

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

Лабораторна робота №1
з дисципліни «Комп'ютерні мережі»

**«Стеки мережевих протоколів.
Аналізатор мережевого трафіку Wireshark»**

Виконала студентка групи: КВ-11

ПІБ: Михайліченко Софія Віталіївна

Перевірив: _____

Київ 2024

Мета роботи:

Засвоєння функцій модулів різних рівнів еталонної моделі OSI, процедури інкапсуляції та формування повідомлень для передачі в мережу; ознайомлення та вивчення аналізатора мережевого трафіку Wireshark.

План виконання лабораторної роботи:

1. Ознайомитися та засвоїти теоретичні відомості про еталонну модель взаємодії відкритих систем OSI та стек мережевих протоколів TCP/IP.
2. Ознайомитися з можливостями аналізатора мережевого трафіку Wireshark.
3. За допомогою аналізатора Wireshark виконати захоплення та провести аналіз мережевих пакетів.

Завдання:

1. При виконанні роботи використовується програмне забезпечення для аналізу протоколів комп'ютерних мереж Wireshark. Запустити відповідну програму.
2. Вибрати інтерфейс для захоплення трафіку (меню Capture/Interface) та активізувати режим захоплення.
3. Скопіювати через мережу файл розміром кілька десятків Мбайт.
4. Завершити захоплення трафіку та перейти до режиму аналізу. В захопленому фрагменті виберіть кадр, який містить пакет TCP. Виділіть складові частини кадру. Знайдіть в кадрі транспортні, логічні та фізичні адреси відправника та отримувача.

Короткі теоретичні відомості:

1. Еталонна модель OSI:

Модель OSI (Open Systems Interconnection) складається з семи рівнів, кожен з яких виконує специфічні функції для забезпечення комунікації між комп'ютерами.

- **Фізичний рівень:**

Відповідає за передачу бітів через фізичні середовища (кабелі, бездротові канали).

- **Канальний рівень:**

Забезпечує надійну передачу даних між сусідніми пристроями, включаючи контроль помилок і управління доступом до середовища.

- **Мережевий рівень:**

Відповідає за маршрутизацію пакетів між різними мережами, використовуючи IP-адресацію.

- **Транспортний рівень:**

Забезпечує надійну передачу даних між кінцевими точками, включаючи сегментацію, контроль потоку та корекцію помилок (TCP, UDP).

- **Сеансовий рівень:**

Встановлює, управляє та завершує сеанси зв'язку між додатками.

- **Представницький рівень:**

Відповідає за форматування та кодування даних, забезпечуючи їхню сумісність між різними системами.

- **Прикладний рівень:**

Інтерфейс для користувача та додатків, що забезпечує доступ до мережевих сервісів (HTTP, FTP, SMTP).

2. Стек протоколів TCP/IP:

Стек TCP/IP є основою Інтернету і складається з чотирьох рівнів:

- **Прикладний рівень:** Включає протоколи, які забезпечують доступ до мережевих сервісів (HTTP, FTP).

- **Транспортний рівень:** Включає TCP (надійний, з контролем помилок) та UDP (швидкий, без контролю помилок).
- **Мережевий рівень:** Включає IP-протокол, який відповідає за адресацію та маршрутизацію пакетів.
- **Мережевих інтерфейсів:** Включає протоколи, що забезпечують передачу даних через фізичні середовища (Ethernet, Wi-Fi).

3. Інкапсуляція:

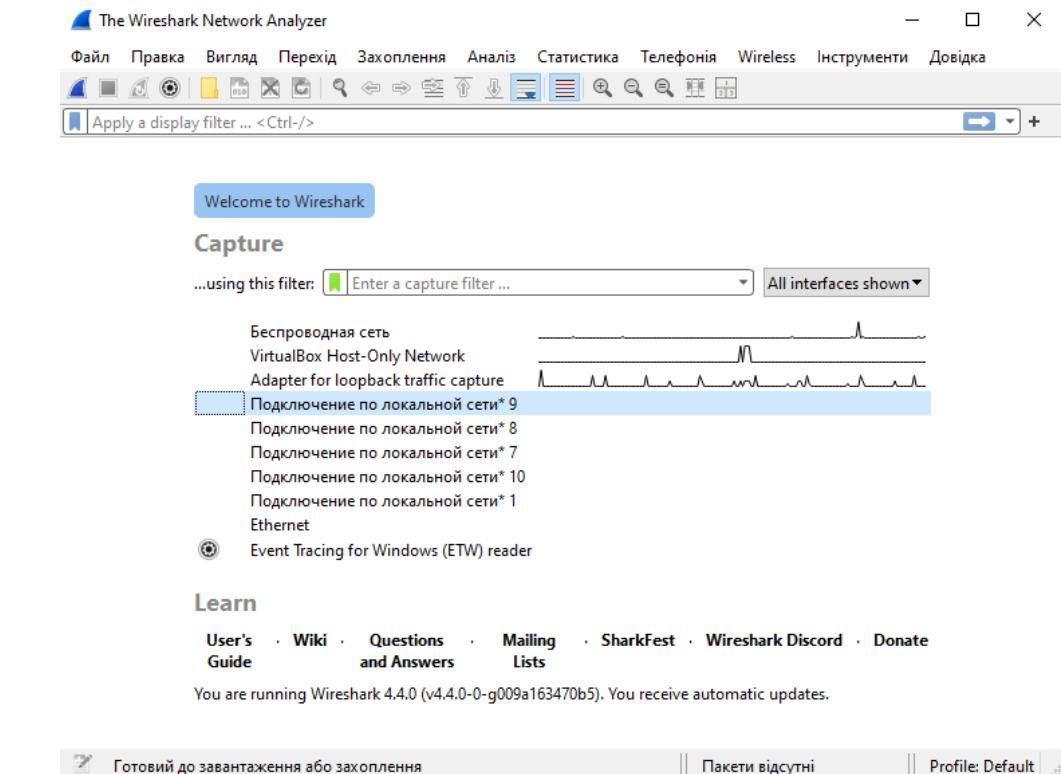
Інкапсуляція — це процес, при якому дані на вищому рівні обгортаються в заголовки на нижчому рівні. Наприклад, дані на прикладному рівні обгортаються в TCP-сегменти, які, в свою чергу, обгортаються в IP-пакети, а потім у Ethernet-кадри. Це дозволяє передавати дані через різні мережеві технології.

4. Wireshark:

Wireshark — це потужний інструмент для аналізу мережевого трафіку, який дозволяє захоплювати, переглядати та аналізувати пакети в реальному часі. Користувачі можуть фільтрувати дані за різними критеріями (IP-адреси, порти, протоколи) та вивчати вміст пакетів, включаючи заголовки та дані. Wireshark підтримує безліч протоколів і є незамінним інструментом для мережевих адміністраторів та фахівців з безпеки.

