

1. Мета роботи

Метою даної лабораторної роботи є оволодіння методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

2. Хід роботи

Під час виконання лабораторної роботи виконано наступні дії:

1. Запущено веб-браузер.

2. Запущено Wireshark.

3. В Wireshark активовано діалог вибору мережевого інтерфейсу для захоплення: 'Capture >> Interfaces'.

4. Обрано інтерфейс, для якого відображається найбільша кількість захоплених пакетів, - 'Wi-Fi: en0' та натиснуто кнопку Start навпроти нього.

5. Відкрито в браузері сторінку за наступною адресою:
<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

Пакети зі вмістом зазначеної веб-сторінки були захоплені Wireshark.

6. Зупинено захоплення пакетів за допомогою команди 'Capture >> Stop'.

7. Введено текст «http» в поле фільтрації та натиснуто Apply. У вікні лістингу пакетів залишилися тільки ті, які були створені протоколом HTTP.

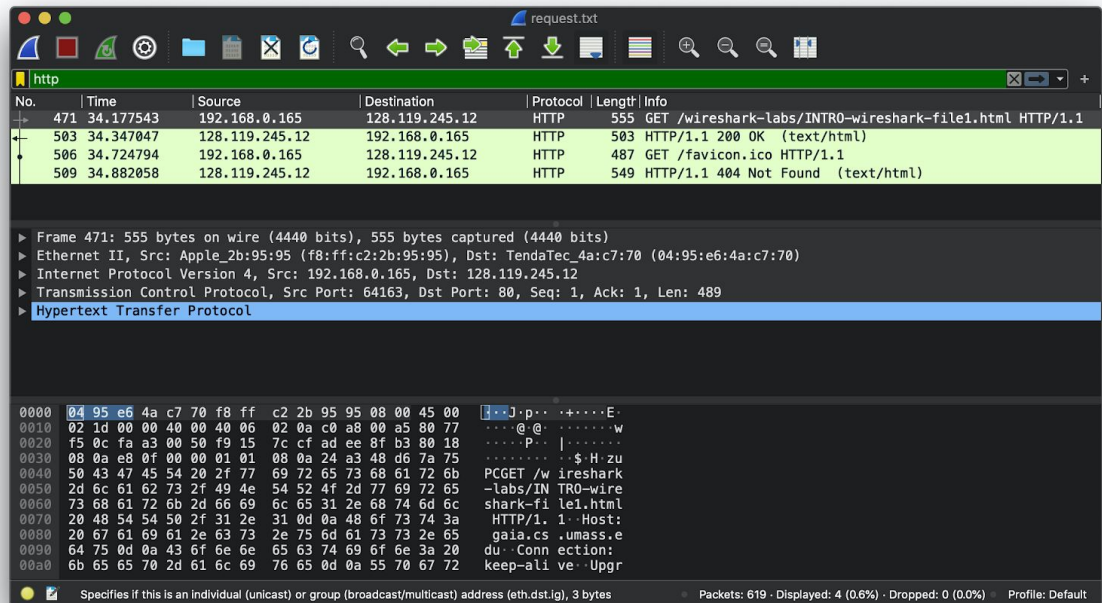


Рис. 1. Результат застосування фільтру http

8. Обрано перший пакет HTTP, який відобразився у вікні лістингу, це було повідомлення GET протоколу HTTP. Також цей пакет міщував інформацію про інші протоколи нижчих рівнів: TCP, IP, Ethernet.

