораторна робота 3.4

1. Почніть захоплення пакетів.
2. Виконайте nslookup для домену www.mit.edu за допомогою команди nslookup www.aiit.or.kr bitsy.mit.edu
3. Посилання на адресу bitsy.mit.edu викликає помилку типу DNS request timed out, замість неї використаємо безкоштовний DNS сервер від Google з IP адресою 8.8.8.8 , тобто команда для роботи буде виглядати таким чином: nslookup www.aiit.or.kr 8.8.8.8.
4. Зупиніть захоплення пакетів.
5. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.
6. Закрийте Wireshark.

3.2. Контрольні запитання

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?

DNS запит був направлений на IP-адресу 8.8.8.8, яка не є адресою локального DNS серверу. Ця адреса відповідає адресі безкоштовного DNS серверу від Google. Доменне ім'я серверу не було знайдене, найбільш вірогідно, що воно відсутнє.



No.	Time	Source	Destination	Protocol	Leng	Info
28	04:28:48,041080	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48,116614	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48,117212	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48,196612	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48,197067	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48,271952	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48,272586	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48,436562	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0006 A www.aiit.or.kr
38	04:28:49,013879	8.8.8.8	192.168.1.4	DNS	90	Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225

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

Запит DNS визначається як 0x0100 «standard query», тобто стандартний запит. Запит і відповідь об'єднує спільний transaction ID, який для досліджуваного запиту складає 0x0006. Число записане у шістнадцятковій системі числення, у десятковій системі числення число має значення 6. Запит вимагає від сервера надати такі данні сайту www.aiit.or.kr: type A, class IN

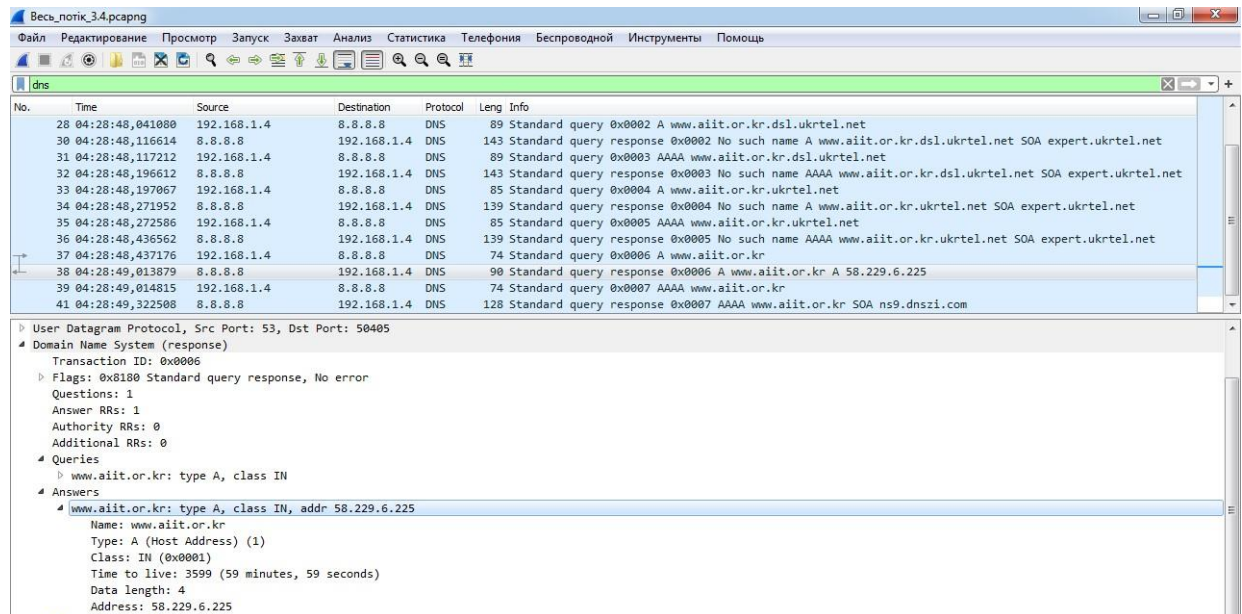
The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets, with packet 37 selected. The middle pane shows the details of packet 37, which is a DNS Standard query. The bottom pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Leng	Info
28	04:28:48,041080	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48,116614	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48,117212	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48,196612	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48,197067	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48,271952	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48,272586	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48,436562	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0006 A www.aiit.or.kr
38	04:28:49,013879	8.8.8.8	192.168.1.4	DNS	90	Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225
39	04:28:49,014815	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0007 AAAA www.aiit.or.kr
41	04:28:49,322508	8.8.8.8	192.168.1.4	DNS	128	Standard query response 0x0007 AAAA www.aiit.or.kr SOA ns9.dnszi.com

