

Міністерство науки і освіти України
Національний Університет “Львівська Політехніка”
Інститут комп’ютерних наук та інформаційних технологій

Кафедра САП



Звіт

з виконання лабораторної роботи № 8
із дисципліни: “Операційні системи”

Виконав:

ст. групи ПП-25
Федорич Олександр

Прийняла:

кандидат технічних наук,
старший викладач
кафедри САП
Нестор Н. І.

Львів – 2024

Тема: “Вивчення можливості програми сніфера Wireshark для аналізу пакетів протоколу HTTP.”

Мета: “Вивчити роботу мережного сніфера та роботу протоколу HTTP.”

ВИКОНАННЯ ЗАВДАННЯ

1. Завантаження Wireshark.

Заходжу на офіційний сайт програми Wireshark(<https://www.wireshark.org/>) та завантажую інсталятор.

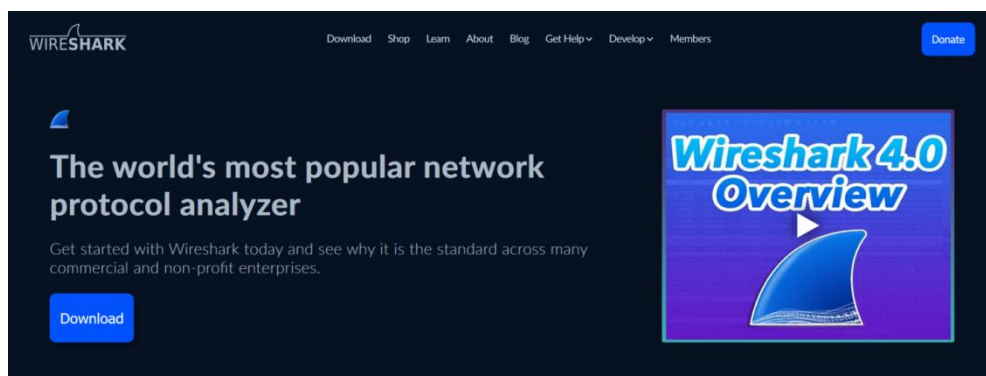


Рис. 1. Офіційний сайт програми Wireshark.

Запускаю інсталятор та встановлюю програму Wireshark на мій ПК.

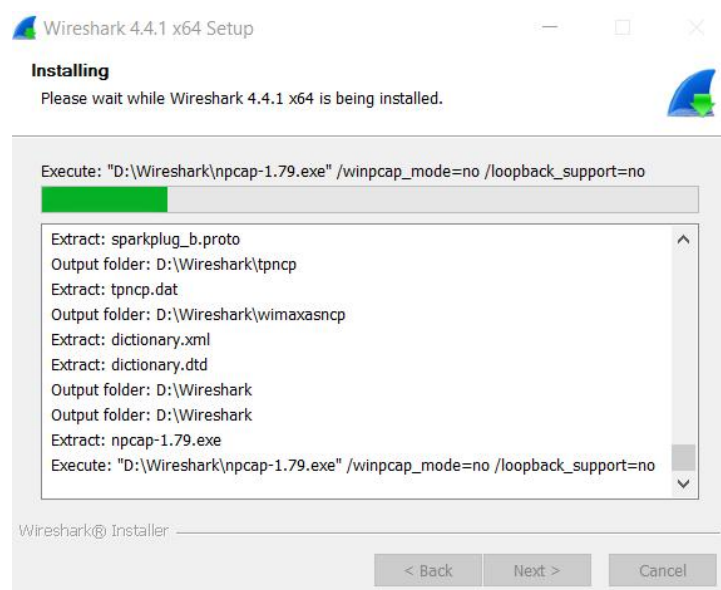


Рис. 2. Процес встановлення програми Wireshark.

2. Запуск Wireshark.

Запускаю встановлену програму Wireshark та мені показується головне меню.

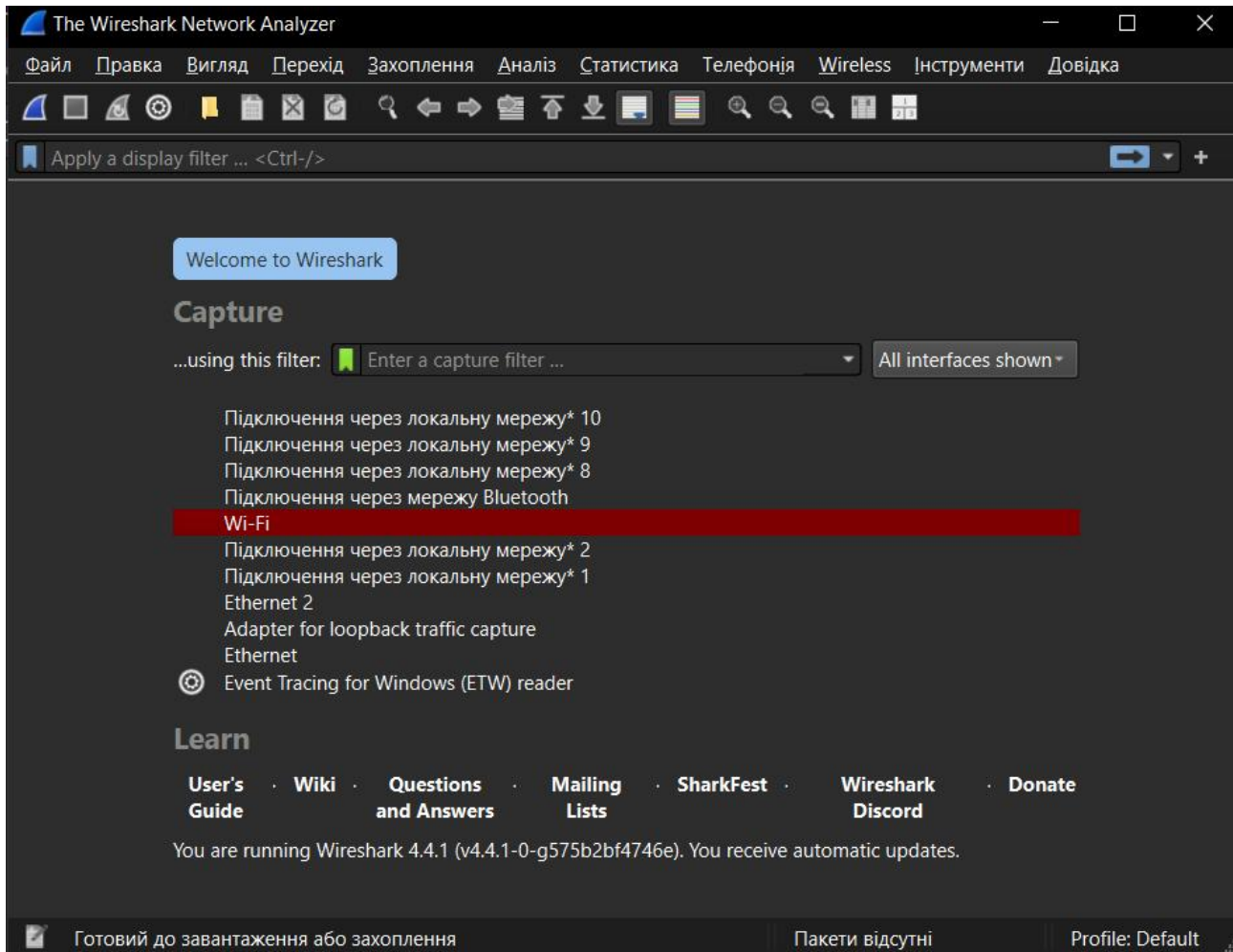


Рис. 3. Головне меню програми Wireshark.

