

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-ЗП91

Вдовенко А.М.

Прийняв: Кухарєв С.О.

Київ – 2020

## Лабораторна робота №1

### Хід роботи

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
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)

Захват из Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
19	3.330982	192.168.0.103	216.58.215.78	UDP	76	61999 → 443 Len=34
20	4.110133	192.168.0.103	74.125.205.188	TCP	55	54481 → 5228 [ACK] Seq=1 Ack=1 Win=256 Len=1
21	4.153073	74.125.205.188	192.168.0.103	TCP	66	5228 → 54481 [ACK] Seq=1 Ack=2 Win=262 Len=0 SLE=1 SRE=2
22	4.291213	192.168.0.103	172.217.20.174	TCP	55	54614 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled ...
23	4.315425	172.217.20.174	192.168.0.103	TCP	66	443 → 54614 [ACK] Seq=1 Ack=2 Win=242 Len=0 SLE=1 SRE=2
24	4.839084	192.168.0.103	216.58.209.14	TCP	54	54492 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0
25	4.839158	192.168.0.103	216.58.215.112	TCP	54	54559 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0
26	4.839189	192.168.0.103	77.120.15.13	TCP	54	54493 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
27	4.856793	77.120.15.13	192.168.0.103	TCP	60	80 → 54493 [FIN, ACK] Seq=1 Ack=2 Win=282 Len=0
28	4.856829	192.168.0.103	77.120.15.13	TCP	54	54493 → 80 [ACK] Seq=2 Ack=2 Win=256 Len=0
29	4.863571	216.58.209.14	192.168.0.103	TCP	60	80 → 54492 [FIN, ACK] Seq=1 Ack=2 Win=263 Len=0
30	4.863610	192.168.0.103	216.58.209.14	TCP	54	54492 → 80 [ACK] Seq=2 Ack=2 Win=258 Len=0
31	4.870754	216.58.215.112	192.168.0.103	TCP	60	80 → 54559 [FIN, ACK] Seq=1 Ack=2 Win=254 Len=0
32	4.870793	192.168.0.103	216.58.215.112	TCP	54	54559 → 80 [ACK] Seq=2 Ack=2 Win=258 Len=0
33	4.951156	192.168.0.103	64.233.165.189	UDP	75	54347 → 443 Len=33

> Frame 30: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{5D269C81-0675-4786-BA9F-91DAFBA3D47B}, id 0  
> Ethernet II, Src: Giga-Byt\_03:f8:9e (fc:aa:14:03:f8:9e), Dst: Tp-LinkT\_e3:01:00 (50:c7:bf:e3:01:00)  
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 216.58.209.14  
> Transmission Control Protocol, Src Port: 54492, Dst Port: 80, Seq: 2, Ack: 2, Len: 0

0000

50 c7 bf e3 01 00 fc aa 14 03 f8 9e 08 00 45 00

P-----E-

0010

00 28 73 62 40 00 80 06 1d 15 c0 a8 00 67 d8 3a

.(sb@---g:

0020

d1 0e d4 dc 00 50 57 bc 66 3c 6d 1b b6 09 50 10

-----PW fcm--P-

0030

01 02 8e 2f 00 00

---/..

Ethernet: <live capture in progress>

Пакеты: 447 · Показаны: 447 (100.0%)

