

Лабораторна робота №1

Основи захоплення та аналізу пакетів

Виконав студент групи ІС-зп91

Сливчак Гліб

Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

1.1. Хід роботи

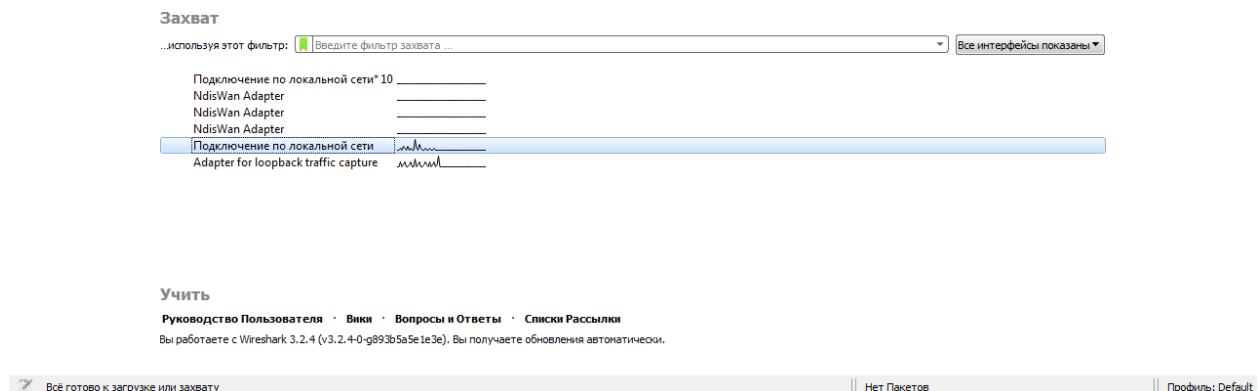
Необхідно виконати наступні дії:

1. Запустіть веб-браузер.
2. Запустіть Wireshark.
3. В Wireshark активуйте діалог вибору мережевого інтерфейсу для захоплення:

Capture >> Interfaces (або ж Ctrl + I)

4. Далі виберіть той інтерфейс, для якого відображається найбільша кількість захоплених пакетів та натисніть кнопку Start навпроти нього:

- у випадку коли інтерфейс ще не ввімкнено можна вибрати any;
- у випадку, коли ви плануєте тестувати локальну комунікацію процесів, можна вибрати lo, loopback або any;



Для виконання лабораторної роботи була обрана локальна мережа. Мережа “adapter for loopback traffic capture” не була обрана, оскільки в такому випадку захоплення пакетів HTTP не відбувалось.

5. Поки Wireshark захоплює пакети, відкрийте в браузері сторінку за наступною адресою:

<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

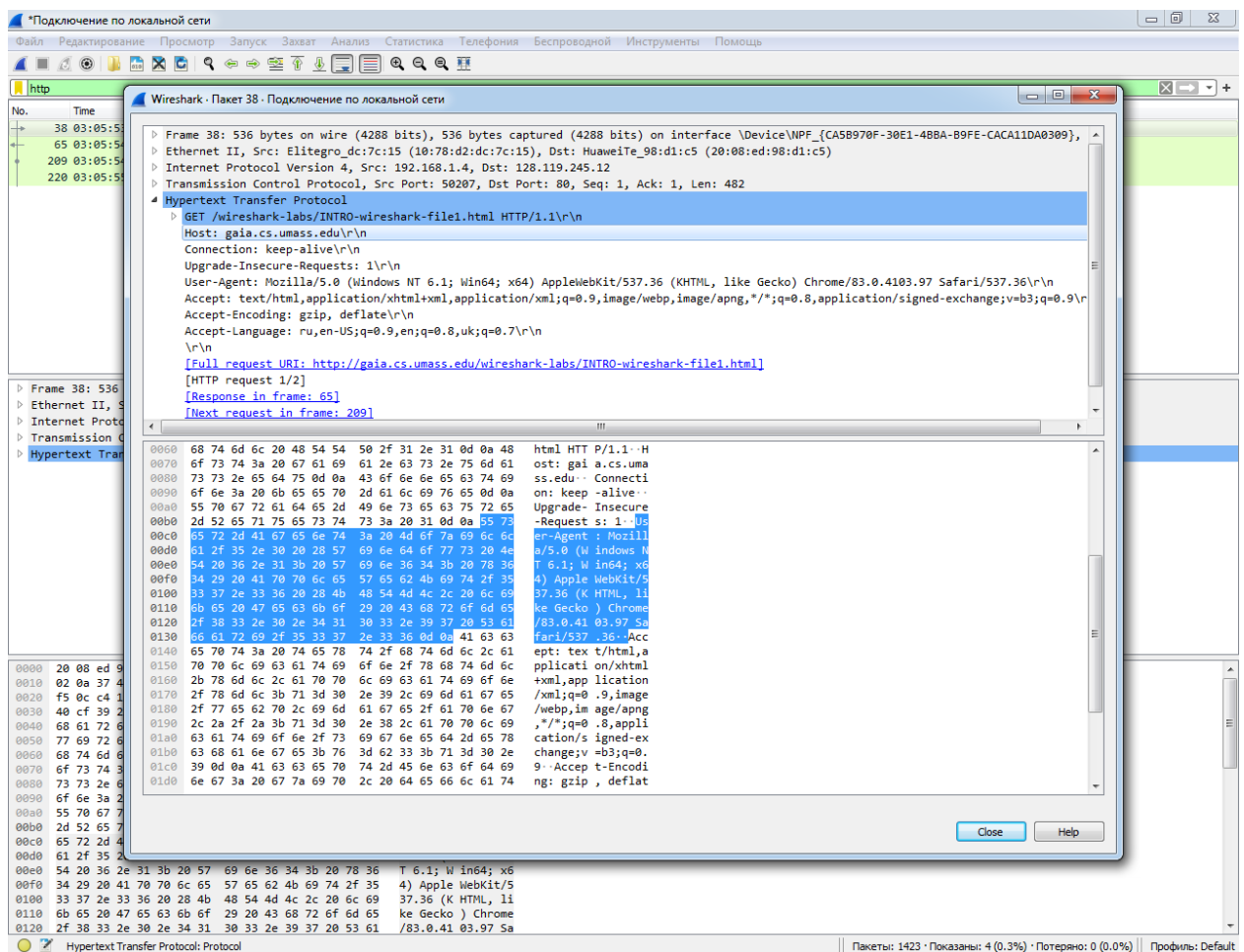
Пакети зі вмістом зазначеної веб-сторінки повинні бути захоплені Wireshark.

6. Зупиніть захоплення пакетів за допомогою команди Capture >> Stop (або Ctrl+ E)

7. Введіть текст «http» в поле фільтрації та натисніть Apply, у вікні лістингу пакетів мають залишитися тільки пакети, які були створені протоколом HTTP.

8. Виберіть перший пакет HTTP, який відображається в вікні лістингу, це має бути повідомлення GET протоколу HTTP. Також цей пакет має вміщувати інформації інших протоколів нижчих рівнів: TCP, IP, Ethernet.

9. У вікні деталей заголовків розкрийте деталі, пов'язані з протоколом HTTP та скрийте детальну інформацію про інші протоколи.



10. Роздрукуйте перші пакети запиту та відповіді. Для цього слід виділити пакет, який бажано роздрукувати, та активувати команду File > Print, та налаштувати його

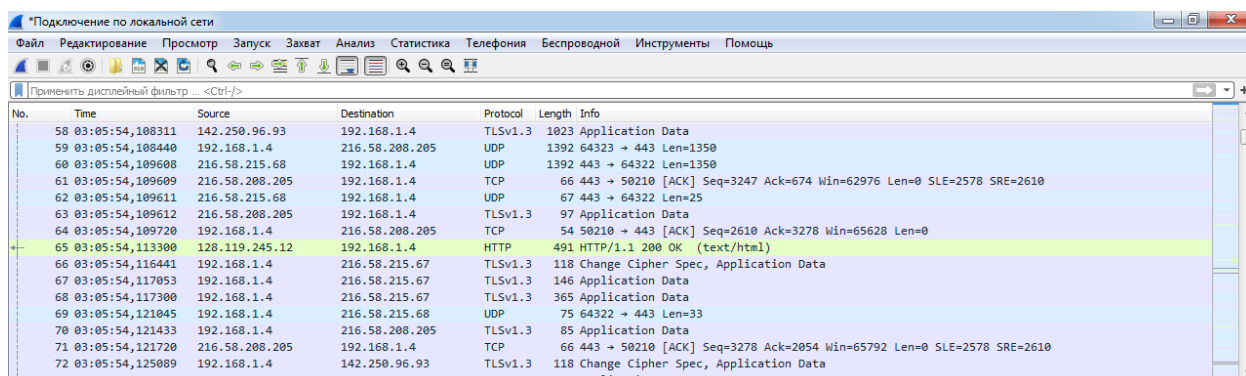
11. Перевірте, що у роздрукованих файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколу.

12. Закрийте Wireshark.

1.2. Контрольні запитання

1. Які протоколи відображались в вікні лістингу протоколів до включення фільтрації?

До включення фільтра відображались різноманітні протоколи типу UDP, TCP, HTTP, TLSv1.3.

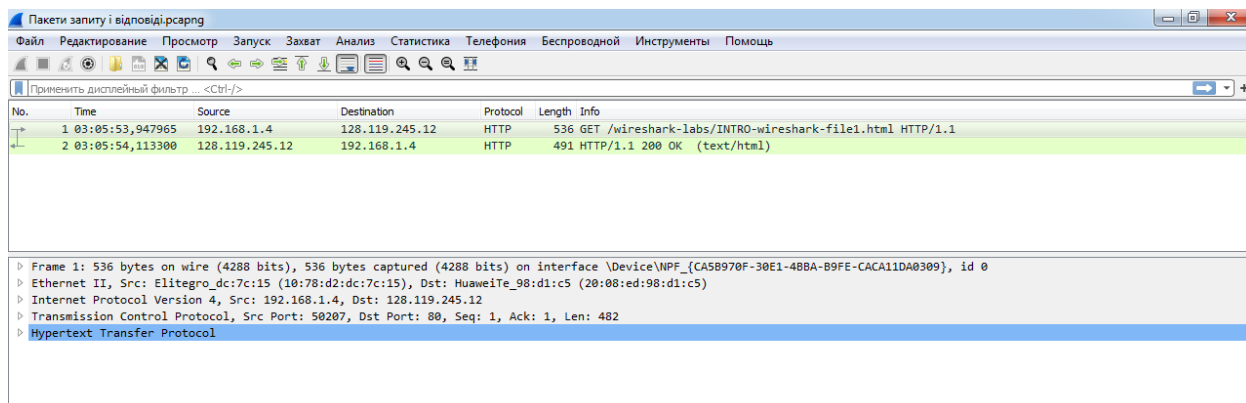


Скріншот вікна "Підключення по локальній мережі" у Wireshark. Таблиця пакетів показує різноманітні протоколи: TLSv1.3, UDP, TCP, та HTTP. Пакет 65 виділений жовтим кольором.