Обираю символ опції захоплення.



Рис. 4. Опції захоплення.

Мені відкривається меню опцій захоплення. Обираю підпункт WI-FI, щоб відслідковувати протоколи, що проходять крізь цей інтерфейс.

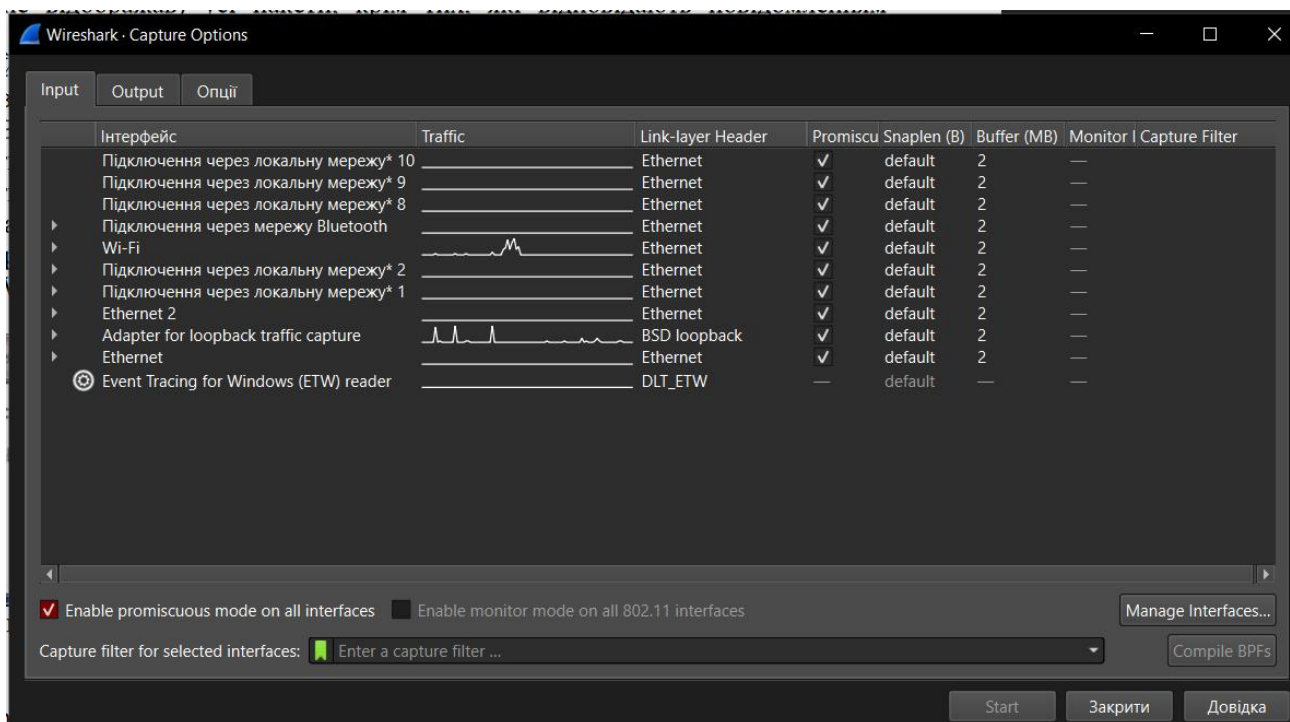


Рис. 5. Меню опцій захоплення.

Мені відкривається меню інтерфейсу WI-FI, яке вже відслідковує протоколи що проходять через цей інтерфейс.

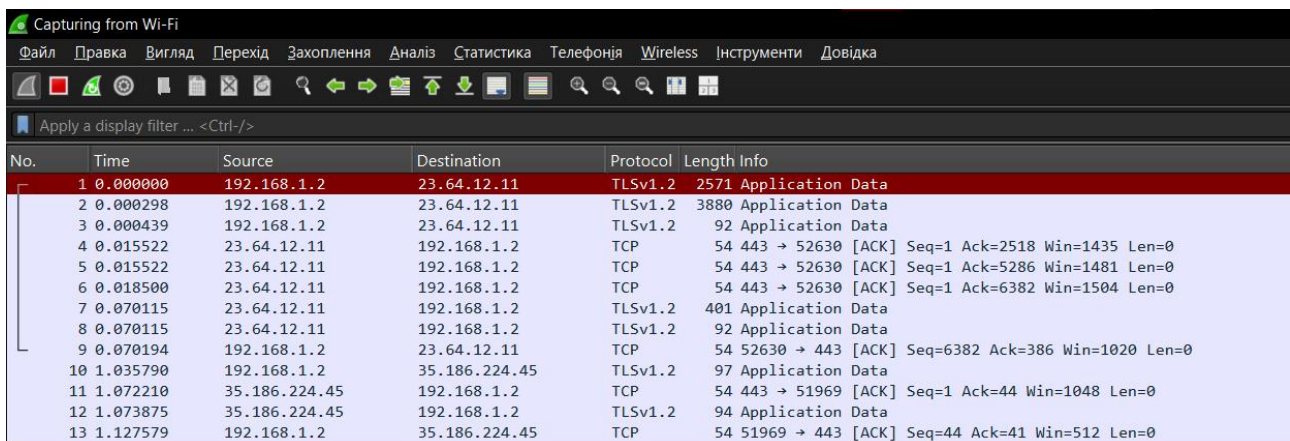
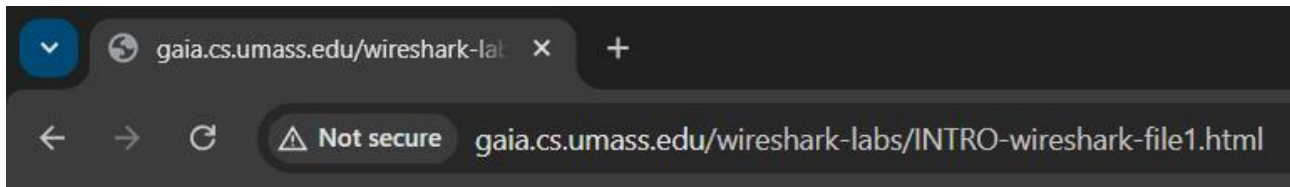


Рис. 6. Інтерфейс WI-FI.