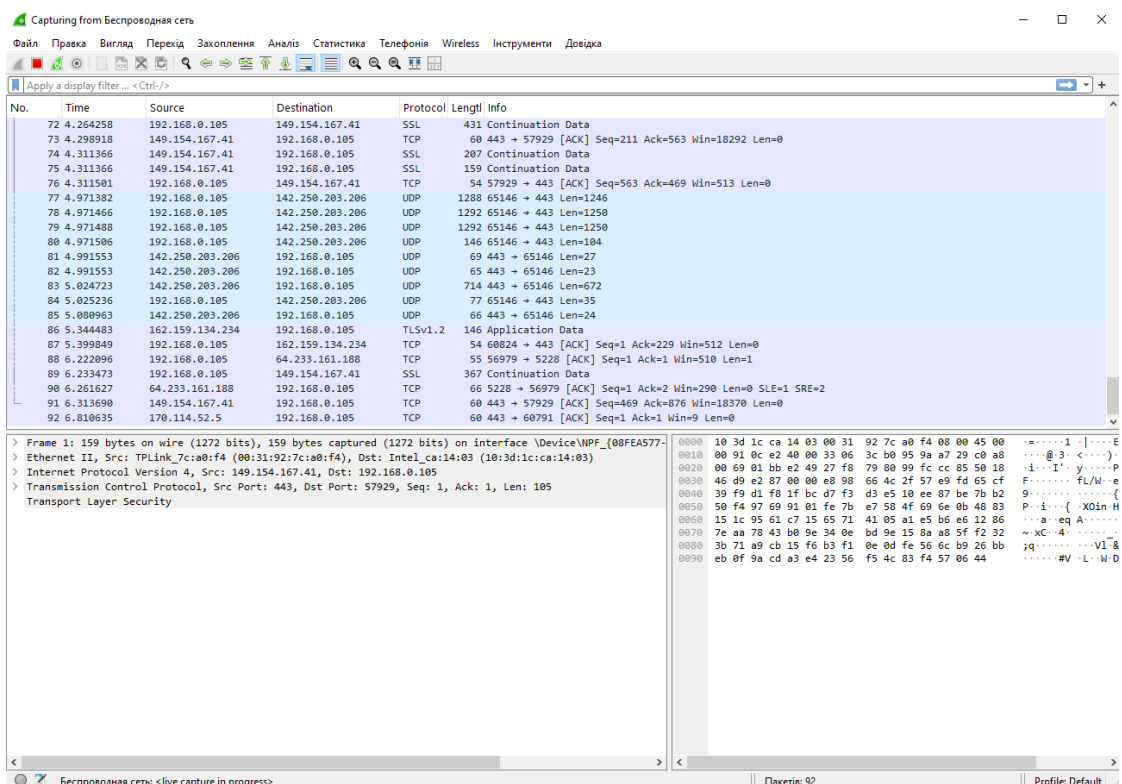
Порядок виконання роботи:

Початкове вікно програми Wireshark:



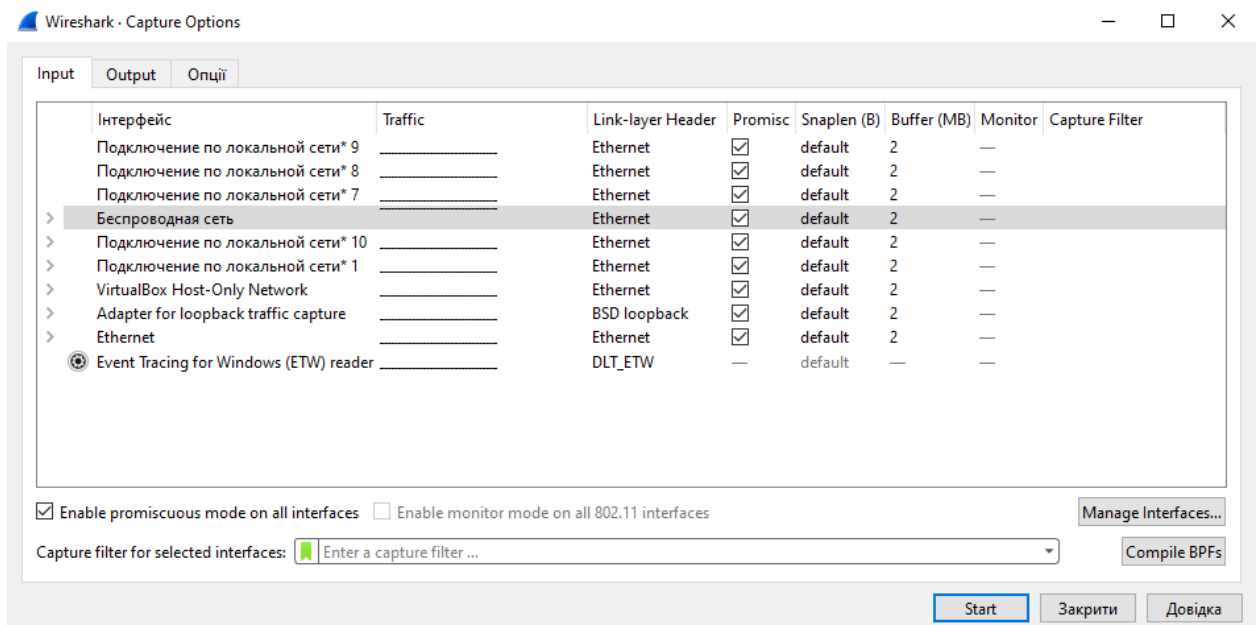
Тепер ми можемо розпочати захоплення пакетів, вибравши інтерфейс, і спостерігатимемо за процесом захоплення трафіку:

Це вікно також називають головним вікном програми.

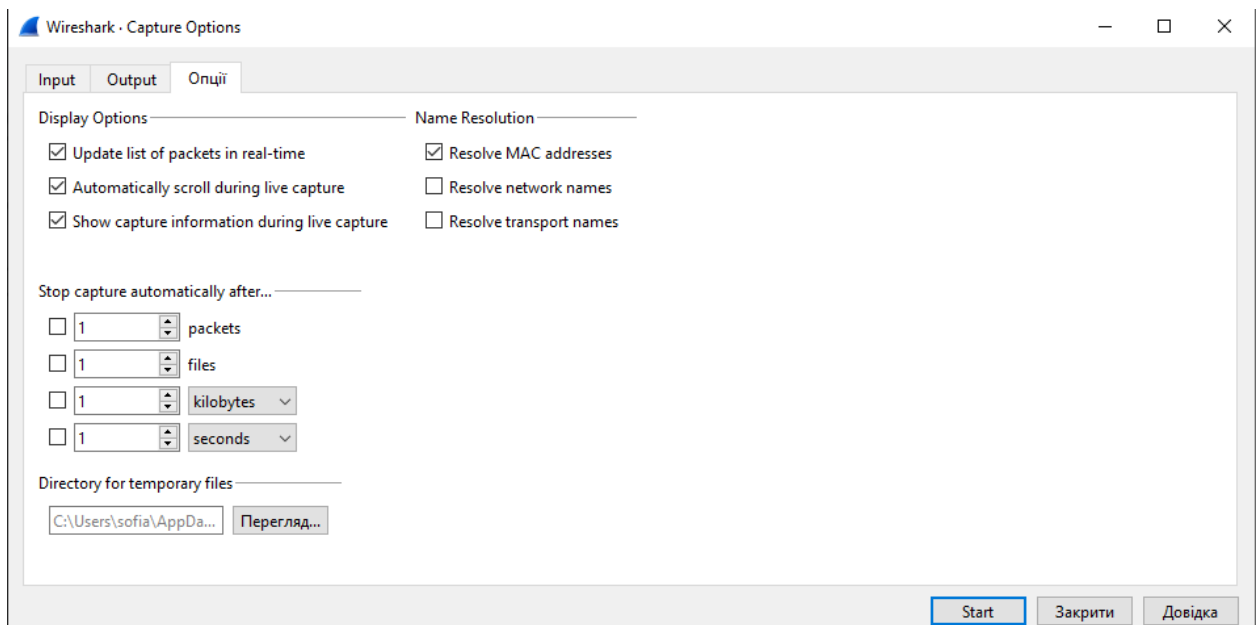


Наступним потрібно просканувати інтерфейс під час захоплення файлу розміром кілька десятків Мбайт:

Спочатку перевіримо параметри захоплення трафіку.



Як бачимо, мережевий адаптер працює у promiscuous mode, що дозволяє програмі захоплювати не тільки пакети, які були адресовані комп'ютеру, на якому вона встановлена.