No.	Time	Source	Destination	Protocol	Length	Info
58	03:05:54,108311	142.250.96.93	192.168.1.4	TLSv1.3	1023	Application Data
59	03:05:54,108440	192.168.1.4	216.58.208.205	UDP	1392	64323 → 443 Len=1350
60	03:05:54,109608	216.58.215.68	192.168.1.4	UDP	1392	443 → 64322 Len=1350
61	03:05:54,109609	216.58.208.205	192.168.1.4	TCP	66	443 → 50210 [ACK] Seq=3247 Ack=674 Win=62976 Len=0 SLE=2578 SRE=2610
62	03:05:54,109611	216.58.215.68	192.168.1.4	UDP	67	443 → 64322 Len=25
63	03:05:54,109612	216.58.208.205	192.168.1.4	TLSv1.3	97	Application Data
64	03:05:54,109720	192.168.1.4	216.58.208.205	TCP	54	50210 → 443 [ACK] Seq=2610 Ack=3278 Win=65628 Len=0
65	03:05:54,113300	128.119.245.12	192.168.1.4	HTTP	491	HTTP/1.1 200 OK (text/html)
66	03:05:54,116441	192.168.1.4	216.58.215.67	TLSv1.3	118	Change Cipher Spec, Application Data
67	03:05:54,117053	192.168.1.4	216.58.215.67	TLSv1.3	146	Application Data
68	03:05:54,117300	192.168.1.4	216.58.215.67	TLSv1.3	365	Application Data
69	03:05:54,121045	192.168.1.4	216.58.215.68	UDP	75	64322 → 443 Len=33
70	03:05:54,121433	192.168.1.4	216.58.208.205	TLSv1.3	85	Application Data
71	03:05:54,121720	216.58.208.205	192.168.1.4	TCP	66	443 → 50210 [ACK] Seq=3278 Ack=2054 Win=65792 Len=0 SLE=2578 SRE=2610
72	03:05:54,125089	192.168.1.4	142.250.96.93	TLSv1.3	118	Change Cipher Spec, Application Data
73	03:05:54,125820	192.168.1.4	142.250.96.93	TLSv1.3	146	Application Data

2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?

В збережених пакетах запиту та відповіді використовуються протоколи HTTP



Скріншот вікна "Пакети запиту і відповіді: pcapng" у Wireshark. Таблиця пакетів показує HTTP GET запит та відповідь. Деталі пакету 2 показують інформацію про Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, та Hypertext Transfer Protocol.

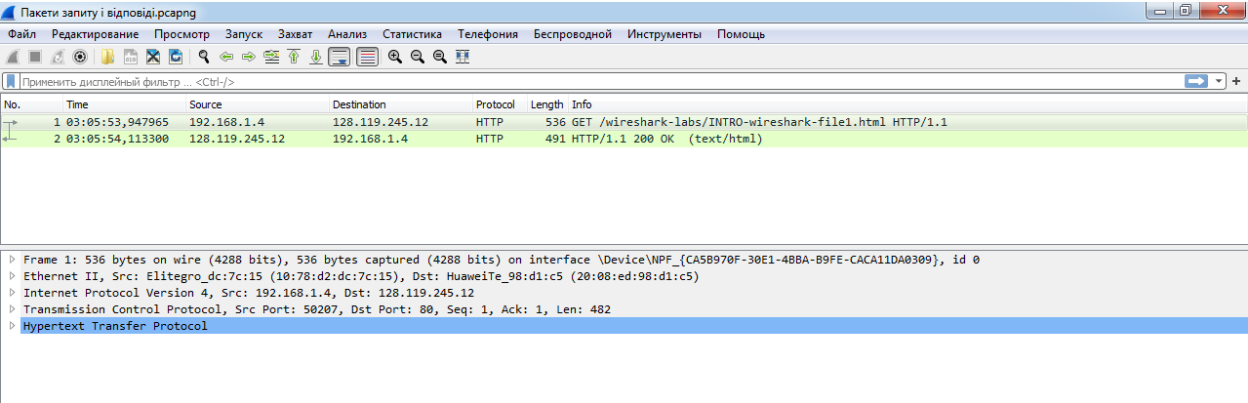
No.	Time	Source	Destination	Protocol	Length	Info
1	03:05:53,947965	192.168.1.4	128.119.245.12	HTTP	536	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2	03:05:54,113300	128.119.245.12	192.168.1.4	HTTP	491	HTTP/1.1 200 OK (text/html)

Деталі пакету 2:

- Frame 1: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{C45B970F-30E1-48BA-B9FE-CACA11D40309}, 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: 128.119.245.12
- Transmission Control Protocol, Src Port: 50207, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
- Hypertext Transfer Protocol

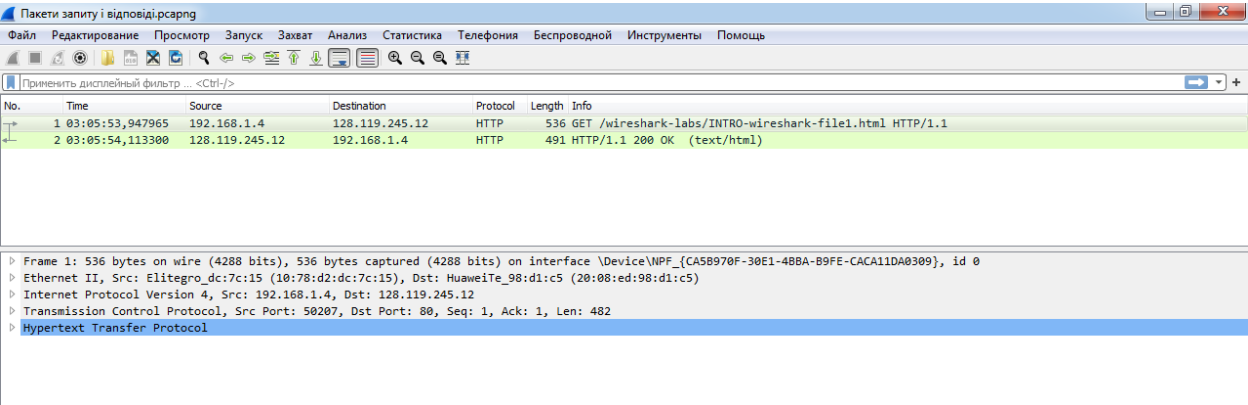
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Тривалість періоду часу, що пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера, складає 165335 мікросекунд ($1000000-947965+113300=165335$ мікросекунд)



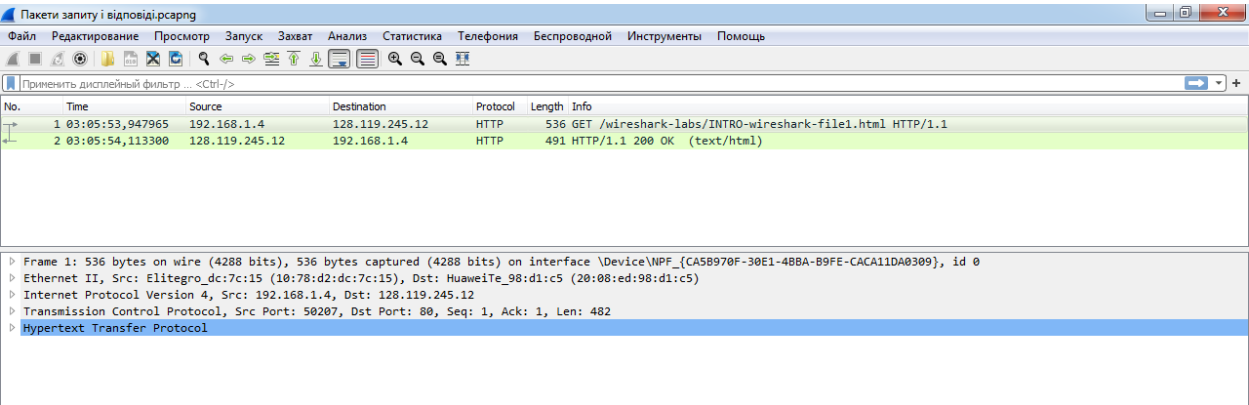
4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?

	Вихідна адреса	Цільова адреса
Пакет із запитом	192.168.1.4	128.119.245.12
Пакет із відповіддю	128.119.245.12	192.168.1.4



5. Яким був перший рядок запиту на рівні протоколу HTTP?
6. Яким був перший рядок відповіді на рівні протоколу HTTP?

	Перший рядок
Пакет запиту	Запит GET /wireshark-labs/INTRO-wireshark-file1.html
Пакет відповіді	Відповідь сервера із статус кодом 200 (Ok)



Пакет запиту

No.	Time	Source	Destination
Protocol Length Info			
1	03:05:53,947965	192.168.1.4	128.119.245.12
HTTP	536	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	

Frame 1: 536 bytes on wire (4288 bits), 536 bytes captured (4288 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: 128.119.245.12
Transmission Control Protocol, Src Port: 50207, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
Hypertext Transfer Protocol

Пакет відповіді

No.	Time	Source	Destination
Protocol Length Info			
2	03:05:54,113300	128.119.245.12	192.168.1.4
HTTP	491	HTTP/1.1 200 OK (text/html)	

Frame 2: 491 bytes on wire (3928 bits), 491 bytes captured (3928 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: 128.119.245.12, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 80, Dst Port: 50207, Seq: 1, Ack: 483, Len: 437
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)

Лабораторна робота №2

Протокол HTTP

Виконав студент групи ІС-зп91

Сливчак Гліб

Мета роботи: аналіз деталей роботи протоколу HTTP.

<i>Лабораторна робота 2.1</i>	2
<i>Лабораторна робота 2.2</i>	6
<i>Лабораторна робота 2.3</i>	11
<i>Лабораторна робота 2.4</i>	15

Лабораторна робота 2.1

2.1. Хід роботи

Необхідно виконати наступні дії:

1. Запустіть веб-браузер, очистіть кеш браузера:
 - a. для Firefox виконайте Tools >> Clear Private Data (або Ctrl + Shift + Del)
 - b. для MS IE виконайте Tools >> Internet Options >> Delete File
2. Запустіть Wireshark, введіть «http» в поле фільтрації, почніть захоплення пакетів.
3. Відкрийте за допомогою браузера одну із зазначених нижче адрес:
 - a. <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>
 - b. <http://194.44.29.242/index.html>

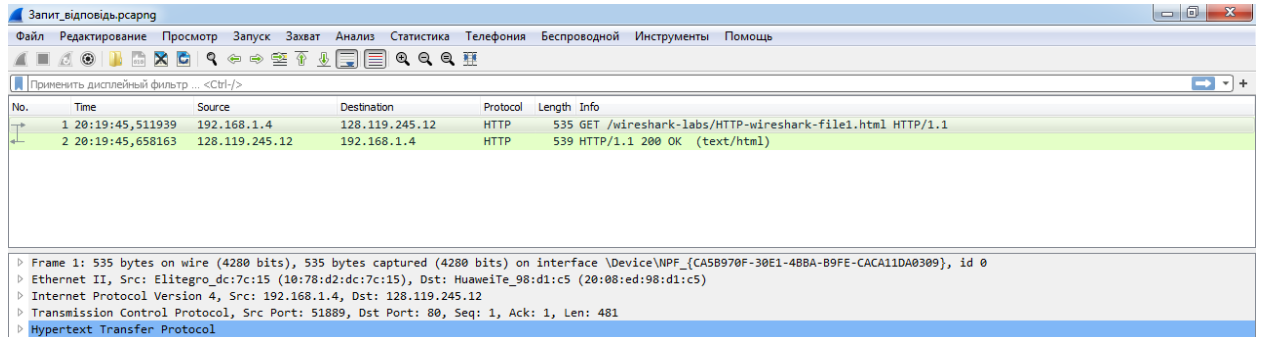
Була обрана адреса <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

4. Зупиніть захоплення пакетів.
5. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім HTTP (за допомогою знаків +/-).
6. Приготуйте відповіді на контрольні запитання 1-7, роздрукуйте необхідні для цього пакети.