3. Аналіз HTTP-запитів з сайту: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

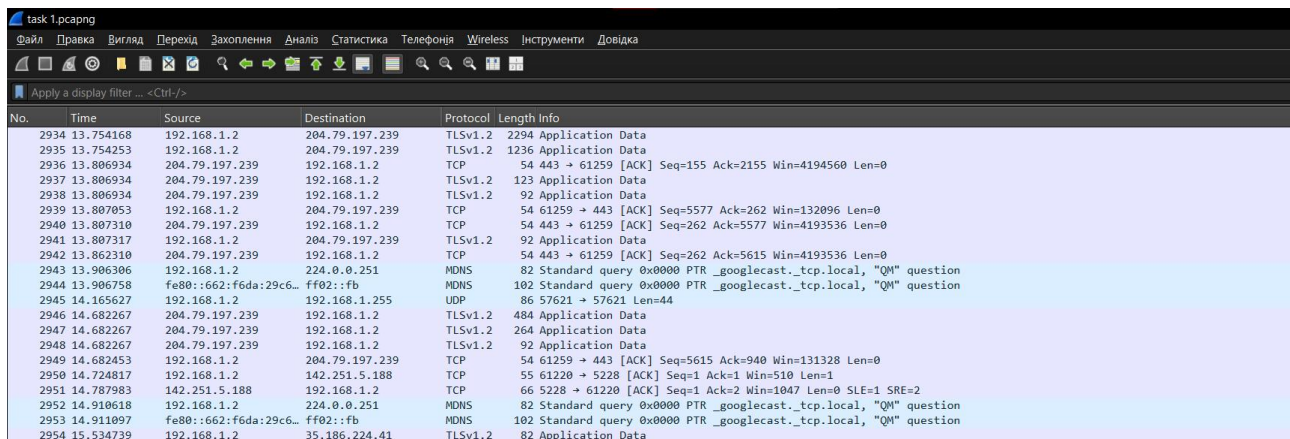
Заходжу на сайт із запущеним до цього інтерфейсом WI-FI програми Wireshark.



Congratulations! You've downloaded the first Wireshark lab file!

Рис. 7. Вміст сайту.

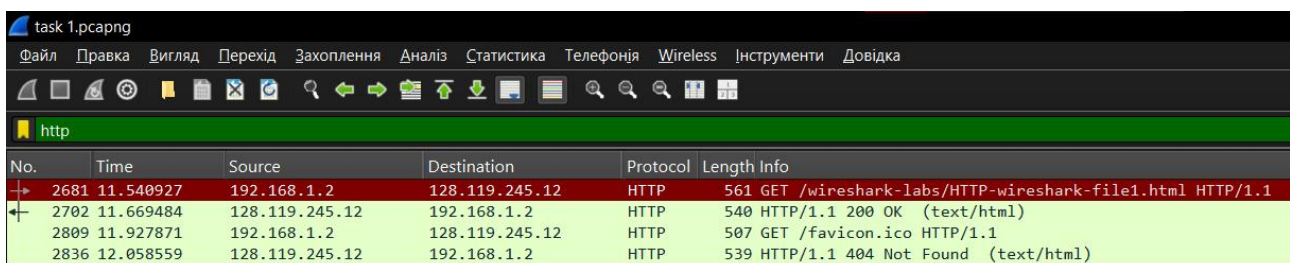
Інтерфейс WI-FI зафіксує протоколи які відбулись при заходженні на вище наведений сайт.



No.	Time	Source	Destination	Protocol	Length	Info
2934	13.754168	192.168.1.2	204.79.197.239	TLSv1.2	2294	Application Data
2935	13.754253	192.168.1.2	204.79.197.239	TLSv1.2	1236	Application Data
2936	13.806934	204.79.197.239	192.168.1.2	TCP	54	443 → 61259 [ACK] Seq=155 Ack=2155 Win=4194560 Len=0
2937	13.806934	204.79.197.239	192.168.1.2	TLSv1.2	123	Application Data
2938	13.806934	204.79.197.239	192.168.1.2	TLSv1.2	92	Application Data
2939	13.807053	192.168.1.2	204.79.197.239	TCP	54	61259 → 443 [ACK] Seq=5577 Ack=262 Win=132096 Len=0
2940	13.807310	204.79.197.239	192.168.1.2	TCP	54	443 → 61259 [ACK] Seq=262 Ack=5577 Win=4193536 Len=0
2941	13.807317	192.168.1.2	204.79.197.239	TLSv1.2	92	Application Data
2942	13.862310	204.79.197.239	192.168.1.2	TCP	54	443 → 61259 [ACK] Seq=262 Ack=5615 Win=4193536 Len=0
2943	13.906306	192.168.1.2	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
2944	13.906758	fe80::662:f6da:29c6::	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
2945	14.165627	192.168.1.2	192.168.1.255	UDP	86	57621 → 57621 Len=44
2946	14.682267	204.79.197.239	192.168.1.2	TLSv1.2	484	Application Data
2947	14.682267	204.79.197.239	192.168.1.2	TLSv1.2	264	Application Data
2948	14.682267	204.79.197.239	192.168.1.2	TLSv1.2	92	Application Data
2949	14.682453	192.168.1.2	204.79.197.239	TCP	54	61259 → 443 [ACK] Seq=5615 Ack=940 Win=131328 Len=0
2950	14.724817	192.168.1.2	142.251.5.188	TCP	55	61220 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
2951	14.787983	142.251.5.188	192.168.1.2	TCP	66	5228 → 61220 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
2952	14.910618	192.168.1.2	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
2953	14.911097	fe80::662:f6da:29c6::	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
2954	15.534739	192.168.1.2	35.186.224.41	TLSv1.2	82	Application Data

Рис. 8. Захоплені протоколи.

У фільтрі протоколів записую http та запускаю. Виводиться екран всіх http запитів.



No.	Time	Source	Destination	Protocol	Length	Info
2681	11.540927	192.168.1.2	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2702	11.669484	128.119.245.12	192.168.1.2	HTTP	540	HTTP/1.1 200 OK (text/html)
2809	11.927871	192.168.1.2	128.119.245.12	HTTP	507	GET /favicon.ico HTTP/1.1
2836	12.058559	128.119.245.12	192.168.1.2	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Рис. 9. Протоколи які пройшли крізь фільтр.

Обираю перший GET запит до сервера та досліджую його вміст.