Також можемо переконаватися, що ввімкнено Resolve MAC addresses; дана опція дозволяє Wireshark трансліювати знайдені мережеві адреси в імена.

Результат захоплення під час завантаження файлу:

Беспроводная сеть

Файл

Правка

Вид

Переход

Заполнения

Анализ

Статистика

Телефония

Wireless

Инструменты

Довідка

Apply a display filter ... <Ctrl-/>

No.

Time

Source

Destination

Protocol

Length

Info

1	0.000000	192.168.1.103	142.250.187.202	UDP	71	49567 → 443 Len=29
2	0.057107	142.250.187.202	192.168.1.103	UDP	67	443 → 49567 Len=25
3	0.455633	192.168.1.103	149.154.167.41	SSL	223	Continuation Data
4	0.486762	149.154.167.41	192.168.1.103	TCP	54	443 → 65191 [ACK] Seq=1 Ack=170 Win=32768 Len=0
5	0.487459	149.154.167.41	192.168.1.103	SSL	143	Continuation Data
6	0.530671	192.168.1.103	149.154.167.41	TCP	54	65191 → 443 [ACK] Seq=170 Ack=90 Win=2052 Len=0
7	0.750596	192.168.1.103	212.58.120.19	UDP	62	40794 → 20218 Len=20
8	0.751127	192.168.1.103	212.58.120.19	TCP	66	54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9	1.061016	192.168.1.103	37.215.29.165	UDP	62	40794 → 6881 Len=20
10	1.466052	192.168.1.103	104.22.0.235	TCP	66	54707 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	1.478458	104.22.0.235	192.168.1.103	TCP	66	443 → 54707 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192
12	1.478535	192.168.1.103	104.22.0.235	TCP	54	54707 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
13	1.478903	192.168.1.103	104.22.0.235	TLShv.1.2	431	Client Hello (SNI=ap11.reasonsecurity.com)
14	1.503642	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=1 Ack=378 Win=73728 Len=0
15	1.503642	104.22.0.235	192.168.1.103	TLShv.1.2	169	Server Hello, Change Cipher Spec, Encrypted Handshake Message
16	1.504386	192.168.1.103	104.22.0.235	TLShv.1.2	635	Change Cipher Spec, Encrypted Handshake Message, Application Data
17	1.557777	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=116 Ack=959 Win=73728 Len=0
18	1.557841	192.168.1.103	104.22.0.235	TLShv.1.2	164	Application Data
19	1.573524	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=116 Ack=1069 Win=73728 Len=0
20	1.670998	192.168.1.103	142.250.187.202	UDP	71	49567 → 443 Len=29
21	1.699368	104.22.0.235	192.168.1.103	TLShv.1.2	676	Application Data
22	1.699368	104.22.0.235	192.168.1.103	TLShv.1.2	85	Encrypted Alert
23	1.699505	192.168.1.103	104.22.0.235	TCP	54	54707 → 443 [ACK] Seq=1069 Ack=770 Win=130816 Len=0
24	1.700099	192.168.1.103	104.22.0.235	TCP	54	54707 → 443 [FIN, ACK] Seq=1069 Ack=770 Win=130816 Len=0
25	1.716844	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=770 Ack=1070 Win=73728 Len=0
26	1.730037	142.250.187.202	192.168.1.103	UDP	67	443 → 49567 Len=25
27	1.750995	192.168.1.103	20.199.120.182	TCP	55	49437 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1
28	1.751140	192.168.1.103	212.58.120.19	TCP	66	[TCP Retransmission] 54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
29	1.792166	20.199.120.182	192.168.1.103	TCP	66	443 → 49437 [ACK] Seq=1 Ack=2 Win=7283 Len=0 SLE=1 SRE=2
30	1.907063	2001.0:284a:364:244::2a02:ab88:2407:200e	2001.0:284a:364:244::2a02:ab88:2407:200e	Teredo	94	Direct IPv6 Connectivity Test id=0xcd63, seq=42333, hop limit=21
31	2.440423	192.168.1.103	208.89.12.87	TLShv.1.2	222	Application Data
32	2.4404501	192.168.1.103	208.89.12.87	TLShv.1.2	100	Application Data
33	2.556624	208.89.12.87	192.168.1.103	TCP	54	443 → 53712 [ACK] Seq=1 Ack=215 Win=25763 Len=0

Frame 28: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface Device\NPF_{08FEA577-06-00-00-00} (08FEA577-06-00-00-00)

Ethernet II, Src: Intel c:\4c

Далі згідно завдання нам потрібно перейти до режиму аналізу та визначити у захопленому фрагменті кадр, який містить пакет TCP:

Беспробная сеть

Файл

Правка

Вид

Перехід

Захоплення

Аналіз

Статистика

Телефонія

Wireless

Інструменти

Довідка

tcp

No.

Time

Source

Destination

Protocol

Length

Info

50	3.368128	124.225.126.114	192.168.1.103	TCP	54	19131 → 54708 [ACK] Seq=1 Ack=69 Win=65536 Len=0
52	3.368128	124.225.126.114	192.168.1.103	TCP	54	19131 → 54708 [RST, ACK] Seq=1 Ack=69 Win=65536 Len=0
47	3.057460	124.225.126.114	192.168.1.103	TCP	66	19131 → 54708 [SYN, ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=1440 SACK_PERM WS=16384
29	1.792163	20.199.120.182	192.168.1.103	TCP	66	443 → 40437 [ACK] Seq=1 Ack=2 Win=7283 Len=0 SLE=1 SRE=2
19590	8.464420	134.224.240.225	192.168.1.103	TCP	54	443 → 52995 [ACK] Seq=1 Ack=31 Win=0 Len=0
28568	11.297661	20.42.65.94	192.168.1.103	TCP	66	443 → 53694 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
37878	12.953694	151.101.130.49	192.168.1.103	TCP	66	443 → 53709 [ACK] Seq=1 Ack=2 Win=303 Len=0 SLE=1 SRE=2
33	2.556624	208.89.12.87	192.168.1.103	TCP	54	443 → 53712 [ACK] Seq=1 Ack=215 Win=25763 Len=0
42454	13.844278	208.89.12.87	192.168.1.103	TCP	54	443 → 53712 [ACK] Seq=1889 Ack=513 Win=26061 SLE=1 SRE=0
42	2.837366	208.89.12.87	192.168.1.103	TCP	54	443 → 53712 [ACK] Seq=945 Ack=257 Win=25805 Len=0
41135	13.559689	208.89.12.87	192.168.1.103	TCP	54	443 → 53712 [ACK] Seq=945 Ack=471 Win=26019 Len=0
58404	16.747586	185.199.109.154	192.168.1.103	TCP	66	443 → 53833 [ACK] Seq=1 Ack=2 Win=424 Len=0 SLE=1 SRE=2
58794	16.918405	185.199.111.133	192.168.1.103	TCP	66	443 → 53834 [ACK] Seq=1 Ack=2 Win=304 Len=0 SLE=1 SRE=2
34032	12.250437	185.199.109.154	192.168.1.103	TCP	66	443 → 53839 [ACK] Seq=1 Ack=2 Win=298 Len=0 SLE=1 SRE=2
58822	18.091384	34.98.64.218	192.168.1.103	TCP	66	443 → 53847 [ACK] Seq=1 Ack=2 Win=301 Len=0 SLE=1 SRE=2
20836	9.561743	23.52.185.186	192.168.1.103	TCP	66	443 → 54125 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
20730	9.535756	23.52.185.186	192.168.1.103	TCP	66	443 → 54126 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
22080	9.889338	23.52.185.186	192.168.1.103	TCP	66	443 → 54131 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
20834	9.561743	23.52.185.186	192.168.1.103	TCP	66	443 → 54147 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
20835	9.561743	23.52.185.186	192.168.1.103	TCP	66	443 → 54148 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
26324	10.830612	18.66.233.26	192.168.1.103	TCP	54	443 → 54181 [ACK] Seq=41 Ack=2 Win=145 Len=0
26214	10.816330	18.66.233.26	192.168.1.103	TCP	54	443 → 54181 [FIN, ACK] Seq=0 Ack=1 Win=145 Len=0
27005	10.968985	18.66.233.26	192.168.1.103	TCP	54	443 → 54192 [ACK] Seq=41 Ack=2 Win=151 Len=0
26908	10.952192	18.66.233.26	192.168.1.103	TCP	54	443 → 54192 [FIN, ACK] Seq=1 Ack=2 Win=151 Len=0
34346	12.316519	40.99.211.2	192.168.1.103	TCP	54	443 → 54426 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