2.2 Контрольні запитання

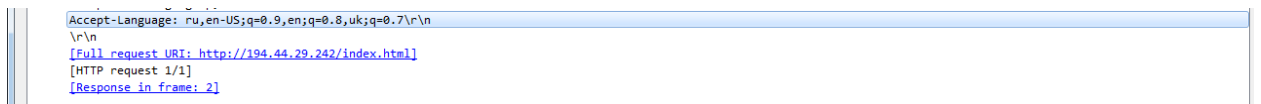
1. Яку версію протоколу HTTP використовує ваш браузер (1.0 чи 1.1)? Яку версію протоколу використовує сервер?

Браузер і сервер використовують протокол HTTP з версією 1.1



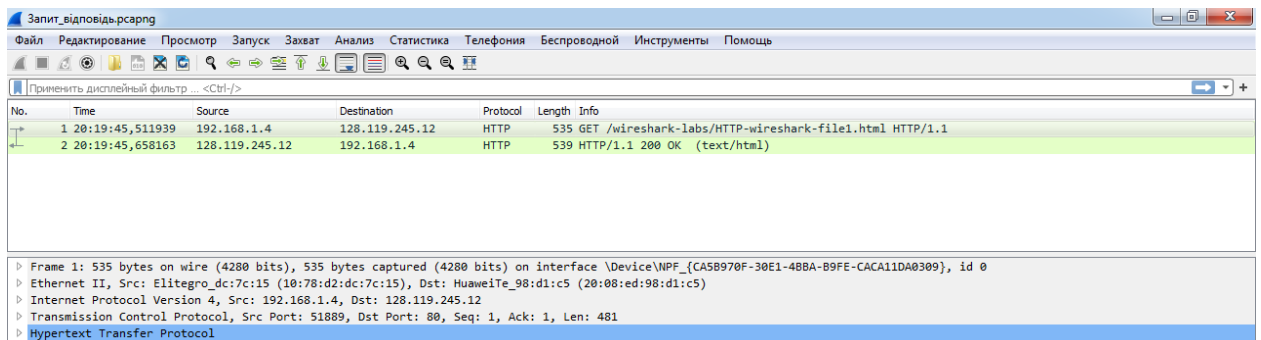
2. Які мови (якщо вказано) браузер може прийняти від сервера?

Браузер може прийняти від сервера російську та англійську мови



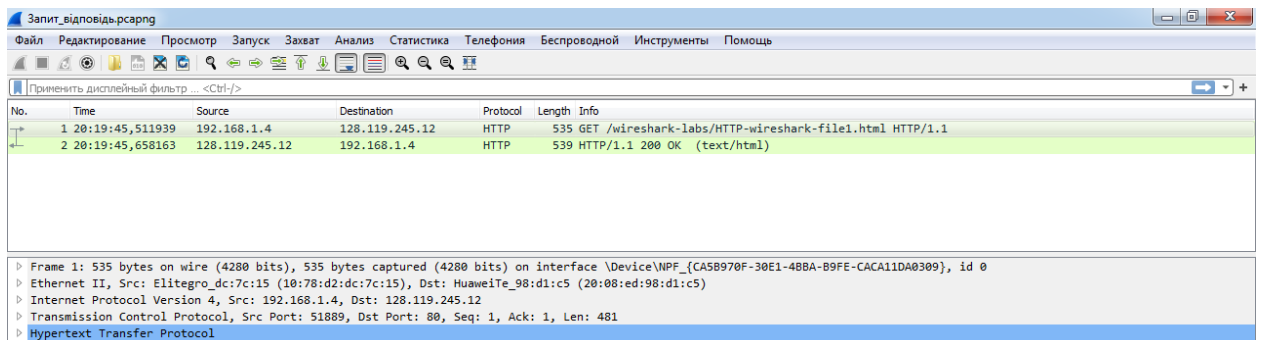
3. Які IP-адреси вашого комп'ютера та цільового веб-сервера?

IP-адреса комп'ютера – 192.168.1.4, цільового веб-сервера – 128.119.245.12



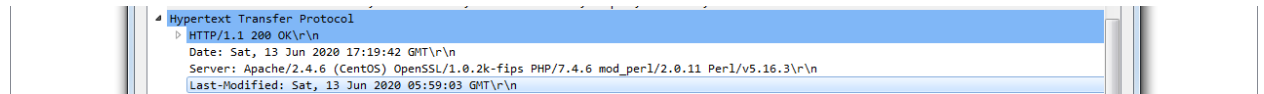
4. Який статусний код сервер повернув у відповіді вашому браузеру?

Сервер повернув браузеру статус код 200 (Ok)



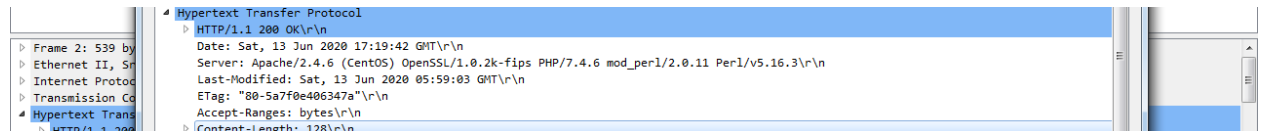
5. Коли на сервері в останній раз був модифікований файл, який запитується браузером?

Востаннє файл на сервері був модифікований 13 червня о 05:59:03 за GMT



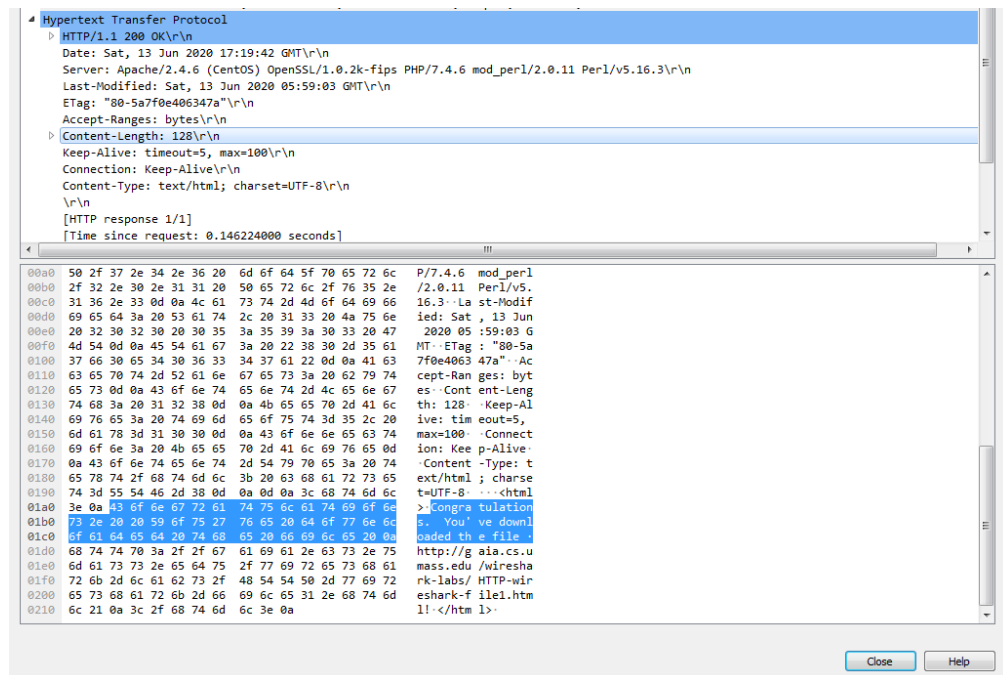
6. Скільки байт контенту повертається сервером?

Сервер повертає 128 байт контенту



7. Переглядаючи нерозібраний байтовий потік пакету, чи бачите ви деякі заголовки в потоці, які не відображаються у вікні деталей пакету? Якщо так, назвіть один з них.

Вірогідно, прикладом такого фрагменту може бути частина байтового потоку, виділена синім кольором



No.	Time	Source	Destination
1	20:19:45,511939	192.168.1.4	128.119.245.12
HTTP 535 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1			

Frame 1: 535 bytes on wire (4280 bits), 535 bytes captured (4280 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: 128.119.245.12
 Transmission Control Protocol, Src Port: 51889, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
 Hypertext Transfer Protocol

No.	Time	Source	Destination
2	20:19:45,658163	128.119.245.12	192.168.1.4
HTTP 539 HTTP/1.1 200 OK (text/html)			

Frame 2: 539 bytes on wire (4312 bits), 539 bytes captured (4312 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: 128.119.245.12, Dst: 192.168.1.4
 Transmission Control Protocol, Src Port: 80, Dst Port: 51889, Seq: 1, Ack: 482, Len: 485
 Hypertext Transfer Protocol
 Line-based text data: text/html (4 lines)

Лабораторна робота 2.2

2.1. Хід роботи

7. Почніть захоплення пакетів.

8. Відкрийте у браузері ту ж саму сторінку, або ж просто натисніть F5 для її повторного завантаження.

а. Якщо ви працюєте зі сторінкою на gaia.cs.umass.edu (ця сторінка регенерується кожну хвилину) – почніть спочатку та виконайте кроки 1,2,3 та 8.

Використовуємо сторінку: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

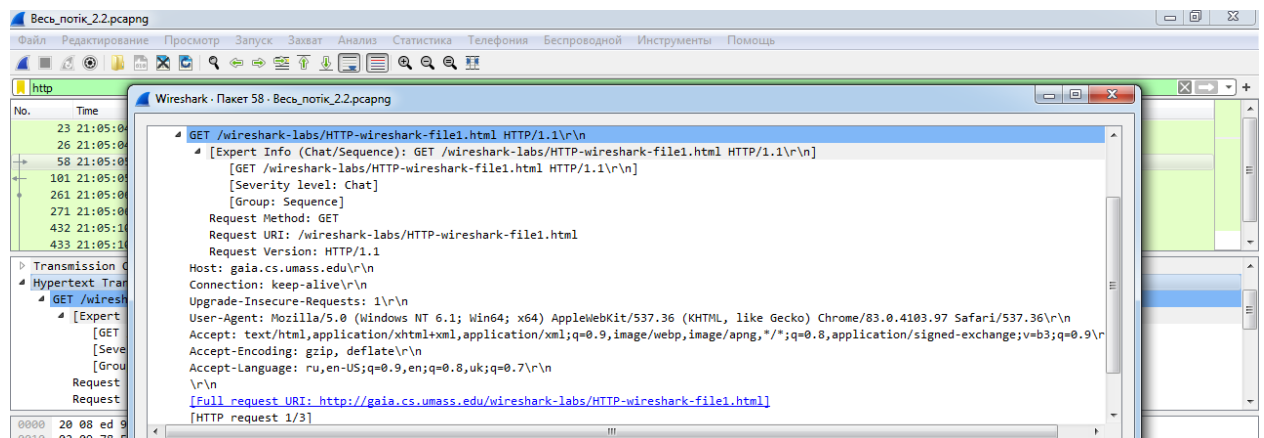
9. Зупиніть захоплення пакетів.

10. Приготуйте відповіді на контрольні запитання 8-11, роздрукуйте необхідні для цього пакети.