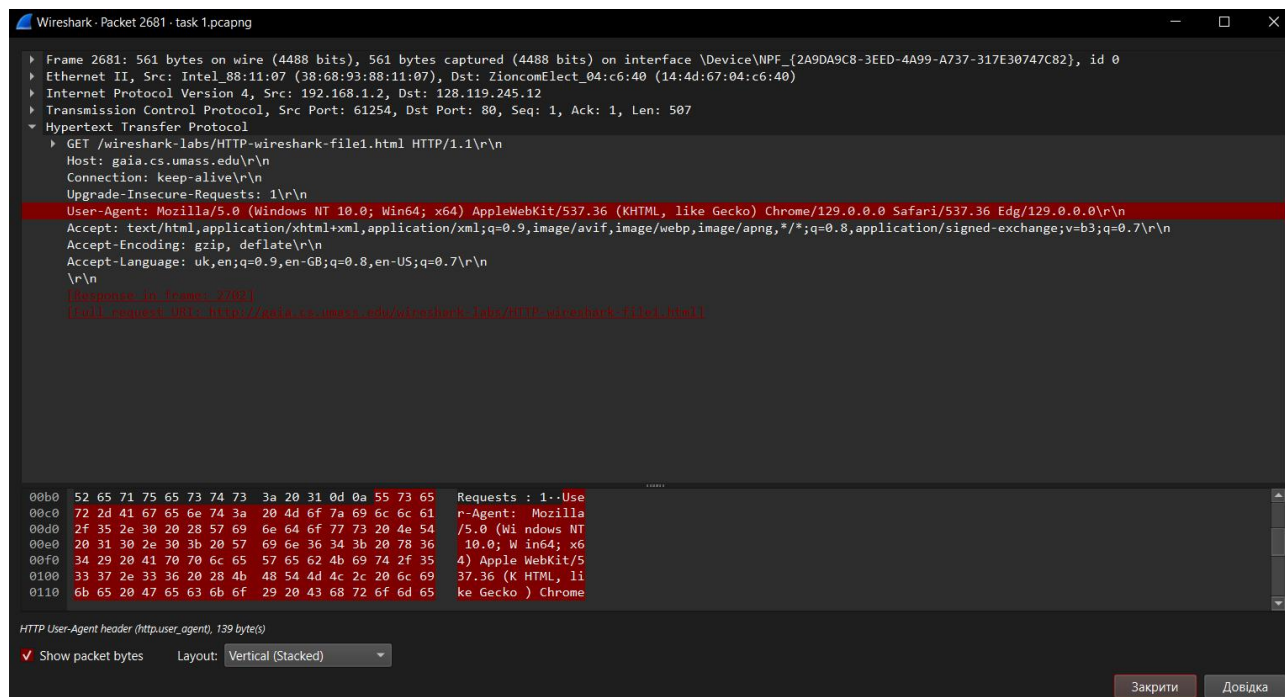


Рис. 10. Вміст GET запиту.

Тепер відключаю фільтр та знаходжу HTTP-запити і протоколи що відбулись між цими запитами.

No.	Time	Source	Destination	Protocol	Length	Info
2681	11.540927	192.168.1.2	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2682	11.591835	13.69.116.104	192.168.1.2	TLSv1.3	409	Application Data, Application Data
2683	11.591835	48.209.164.47	192.168.1.2	TCP	54	443 → 61255 [ACK] Seq=1 Ack=1441 Win=64512 Len=0
2684	11.591835	48.209.164.47	192.168.1.2	TCP	54	443 → 61255 [ACK] Seq=1 Ack=1841 Win=64512 Len=0
2685	11.591835	48.209.164.47	192.168.1.2	TLSv1.3	1506	Server Hello, Change Cipher Spec, Application Data
2686	11.591835	48.209.164.47	192.168.1.2	TCP	1506	443 → 61255 [PSH, ACK] Seq=1453 Ack=1841 Win=64512 Len=1452 [TCP PDU reassembled in 2690]
2687	11.591835	48.209.164.47	192.168.1.2	TCP	1246	443 → 61255 [PSH, ACK] Seq=2905 Ack=1841 Win=64512 Len=1192 [TCP PDU reassembled in 2690]
2688	11.591971	192.168.1.2	48.209.164.47	TCP	54	61255 → 443 [ACK] Seq=1841 Ack=4097 Win=132352 Len=0
2689	11.612133	48.209.164.47	192.168.1.2	TCP	1506	443 → 61255 [ACK] Seq=4097 Ack=1841 Win=64512 Len=1452 [TCP PDU reassembled in 2690]
2690	11.612133	48.209.164.47	192.168.1.2	TLSv1.3	867	Application Data, Application Data
2691	11.612262	192.168.1.2	48.209.164.47	TCP	54	61255 → 443 [ACK] Seq=1841 Ack=6362 Win=132352 Len=0
2692	11.612416	204.79.197.239	192.168.1.2	TLSv1.2	362	Application Data
2693	11.612416	204.79.197.239	192.168.1.2	TLSv1.2	266	Application Data
2694	11.612416	204.79.197.239	192.168.1.2	TLSv1.2	92	Application Data
2695	11.612504	192.168.1.2	204.79.197.239	TCP	54	61246 → 443 [ACK] Seq=5825 Ack=7870 Win=132352 Len=0
2696	11.618389	192.168.1.2	48.209.164.47	TLSv1.3	134	Change Cipher Spec, Application Data
2697	11.618891	192.168.1.2	48.209.164.47	TLSv1.3	146	Application Data
2698	11.619204	192.168.1.2	48.209.164.47	TLSv1.3	481	Application Data
2699	11.619332	192.168.1.2	48.209.164.47	TLSv1.3	1667	Application Data
2700	11.634908	192.168.1.2	13.69.116.104	TCP	54	61237 → 443 [ACK] Seq=129054 Ack=8708 Win=131584 Len=0
2701	11.669484	128.119.245.12	192.168.1.2	TCP	54	80 → 61254 [ACK] Seq=1 Ack=508 Win=30336 Len=0
2702	11.669484	128.119.245.12	192.168.1.2	HTTP	540	HTTP/1.1 200 OK (text/html)

Рис. 11. Протоколи які відбулись між 2 HTTP-запитами.

У стовпці Protocol між HTTP-запитами відображені такі протоколи: TLSv1.3, TLSv1.2, TCP. Час що пройшов до одержання HTTP-запита з повідомленням HTTP/1.1 200 OK становить: $11.669484 - 11.54927 = 0.120214$ секунд.

Тепер я знаходжу пункти Source та Destination щоб визначити IP-адреси клієнта та сервера.

Source	Destination
192.168.1.2	128.119.245.12

Рис. 12. IP-адреси клієнта та сервера.

Source - адреса мого комп'ютера яка становить: 192.168.1.2.

Destination - адреса сервера, що становить: 128.119.245.12.

Щоб роздрукувати ці HTTP-запити я обираю їх та натискаю Ctrl + P.

No.	Time	Source	Destination	Protocol	Length	Info
2681	11.540927	192.168.1.2	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2702	11.669484	128.119.245.12	192.168.1.2	HTTP	540	HTTP/1.1 200 OK (text/html)

Рис. 13. Обрані для друку HTTP-запити.

Мені виводиться вікно Wireshark Роздрукувати та я налаштовую опції друку.