> Frame 50: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{08FEA577-08-00-00-00} Ethernet II, Src: MercuryComm_08:c0:a5:dd:08:cf:1e, Dst: Intel_c0:a1:10:00:00:00:00:00:00

Internet Protocol Version 4, Src: 124.225.126.114, Dst: 192.168.1.103

Transmission Control Protocol, Src Port: 19131, Dst Port: 54708, Seq: 1, Ack: 69, Len: 0

0000 10 3d 1c ca 14 03 c0 a5 dd 08 cf 1e 08 00 45 00E

0010 00 28 dd 3d 40 00 31 06 af 2f 7c e1 7e 72 c0 a8 (.=@.1./~.~

0020 01 67 4a bb d5 b4 1d cb 9d 65 3e 42 19 a2 50 10 g3.....e3~.P

0030 00 04 be e8 00 00

Transmission Control Protocol: Protocol

Пакети: 58892 · Displayed: 203 (0.3%) · Dropped: 0 (0.0%)

Profile: Default

У даному кадрі нам потрібно виділити його складові частини:

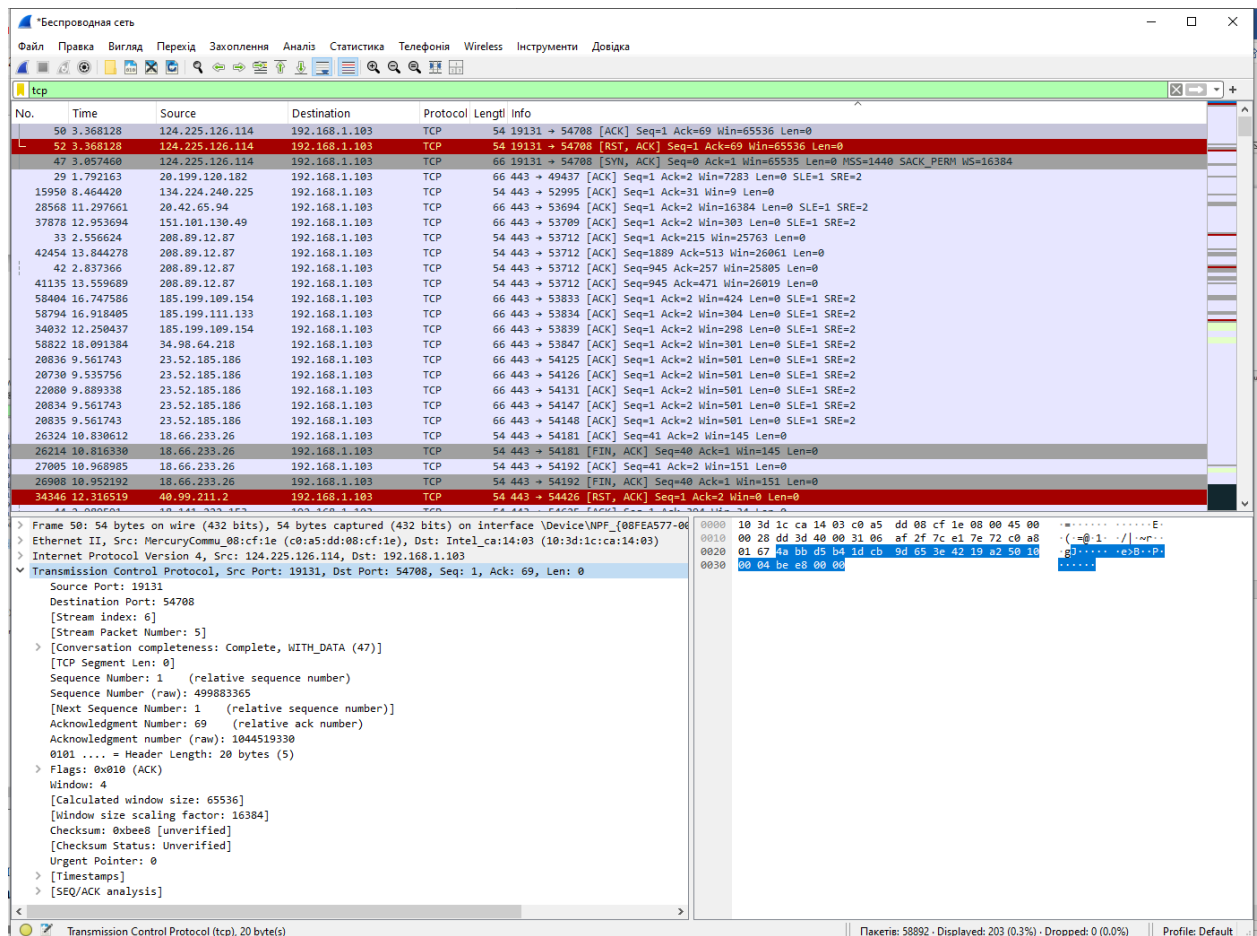
- Заголовок кадру:

Wireshark packet capture showing a TCP RST packet. The packet list shows packet 54 as a RST from 192.168.1.103 to 124.225.126.114. The packet details show Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

- IP-заголовок:

Wireshark packet capture showing the IP header of packet 54. The packet details pane is expanded to show the Internet Protocol Version 4 header, including fields like Version, Header Length, Differentiated Services Field, Total Length, Identification, Flags, Fragment Offset, Time to Live, Protocol, Header Checksum, Source Address, and Destination Address.

- TCP-заголовок:

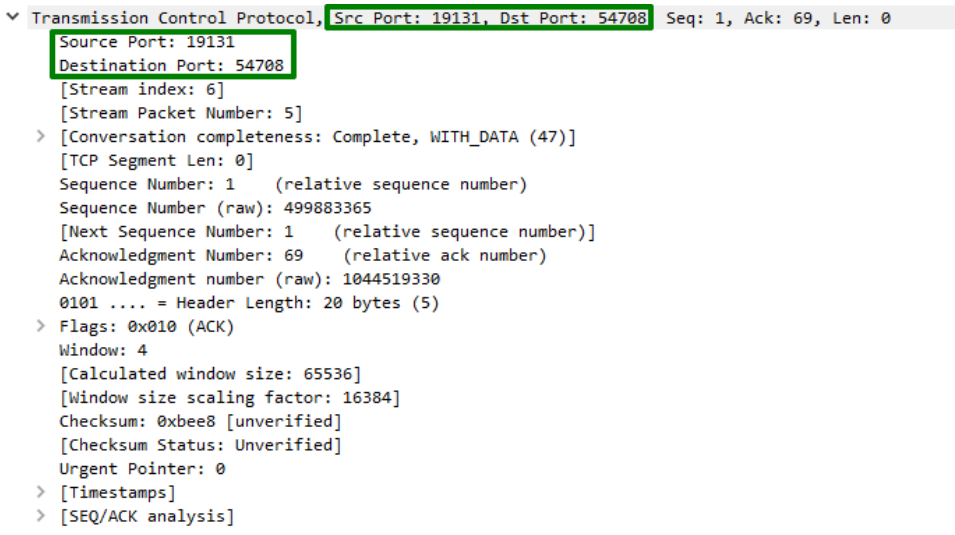


Також знайдемо у кадрі транспортні, логічні та фізичні адреси відправника та отримувача:

Адреса	Транспортна	Логічна	Фізична
Відправника	19131	124.225.126.114	c0:a5:dd:08:cf:1e
Отримувача	54708	192.168.1.103	10:3d:1c:ca:14:03

Source — відправник, **Destination** — отримувач

Транспорна



Логічна

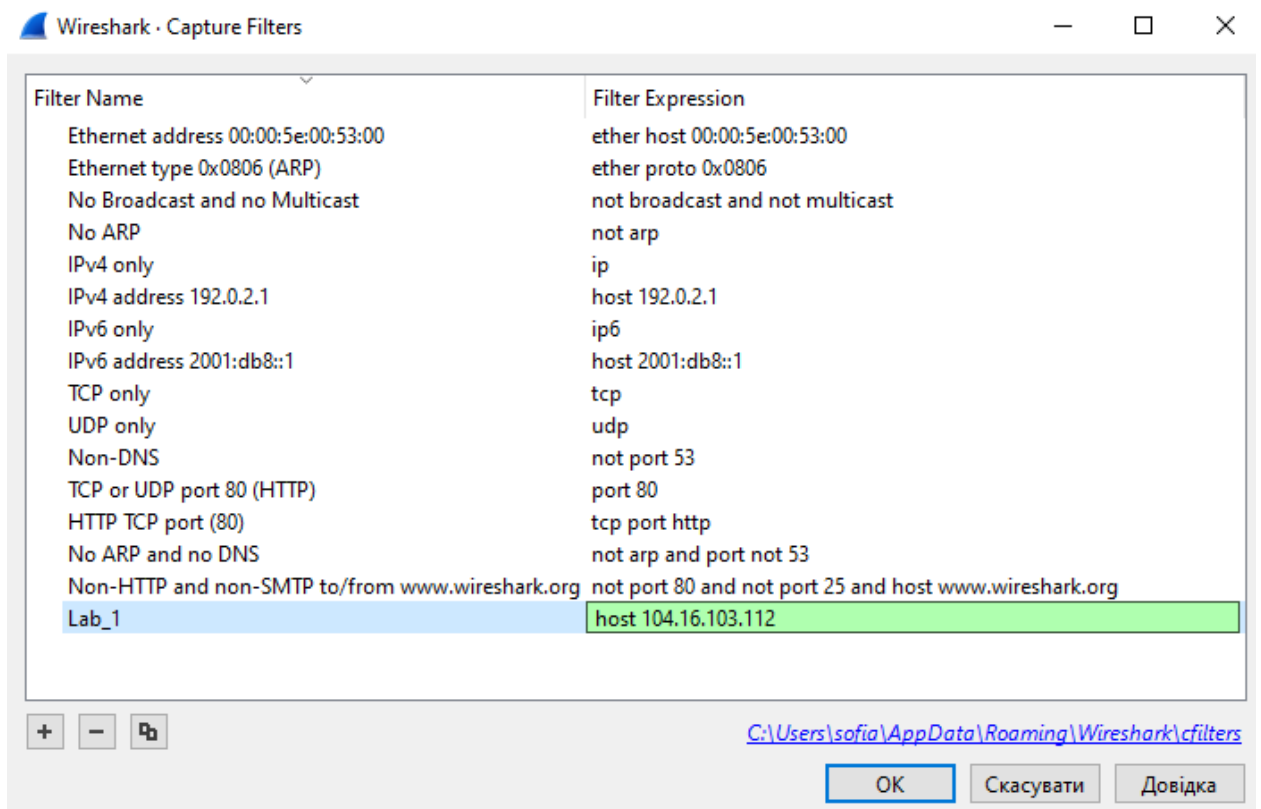
```
Internet Protocol Version 4, Src: 124.225.126.114, Dst: 192.168.1.103
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xdd3d (56637)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 49
    Protocol: TCP (6)
    Header Checksum: 0xaf2f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 124.225.126.114
    Destination Address: 192.168.1.103
    [Stream index: 9]
```

Фізична

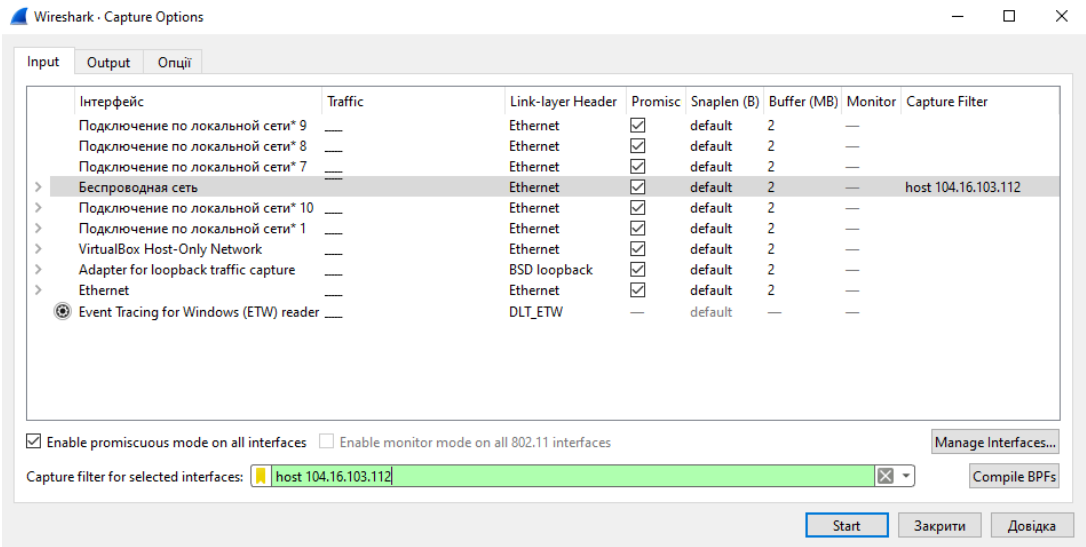
```
▼ Ethernet II, Src: MercuryCommu 08:cf:1e (c0:a5:dd:08:cf:1e), Dst: Intel ca:14:03 (10:3d:1c:ca:14:03)
  > Destination: Intel_ca:14:03 (10:3d:1c:ca:14:03)
  > Source: MercuryCommu_08:cf:1e (c0:a5:dd:08:cf:1e)
    Type: IPv4 (0x0800)
    [Stream index: 0]
```

