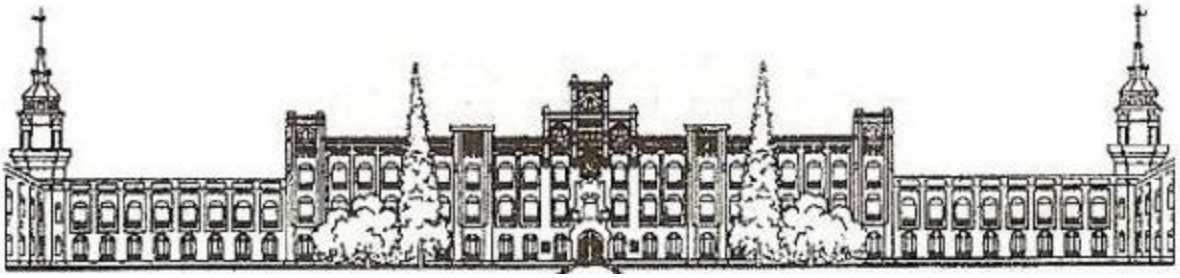


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА ММСА

Лабораторна робота № 1

З дисципліни: Комп'ютерні мережі

Основи захоплення та аналізу пакетів

Виконав:

Студент III курсу

Групи КА-74

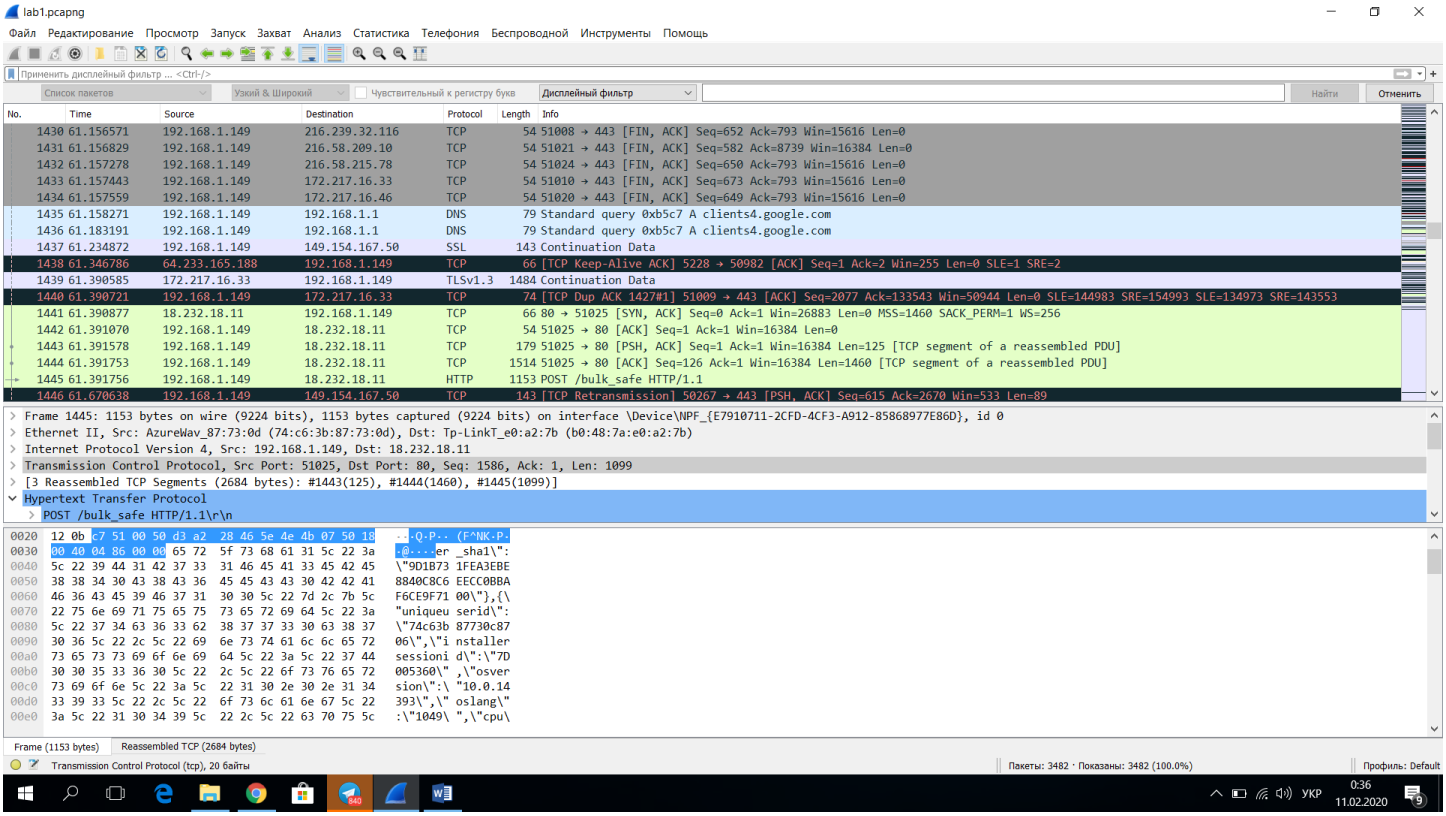
Чорний В.В.