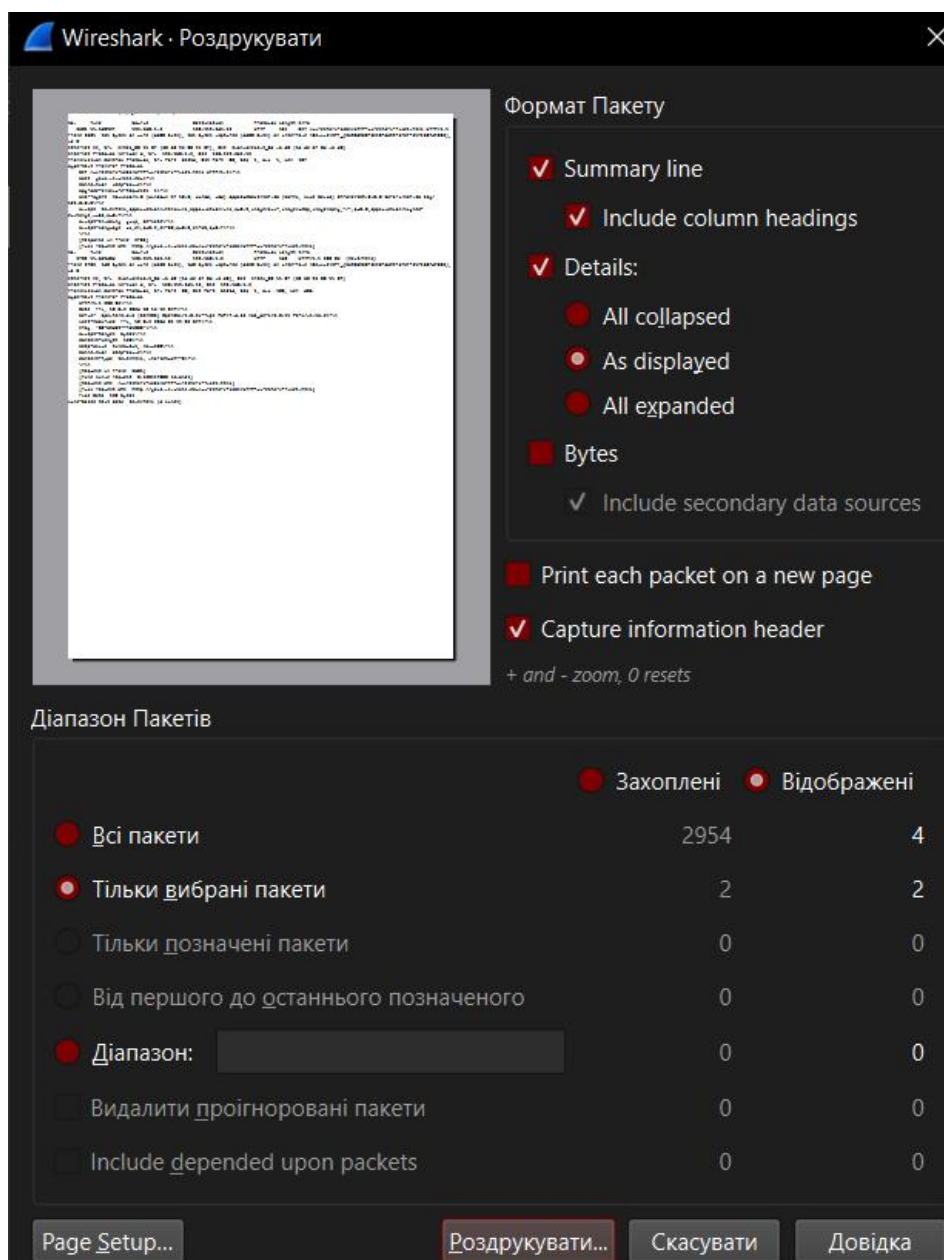


Рис. 14. Вікно Wireshark Роздрукувати.

Зберігаю вміст друку у форматі pdf та переглядаю його.

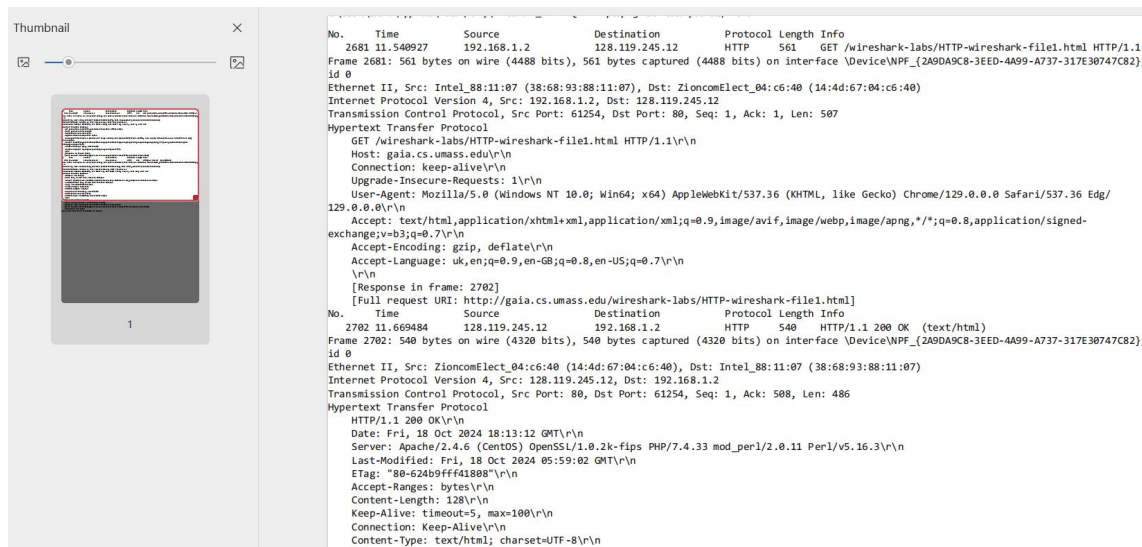


Рис. 15. Вміст роздрукованих HTTP-запитів.

Тепер я переглядаю 1 рядок цих запитів щоб дізнатись яку HTTP версію вони використовують.

```
561 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
540 HTTP/1.1 200 OK (text/html)
```

Рис. 16. Перші рядки HTTP-запитів.

Браузер використовує версію HTTP - 1.1, сервер використовує версію HTTP - 1.1.

Знаходжу підпункт у HTTP-запиті, що зветься Accept-Language.

```
Accept-Language: uk,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
```

Рис. 17. Підпункт Accept-Language.

Браузер вказує серверу на такі підтримувані мови: uk, en.

Знаходжу HTTP відповідь від сервера до клієнта.

```
HTTP/1.1 200 OK (text/html)
```

Рис. 18. HTTP відповідь сервера.

Код стану повернення сервер браузеру становить: 200.

Тепер знаходжу у HTTP-запиті рядок Last-Modified.

```
Last-Modified: Fri, 18 Oct 2024 05:59:02 GMT\r\n
```

Рис. 19. Вміст рядка Last-Modified.

Дата останньої зміни становить: 18.10.2024 05:59:02.

Також знаходжу у HTTP-запиті рядок Content-Length.

```
Content-Length: 128\r\n
```

Рис. 20. Вміст рядка Content-Length.