Створення фільтрів у Wireshark

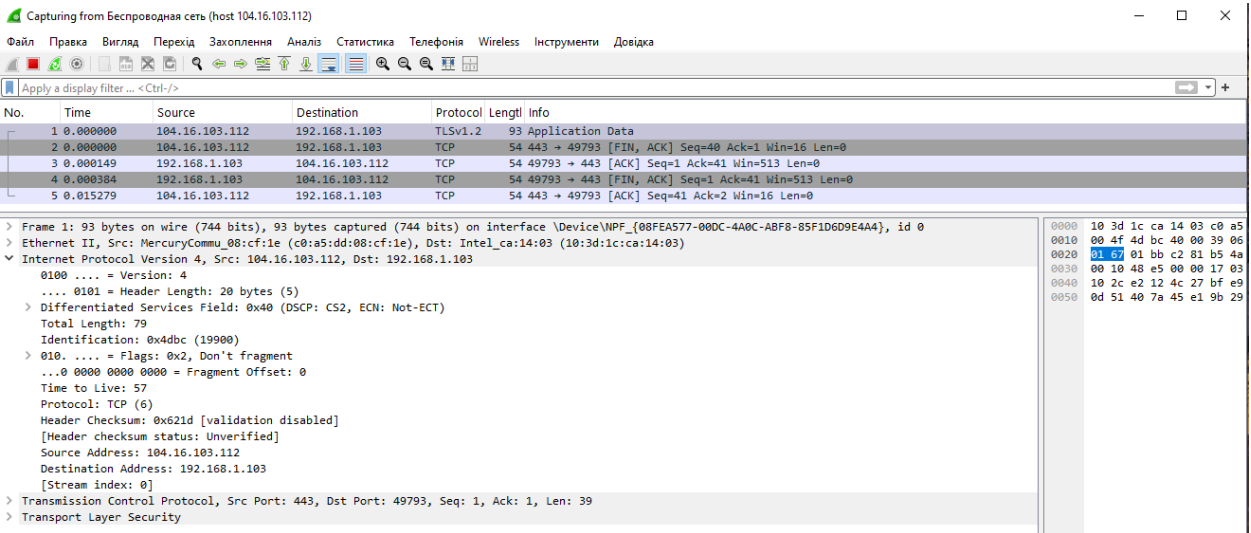
Створимо фільтр Download File, який буде захоплювати пакети з логічною адресою:



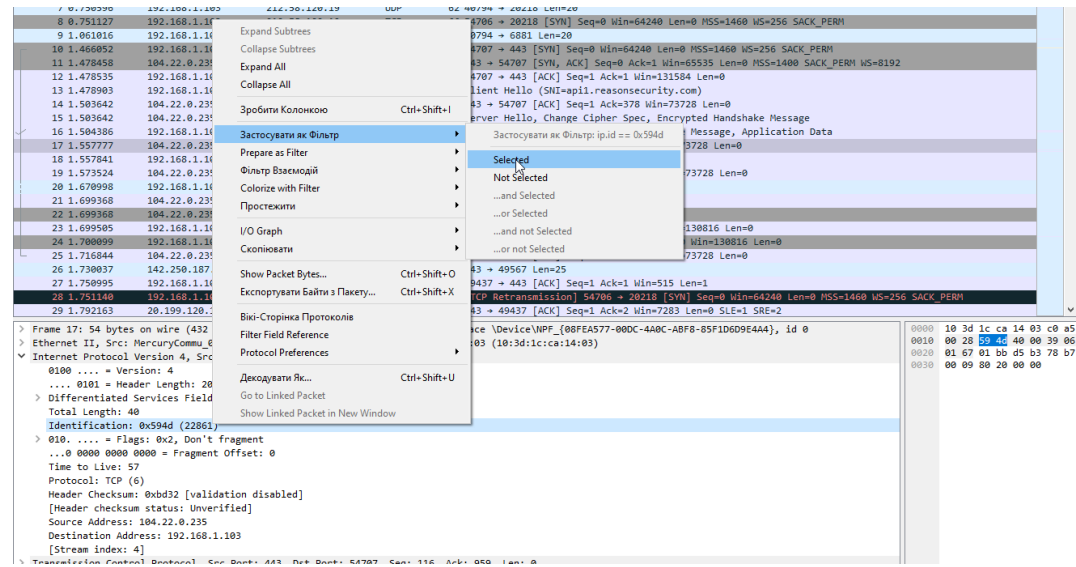
Вибираємо інтерфейс та сам фільтр, слідуємо, щоб рядок фільтра позеленів, що свідчить про його коректність:



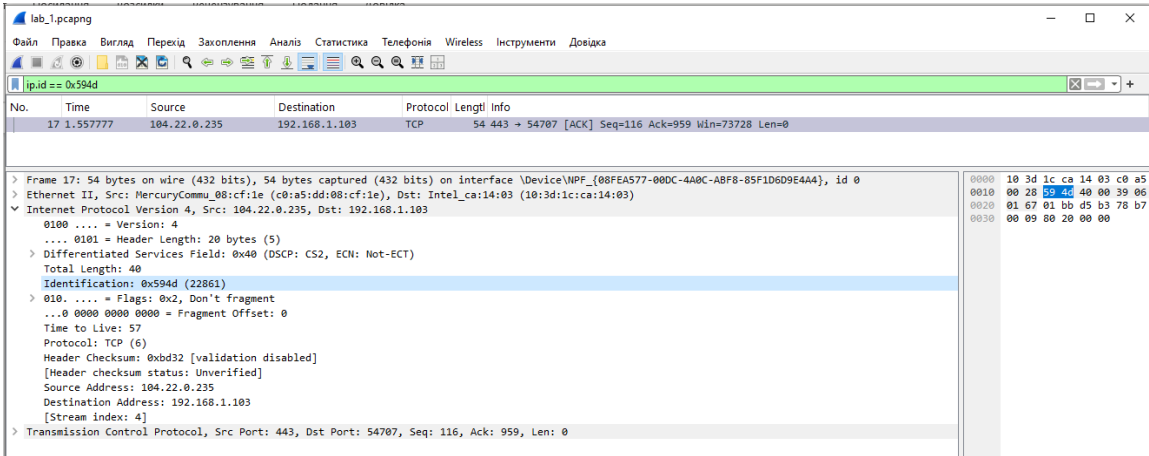
Результати захоплення зі застосуванням фільтру:



Також можна застосовувати фільтр виділивши будь-яку область пакету:



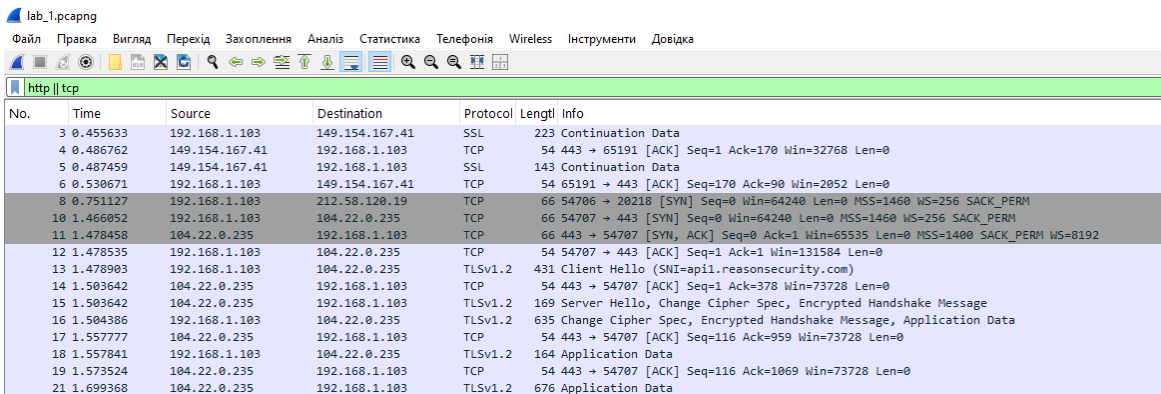
Результат використання фільтру:



No.	Time	Source	Destination	Protocol	Length	Info
17	1.557777	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=116 Ack=959 Win=73728 Len=0