2.2 Контрольні запитання

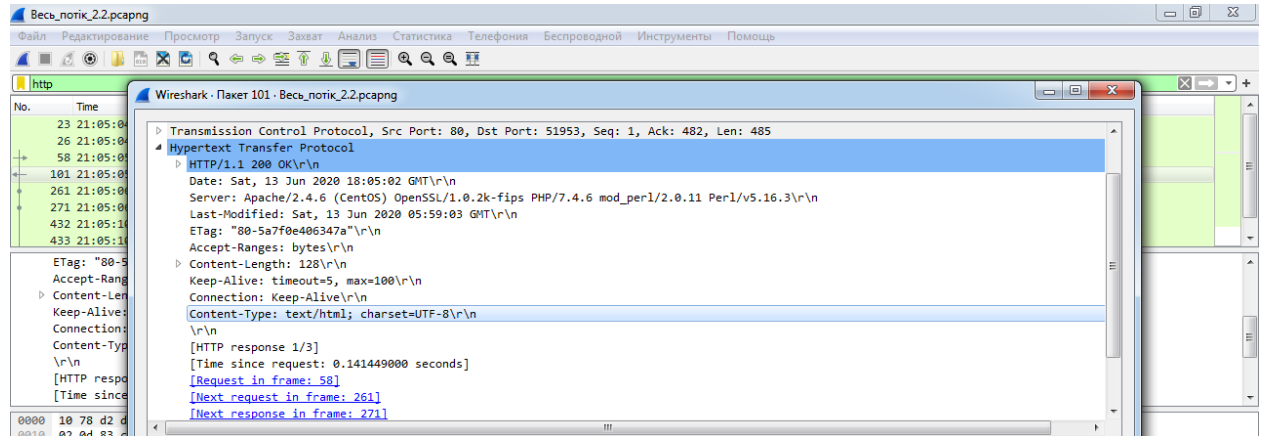
8. Перевірте вміст першого запиту HTTP GET від вашого браузера до сервера. Чи є в ньому заголовок IF-MODIFIED-SINCE?

В першому GET запиті від браузера до сервера рядок IF-MODIFIED-SINCE відсутній



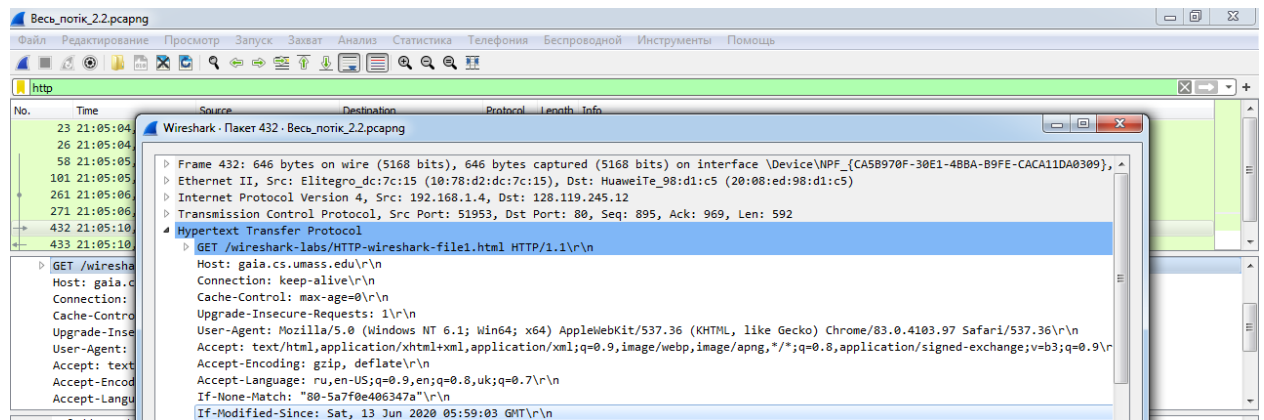
9. Перевірте вміст першої відповіді сервера. Чи повернув сервер вміст файлу безпосередньо у відповіді

Так, сервер дав код відповіді 200 (Ok) і повернув контент типу text.html вагою 128 байт



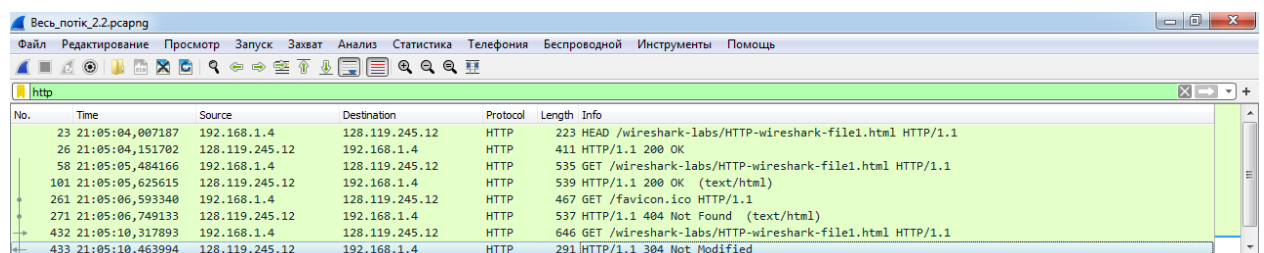
10. Перевірте вміст другого запиту HTTP GET. Чи є в ньому заголовок IF-MODIFIED-SINCE? Якщо так, яке значення йому відповідає?

У другому GET запиті від браузера з'являється заголовок If-Modified-Since, який набуває значення: субота, 13 червня 2020 року, 05:59:03 за GMT



11. Який код та опис статусу другої відповіді сервера? Чи повернув сервер вміст файлу безпосередньо у відповіді?

Сервер на другий GET запит файлу text.html надає у відповідь статус код 304 (Not Modified), вміст файлу безпосередньо не повертає



Роздруківка запитів

No.	Time	Source	Destination
Protocol Length Info	58 21:05:05,484166	192.168.1.4	128.119.245.12
HTTP	535	GET /wireshark-labs/HTTP-wireshark-file1.html	HTTP/1.1

Frame 58: 535 bytes on wire (4280 bits), 535 bytes captured (4280 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: 128.119.245.12
 Transmission Control Protocol, Src Port: 51953, Dst Port: 80, Seq: 1, Ack: 1, Len: 481

Hypertext Transfer Protocol

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97
Safari/537.36\r\n
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ru,en-US;q=0.9,en;q=0.8,uk;q=0.7\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-
wireshark-file1.html]
[HTTP request 1/3]
[Response in frame: 101]
[Next request in frame: 261]
```

No.	Time	Source	Destination
Protocol Length Info	101 21:05:05,625615	128.119.245.12	192.168.1.4
HTTP	539	HTTP/1.1 200 OK (text/html)	

Frame 101: 539 bytes on wire (4312 bits), 539 bytes captured (4312 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: 128.119.245.12, Dst: 192.168.1.4
 Transmission Control Protocol, Src Port: 80, Dst Port: 51953, Seq: 1, Ack: 482, Len: 485

Hypertext Transfer Protocol

```
HTTP/1.1 200 OK\r\n
Date: Sat, 13 Jun 2020 18:05:02 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.6
mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sat, 13 Jun 2020 05:59:03 GMT\r\n
ETag: "80-5a7f0e406347a"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/3]
[Time since request: 0.141449000 seconds]
```

[Request in frame: 58]
 [Next request in frame: 261]
 [Next response in frame: 271]
 [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
 File Data: 128 bytes
 Line-based text data: text/html (4 lines)

No.	Time	Source	Destination
Protocol Length Info			
432	21:05:10,317893	192.168.1.4	128.119.245.12
HTTP	646	GET /wireshark-labs/HTTP-wireshark-file1.html	HTTP/1.1

Frame 432: 646 bytes on wire (5168 bits), 646 bytes captured (5168 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: 128.119.245.12
 Transmission Control Protocol, Src Port: 51953, Dst Port: 80, Seq: 895, Ack: 969, Len: 592

Hypertext Transfer Protocol

```

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97
Safari/537.36\r\n
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ru,en-US;q=0.9,en;q=0.8,uk;q=0.7\r\n
If-None-Match: "80-5a7f0e406347a"\r\n
If-Modified-Since: Sat, 13 Jun 2020 05:59:03 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 3/3]
[Prev request in frame: 261]
[Response in frame: 433]
  
```

No.	Time	Source	Destination
Protocol Length Info			
433	21:05:10,463994	128.119.245.12	192.168.1.4
HTTP	291	HTTP/1.1 304 Not Modified	

Frame 433: 291 bytes on wire (2328 bits), 291 bytes captured (2328 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: 128.119.245.12, Dst: 192.168.1.4
 Transmission Control Protocol, Src Port: 80, Dst Port: 51953, Seq: 969, Ack: 1487, Len: 237

Hypertext Transfer Protocol

```

HTTP/1.1 304 Not Modified\r\n
Date: Sat, 13 Jun 2020 18:05:07 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.6
mod_perl/2.0.11 Perl/v5.16.3\r\n
  
```