Розмір змісту, що повернув сервер браузеру становить: 128 байт.

Переглядаю всі заголовки HTTP-запиту, які не відображені у списку пакетів.

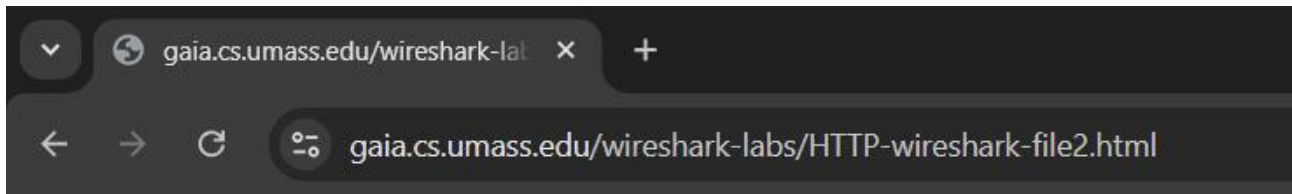
```
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36 Edg/129.0.0.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: uk,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
\r\n
[Response in Frame: 2(02)]
[Full connect URL: https://gaia.cs.umass.edu/signedark-labs/HTTP-signedark-71ed.html]
```

Рис. 21. HTTP-заголовки.

Не відображені у списку пакетів заголовки: Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, Accept-Language.

4. Аналіз HTTP-запитів з сайту: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

Заходжу на сайт із запущеним до цього інтерфейсом WI-FI програми Wireshark.



Congratulations again! Now you've downloaded the file lab2-2.html.

This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE field in your browser's HTTP GET request to the server.

Рис. 22. Вміст сайту.

У фільтрі протоколів записую http та запускаю. Виводиться екран всіх http запитів.

A screenshot of the Wireshark interface showing a list of captured packets. The filter bar at the top is set to 'http'. The packet list shows four HTTP requests from 192.168.1.2 to 128.119.245.12.

No.	Time	Source	Destination	Protocol	Length	Info
1721	36.785857	192.168.1.2	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1789	36.983101	128.119.245.12	192.168.1.2	HTTP	784	HTTP/1.1 200 OK (text/html)
2782	51.773799	192.168.1.2	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2784	51.898789	128.119.245.12	192.168.1.2	HTTP	294	HTTP/1.1 304 Not Modified

Рис. 23. HTTP-запити, що пройшли крізь фільтр.

Заходжу у перший GET-запит до HTTP сервера та переглядаю його вміст.

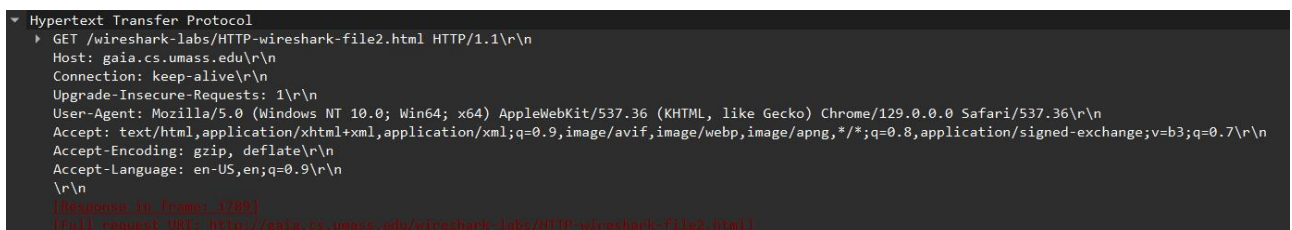


Рис. 24. Вміст першого HTTP-запиту.

Рядок If-Modifid-Since відсутній у першому GET запиті.

Тепер я знаходжу рядок Line-based text data у HTTP-запиті.

```
[Time since request: 0.197244000 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
▼ Line-based text data: text/html (10 lines)
  \n
  <html>\n
  \n
  Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
  This file's last modification date will not change. <p>\n
  Thus if you download this multiple times on your browser, a complete copy <br>\n
  will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
  </html>\n
```

Рис. 25. Вміст переданого html файлу.

Сервер повертає вміст файлу.

Тепер заходжу на 2 GET-запит.

```
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/HTTP-wireshark-file2.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 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  If-None-Match: "173-624b9fff41038"\r\n
  If-Modified-Since: Fri, 18 Oct 2024 05:59:01 GMT\r\n
  \r\n
  [Accepted in frame: 2704]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Рис. 26. Вміст 2 GET-запита.

Рядок If-Modified-Sence наявний у другому GET запиті. Інформація цього рядка становить: Fri, 18 Oct 2024 05:59:01 GMT\r\n.

Тепер знаходжу 2 відповідь від сервера та переглядаю його вміст.

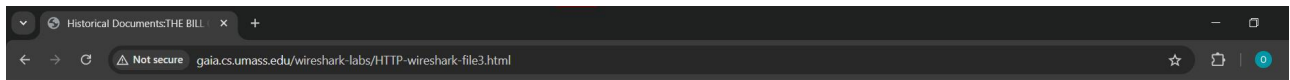
```
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 304 Not Modified\r\n
  Date: Fri, 18 Oct 2024 18:40:52 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "173-624b9fff41038"\r\n
  \r\n
  [Request in frame: 2702]
  [Time since request: 0.124990000 seconds]
  [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Рис. 27. Вміст 2 відповіді від сервера.

Сервер повертає код 304, фразу Not Modified та він не повертає вміст файлу.

5. Аналіз HTTP-запитів з сайту: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

Заходжу на сайт із запущеним до цього інтерфейсом WI-FI програми Wireshark.



THE BILL OF RIGHTS
Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution:

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

Рис. 28. Вміст сайту.

Завдяки фільтру залишаю HTTP-запити.

No.	Time	Source	Destination	Protocol	Length	Info
973	51.988417	192.168.1.2	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
983	52.111163	128.119.245.12	192.168.1.2	HTTP	559	HTTP/1.1 200 OK (text/html)

Рис. 29. HTTP-запити.

Потім знаходжу ці HTTP-запити та TCP протоколи, що відбулись між цими HTTP-запитами.