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

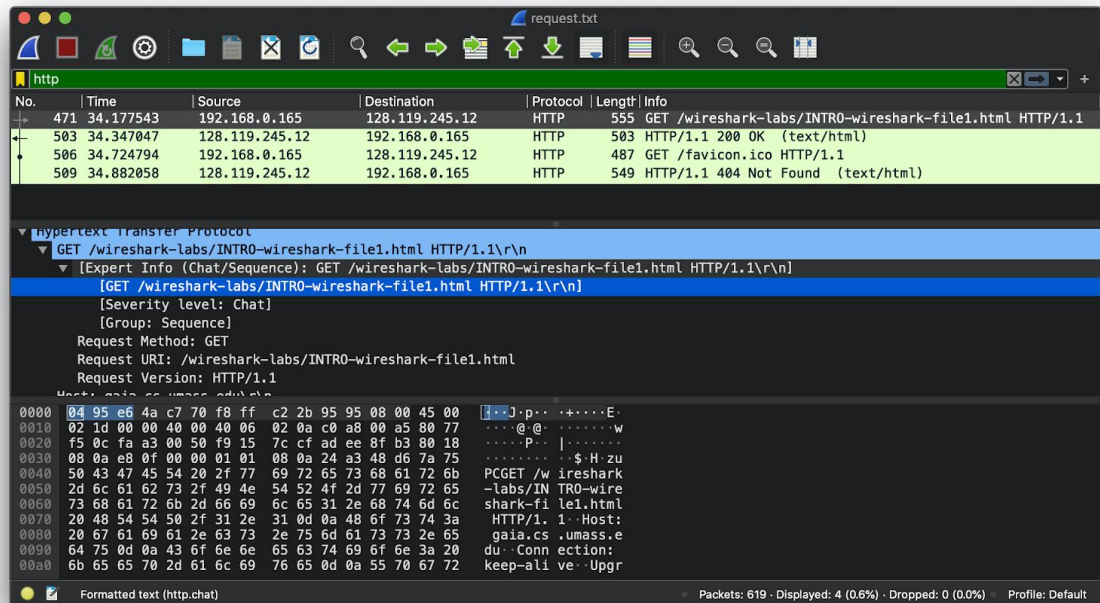


Рис. 2. Деталі заголовку запиту

10. Збережено перші пакети запиту та відповіді у відповідні файли:

Vysotskyi_Request_INTRO-wireshark.txt та

Vysotskyi-Response_INTRO-wireshark.txt.

11. Перевірено, що у збережених файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколи.

3. Відповіді на контрольні питання

3.1 Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?

У вікні лістингу протоколів до включення фільтрації відображалися наступні протоколи: TCP, UDP, DNS, TLSv1.2, HTTP, та інші.