Профиль: Default

Рис 1.1 – Результати виклику

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

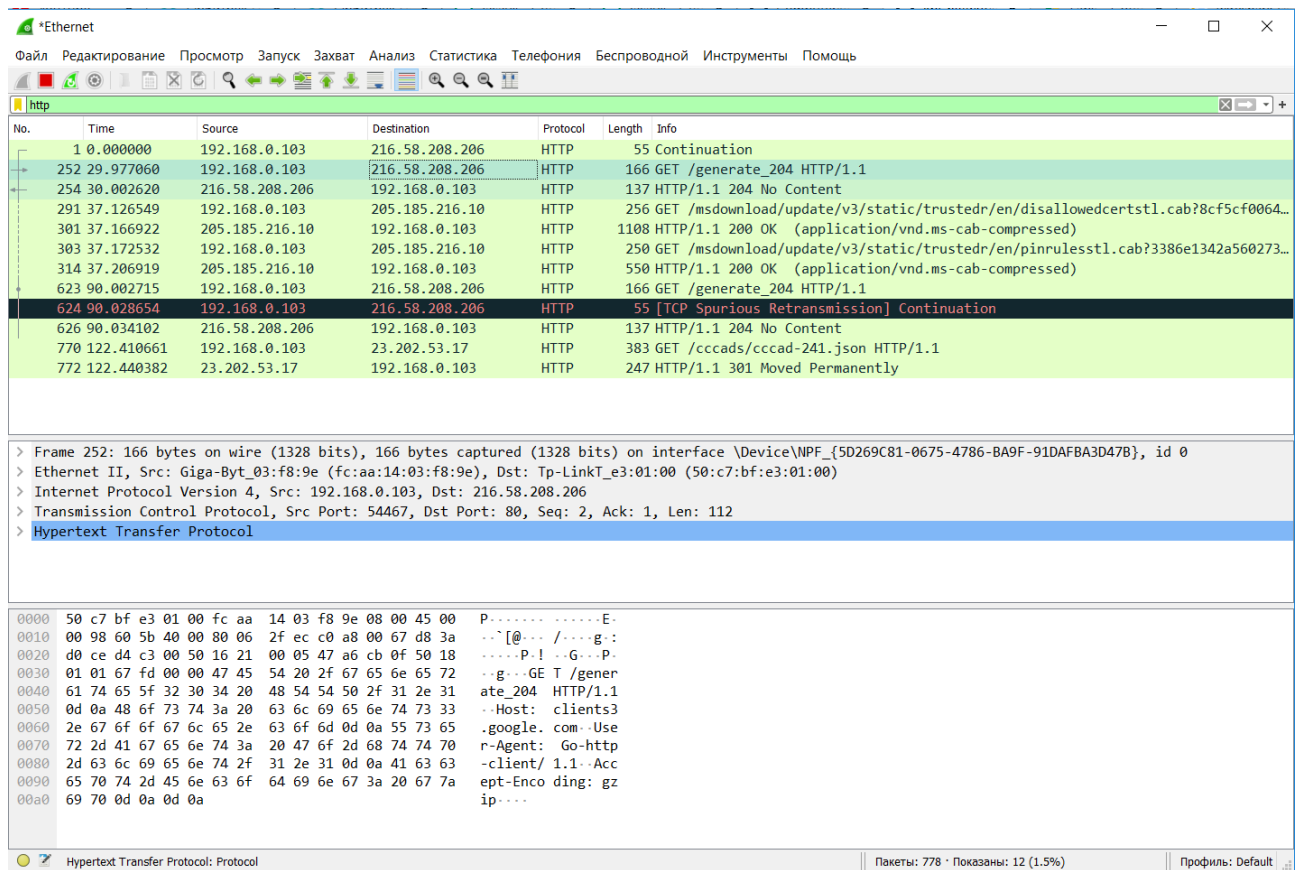


Рис 1.2 – Результати фільтрації

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 відкрийте детальну інформацію про інші протоколи.