No.	Time	Source	Destination	Protocol	Length	Info
973	51.988417	192.168.1.2	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
974	51.988732	192.168.1.2	151.101.129.91	QUIC	592	Protected Payload (KP0), DCID=1d85d86e71a9f8a4fa193a72b005af61ea
975	52.034707	151.101.129.91	192.168.1.2	QUIC	327	Protected Payload (KP0)
976	52.040310	151.101.129.91	192.168.1.2	QUIC	66	Protected Payload (KP0)
977	52.068957	192.168.1.2	151.101.129.91	QUIC	83	Protected Payload (KP0), DCID=1d85d86e71a9f8a4fa193a72b005af61ea
978	52.107155	128.119.245.12	192.168.1.2	TCP	54	80 → 61564 [ACK] Seq=1 Ack=473 Win=30336 Len=0
979	52.110230	128.119.245.12	192.168.1.2	TCP	1506	80 → 61564 [ACK] Seq=1 Ack=473 Win=30336 Len=1452 [TCP PDU reassembled in 983]
980	52.110443	128.119.245.12	192.168.1.2	TCP	1506	80 → 61564 [ACK] Seq=1453 Ack=473 Win=30336 Len=1452 [TCP PDU reassembled in 983]
981	52.110466	128.119.245.12	128.119.245.12	TCP	54	61564 → 80 [ACK] Seq=473 Ack=2905 Win=132096 Len=0
982	52.110874	128.119.245.12	192.168.1.2	TCP	1506	80 → 61564 [ACK] Seq=2905 Ack=473 Win=30336 Len=1452 [TCP PDU reassembled in 983]
983	52.111163	128.119.245.12	192.168.1.2	HTTP	559	HTTP/1.1 200 OK (text/html)
984	52.111195	128.119.245.12	128.119.245.12	TCP	54	61564 → 80 [ACK] Seq=473 Ack=4862 Win=132096 Len=0

Рис. 30. Протоколи, що відбулись між HTTP-запитами.

Мій браузер відправив 1 GET запит. У пакеті з номером 973 міститься запит на файл “Білля про права”. Пакет з номером 983 містить відповідь від сервера. Ця відповідь містить код 200 та відповідь OK. Необхідно 5 TCP-сегментів для передачі HTTP-відповіді і файлу “Білля про права”.

6. Аналіз HTTP-запитів з сайту: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

Заходжу на сайт із запущеним до цього інтерфейсом WI-FI програми Wireshark.

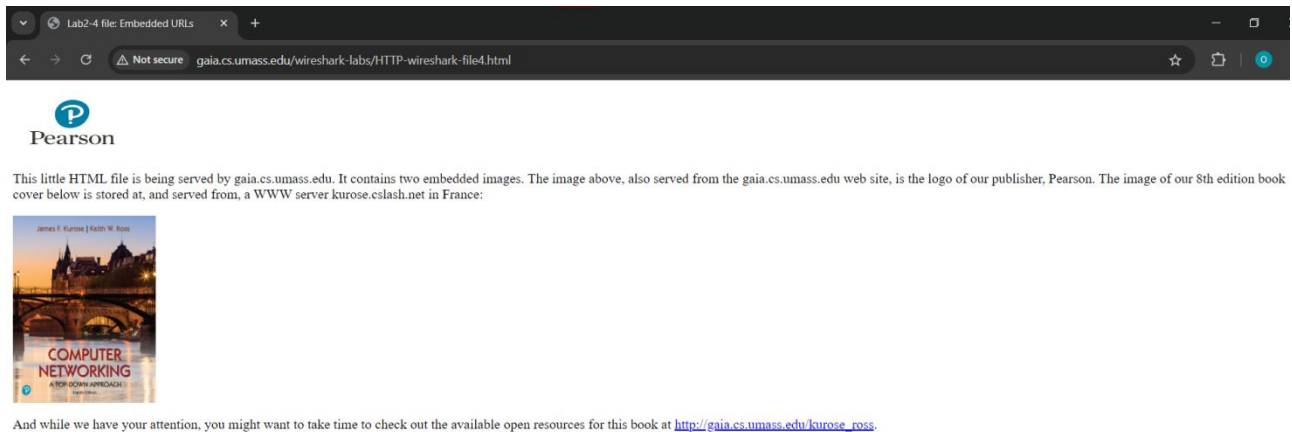


Рис. 31. Вміст сайту.

Завдяки фільтру залишаю тільки HTTP-запити.

http					
No.	Time	Source	Destination	Protocol	Length Info
1131	33.382444	192.168.1.2	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1138	33.503848	128.119.245.12	192.168.1.2	HTTP	1355 HTTP/1.1 200 OK (text/html)
1139	33.545742	192.168.1.2	128.119.245.12	HTTP	472 GET /pearson.png HTTP/1.1
1146	33.671323	128.119.245.12	192.168.1.2	HTTP	761 HTTP/1.1 200 OK (PNG)
1150	33.671697	192.168.1.2	178.79.137.164	HTTP	439 GET /8E_cover_small.jpg HTTP/1.1
1152	33.712721	178.79.137.164	192.168.1.2	HTTP	225 HTTP/1.1 301 Moved Permanently

Рис. 32. HTTP-запити.

Мій браузер відправив 3 GET запити на такі ір-адреси: 128.119.245.12 та 178.79.137.163. Зображення із обох сайтів мій браузер завантажив послідовно оскільки повідомлення HTTP/1.1 200 OK (PNG) на картку pearson.png прийшло до GET-запиту на інше зображення.

7. Аналіз HTTP-запитів з сайту: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

Заходжу на сайт із запущеним до цього інтерфейсом WI-FI програми Wireshark. Мені виводиться вікно для ідентифікації.

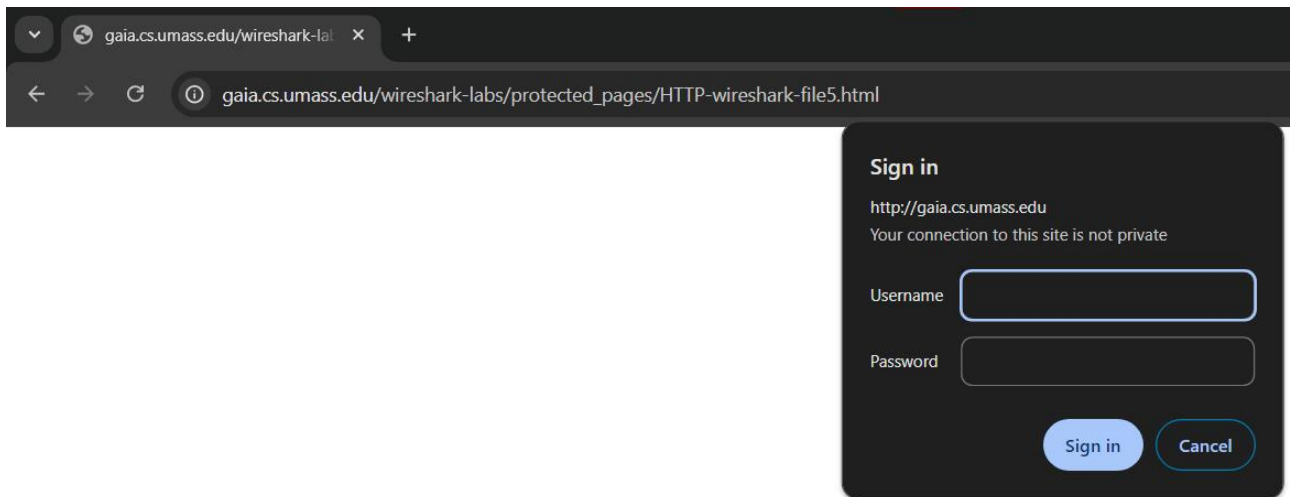


Рис. 33. Вікно для ідентифікації.

Вводжу логін: wireshark-students, пароль: network.