Frame 37: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CA5B970F-30E1-48BA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 50405, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0006
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.aiit.or.kr: type A, class IN

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

На запит була надана одна відповідь, що містила назву адреси, що вимагалась, її тип, клас, адреса серверу. У випадку досліджуваної відповіді була надана така інформація щодо сайту www.aiit.or.kr: type A, class IN, addr 58.229.6.225

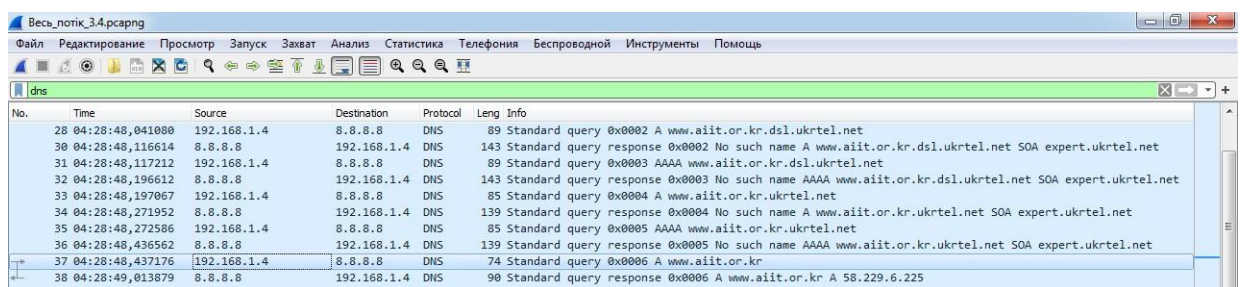


7. Виконайте nslookup для домену www.mit.edu за допомогою команди nslookup www.aiit.or.kr bitsy.mit.edu
8. Посилання на адресу bitsy.mit.edu викликає помилку типу DNS request timed out, замість неї використаємо безкоштовний DNS сервер від Google з IP адресою 8.8.8.8 , тобто команда для роботи буде виглядати таким чином: nslookup www.aiit.or.kr 8.8.8.8.
9. Зупиніть захоплення пакетів.
10. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.
11. Закрийте Wireshark.

3.2. Контрольні запитання

17. 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?

DNS запит був направлений на IP-адресу 8.8.8.8, яка не є адресою локального DNS серверу. Ця адреса відповідає адресі безкоштовного DNS серверу від Google. Доменне ім'я серверу не було знайдене, найбільш вірогідно, що воно відсутнє.



No.	Time	Source	Destination	Protocol	Length	Info
28	04:28:48,041080	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48,116614	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48,117212	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48,196612	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48,197067	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48,271952	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48,272586	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48,436562	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0006 A www.aiit.or.kr
38	04:28:49,013879	8.8.8.8	192.168.1.4	DNS	90	Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225

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

Запит DNS визначається як 0x0100 «standard query», тобто стандартний запит. Запит і відповідь об'єднує спільний transaction ID, який для досліджуваного запиту складає 0x0006. Число записане у шістнадцятковій системі числення, у десятковій системі числення число має значення 6. Запит вимагає від сервера надати такі данні сайту www.aiit.or.kr: type A, class IN