```
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=98\r\n
ETag: "80-5a7f0e406347a"\r\n
\r\n
[HTTP response 3/3]
[Time since request: 0.146101000 seconds]
[Prev request in frame: 261]
[Prev response in frame: 271]
[Request in frame: 432]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-
file1.html]
```

Лабораторна робота 2.3

2.1. Хід роботи

11. Виберіть адрес деякого ресурсу (наприклад, зображення), розмір якого перевищує 8192 байти.

a. Можна, наприклад, використати:

<http://www.dilbert.com/dyn/strip/000000000/00000000/0000000/000000/7000/3000/400/73435/73435.strip.gif>

b. або:

<http://www.dilbert.com/dyn/strip/000000000/00000000/0000000/000000/7000/7000/300/77356/77356.strip.sunday.gif>

c. або будь-який не дуже великий файл з серверу 194.44.29.242.

Оберемо зображення:

http://selaginella.myspecies.info/sites/selaginella.myspecies.info/files/styles/large/public/Selaginella%20amblyphylla_2924.001.jpg?itok=SB9aL_Vd

12. Почніть захоплення пакетів та очистіть кеш браузера.

13. Відкрийте обраний ресурс браузером.

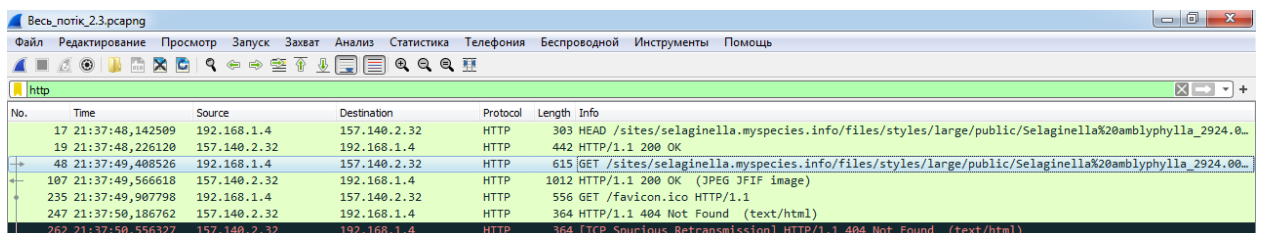
14. Зупиніть захоплення пакетів.

15. Пригоуйте відповіді на запитання 12-15. При необхідності роздрукуйте деякі пакети з відповіді сервера.

2.2 Контрольні запитання

12. Скільки повідомлень HTTP GET було відправлено вашим браузером?

Браузер надіслав 2 GET запити

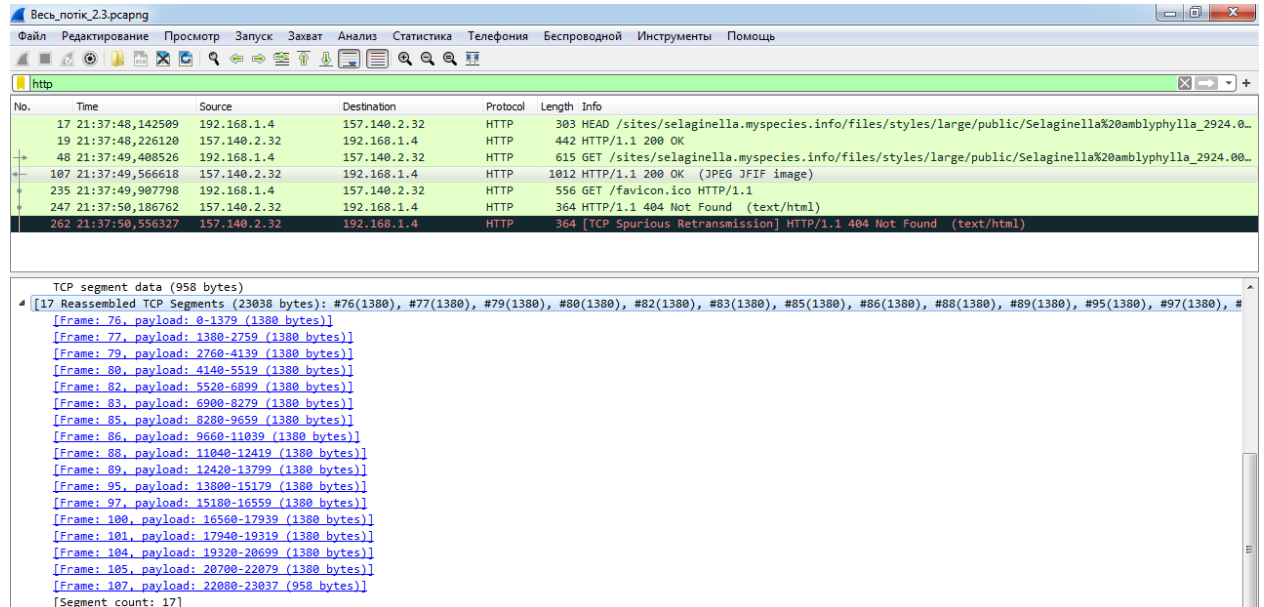


The screenshot shows a Wireshark capture of network traffic. The top pane displays the packet list, and the bottom pane shows the details of the selected packet (No. 48). The packet list shows several HTTP requests, including HEAD, GET, and 404 Not Found responses. The details pane for packet 48 shows the HTTP request structure, including the status line (200 OK), headers, and the body (JPEG image data).

No.	Time	Source	Destination	Protocol	Length	Info
17	21:37:48,142509	192.168.1.4	157.140.2.32	HTTP	303	HEAD /sites/selaginella.myspecies.info/files/styles/large/public/Selaginella%20amblyphylla_2924.001.jpg HTTP/1.1
19	21:37:48,226120	157.140.2.32	192.168.1.4	HTTP	442	HTTP/1.1 200 OK
48	21:37:49,408526	192.168.1.4	157.140.2.32	HTTP	615	GET /sites/selaginella.myspecies.info/files/styles/large/public/Selaginella%20amblyphylla_2924.001.jpg HTTP/1.1
107	21:37:49,566618	157.140.2.32	192.168.1.4	HTTP	1012	HTTP/1.1 200 OK (JPEG image)
235	21:37:49,907798	192.168.1.4	157.140.2.32	HTTP	556	GET /favicon.ico HTTP/1.1
247	21:37:50,186762	157.140.2.32	192.168.1.4	HTTP	364	HTTP/1.1 404 Not Found (text/html)
262	21:37:50,556327	157.140.2.32	192.168.1.4	HTTP	364	[TCP Spurious Retransmission] HTTP/1.1 404 Not Found (text/html)

13. Скільки пакетів TCP було необхідно для доставки одної відповіді HTTP-сервера?

Якщо розглядати протокол номер 107, то для його доставки знадобилось 17 пакетів TCP



Весь_порт_23.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

No.	Time	Source	Destination	Protocol	Length	Info
17	21:37:48,142509	192.168.1.4	157.140.2.32	HTTP	303	HEAD /sites/selaginella.myspecies.info/files/styles/large/public/Selaginella%20amblyphylla_2924.0...
19	21:37:48,226120	157.140.2.32	192.168.1.4	HTTP	442	HTTP/1.1 200 OK
48	21:37:49,408526	192.168.1.4	157.140.2.32	HTTP	615	GET /sites/selaginella.myspecies.info/files/styles/large/public/Selaginella%20amblyphylla_2924.00...
107	21:37:49,566618	157.140.2.32	192.168.1.4	HTTP	1012	HTTP/1.1 200 OK (JPEG JFIF image)
235	21:37:49,907798	192.168.1.4	157.140.2.32	HTTP	556	GET /favicon.ico HTTP/1.1
247	21:37:50,106762	157.140.2.32	192.168.1.4	HTTP	364	HTTP/1.1 404 Not Found (text/html)
262	21:37:50,556327	157.140.2.32	192.168.1.4	HTTP	364	[TCP Spurious Retransmission] HTTP/1.1 404 Not Found (text/html)

TCP segment data (958 bytes)

[17 Reassembled TCP Segments (23038 bytes): #76(1380), #77(1380), #79(1380), #80(1380), #82(1380), #83(1380), #85(1380), #86(1380), #88(1380), #89(1380), #95(1380), #97(1380), #...

[Frame: 76, payload: 0-1379 (1380 bytes)]

[Frame: 77, payload: 1380-2759 (1380 bytes)]

[Frame: 79, payload: 2760-4139 (1380 bytes)]

[Frame: 80, payload: 4140-5519 (1380 bytes)]

[Frame: 82, payload: 5520-6899 (1380 bytes)]

[Frame: 83, payload: 6900-8279 (1380 bytes)]

[Frame: 85, payload: 8280-9659 (1380 bytes)]

[Frame: 86, payload: 9660-11039 (1380 bytes)]

[Frame: 88, payload: 11040-12419 (1380 bytes)]

[Frame: 89, payload: 12420-13799 (1380 bytes)]

[Frame: 95, payload: 13800-15179 (1380 bytes)]

[Frame: 97, payload: 15180-16559 (1380 bytes)]

[Frame: 100, payload: 16560-17939 (1380 bytes)]

[Frame: 101, payload: 17940-19319 (1380 bytes)]

[Frame: 104, payload: 19320-20699 (1380 bytes)]

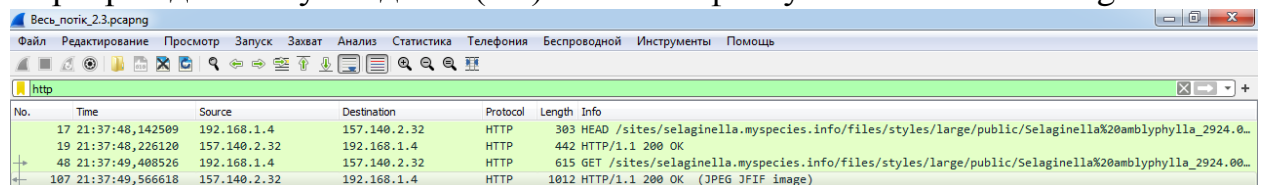
[Frame: 105, payload: 20700-22079 (1380 bytes)]

[Frame: 107, payload: 22080-23037 (958 bytes)]

[Segment count: 17]

14. Який код та опис статусу був у відповіді сервера?

Сервер надав статус код 200 (Ok) з описом файлу як JPEG JGIG image



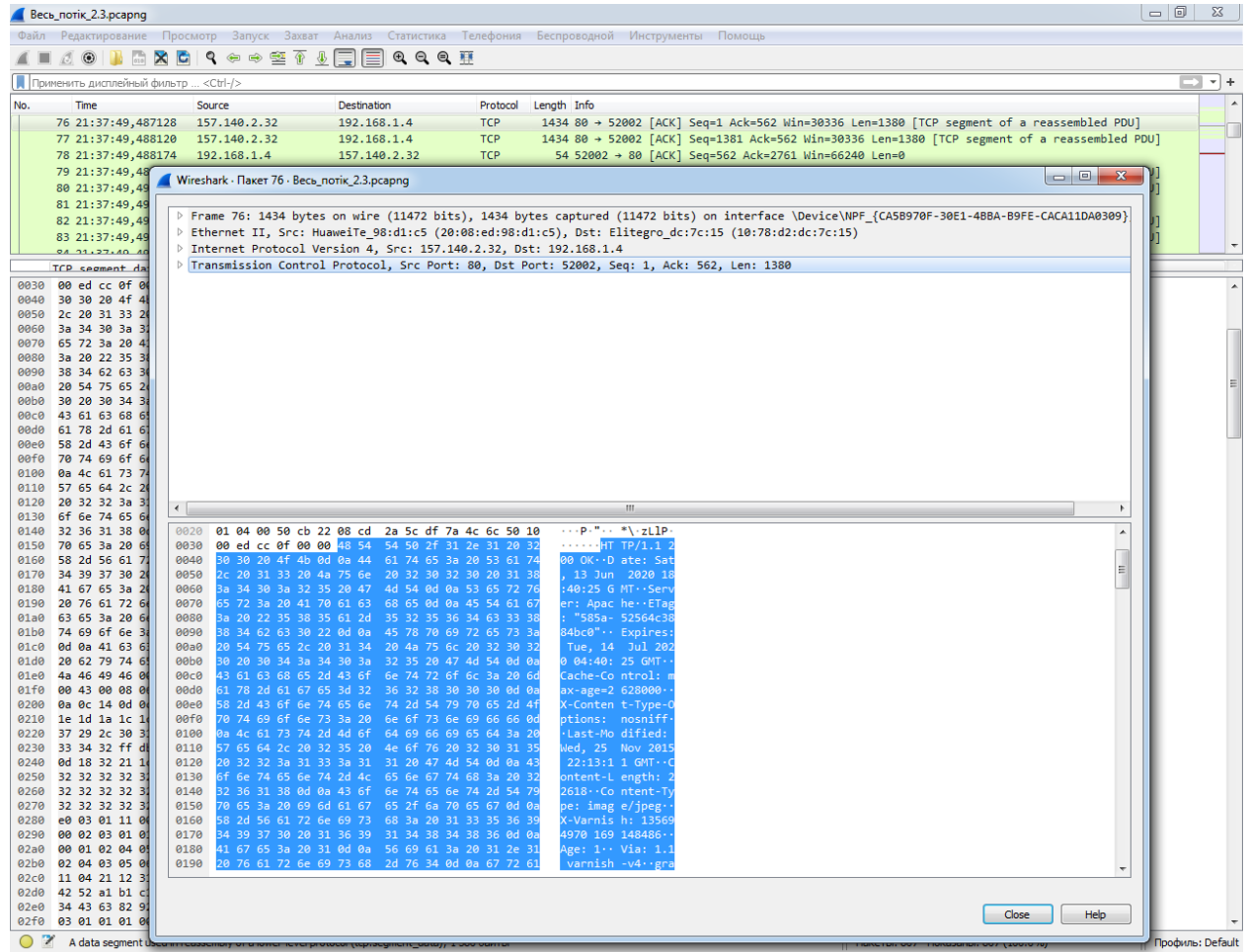
Весь_порт_23.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

No.	Time	Source	Destination	Protocol	Length	Info
17	21:37:48,142509	192.168.1.4	157.140.2.32	HTTP	303	HEAD /sites/selaginella.myspecies.info/files/styles/large/public/Selaginella%20amblyphylla_2924.0...
19	21:37:48,226120	157.140.2.32	192.168.1.4	HTTP	442	HTTP/1.1 200 OK
48	21:37:49,408526	192.168.1.4	157.140.2.32	HTTP	615	GET /sites/selaginella.myspecies.info/files/styles/large/public/Selaginella%20amblyphylla_2924.00...
107	21:37:49,566618	157.140.2.32	192.168.1.4	HTTP	1012	HTTP/1.1 200 OK (JPEG JFIF image)

15. Чи зустрічаються у даних пакетів-продовжень протоколу TCP стрічки з кодом та описом статусу відповіді, або ж якісь заголовки протоколу HTTP? Так, в потоці протоколу TCP можна знайти статус код HTTP протоколу (HTTP/1.1 200 Ok на початку виділеного синього фрагменту)



Роздруківка запитів браузера та відповідей сервера