No.	Time	Source	Destination	Protocol	Length	Info
155	10.493079	192.168.0.165	18.185.73.246	TLSv1.2	252	Application Data
156	10.526536	18.185.73.246	192.168.0.165	TCP	66	443 → 63760 [ACK] Seq=2801 Ack=1196 Win=694 Len=0 TSval=
157	10.526540	18.185.73.246	192.168.0.165	TLSv1.2	745	Application Data
158	10.526541	18.185.73.246	192.168.0.165	TLSv1.2	108	Application Data
159	10.526621	192.168.0.165	18.185.73.246	TCP	66	63760 → 443 [ACK] Seq=1196 Ack=3480 Win=2037 Len=0 TSva
160	10.526621	192.168.0.165	18.185.73.246	TCP	66	63760 → 443 [ACK] Seq=1196 Ack=3522 Win=2036 Len=0 TSva
161	10.895158	192.168.0.165	3.80.20.198	TLSv1.2	281	Application Data
162	10.909460	fe80::460:8a8a:14b...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
163	11.016843	3.80.20.198	192.168.0.165	TCP	66	443 → 63764 [ACK] Seq=1 Ack=216 Win=24 Len=0 TSval=1679
164	11.017313	3.80.20.198	192.168.0.165	TLSv1.2	259	Application Data
165	11.017405	192.168.0.165	3.80.20.198	TCP	66	63764 → 443 [ACK] Seq=216 Ack=194 Win=2044 Len=0 TSval=
166	11.325225	192.168.0.165	216.58.215.99	UDP	133	52693 → 443 Len=91
167	11.370377	216.58.215.99	192.168.0.165	UDP	181	443 → 52693 Len=139
168	11.370383	216.58.215.99	192.168.0.165	UDP	60	443 → 52693 Len=18
169	11.370835	192.168.0.165	216.58.215.99	UDP	70	52693 → 443 Len=28
170	12.069167	192.168.0.165	192.168.0.1	DNS	76	Standard query 0xe92e A drive.google.com
171	12.078596	192.168.0.133	224.0.0.251	MDNS	179	Standard query 0x0000 PTR _companion-link._tcp.local, "
172	12.078602	fe80::460:8a8a:14b...	ff02::fb	MDNS	199	Standard query 0x0000 PTR _companion-link._tcp.local, "
173	12.078604	192.168.0.1	192.168.0.165	DNS	340	Standard query response 0xe92e A drive.google.com A 172
174	12.081002	192.168.0.165	172.217.16.14	UDP	1392	60792 → 443 Len=1350
175	12.096601	192.168.0.165	216.58.215.110	UDP	65	49425 → 443 Len=23
176	12.112119	192.168.0.165	193.41.63.113	TLSv1.2	737	Application Data
177	12.118936	172.217.16.14	192.168.0.165	UDP	1392	443 → 60792 Len=1350
178	12.118939	216.58.215.110	192.168.0.165	UDP	64	443 → 49425 Len=22
179	12.118940	193.41.63.113	192.168.0.165	TLSv1.2	899	Application Data
180	12.119000	192.168.0.165	193.41.63.113	TCP	66	63797 → 443 [ACK] Seq=2016 Ack=2500 Win=2034 Len=0 TSva
181	12.119333	192.168.0.165	172.217.16.14	UDP	70	60792 → 443 Len=28
182	12.120202	192.168.0.165	172.217.16.14	UDP	1392	60792 → 443 Len=1350
183	12.120267	192.168.0.165	172.217.16.14	UDP	123	60792 → 443 Len=81
184	12.120531	192.168.0.165	172.217.16.14	UDP	1392	60792 → 443 Len=1350
185	12.120574	192.168.0.165	172.217.16.14	UDP	1392	60792 → 443 Len=1350
186	12.120583	192.168.0.165	172.217.16.14	UDP	1392	60792 → 443 Len=1350
187	12.120600	192.168.0.165	172.217.16.14	UDP	286	60792 → 443 Len=244
188	12.124881	192.168.0.165	193.41.63.92	TCP	1434	63842 → 443 [ACK] Seq=2059 Ack=750 Win=2048 Len=1368 TS
189	12.124882	192.168.0.165	193.41.63.92	TLSv1.2	552	Application Data
190	12.124882	192.168.0.165	193.41.63.92	TLSv1.2	252	Application Data
191	12.130111	193.41.63.92	192.168.0.165	TCP	66	443 → 63842 [ACK] Seq=750 Ack=3427 Win=363 Len=0 TSval=

Рис. 3. Інформація про протоколи до включення фільтрації

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

У пакеті запиту використовувались - eth:ethertype:ip:tcp:http протоколи, у пакеті відповіді - eth:ethertype:ip:tcp:http:data-text-lines протоколи.