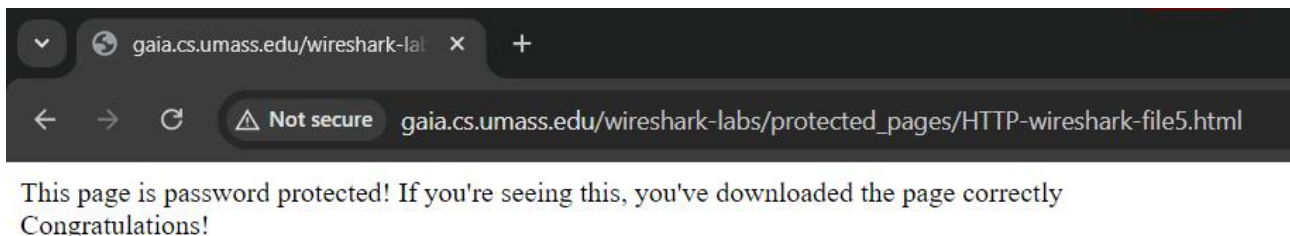


Рис. 34. Вміст сайту.

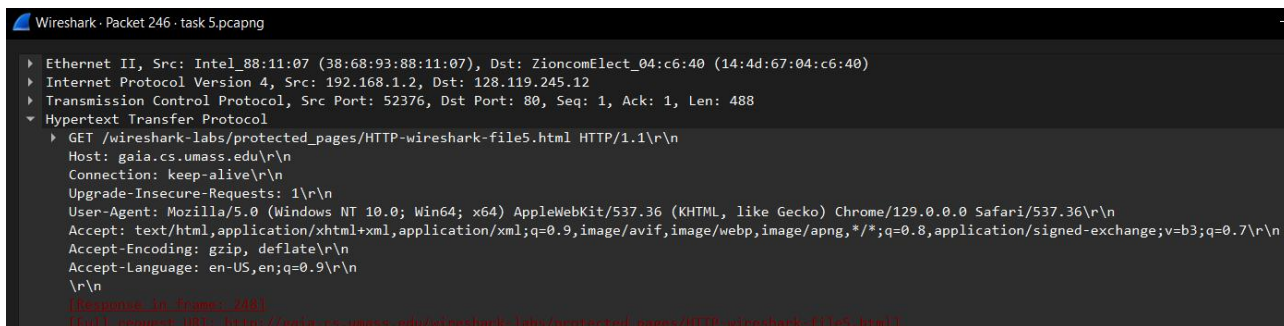
У фільтрі залишаю тільки HTTP-запити.

http						
No.	Time	Source	Destination	Protocol	Length	Info
246	3.057283	192.168.1.2	128.119.245.12	HTTP	542	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
248	3.184631	128.119.245.12	192.168.1.2	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
299	15.445769	192.168.1.2	128.119.245.12	HTTP	627	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
304	15.571865	128.119.245.12	192.168.1.2	HTTP	544	HTTP/1.1 200 OK (text/html)
305	15.572433	192.168.1.2	128.119.245.12	HTTP	712	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
307	15.644789	192.168.1.2	128.119.245.12	HTTP	488	GET /favicon.ico HTTP/1.1
309	15.695894	128.119.245.12	192.168.1.2	HTTP	293	HTTP/1.1 304 Not Modified
311	15.764985	128.119.245.12	192.168.1.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Рис. 35. HTTP-запити.

На перший GET запит сервер надсилає код 401 та фразу Unauthorized.

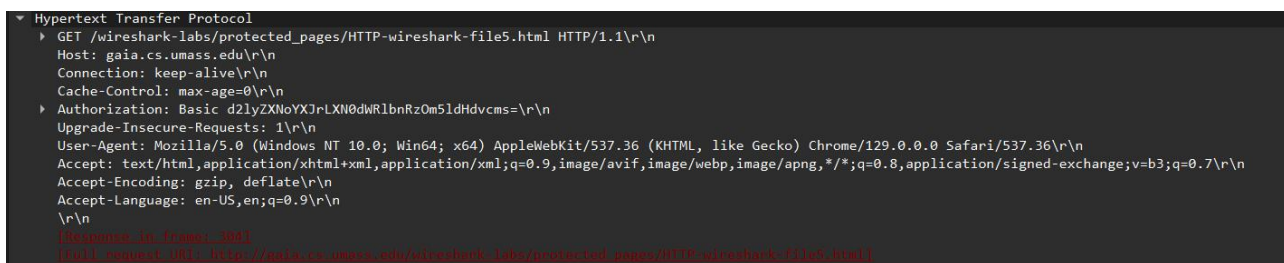
Переглядаю вміст першого GET-запиту.



```
Wireshark · Packet 246 · task 5.pcapng
└─ Ethernet II, Src: Intel_88:11:07 (38:68:93:88:11:07), Dst: ZioncomElect_04:c6:40 (14:4d:67:04:c6:40)
└─ Internet Protocol Version 4, Src: 192.168.1.2, Dst: 128.119.245.12
└─ Transmission Control Protocol, Src Port: 52376, Dst Port: 80, Seq: 1, Ack: 1, Len: 488
  └─ Hypertext Transfer Protocol
    └─ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      \r\n
      [Hex dump in frames: 248]
      (Click request 185 to view /gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html)
```

Рис. 36. Вміст 1 GET-запиту.

Переглядаю вміст другого GET-запиту.



```
Hypertext Transfer Protocol
└─ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
  Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmM=\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Hex dump in frames: 280]
  (Click request 185 to view /gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html)
```

Рис. 36. Вміст 2 GET-запиту.

У другому GET запиті додалися такі поля: Authorization, Cache-Control.

Рядок з підзаголовка Authorization передаю у конвертер з Base64.



Source data from the Base64 string:

wireshark-students

Type (or copy-paste) some text to a textbox below. The text can be a Base64 string to decode or any string to encode to a Base64.

d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmM=

or select a file to convert to a Base64 string.

Browse... No file selected. Convert the source data

What to do with the source data:

- ☐ encode the source data to a Base64 string (base64 encoding)
Maximum characters per line: 76
- ☒ decode the data from a Base64 string (base64 decoding)

Output data:

- ☒ output to a textbox (as a string)
- ☐ export to a binary file, filename: base64.bin

Рис. 37. Вміст перекладеного з Base64 рядка.

ВИСНОВОК

У процесі вивчення можливостей програми сніфера Wireshark для аналізу пакетів протоколу HTTP було отримано цінні знання про функціонування мережевих протоколів та їх аналіз. Wireshark дозволяє в реальному часі фіксувати і детально аналізувати мережеві пакети, що робить його незамінним інструментом для фахівців у галузі комп'ютерних мереж.

Аналіз HTTP-трафіку через Wireshark відкриває можливості для розуміння структури запитів і відповідей, а також для виявлення потенційних проблем у роботі веб-додатків. Це дозволяє не лише виявляти помилки, але й підвищувати безпеку, вивчаючи, які дані передаються між клієнтом і сервером.