No.	Time	Source	Destination
48	21:37:49,408526	192.168.1.4	157.140.2.32
HTTP 615 GET /sites/selaginella.myspecies.info/files/styles/large/public/Selaginella%20amblyphylla_2924.001.jpg?itok=SB9aL_Vd HTTP/1.1			

Frame 48: 615 bytes on wire (4920 bits), 615 bytes captured (4920 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: 157.140.2.32
 Transmission Control Protocol, Src Port: 52002, Dst Port: 80, Seq: 1, Ack: 1, Len: 561
 Hypertext Transfer Protocol

No.	Time	Source	Destination
107	21:37:49,566618	157.140.2.32	192.168.1.4
HTTP 1012 HTTP/1.1 200 OK (JPEG JFIF image)			

Frame 107: 1012 bytes on wire (8096 bits), 1012 bytes captured (8096 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: 157.140.2.32, Dst: 192.168.1.4
 Transmission Control Protocol, Src Port: 80, Dst Port: 52002, Seq: 22081, Ack: 562, Len: 958
 [17 Reassembled TCP Segments (23038 bytes): #76(1380), #77(1380), #79(1380), #80(1380), #82(1380), #83(1380), #85(1380), #86(1380), #88(1380), #89(1380), #95(1380), #97(1380), #100(1380), #101(1380), #104(1380), #105(1380), #107(958)]
 Hypertext Transfer Protocol
 JPEG File Interchange Format

Лабораторна робота 2.4

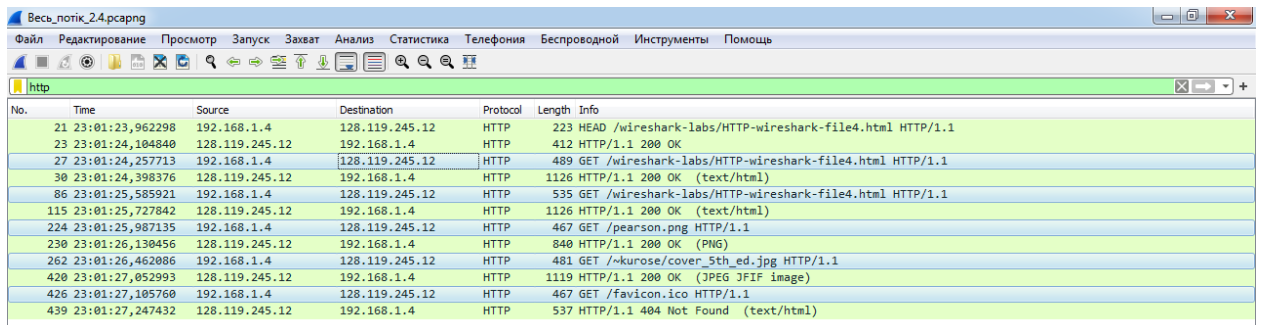
2.1. Хід роботи

16. Почніть захоплення пакетів.
17. Відкрийте сторінку за адресою <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>, також можна використати будь-яку нескладну сторінку з невеликою кількістю зовнішніх ресурсів.
18. Зупиніть захоплення пакетів.
19. Приготуйте відповіді на запитання 16, 17. Роздрукуйте необхідні для цього пакети.
20. Закрийте Wireshark.

2.2 Контрольні запитання

12. Скільки запитів HTTP GET було відправлено вашим браузером? Якими були цільові IP-адреси запитів?

Під час виконання лабораторної роботи було відправлено браузером 5 GET запитів, цільовою IP-адресою для всіх протоколів була адреса – 128.119.245.12



No.	Time	Source	Destination	Protocol	Length	Info
21	23:01:23,962298	192.168.1.4	128.119.245.12	HTTP	223	HEAD /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
23	23:01:24,104840	128.119.245.12	192.168.1.4	HTTP	412	HTTP/1.1 200 OK
27	23:01:24,257713	192.168.1.4	128.119.245.12	HTTP	489	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
30	23:01:24,398376	128.119.245.12	192.168.1.4	HTTP	1126	HTTP/1.1 200 OK (text/html)
86	23:01:25,585921	192.168.1.4	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
115	23:01:25,727842	128.119.245.12	192.168.1.4	HTTP	1126	HTTP/1.1 200 OK (text/html)
224	23:01:25,987135	192.168.1.4	128.119.245.12	HTTP	467	GET /pearson.png HTTP/1.1
230	23:01:26,130456	128.119.245.12	192.168.1.4	HTTP	840	HTTP/1.1 200 OK (PNG)
262	23:01:26,462086	192.168.1.4	128.119.245.12	HTTP	481	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
420	23:01:27,052993	128.119.245.12	192.168.1.4	HTTP	1119	HTTP/1.1 200 OK (JPEG JFIF image)
426	23:01:27,105760	192.168.1.4	128.119.245.12	HTTP	467	GET /favicon.ico HTTP/1.1
439	23:01:27,247432	128.119.245.12	192.168.1.4	HTTP	537	HTTP/1.1 404 Not Found (text/html)

13. Чи можете ви встановити, чи були ресурси отримані паралельно чи послідовно? Яким чином?

No.	Time	Source	Destination	Protocol	Length	Info
21	23:01:23,962298	192.168.1.4	128.119.245.12	HTTP	223	HEAD /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
23	23:01:24,104840	128.119.245.12	192.168.1.4	HTTP	412	HTTP/1.1 200 OK
27	23:01:24,257713	192.168.1.4	128.119.245.12	HTTP	489	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
30	23:01:24,398376	128.119.245.12	192.168.1.4	HTTP	1126	HTTP/1.1 200 OK (text/html)
86	23:01:25,585921	192.168.1.4	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
115	23:01:25,727842	128.119.245.12	192.168.1.4	HTTP	1126	HTTP/1.1 200 OK (text/html)
224	23:01:25,987135	192.168.1.4	128.119.245.12	HTTP	467	GET /pearson.png HTTP/1.1
230	23:01:26,130456	128.119.245.12	192.168.1.4	HTTP	840	HTTP/1.1 200 OK (PNG)
262	23:01:26,462086	192.168.1.4	128.119.245.12	HTTP	481	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
420	23:01:27,052993	128.119.245.12	192.168.1.4	HTTP	1119	HTTP/1.1 200 OK (JPEG JFIF image)
426	23:01:27,105760	192.168.1.4	128.119.245.12	HTTP	467	GET /favicon.ico HTTP/1.1
439	23:01:27,247432	128.119.245.12	192.168.1.4	HTTP	537	HTTP/1.1 404 Not Found (text/html)

Ресурси від сервера найбільш вірогідно надійшли послідовно, оскільки час надходження відповідей відрізняється. Якщо не враховувати різниці надходження відповідей від сервера, які лежать в діапазоні $0 < t < 1$ мікросекунд, то тоді можна висунути інші припущення. Назвемо умовно отримані файли відповідно номерам пакетів відповідей сервера на GET запити, а саме 30, 115, 239 та 420. Файли 30, 115 і 420 прийшли паралельно, оскільки вони надійшли на різні Destination ports, а саме на порти 52221, 52222 і 52230, файл 230 прийшов послідовно після файлу 115 на порт 52222.

Запити і відповіді від сервера
Пакети 27 і 30

No.	Time	Source	Destination
Protocol Length Info			
27	23:01:24,257713	192.168.1.4	128.119.245.12
HTTP	489	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	

Frame 27: 489 bytes on wire (3912 bits), 489 bytes captured (3912 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: 128.119.245.12
Transmission Control Protocol, Src Port: 52221, Dst Port: 80, Seq: 1, Ack: 1, Len: 435
Hypertext Transfer Protocol

No.	Time	Source	Destination
Protocol Length Info			
30	23:01:24,398376	128.119.245.12	192.168.1.4
HTTP	1126	HTTP/1.1 200 OK (text/html)	

Frame 30: 1126 bytes on wire (9008 bits), 1126 bytes captured (9008 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: 128.119.245.12, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 80, Dst Port: 52221, Seq: 1, Ack: 436, Len: 1072
Hypertext Transfer Protocol
Line-based text data: text/html (17 lines)

Пакети 86 i 115

No.	Time	Source	Destination
Protocol Length Info			
86	23:01:25,585921	192.168.1.4	128.119.245.12
HTTP	535	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	