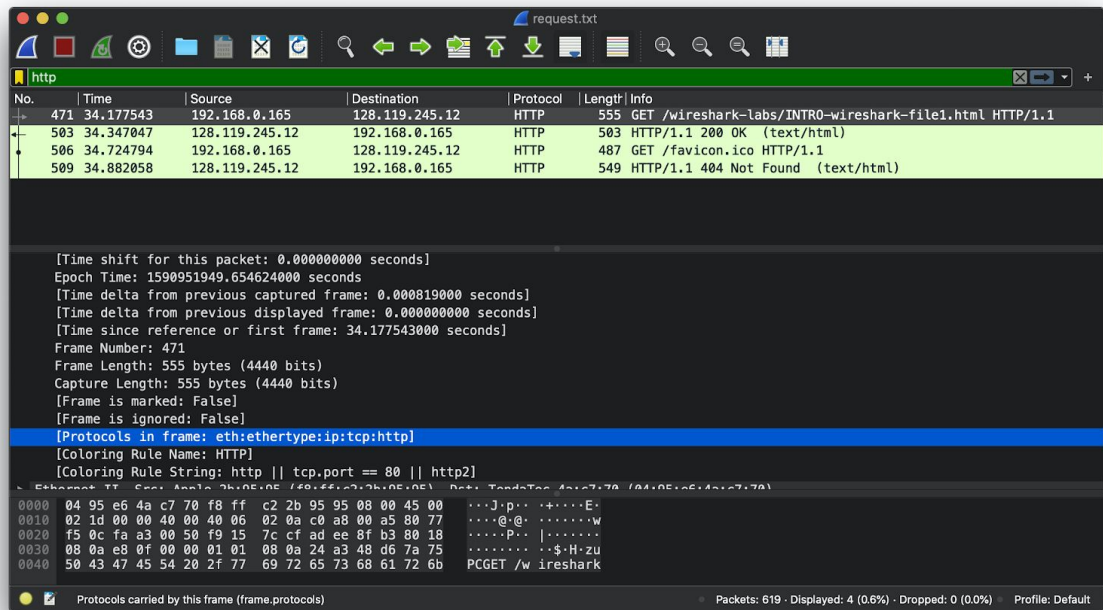


Рис. 4. Протоколи, які використовувались у пакеті запиту

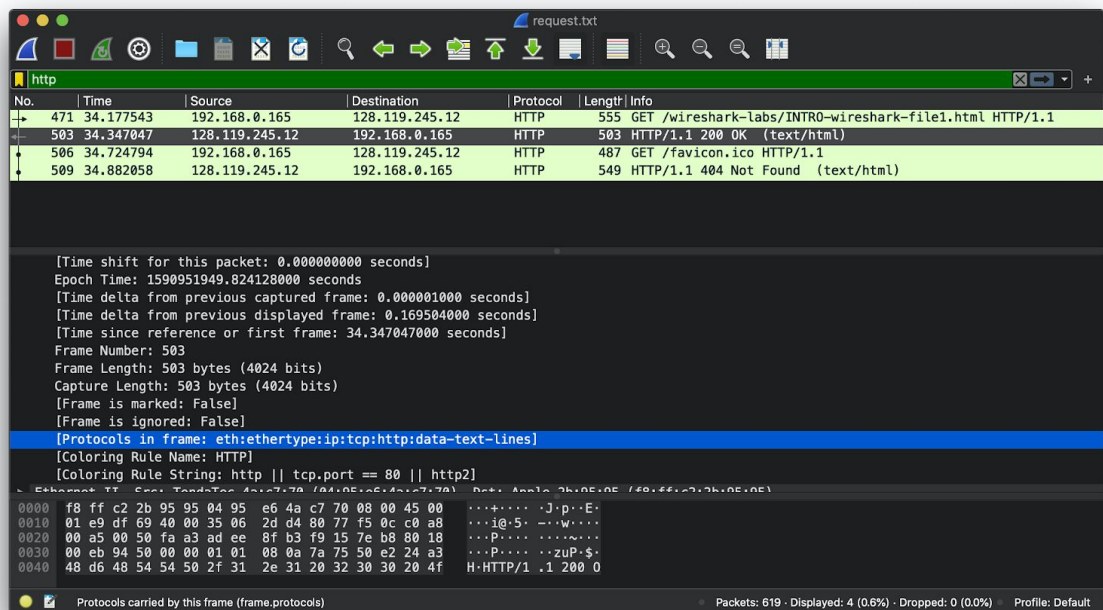


Рис. 5. Протоколи, які використовувались у пакеті відповіді

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

Час відправки пакету запиту - 22:05:49.654624000 EEST, час отримання пакету відповіді 22:05:49.824128000 EEST, період часу між пакетом запиту та відповіді склав приблизно 0.17 с.

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

Для пакету запиту:

Source - 192.168.0.165, Destination - 128.119.245.12;

Для пакету відповіді:

Source - 128.119.245.12, Destination - 192.168.0.165.