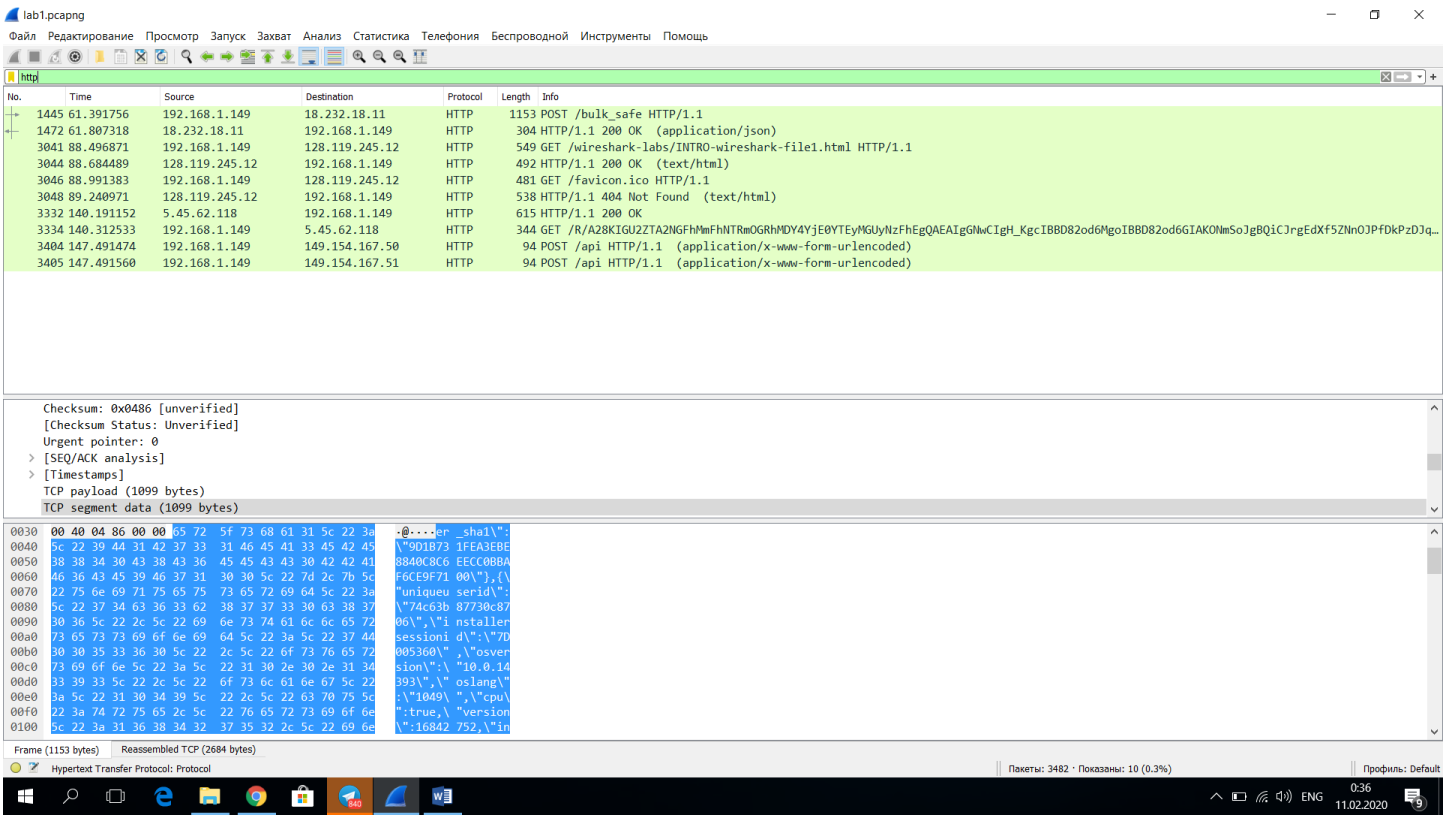
Перевірив: Кухарєв С. О.