Frame 86: 535 bytes on wire (4280 bits), 535 bytes captured (4280 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: 128.119.245.12
 Transmission Control Protocol, Src Port: 52222, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
 Hypertext Transfer Protocol

No.	Time	Source	Destination
Protocol Length Info			
115	23:01:25,727842	128.119.245.12	192.168.1.4
HTTP	1126	HTTP/1.1 200 OK (text/html)	

Frame 115: 1126 bytes on wire (9008 bits), 1126 bytes captured (9008 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: 128.119.245.12, Dst: 192.168.1.4
 Transmission Control Protocol, Src Port: 80, Dst Port: 52222, Seq: 1, Ack: 482, Len: 1072
 Hypertext Transfer Protocol
 Line-based text data: text/html (17 lines)

Пакети 224 i 230

No.	Time	Source	Destination
Protocol Length Info			
224	23:01:25,987135	192.168.1.4	128.119.245.12
HTTP	467	GET /pearson.png HTTP/1.1	

Frame 224: 467 bytes on wire (3736 bits), 467 bytes captured (3736 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: 128.119.245.12
 Transmission Control Protocol, Src Port: 52222, Dst Port: 80, Seq: 482, Ack: 1073, Len: 413
 Hypertext Transfer Protocol

No.	Time	Source	Destination
Protocol Length Info			
230	23:01:26,130456	128.119.245.12	192.168.1.4
HTTP	840	HTTP/1.1 200 OK (PNG)	

Frame 230: 840 bytes on wire (6720 bits), 840 bytes captured (6720 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: 128.119.245.12, Dst: 192.168.1.4
 Transmission Control Protocol, Src Port: 80, Dst Port: 52222, Seq: 3897, Ack: 895, Len: 786
 [3 Reassembled TCP Segments (3610 bytes): #227(1412), #228(1412), #230(786)]
 Hypertext Transfer Protocol
 Portable Network Graphics

Пакети 262 i 420

No.	Time	Source	Destination
262	23:01:26,462086	192.168.1.4	128.119.245.12
HTTP 481 GET /~kurose/cover_5th_ed.jpg HTTP/1.1			

Frame 262: 481 bytes on wire (3848 bits), 481 bytes captured (3848 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: 128.119.245.12
 Transmission Control Protocol, Src Port: 52230, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
 Hypertext Transfer Protocol

No.	Time	Source	Destination
420	23:01:27,052993	128.119.245.12	192.168.1.4
HTTP 1119 HTTP/1.1 200 OK (JPEG JFIF image)			

Frame 420: 1119 bytes on wire (8952 bits), 1119 bytes captured (8952 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: 128.119.245.12, Dst: 192.168.1.4
 Transmission Control Protocol, Src Port: 80, Dst Port: 52230, Seq: 100253, Ack: 428, Len: 1065
 [72 Reassembled TCP Segments (101317 bytes): #269(1412), #270(1412), #272(1412), #273(1412), #275(1412), #276(1412), #278(1412), #279(1412), #281(1412), #282(1412), #294(1412), #295(1412), #297(1412), #298(1412), #300(1412), #301(1412), #30]
 Hypertext Transfer Protocol
 JPEG File Interchange Format

Лабораторна робота №3

Протокол DNS

Виконав студент групи ІС-зп91

Сливчак Гліб

Мета роботи: аналіз деталей роботи протоколу DNS.

Лабораторна робота 3.1	2
Лабораторна робота 3.2	8
Лабораторна робота 3.3	12
Лабораторна робота 3.4	16

Лабораторна робота 3.1

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.

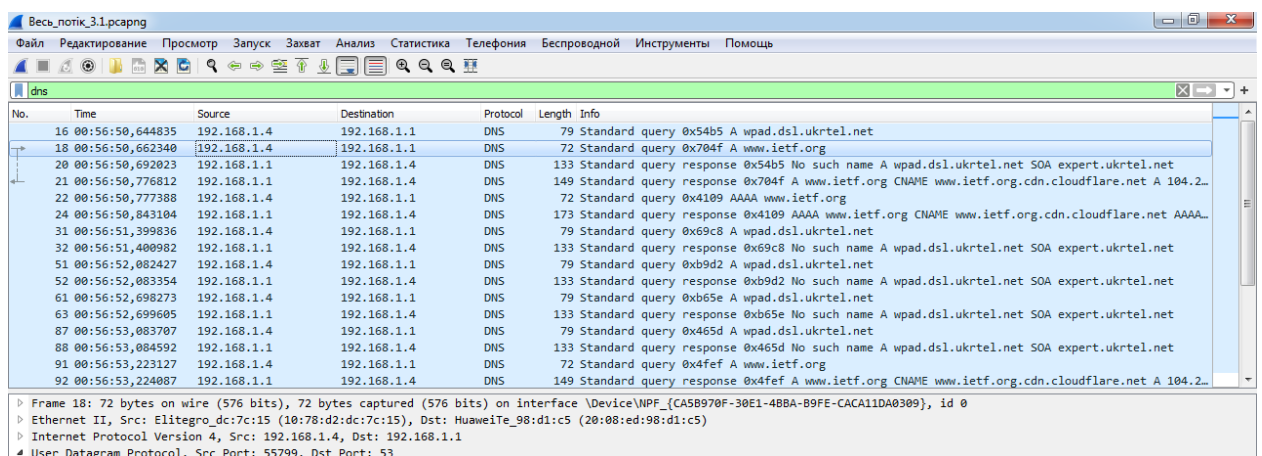
5. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/-).

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

3.2. 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 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
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_{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: 55799, Dst Port: 53

Весь_поток_3.1.pcapng						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
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 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
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_{C45B970F-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:dc7c: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

Весь_поток_3.1.pcapng						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
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 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
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_{C45B970F-30E1-4BBA-B9FE-CACA11DA0309}, id 0
 Ethernet II, Src: Elitegro_dc7c:15 (10:78:d2:dc7c: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

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 104.20.0.85 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

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 104.20.0.85 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

Frame 21: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{C45B970F-30E1-4BBA-B9FE-CACA11D0A0309}, 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)
Transaction ID: 0x704f
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
Answers
www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

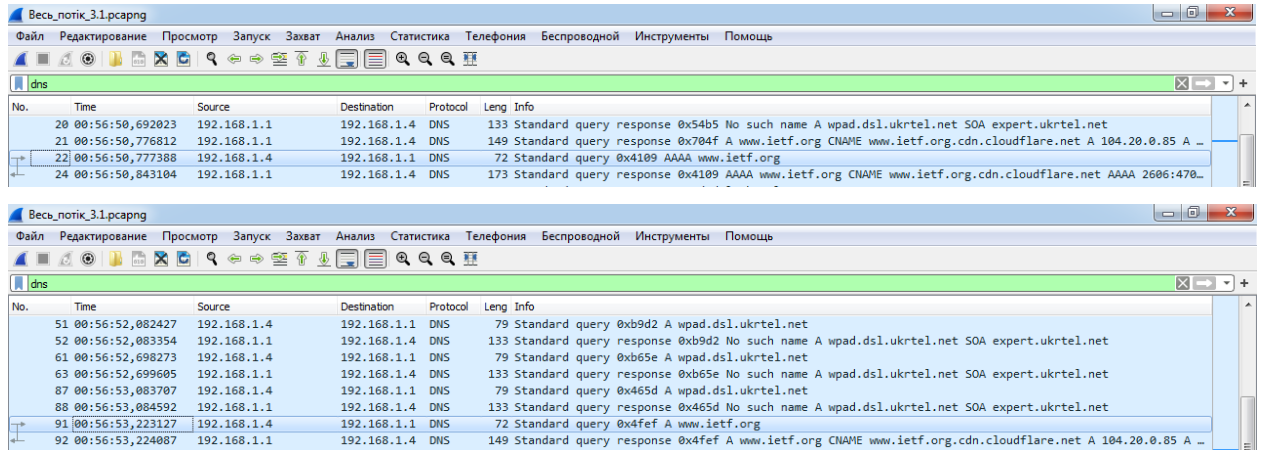
5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

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

No.	Time	Source	Destination	Protocol	Length	Info
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 104.20.0.85 A ...
22	00:56:50,777388	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x4109 AAAA www.ietf.org
23	00:56:50,799639	fe80::814e:4f50:a4e...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
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...
25	00:56:50,845269	192.168.1.4	104.20.0.85	TCP	66	49409 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
26	00:56:50,901513	104.20.0.85	192.168.1.4	TCP	66	80 → 49409 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
27	00:56:50,901700	192.168.1.4	104.20.0.85	TCP	54	49409 → 80 [ACK] Seq=1 Ack=1 Win=65800 Len=0
28	00:56:50,902078	192.168.1.4	104.20.0.85	HTTP	178	HEAD / HTTP/1.1
29	00:56:50,965575	104.20.0.85	192.168.1.4	TCP	60	80 → 49409 [ACK] Seq=1 Ack=125 Win=65536 Len=0