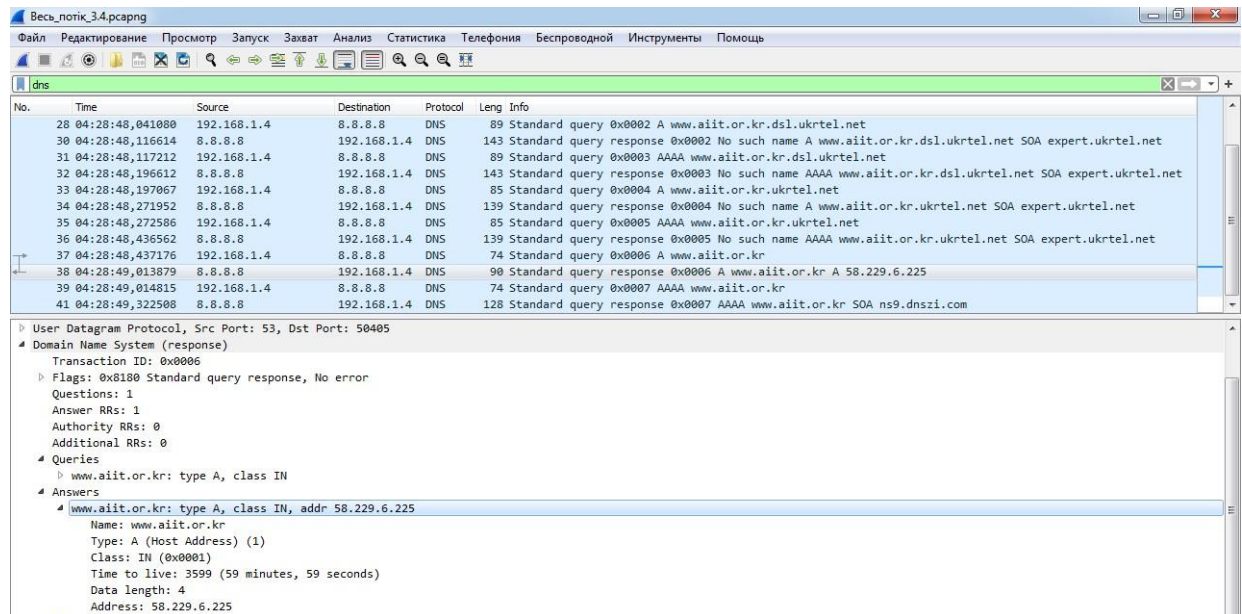
The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets, with packet 37 selected. The middle pane shows the details of packet 37, which is a DNS Standard query. The bottom pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Leng	Info
28	04:28:48,041080	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48,116614	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48,117212	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48,196612	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48,197067	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48,271952	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48,272586	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48,436562	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0006 A www.aiit.or.kr
38	04:28:49,013879	8.8.8.8	192.168.1.4	DNS	90	Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225
39	04:28:49,014815	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0007 AAAA www.aiit.or.kr
41	04:28:49,322508	8.8.8.8	192.168.1.4	DNS	128	Standard query response 0x0007 AAAA www.aiit.or.kr SOA ns9.dnszi.com

Frame 37: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CA5B970F-30E1-48BA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 50405, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0006
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.aiit.or.kr: type A, class IN

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

На запит була надана одна відповідь, що містила назву адреси, що вимагалась, її тип, клас, адреса серверу. У випадку досліджуваної відповіді була надана така інформація щодо сайту www.aiit.or.kr: type A, class IN, addr 58.229.6.225



5. захоплення пакетів.

6. Виконайте nslookup для домену www.mit.edu за допомогою команди nslookup -type=NS mit.edu

Посилання на адресу mit.edu викликає помилку типу DNS request timed out, замість неї використаємо адресу redhat.com, тобто команда для роботи буде виглядати таким чином: nslookup -type=NS redhat.com

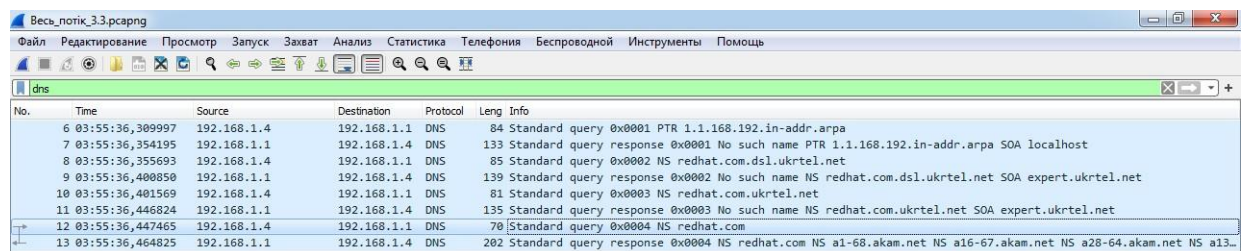
7. Зупиніть захоплення пакетів.

8. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети.

Контрольні запитання

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

Запит DNS був направлений на адресу 192.168.1.1, яка є адресою локального DNS серверу за замовченням



The screenshot shows a Wireshark capture of network traffic on the 'dns' filter. The table below represents the data visible in the packet list pane.