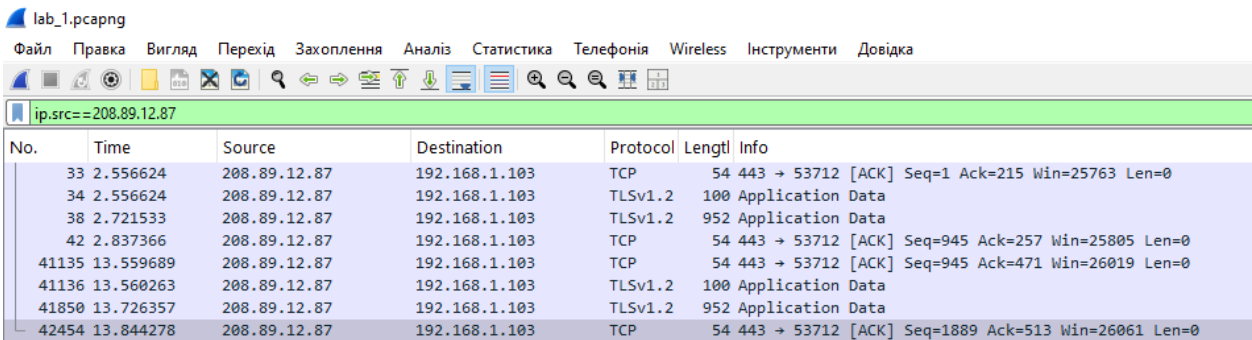
> Frame 17: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{08FEA577-00DC-4A0C-ABF8-85F1D6D9E4A4}, id 0
> Ethernet II, Src: MercuryCommu_08:cf:1e (c0:a5:dd:08:cf:1e), Dst: Intel_ca:14:03 (10:3d:1c:ca:14:03)
> Internet Protocol Version 4, Src: 104.22.0.235, Dst: 192.168.1.103
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x40 (DSCP: CS2, ECN: Not-ECT)
 Total Length: 40
 Identification: 0x594d (22861)
 > 010 = Flags: 0x2, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 57
 Protocol: TCP (6)
 Header Checksum: 0xbd32 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 104.22.0.235
 Destination Address: 192.168.1.103
 [Stream index: 4]
> Transmission Control Protocol, Src Port: 443, Dst Port: 54707, Seq: 116, Ack: 959, Len: 0

Фільтрацію за одним протоколом ми вже виконували, зараз виконаємо за кількома:



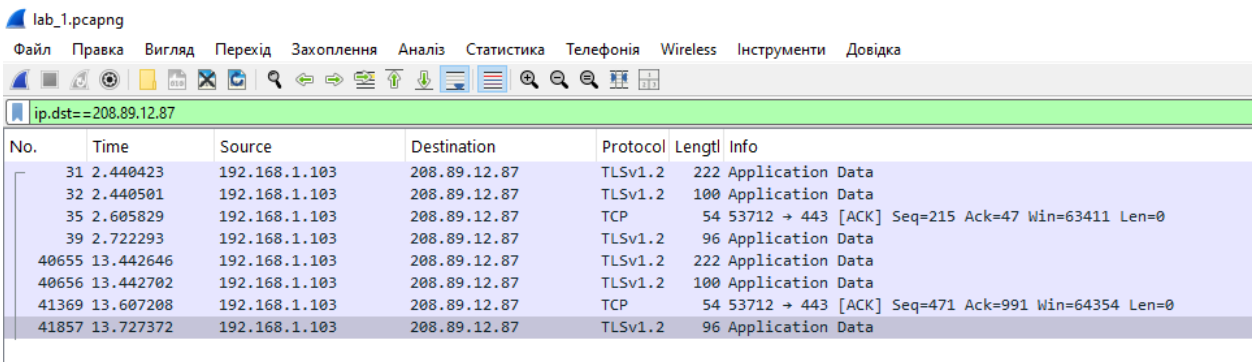
No.	Time	Source	Destination	Protocol	Length	Info
3	0.455633	192.168.1.103	149.154.167.41	SSL	223	Continuation Data
4	0.486762	149.154.167.41	192.168.1.103	TCP	54	443 → 65191 [ACK] Seq=1 Ack=170 Win=32768 Len=0
5	0.487459	149.154.167.41	192.168.1.103	SSL	143	Continuation Data
6	0.530671	192.168.1.103	149.154.167.41	TCP	54	65191 → 443 [ACK] Seq=170 Ack=90 Win=2052 Len=0
8	0.751127	192.168.1.103	212.58.128.19	TCP	66	54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10	1.466052	192.168.1.103	104.22.0.235	TCP	66	54707 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	1.478458	104.22.0.235	192.168.1.103	TCP	66	443 → 54707 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192
12	1.478535	192.168.1.103	104.22.0.235	TCP	54	54707 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
13	1.478903	192.168.1.103	104.22.0.235	TLSv1.2	431	Client Hello (SNI=api1.reasonsecurity.com)
14	1.503642	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=1 Ack=378 Win=73728 Len=0
15	1.503642	104.22.0.235	192.168.1.103	TLSv1.2	169	Server Hello, Change Cipher Spec, Encrypted Handshake Message
16	1.504386	192.168.1.103	104.22.0.235	TLSv1.2	635	Change Cipher Spec, Encrypted Handshake Message, Application Data
17	1.557777	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=116 Ack=959 Win=73728 Len=0
18	1.557841	192.168.1.103	104.22.0.235	TLSv1.2	164	Application Data
19	1.573524	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=116 Ack=1069 Win=73728 Len=0
21	1.699368	104.22.0.235	192.168.1.103	TLSv1.2	676	Application Data

Фільтр за адресою IP відправника:



No.	Time	Source	Destination	Protocol	Length	Info
33	2.556624	208.89.12.87	192.168.1.103	TCP	54	443 → 53712 [ACK] Seq=1 Ack=215 Win=25763 Len=0
34	2.556624	208.89.12.87	192.168.1.103	TLSv1.2	100	Application Data
38	2.721533	208.89.12.87	192.168.1.103	TLSv1.2	952	Application Data
42	2.837366	208.89.12.87	192.168.1.103	TCP	54	443 → 53712 [ACK] Seq=945 Ack=257 Win=25805 Len=0
41135	13.559689	208.89.12.87	192.168.1.103	TCP	54	443 → 53712 [ACK] Seq=945 Ack=471 Win=26019 Len=0
41136	13.560263	208.89.12.87	192.168.1.103	TLSv1.2	100	Application Data
41850	13.726357	208.89.12.87	192.168.1.103	TLSv1.2	952	Application Data
42454	13.844278	208.89.12.87	192.168.1.103	TCP	54	443 → 53712 [ACK] Seq=1889 Ack=513 Win=26061 Len=0

Фільтр за адресою IP одержувача:



No.	Time	Source	Destination	Protocol	Length	Info
31	2.440423	192.168.1.103	208.89.12.87	TLSv1.2	222	Application Data
32	2.440501	192.168.1.103	208.89.12.87	TLSv1.2	100	Application Data
35	2.605829	192.168.1.103	208.89.12.87	TCP	54	53712 → 443 [ACK] Seq=215 Ack=47 Win=63411 Len=0
39	2.722293	192.168.1.103	208.89.12.87	TLSv1.2	96	Application Data
40655	13.442646	192.168.1.103	208.89.12.87	TLSv1.2	222	Application Data
40656	13.442702	192.168.1.103	208.89.12.87	TLSv1.2	100	Application Data
41369	13.607208	192.168.1.103	208.89.12.87	TCP	54	53712 → 443 [ACK] Seq=471 Ack=991 Win=64354 Len=0
41857	13.727372	192.168.1.103	208.89.12.87	TLSv1.2	96	Application Data