30	00:56:51,371155	104.20.0.85	192.168.1.4	HTTP	492	HTTP/1.1 302 Found
31	00:56:51,399836	192.168.1.4	192.168.1.1	DNS	79	Standard query 0x69c8 A wpad.dsl.ukrtel.net

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	00:56:50,692023	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 0x784f 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
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
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

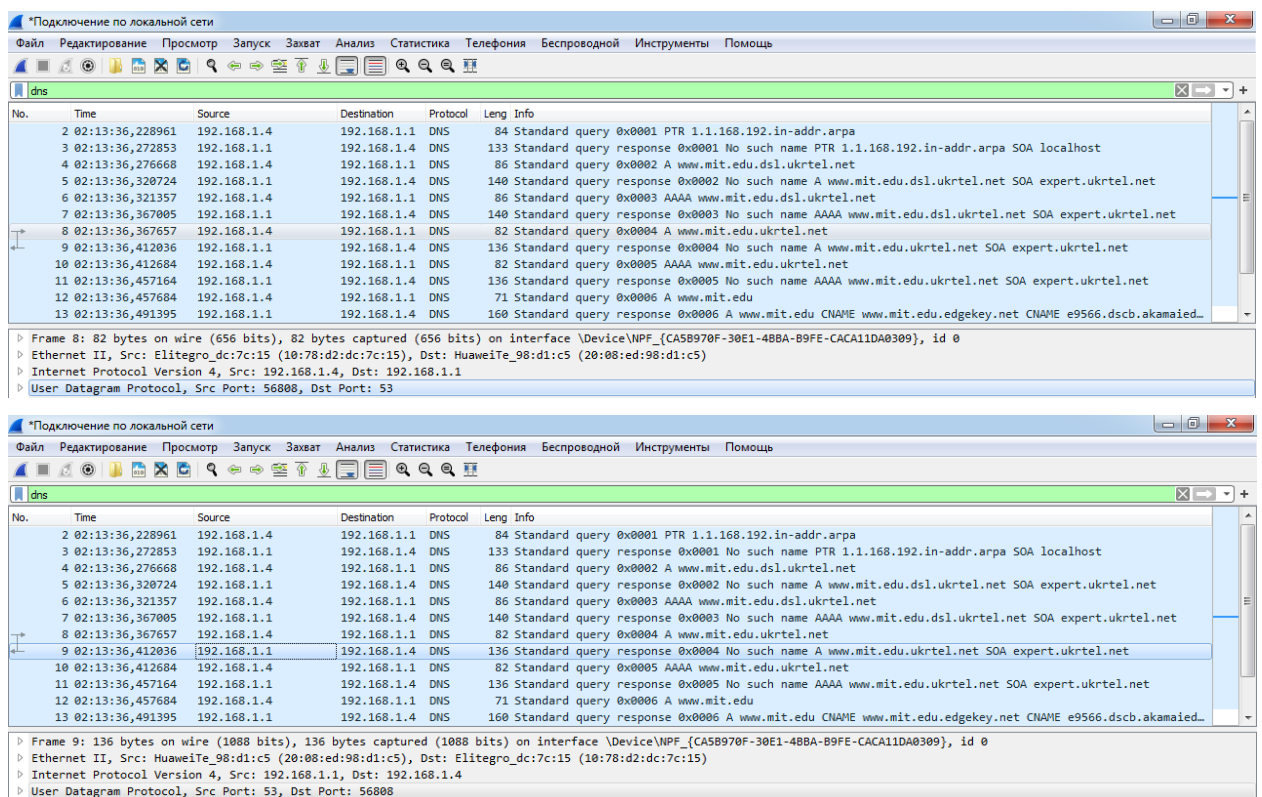
3.1. Хід роботи

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.

3.2. Контрольні запитання

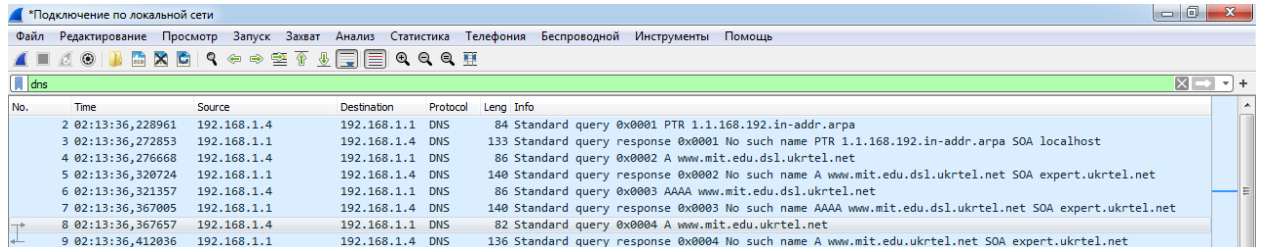
7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

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?

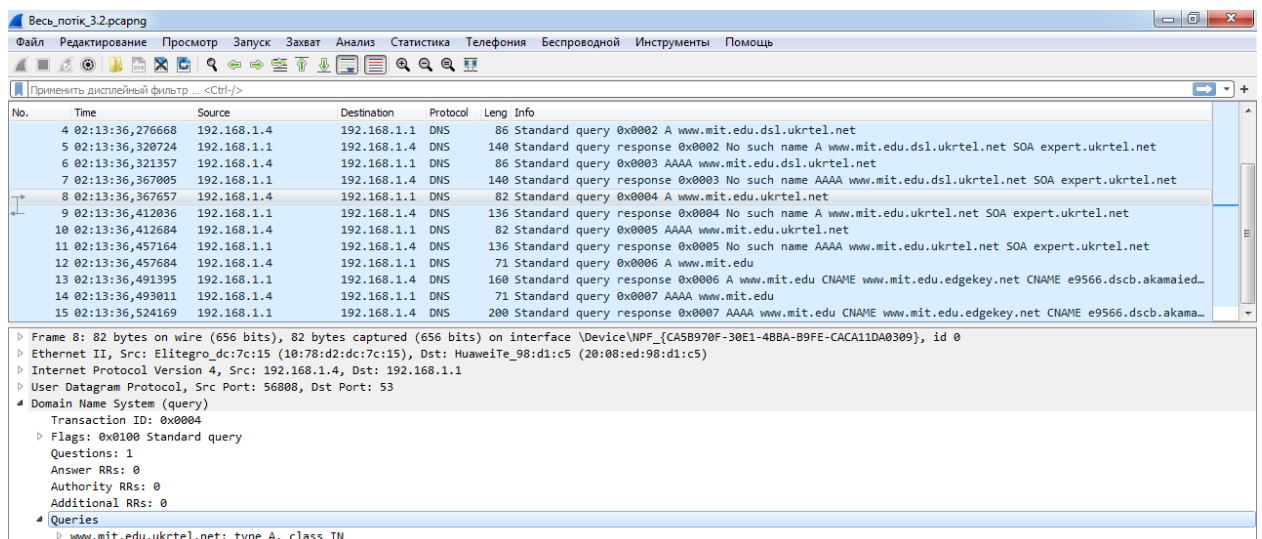
Запит DNS був направлений на адресу 192.168.1.1, яка є адресою локального DNS серверу за замовченням



No.	Time	Source	Destination	Protocol	Leng	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 0x004. 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	Leng	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_{C458970F-30E1-48BA-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	280 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_{CA58970F-30E1-48BA-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: 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

Answers

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

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

e9566.dscb.akamaiedge.net: type A, class IN, addr 104.104.191.7

[Request In: 12]

[Time: 0.033711000 seconds]

DNS запити і відповіді, закладені у пакети 12 і 13

ВІДПОВІДНО

No.	Time	Source	Destination	
	12 02:13:36,457684	192.168.1.4	192.168.1.1	DNS
71	Standard query 0x0006 A www.mit.edu			

Frame 12: 71 bytes on wire (568 bits), 71 bytes captured (568 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: 56810, Dst Port: 53
 Domain Name System (query)

No.	Time	Source	Destination	
	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 A 104.104.191.7			

Frame 13: 160 bytes on wire (1280 bits), 160 bytes captured (1280 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: 56810
 Domain Name System (response)

Лабораторна робота 3.3

3.1. Хід роботи

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

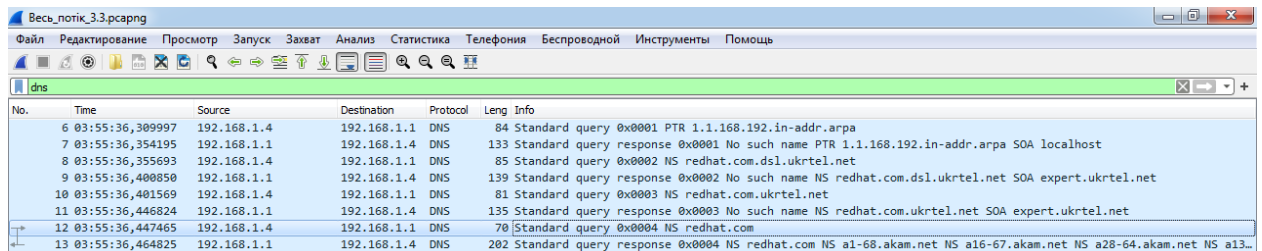
Посилання на адресу mit.edu викликає помилку типу DNS request timed out, замість неї використаємо адресу redhat.com, тобто команда для роботи буде виглядати таким чином: nslookup -type=NS redhat.com

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

3.2. 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 table below represents the data visible in the packet list pane.

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»?

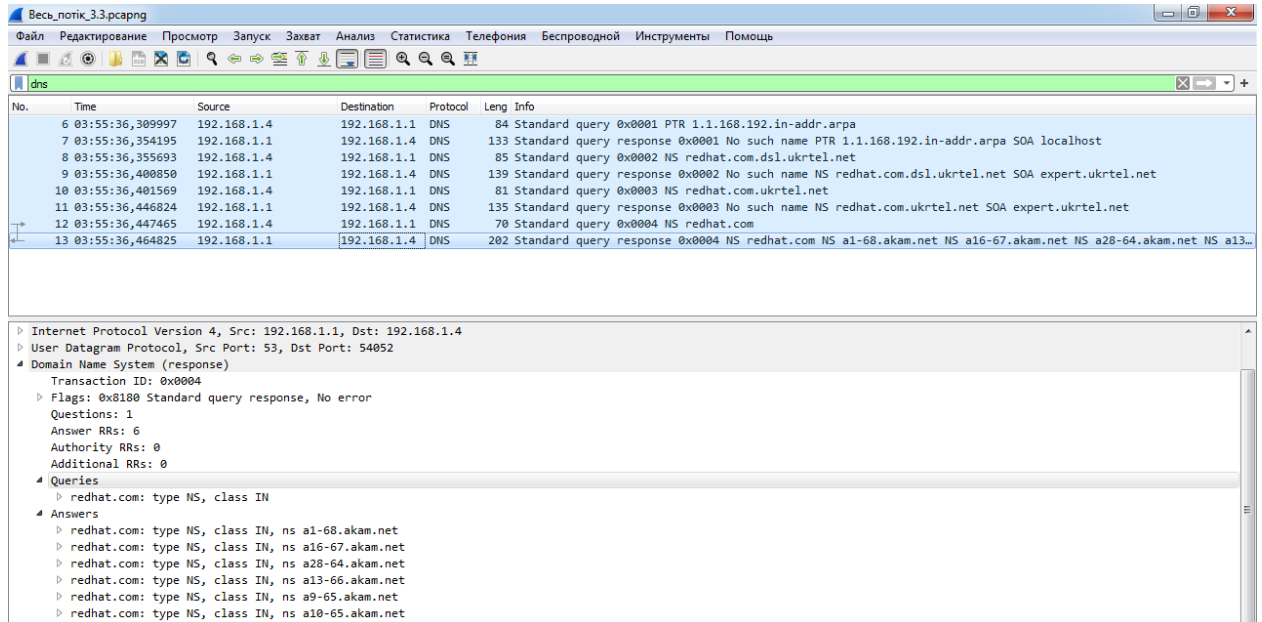
Запит DNS визначається як 0x0100 «standard query», тобто стандартний запит. Запит і відповідь об'єднує спільний transaction ID, який для досліджуваного запиту складає 0x0004. Число записане у шістнадцятковій системі числення, у десятковій системі числення число має значення 4. Запит вимагає від сервера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

The screenshot shows 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-30E1-4BBA-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: 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	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-

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: 0x8180 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

Роздруківка запиту і відповіді, що закладені у пакети 12 і 13 відповідно

No.	Time	Source	Destination
70	03:55:36,447465	192.168.1.4	192.168.1.1
Standard query 0x0004 NS redhat.com			

Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 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: 54052, Dst Port: 53
 Domain Name System (query)

No.	Time	Source	Destination
202	03:55:36,464825	192.168.1.1	192.168.1.4
Standard query response 0x0004 NS redhat.com NS a1-68.akam.net NS a16-67.akam.net NS a28-64.akam.net NS a13-66.akam.net NS a9-65.akam.net NS a10-65.akam.net			

Frame 13: 202 bytes on wire (1616 bits), 202 bytes captured (1616 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: 54052
 Domain Name System (response)

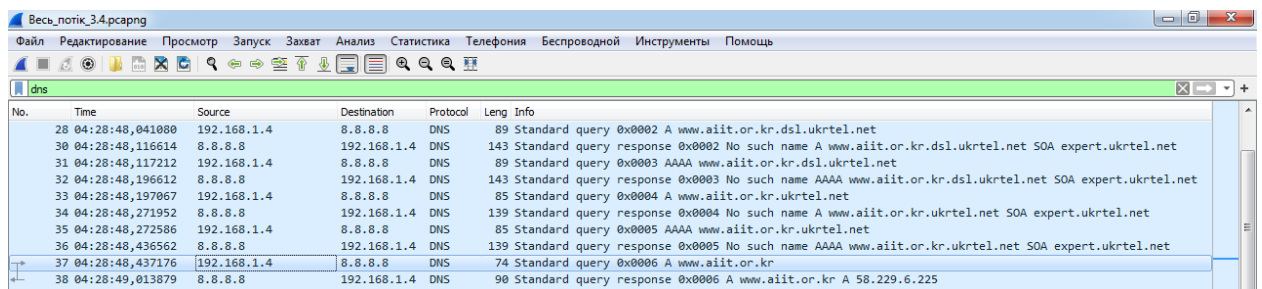
Лабораторна робота 3.4

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	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

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

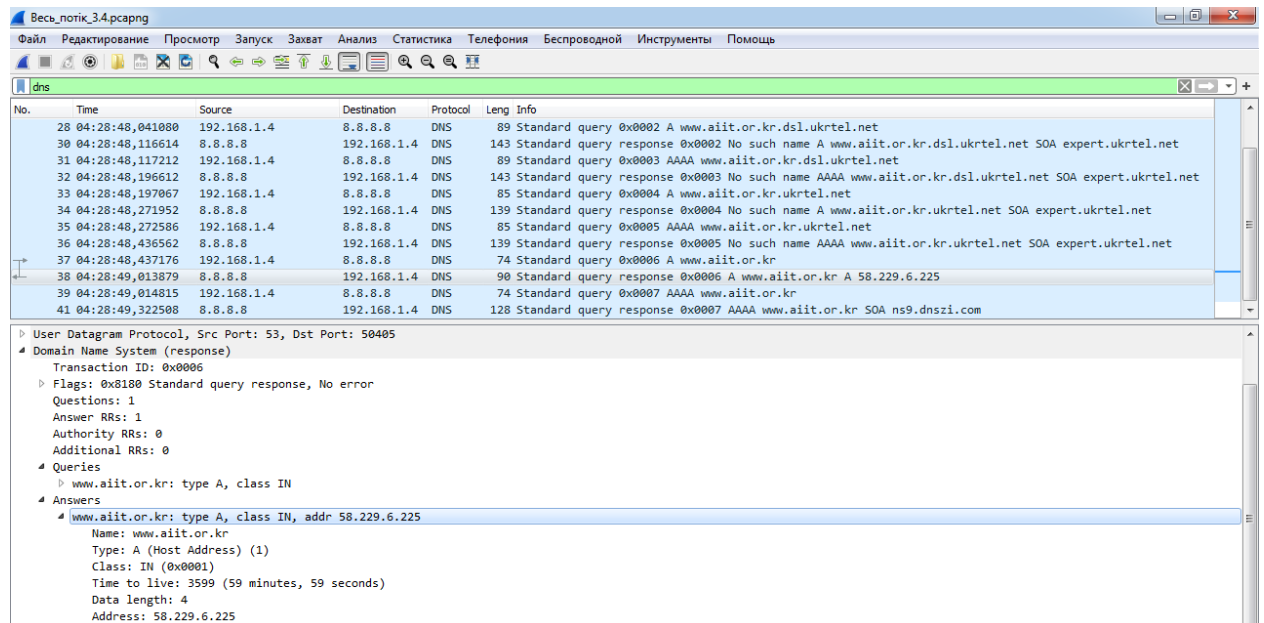
The screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list pane on the left shows several DNS packets. The packet details pane on the right is expanded for packet 37, which is a Standard query (type A, class IN) for the domain www.aiit.or.kr. The packet bytes pane at the bottom 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 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 ns9.dnszi.com

Frame 37: 74 bytes on wire (592 bits), 74 bytes captured (592 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: 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



Роздруківка пакетів 37 і 38, що містять досліджувані запит і відповідь

No.	Time	Source	Destination	
37	04:28:48,437176	192.168.1.4	8.8.8.8	DNS
74	Standard query 0x0006 A www.aiit.or.kr			

Frame 37: 74 bytes on wire (592 bits), 74 bytes captured (592 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: 8.8.8.8
 User Datagram Protocol, Src Port: 50405, Dst Port: 53
 Domain Name System (query)

No.	Time	Source	Destination	
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			

Frame 38: 90 bytes on wire (720 bits), 90 bytes captured (720 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: 8.8.8.8, Dst: 192.168.1.4
 User Datagram Protocol, Src Port: 53, Dst Port: 50405
 Domain Name System (response)