No.	Time	Source	Destination	Protocol	Leng	Info
6	03:55:36,309997	192.168.1.4	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
7	03:55:36,354195	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
8	03:55:36,355693	192.168.1.4	192.168.1.1	DNS	85	Standard query 0x0002 NS redhat.com.dsl.ukrtel.net
9	03:55:36,400850	192.168.1.1	192.168.1.4	DNS	139	Standard query response 0x0002 No such name NS redhat.com.dsl.ukrtel.net SOA expert.ukrtel.net
10	03:55:36,401569	192.168.1.4	192.168.1.1	DNS	81	Standard query 0x0003 NS redhat.com.ukrtel.net
11	03:55:36,446824	192.168.1.1	192.168.1.4	DNS	135	Standard query response 0x0003 No such name NS redhat.com.ukrtel.net SOA expert.ukrtel.net
12	03:55:36,447465	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x0004 NS redhat.com
13	03:55:36,464825	192.168.1.1	192.168.1.4	DNS	202	Standard query response 0x0004 NS redhat.com NS a1-68.akam.net NS a16-67.akam.net NS a28-64.akam.net NS a13-

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

Запит DNS визначається як 0x0100 «standard query», тобто стандартний запит. Запит і відповідь об'єднує спільний transaction ID, який для досліджуваного запиту складає 0x0004. Число записане у шістнадцятковій системі числення, у десятковій системі числення число має значення 4. Запит вимагає від сервера надати такі данні сайту redhat.com: type NS, class IN

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets, with packet 13 selected. The middle pane shows the details of the selected packet, which is a DNS Standard query response. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Leng	Info
6	03:55:36,309997	192.168.1.4	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
7	03:55:36,354195	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
8	03:55:36,355693	192.168.1.4	192.168.1.1	DNS	85	Standard query 0x0002 NS redhat.com.dsl.ukrtel.net
9	03:55:36,400850	192.168.1.1	192.168.1.4	DNS	139	Standard query response 0x0002 No such name NS redhat.com.dsl.ukrtel.net SOA expert.ukrtel.net
10	03:55:36,401569	192.168.1.4	192.168.1.1	DNS	81	Standard query 0x0003 NS redhat.com.ukrtel.net
11	03:55:36,446824	192.168.1.1	192.168.1.4	DNS	135	Standard query response 0x0003 No such name NS redhat.com.ukrtel.net SOA expert.ukrtel.net
12	03:55:36,447465	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x0004 NS redhat.com
13	03:55:36,464825	192.168.1.1	192.168.1.4	DNS	202	Standard query response 0x0004 NS redhat.com NS a1-68.akam.net NS a16-67.akam.net NS a28-64.akam.net NS a13-

Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{CA5B970F-30E1-4B8A-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 54052, 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
redhat.com: type NS, class IN
[Response In: 13]

16. 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?

No.	Time	Source	Destination	Protocol	Length	Info
6	03:55:36.309997	192.168.1.4	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
7	03:55:36.354195	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
8	03:55:36.355693	192.168.1.4	192.168.1.1	DNS	85	Standard query 0x0002 NS redhat.com.dsl.ukrtel.net
9	03:55:36.400850	192.168.1.1	192.168.1.4	DNS	139	Standard query response 0x0002 No such name NS redhat.com.dsl.ukrtel.net SOA expert.ukrtel.net
10	03:55:36.401569	192.168.1.4	192.168.1.1	DNS	81	Standard query 0x0003 NS redhat.com.ukrtel.net
11	03:55:36.446824	192.168.1.1	192.168.1.4	DNS	135	Standard query response 0x0003 No such name NS redhat.com.ukrtel.net SOA expert.ukrtel.net
12	03:55:36.447465	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x0004 NS redhat.com
13	03:55:36.464825	192.168.1.1	192.168.1.4	DNS	202	Standard query response 0x0004 NS redhat.com NS a1-68.akam.net NS a16-67.akam.net NS a28-64.akam.net NS a13-

```

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4
User Datagram Protocol, Src Port: 53, Dst Port: 54052
Domain Name System (response)
  Transaction ID: 0x0004
  Flags: 0x8100 Standard query response, No error
  Questions: 1
  Answer RRs: 6
  Authority RRs: 0
  Additional RRs: 0
  Queries
    redhat.com: type NS, class IN
  Answers
    redhat.com: type NS, class IN, ns a1-68.akam.net
    redhat.com: type NS, class IN, ns a16-67.akam.net
    redhat.com: type NS, class IN, ns a28-64.akam.net
    redhat.com: type NS, class IN, ns a13-66.akam.net
    redhat.com: type NS, class IN, ns a9-65.akam.net
    redhat.com: type NS, class IN, ns a10-65.akam.net
  