Фільтр за MAC адресою:

lab_1.pcapng

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

tcp && eth.addr==c0:a5:dd:08:cf:1e

No.	Time	Source	Destination	Protocol	Length	Info
3	0.455633	192.168.1.103	149.154.167.41	SSL	223	Continuation Data
4	0.486762	149.154.167.41	192.168.1.103	TCP	54	443 → 65191 [ACK] Seq=1 Ack=170 Win=32768 Len=0
5	0.487459	149.154.167.41	192.168.1.103	SSL	143	Continuation Data
6	0.530671	192.168.1.103	149.154.167.41	TCP	54	65191 → 443 [ACK] Seq=170 Ack=90 Win=2052 Len=0
8	0.751127	192.168.1.103	212.58.120.19	TCP	66	54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10	1.466052	192.168.1.103	104.22.0.235	TCP	66	54707 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	1.478458	104.22.0.235	192.168.1.103	TCP	66	443 → 54707 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192
12	1.478535	192.168.1.103	104.22.0.235	TCP	54	54707 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
13	1.478903	192.168.1.103	104.22.0.235	TLSv1.2	431	Client Hello (SNI=apii.reasonsecurity.com)
14	1.503642	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=1 Ack=378 Win=73728 Len=0
15	1.503642	104.22.0.235	192.168.1.103	TLSv1.2	169	Server Hello, Change Cipher Spec, Encrypted Handshake Message
16	1.504386	192.168.1.103	104.22.0.235	TLSv1.2	635	Change Cipher Spec, Encrypted Handshake Message, Application Data
17	1.557777	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=116 Ack=959 Win=73728 Len=0
18	1.557841	192.168.1.103	104.22.0.235	TLSv1.2	164	Application Data
19	1.573524	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=116 Ack=1069 Win=73728 Len=0
21	1.699368	104.22.0.235	192.168.1.103	TLSv1.2	676	Application Data
22	1.699368	104.22.0.235	192.168.1.103	TLSv1.2	85	Encrypted Alert
23	1.699505	192.168.1.103	104.22.0.235	TCP	54	54707 → 443 [ACK] Seq=1069 Ack=770 Win=130816 Len=0
24	1.700099	192.168.1.103	104.22.0.235	TCP	54	54707 → 443 [FIN, ACK] Seq=1069 Ack=770 Win=130816 Len=0
25	1.716844	104.22.0.235	192.168.1.103	TCP	54	443 → 54707 [ACK] Seq=770 Ack=1070 Win=73728 Len=0
27	1.750995	192.168.1.103	20.199.120.182	TCP	55	49437 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1
28	1.751140	192.168.1.103	212.58.120.19	TCP	66	[TCP Retransmission] 54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Фільтр за номером порту:

lab_1.pcapng

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
58857	19.827694	192.168.1.103	2.19.126.158	TCP	66	54715 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
58858	19.851892	2.19.126.158	192.168.1.103	TCP	66	80 → 54715 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM WS=128
58859	19.852014	192.168.1.103	2.19.126.158	TCP	54	54715 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
58860	19.852184	192.168.1.103	2.19.126.158	HTTP	136	GET /ncc.txt HTTP/1.1
58861	19.876711	2.19.126.158	192.168.1.103	TCP	54	80 → 54715 [ACK] Seq=1 Ack=83 Win=64256 Len=0
58862	19.877913	2.19.126.158	192.168.1.103	HTTP	205	HTTP/1.1 200 OK (text/html)
58863	19.878134	192.168.1.103	2.19.126.158	TCP	54	54715 → 80 [FIN, ACK] Seq=83 Ack=152 Win=132096 Len=0
58864	19.903113	2.19.126.158	192.168.1.103	TCP	54	80 → 54715 [FIN, ACK] Seq=152 Ack=84 Win=64256 Len=0
58865	19.903217	192.168.1.103	2.19.126.158	TCP	54	54715 → 80 [ACK] Seq=84 Ack=153 Win=132096 Len=0

Фільтр TCP пакетів з прапором SYN (встановлення з'єднання між пристроями):

lab_1.pcapng

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

tcp.flags.syn==1

No.	Time	Source	Destination	Protocol	Length	Info
8	0.751127	192.168.1.103	212.58.120.19	TCP	66	54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10	1.466052	192.168.1.103	104.22.0.235	TCP	66	54707 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	1.478458	104.22.0.235	192.168.1.103	TCP	66	443 → 54707 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192
28	1.751140	192.168.1.103	212.58.120.19	TCP	66	[TCP Retransmission] 54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
40	2.748836	192.168.1.103	124.225.126.114	TCP	66	54708 → 19131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
41	2.794699	192.168.1.103	37.75.122.191	TCP	66	54704 → 37614 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
47	3.057460	124.225.126.114	192.168.1.103	TCP	66	19131 → 54708 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=16384
57	3.756134	192.168.1.103	212.58.120.19	TCP	66	[TCP Retransmission] 54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
83	4.966588	192.168.1.103	104.16.103.112	TCP	66	54709 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
89	4.982212	104.16.103.112	192.168.1.103	TCP	66	443 → 54709 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192
12557	7.758579	192.168.1.103	212.58.120.19	TCP	66	[TCP Retransmission] 54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12560	7.759134	192.168.1.103	80.93.123.44	TCP	66	54710 → 21429 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17278	8.732854	192.168.1.103	84.54.80.71	TCP	66	54711 → 46749 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17426	8.763873	192.168.1.103	80.93.123.44	TCP	66	[TCP Retransmission] 54710 → 21429 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
21527	9.737109	192.168.1.103	84.54.80.71	TCP	66	[TCP Retransmission] 54711 → 46749 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
26038	10.771896	192.168.1.103	80.93.123.44	TCP	66	[TCP Retransmission] 54710 → 21429 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
31132	11.749214	192.168.1.103	84.54.80.71	TCP	66	[TCP Retransmission] 54711 → 46749 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34138	12.264253	192.168.1.103	13.107.21.239	TCP	66	54712 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34241	12.295067	13.107.21.239	192.168.1.103	TCP	66	443 → 54712 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
48240	14.784787	192.168.1.103	80.93.123.44	TCP	66	[TCP Retransmission] 54710 → 21429 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
53385	15.754873	192.168.1.103	84.54.80.71	TCP	66	[TCP Retransmission] 54711 → 46749 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
53495	15.770812	192.168.1.103	212.58.120.19	TCP	66	[TCP Retransmission] 54706 → 20218 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
58339	16.731057	192.168.1.103	46.98.109.249	TCP	66	54713 → 28163 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
58817	17.738756	192.168.1.103	46.98.109.249	TCP	66	[TCP Retransmission] 54713 → 28163 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
58837	19.502383	192.168.1.103	104.22.0.235	TCP	66	54714 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
58838	19.525618	104.22.0.235	192.168.1.103	TCP	66	443 → 54714 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192
58847	19.747174	192.168.1.103	46.98.109.249	TCP	66	[TCP Retransmission] 54713 → 28163 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
58857	19.827694	192.168.1.103	2.19.126.158	TCP	66	54715 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
58858	19.851892	2.19.126.158	192.168.1.103	TCP	66	80 → 54715 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM WS=128

Висновок:

Лабораторна робота дозволила мені глибше зрозуміти принципи роботи стеків мережових протоколів, зокрема моделі OSI та TCP/IP. Я ознайомилася з функціями різних рівнів моделі, що забезпечують ефективну комунікацію між пристроями. Використання аналізатора Wireshark дало можливість практично застосувати теоретичні знання, захоплюючи та аналізуючи мережевий трафік. Я навчилася виділяти важливі елементи пакетів, такі як заголовки та адреси відправника і отримувача. Створення фільтрів у Wireshark допомогло мені ефективно відслідковувати потрібні пакети, що є важливим для роботи з великими обсягами даних. Загалом, виконана робота підкреслила важливість практичного досвіду в розумінні комп'ютерних мереж і їх функціонування.