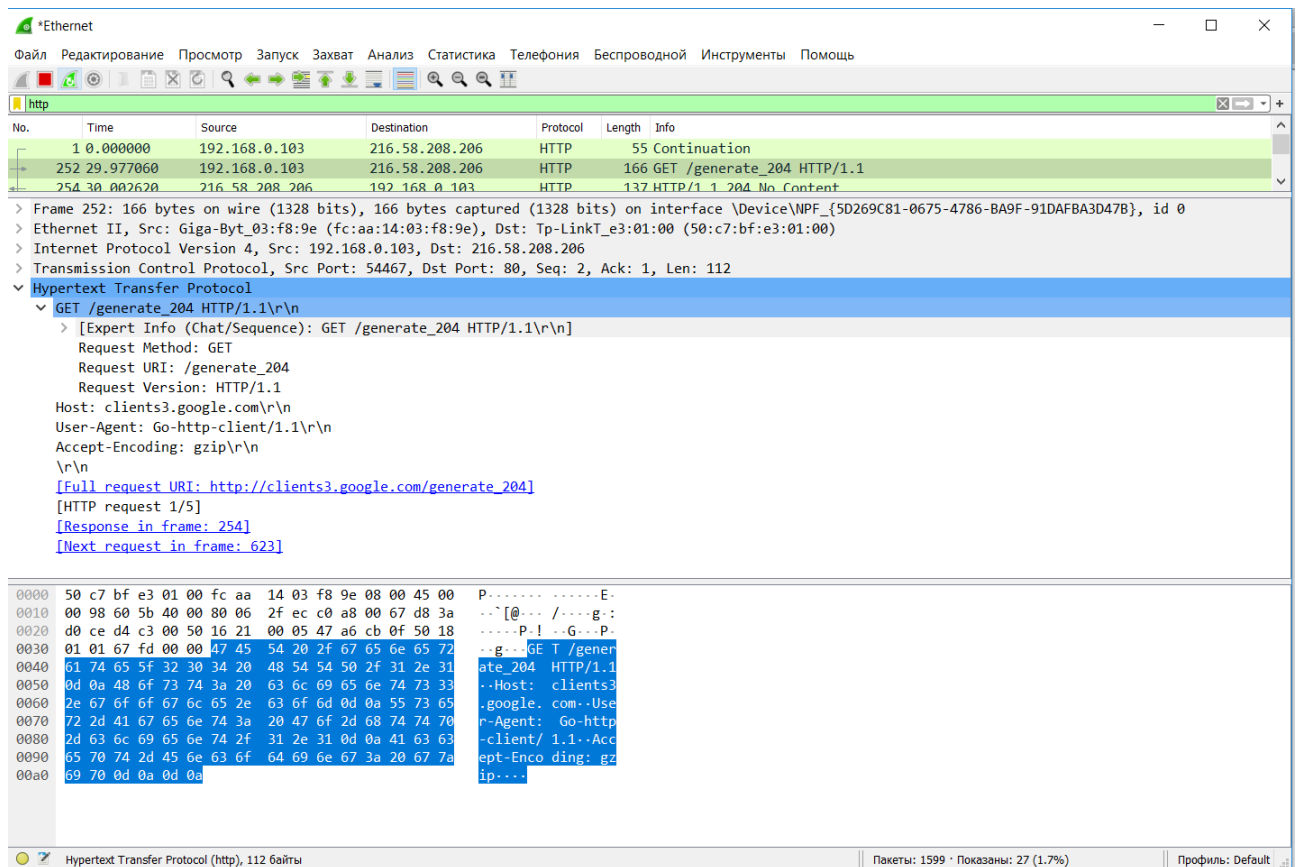


Рис 1.3 – Деталі HTTP пакету

10. Роздрукуйте перші пакети запиту та відповіді. Для цього слід виділити пакет, який бажано роздрукувати, та активувати команду File > Print, та налаштувати його так як показано на Малюнку 3 (ім'я файлу слід змінити на більш інформативне).

### Контрольні запитання:

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

- DNS, TCP, HTTP, UDP, ARP, SSDP,

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

- [Protocols in frame: eth:ethertype:ip:tcp:http]

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

- Request: Arrival Time: May 26, 2020 20:32:59.800332000 FLE Daylight Time
- Response: Arrival Time: May 26, 2020 20:32:59.926965000 FLE Daylight Time
- ~1.266 ms

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

- Request: SRC: 192.168.1.248 DST: 128.119.245.12
- Response: SRC: 128.119.245.12 DST: 192.168.1.248

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

- GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

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

- HTTP/1.1 200 OK\r\n