```

Відповідь містить характеристику адреси www.redhat.com та список адрес серверів сайту. На запит було надано 6 відповідей. У досліджуваній відповіді опис виконаний таким чином:

- redhat.com: type NS, class IN, ns a1-68.akam.net
- redhat.com: type NS, class IN, ns a16-67.akam.net
- redhat.com: type NS, class IN, ns a28-64.akam.net
- redhat.com: type NS, class IN, ns a13-66.akam.net
- redhat.com: type NS, class IN, ns a9-65.akam.net
- redhat.com: type NS, class IN, ns a10-65.akam.net

Сервери були запропоновані лише з використанням доменних імен

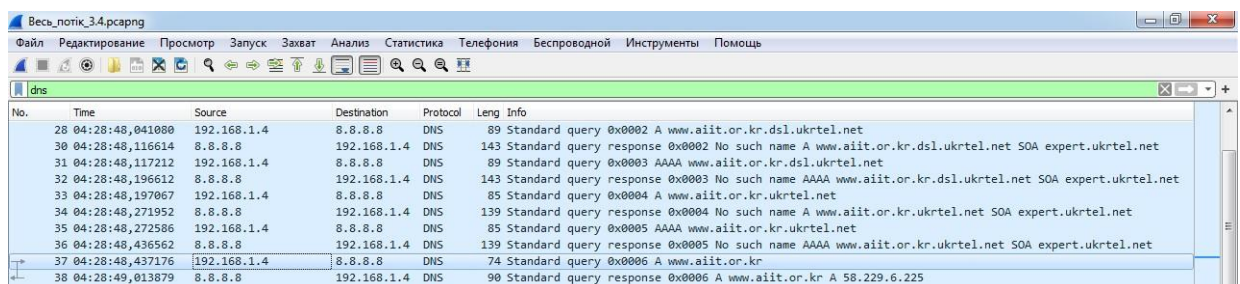
Лабораторна робота 3.4

12. Почніть захоплення пакетів.
13. Виконайте nslookup для домену `www.mit.edu` за допомогою команди `nslookup www.aiit.or.kr bitsy.mit.edu`
14. Посилання на адресу `bitsy.mit.edu` викликає помилку типу `DNS request timed out`, замість неї використаємо безкоштовний DNS сервер від Google з IP адресою `8.8.8.8`, тобто команда для роботи буде виглядати таким чином: `nslookup www.aiit.or.kr 8.8.8.8`.
15. Зупиніть захоплення пакетів.
16. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.
17. Закрийте Wireshark.

3.2. Контрольні запитання

20. 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?

DNS запит був направлений на IP-адресу `8.8.8.8`, яка не є адресою локального DNS серверу. Ця адреса відповідає адресі безкоштовного DNS серверу від Google. Доменне ім'я серверу не було знайдене, найбільш вірогідно, що воно відсутнє.



No.	Time	Source	Destination	Protocol	Info
28	04:28:48.041080	192.168.1.4	8.8.8.8	DNS	89 Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48.116614	8.8.8.8	192.168.1.4	DNS	143 Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48.117212	192.168.1.4	8.8.8.8	DNS	89 Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48.196612	8.8.8.8	192.168.1.4	DNS	143 Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48.197067	192.168.1.4	8.8.8.8	DNS	85 Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48.271952	8.8.8.8	192.168.1.4	DNS	139 Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48.272586	192.168.1.4	8.8.8.8	DNS	85 Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48.436562	8.8.8.8	192.168.1.4	DNS	139 Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48.437176	192.168.1.4	8.8.8.8	DNS	74 Standard query 0x0006 A www.aiit.or.kr
38	04:28:49.013879	8.8.8.8	192.168.1.4	DNS	90 Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225

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

Запит DNS визначається як 0x0100 «standard query», тобто стандартний запит. Запит і відповідь об'єднує спільний transaction ID, який для досліджуваного запиту складає 0x0006. Число записане у шістнадцятковій системі числення, у десятковій системі числення число має значення 6. Запит вимагає від сервера надати такі данні сайту www.aiit.or.kr: type A, class IN