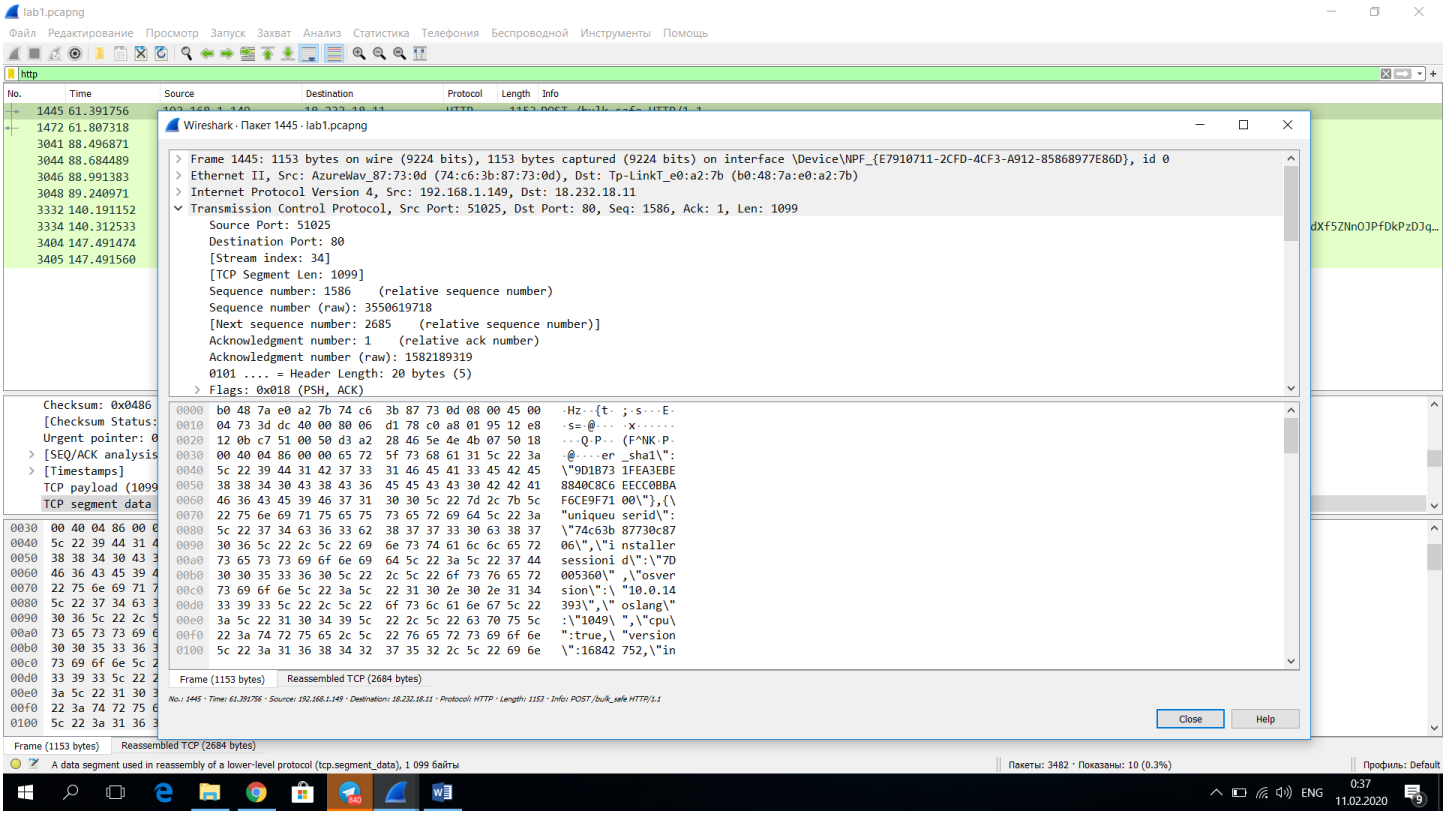
Київ 2020

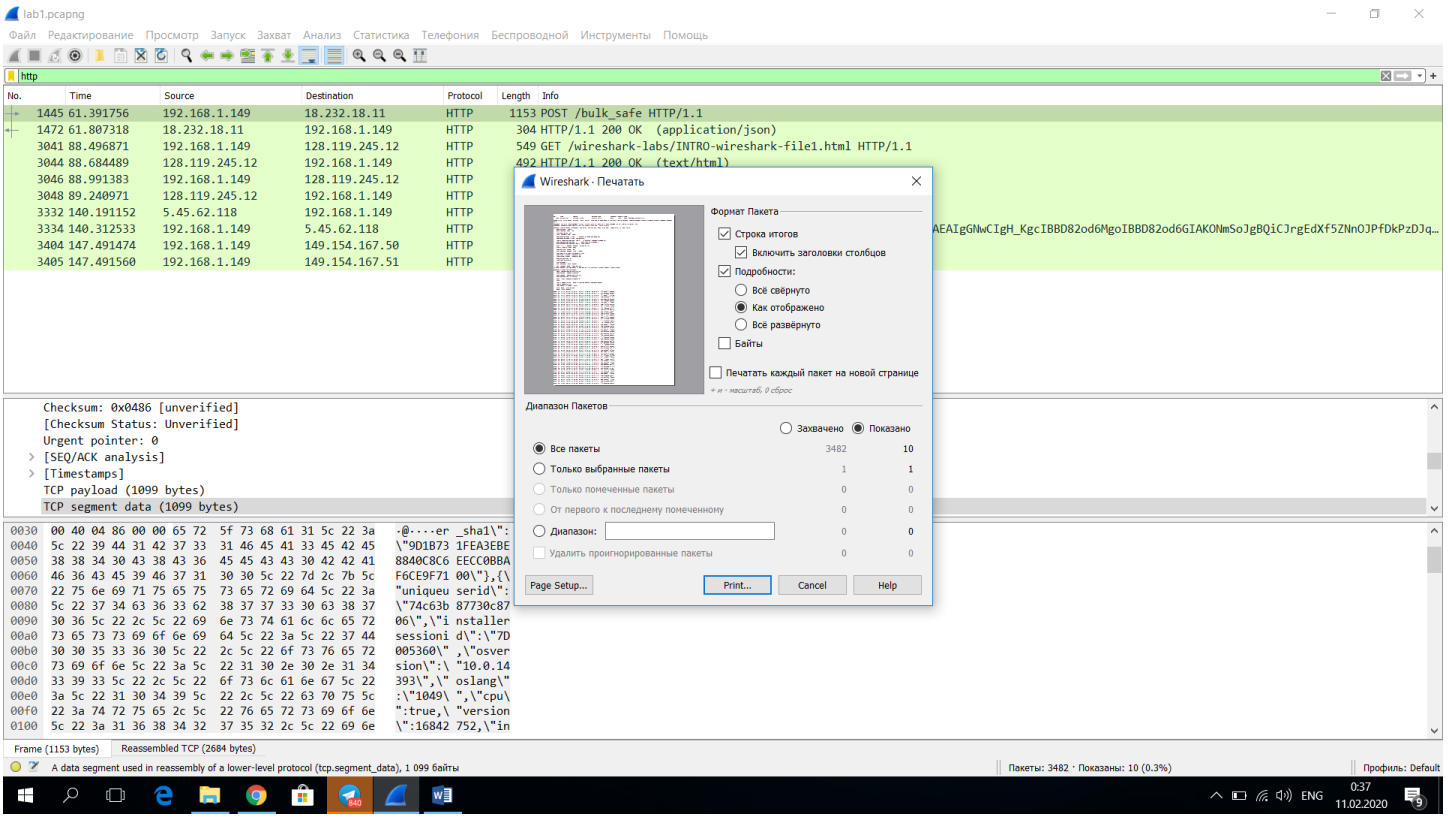
Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