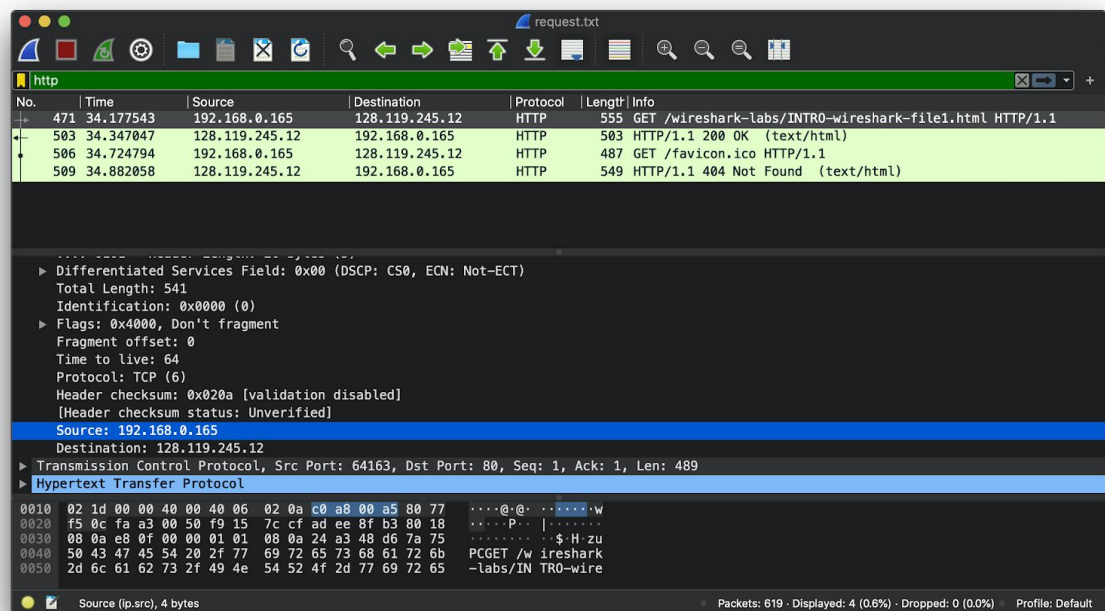


Рис. 6. Інформація про вихідні та цільові адреси пакетів із запитом

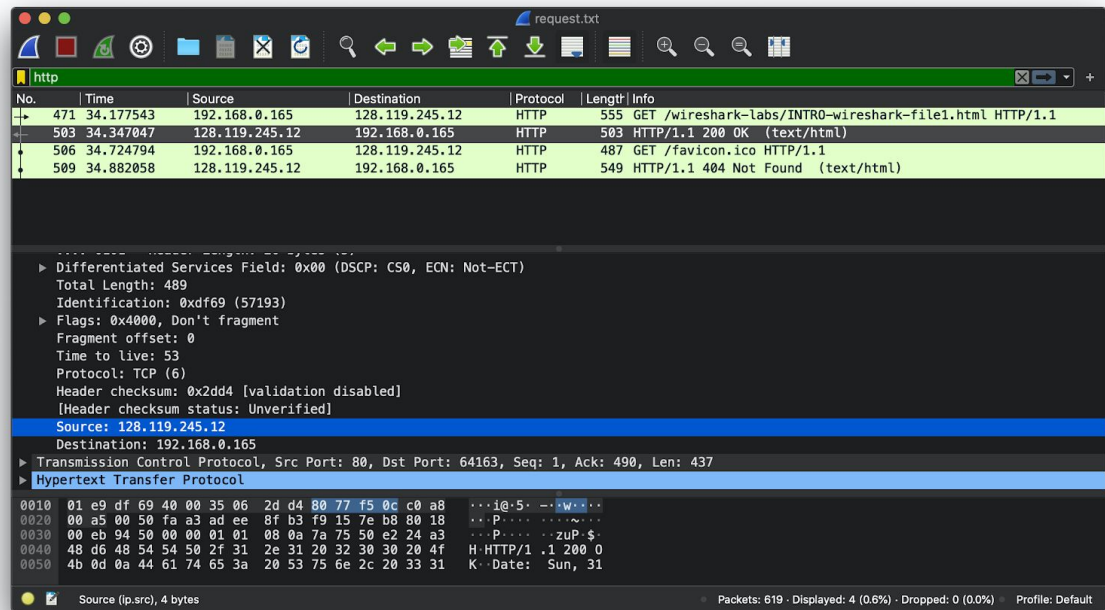


Рис. 7. Інформація про вихідні та цільові адреси пакетів із відповіддю

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

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

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

HTTP/1.1 200 OK\r\n