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets, with packet 37 selected. The middle pane shows the details of packet 37, which is a DNS Standard query (type A, class IN) for the domain www.aiit.or.kr. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Leng	Info
28	04:28:48,041080	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48,116614	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48,117212	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48,196612	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48,197067	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48,271952	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48,272586	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48,436562	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0006 A www.aiit.or.kr
38	04:28:49,013879	8.8.8.8	192.168.1.4	DNS	90	Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225
39	04:28:49,014815	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0007 AAAA www.aiit.or.kr
41	04:28:49,322508	8.8.8.8	192.168.1.4	DNS	128	Standard query response 0x0007 AAAA www.aiit.or.kr SOA ns9.dnszi.com

Frame 37: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CA5B970F-30E1-48BA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 50405, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0006
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.aiit.or.kr: type A, class IN

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

На запит була надана одна відповідь, що містила назву адреси, що вимагалась, її тип, клас, адреса серверу. У випадку досліджуваної відповіді була надана така інформація щодо сайту `www.aiit.or.kr`: type A, class IN, addr 58.229.6.225

Весь_поток_3.4.pcapng

Файл Редактирование Просмотр Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Leng	Info
28	04:28:48,041080	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48,116614	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48,117212	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48,196612	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48,197067	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48,271952	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48,272586	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48,436562	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0006 A www.aiit.or.kr
38	04:28:49,013879	8.8.8.8	192.168.1.4	DNS	90	Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225
39	04:28:49,014815	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0007 AAAA www.aiit.or.kr
41	04:28:49,322508	8.8.8.8	192.168.1.4	DNS	128	Standard query response 0x0007 AAAA www.aiit.or.kr SOA ns9.dnszi.com

User Datagram Protocol, Src Port: 53, Dst Port: 50405

Domain Name System (response)

Transaction ID: 0x0006

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

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

Answers

www.aiit.or.kr: type A, class IN, addr 58.229.6.225

Name: www.aiit.or.kr

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 3599 (59 minutes, 59 seconds)

Data length: 4

Address: 58.229.6.225

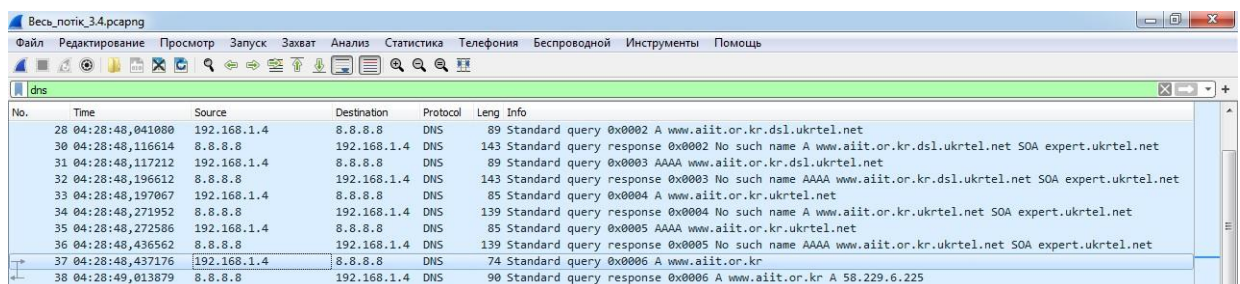
Лабораторна робота 3.4

18. Почніть захоплення пакетів.
19. Виконайте nslookup для домену `www.mit.edu` за допомогою команди `nslookup www.aiit.or.kr bitsy.mit.edu`
20. Посилання на адресу `bitsy.mit.edu` викликає помилку типу `DNS request timed out`, замість неї використаємо безкоштовний DNS сервер від Google з IP адресою `8.8.8.8`, тобто команда для роботи буде виглядати таким чином: `nslookup www.aiit.or.kr 8.8.8.8`.
21. Зупиніть захоплення пакетів.
22. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.
23. Закрийте Wireshark.

3.2. Контрольні запитання

23. 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?

DNS запит був направлений на IP-адресу `8.8.8.8`, яка не є адресою локального DNS серверу. Ця адреса відповідає адресі безкоштовного DNS серверу від Google. Доменне ім'я серверу не було знайдене, найбільш вірогідно, що воно відсутнє.