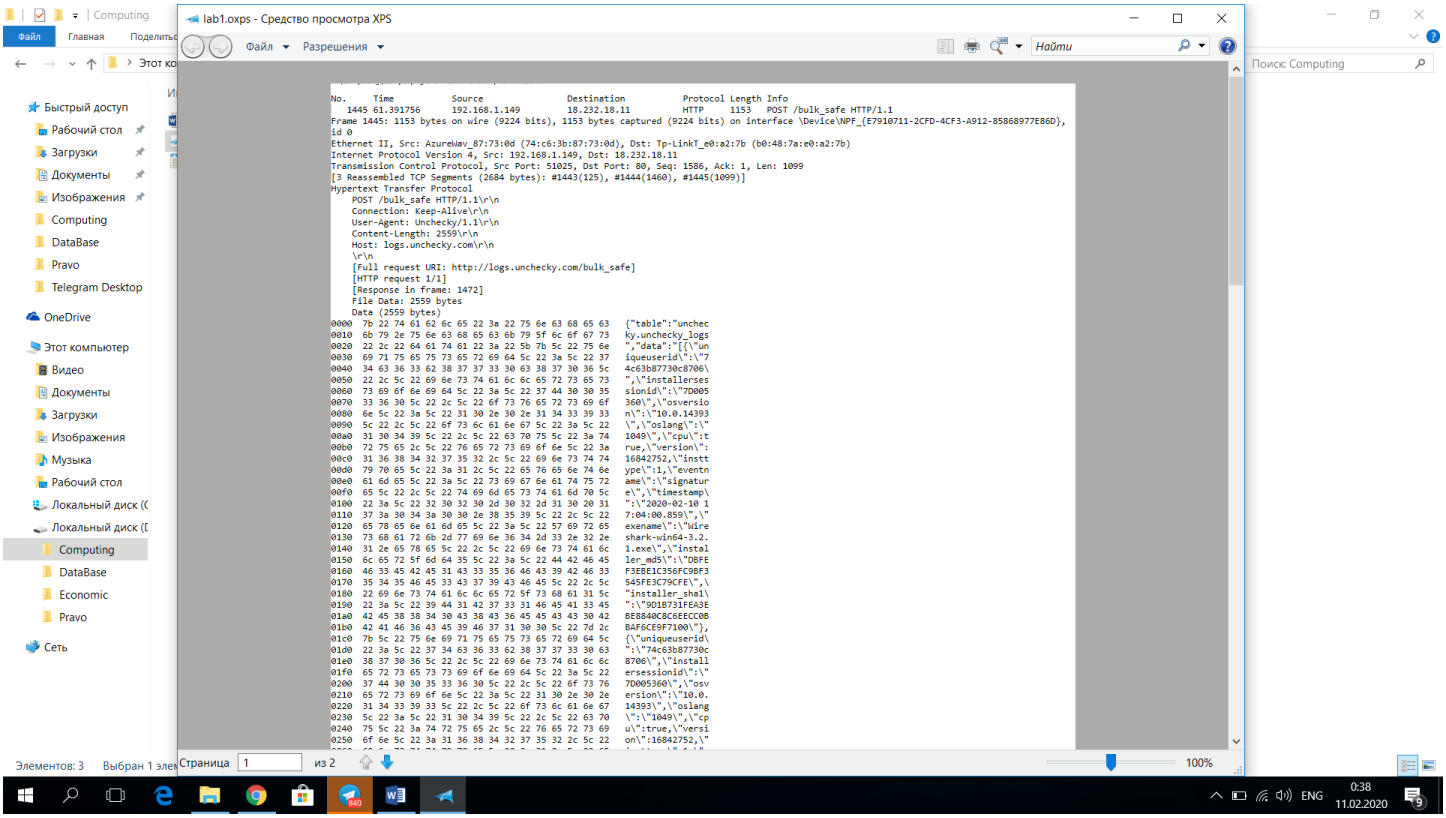
Хід виконання роботи






lab1.pcapng
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
http
No. Time Source Destination Protocol Length Info
1445 61.391756
1472 61.807318
3041 88.496871
3044 88.684489
3046 88.991383
3048 89.240971
3332 140.191152
3334 140.312533
3404 147.491474
3405 147.491560
Wireshark · Пакет 1445 · lab1.pcapng
Frame 1445: 1153 bytes on wire (9224 bits), 1153 bytes captured (9224 bits) on interface \Device\NPF_{E7910711-2CFD-4CF3-A912-85868977E86D}, id 0
Ethernet II, Src: AzureWav_87:73:0d (74:c6:3b:87:73:0d), Dst: Tp-LinkT_e0:a2:7b (b0:48:7a:e0:a2:7b)
Internet Protocol Version 4, Src: 192.168.1.149, Dst: 18.232.18.11
Transmission Control Protocol, Src Port: 51025, Dst Port: 80, Seq: 1586, Ack: 1, Len: 1099
Source Port: 51025
Destination Port: 80
[Stream index: 34]
[TCP Segment Len: 1099]
Sequence number: 1586 (relative sequence number)
Sequence number (raw): 3550619718
[Next sequence number: 2685 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1582189319
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Frame (1153 bytes)
Reassembled TCP (2684 bytes)
Close
Help
Checksum: 0x0486
[Checksum Status:
Urgent pointer: 0
[SEQ/ACK analysis
[Timestamps]
TCP payload (1099
TCP segment data
Frame (1153 bytes)
Reassembled TCP (2684 bytes)
A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1 099 байты
Пакеты: 3482 · Показаны: 10 (0.3%)
Профиль: Default
ENG
0:37
11.02.2020


lab1.pcapng
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
http
No. Time Source Destination Protocol Length Info
1445 61.391756 192.168.1.149 18.232.18.11 HTTP 1153 POST /bulk_safe HTTP/1.1
1472 61.807318 18.232.18.11 192.168.1.149 HTTP 304 HTTP/1.1 200 OK (application/json)
3041 88.496871 192.168.1.149 128.119.245.12 HTTP 549 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3044 88.684489 128.119.245.12 192.168.1.149 HTTP 492 HTTP/1.1 200 OK (text/html)