No.	Time	Source	Destination	Protocol	Info
28	04:28:48,041080	192.168.1.4	8.8.8.8	DNS	89 Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48,116614	8.8.8.8	192.168.1.4	DNS	143 Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48,117212	192.168.1.4	8.8.8.8	DNS	89 Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48,196612	8.8.8.8	192.168.1.4	DNS	143 Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48,197067	192.168.1.4	8.8.8.8	DNS	85 Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48,271952	8.8.8.8	192.168.1.4	DNS	139 Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48,272586	192.168.1.4	8.8.8.8	DNS	85 Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48,436562	8.8.8.8	192.168.1.4	DNS	139 Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS	74 Standard query 0x0006 A www.aiit.or.kr
38	04:28:49,013879	8.8.8.8	192.168.1.4	DNS	90 Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225

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

Запит DNS визначається як 0x0100 «standard query», тобто стандартний запит. Запит і відповідь об'єднує спільний transaction ID, який для досліджуваного запиту складає 0x0006. Число записане у шістнадцятковій системі числення, у десятковій системі числення число має значення 6. Запит вимагає від сервера надати такі данні сайту www.aiit.or.kr: type A, class IN

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets, with packet 37 selected. The middle pane shows the details of packet 37, which is a DNS Standard query. The bottom pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
28	04:28:48,041080	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48,116614	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48,117212	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48,196612	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48,197067	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48,271952	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48,272586	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48,436562	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0006 A www.aiit.or.kr
38	04:28:49,013879	8.8.8.8	192.168.1.4	DNS	90	Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225
39	04:28:49,014815	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0007 AAAA www.aiit.or.kr
41	04:28:49,322508	8.8.8.8	192.168.1.4	DNS	128	Standard query response 0x0007 AAAA www.aiit.or.kr SOA ns9.dnszi.com

Frame 37: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CA5B970F-30E1-48BA-B9FE-CACA11DA0309}, id 0
Ethernet II, Src: Elitegro_dc:7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe_98:d1:c5 (20:08:ed:98:d1:c5)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 50405, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0006
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.aiit.or.kr: type A, class IN

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

На запит була надана одна відповідь, що містила назву адреси, що вимагалась, її тип, клас, адреса серверу. У випадку досліджуваної відповіді була надана така інформація щодо сайту www.aiit.or.kr: type A, class IN, addr 58.229.6.225

Весь_поток_3.4.pcapng

Файл Редактирование Просмотр Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Leng	Info
28	04:28:48,041080	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0002 A www.aiit.or.kr.dsl.ukrtel.net
30	04:28:48,116614	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0002 No such name A www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
31	04:28:48,117212	192.168.1.4	8.8.8.8	DNS	89	Standard query 0x0003 AAAA www.aiit.or.kr.dsl.ukrtel.net
32	04:28:48,196612	8.8.8.8	192.168.1.4	DNS	143	Standard query response 0x0003 No such name AAAA www.aiit.or.kr.dsl.ukrtel.net SOA expert.ukrtel.net
33	04:28:48,197067	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0004 A www.aiit.or.kr.ukrtel.net
34	04:28:48,271952	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0004 No such name A www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
35	04:28:48,272586	192.168.1.4	8.8.8.8	DNS	85	Standard query 0x0005 AAAA www.aiit.or.kr.ukrtel.net
36	04:28:48,436562	8.8.8.8	192.168.1.4	DNS	139	Standard query response 0x0005 No such name AAAA www.aiit.or.kr.ukrtel.net SOA expert.ukrtel.net
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0006 A www.aiit.or.kr
38	04:28:49,013879	8.8.8.8	192.168.1.4	DNS	90	Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225
39	04:28:49,014815	192.168.1.4	8.8.8.8	DNS	74	Standard query 0x0007 AAAA www.aiit.or.kr
41	04:28:49,322508	8.8.8.8	192.168.1.4	DNS	128	Standard query response 0x0007 AAAA www.aiit.or.kr SOA ns9.dnszi.com

User Datagram Protocol, Src Port: 53, Dst Port: 50405

Domain Name System (response)

Transaction ID: 0x0006

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

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

Answers

www.aiit.or.kr: type A, class IN, addr 58.229.6.225

Name: www.aiit.or.kr

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 3599 (59 minutes, 59 seconds)

Data length: 4

Address: 58.229.6.225