3046 88.991383 192.168.1.149 128.119.245.12 HTTP
3048 89.240971 128.119.245.12 192.168.1.149 HTTP
3332 140.191152 5.45.62.118 192.168.1.149 HTTP
3334 140.312533 192.168.1.149 5.45.62.118 HTTP
3404 147.491474 192.168.1.149 149.154.167.50 HTTP
3405 147.491560 192.168.1.149 149.154.167.51 HTTP
Wireshark · Печатать
Формат Пакета
Строка итогов
Включить заголовки столбцов
Подробности:
Всё свёрнуто
Как отображено
Всё развёрнуто
Байты
Печатать каждый пакет на новой странице
Диапазон Пакетов
Захвачено
Показано
Все пакеты 3482 10
Только выбранные пакеты 1 1
Только помеченные пакеты 0 0
От первого к последнему помеченному 0 0
Диапазон: 0 0
Удалить проигнорированные пакеты 0 0
Page Setup...
Print...
Cancel
Help
Checksum: 0x0486 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1099 bytes)
TCP segment data (1099 bytes)
Frame (1153 bytes)
Reassembled TCP (2684 bytes)
A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1 099 байты
Пакеты: 3482 · Показаны: 10 (0.3%)
Профиль: Default
ENG
0:37
11.02.2020



Контрольні питання

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

   TCP, HTTP, DNS, SSL, TLSv1.3, ICMPv6, UDP

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

ICP, Ethernet II, HTTP, TCP.

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

Пройшло 0,002954 с.

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

Запит:

Вихідна:192.168.1.149

Цільова:18.232.18.11

Відповідь:

Вихідний:18.232.18.11

Цільовий:192.168.1.149

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

```
POST /bulk_safe HTTP/1.1
```

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

```
HTTP/1.1 200 OK  (application/json)
```

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Було проаналізовано час за який було відправлено перший запит та отримано першу відповідь, а також було розглянуто протоколи HTTP.