**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

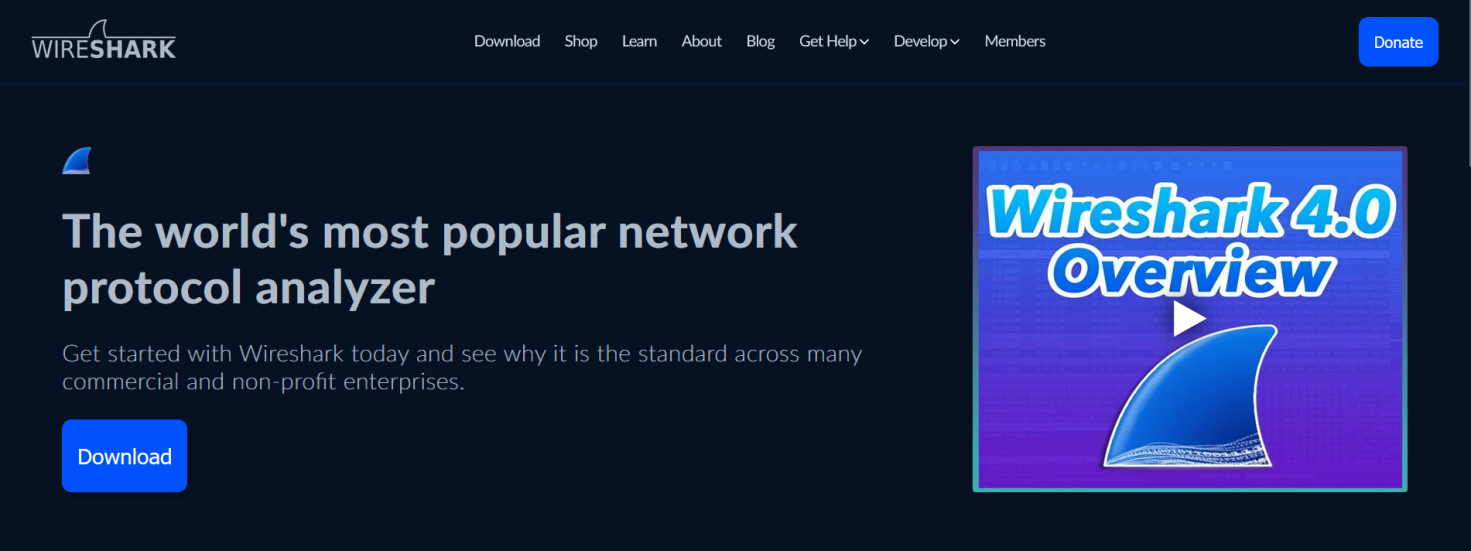
**Тема:** “Вивчення можливостві програми сніфера Wireshark для

аналізу пакетів протоколу HTTP.”

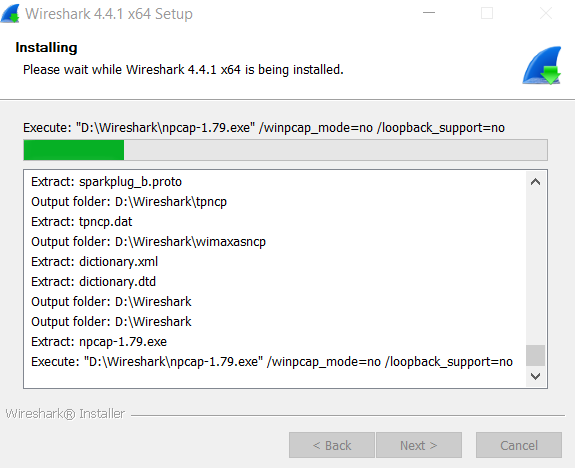
**Мета:** “Вивчити роботу мережного сніфера та роботу проколу HTTP.”

**ВИКОНАННЯ ЗАВДАННЯ**

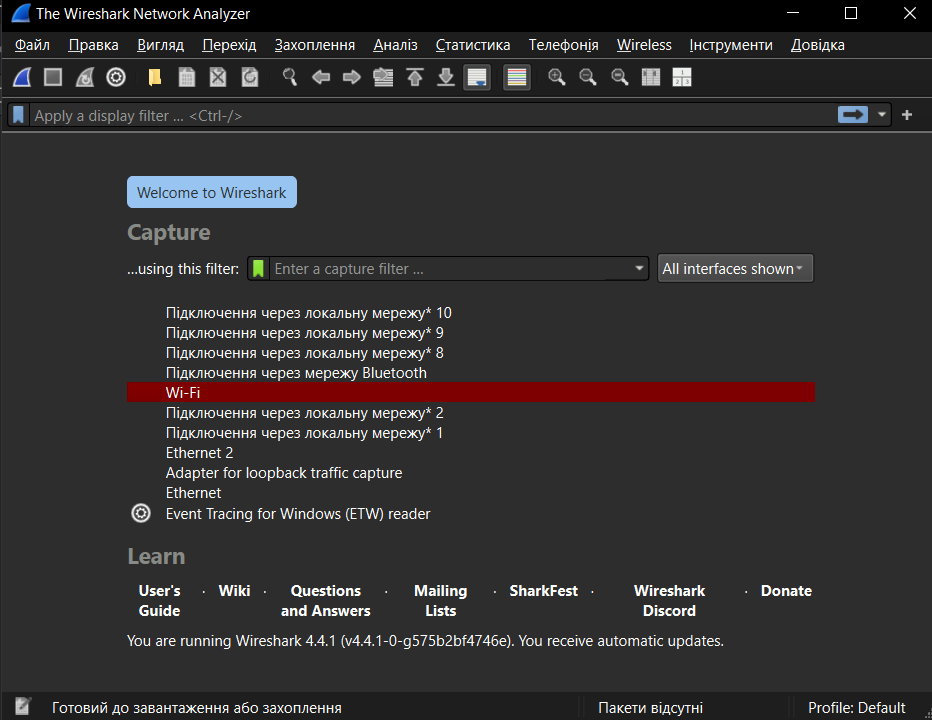
1. Завантаження Wireshark.

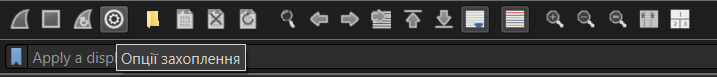


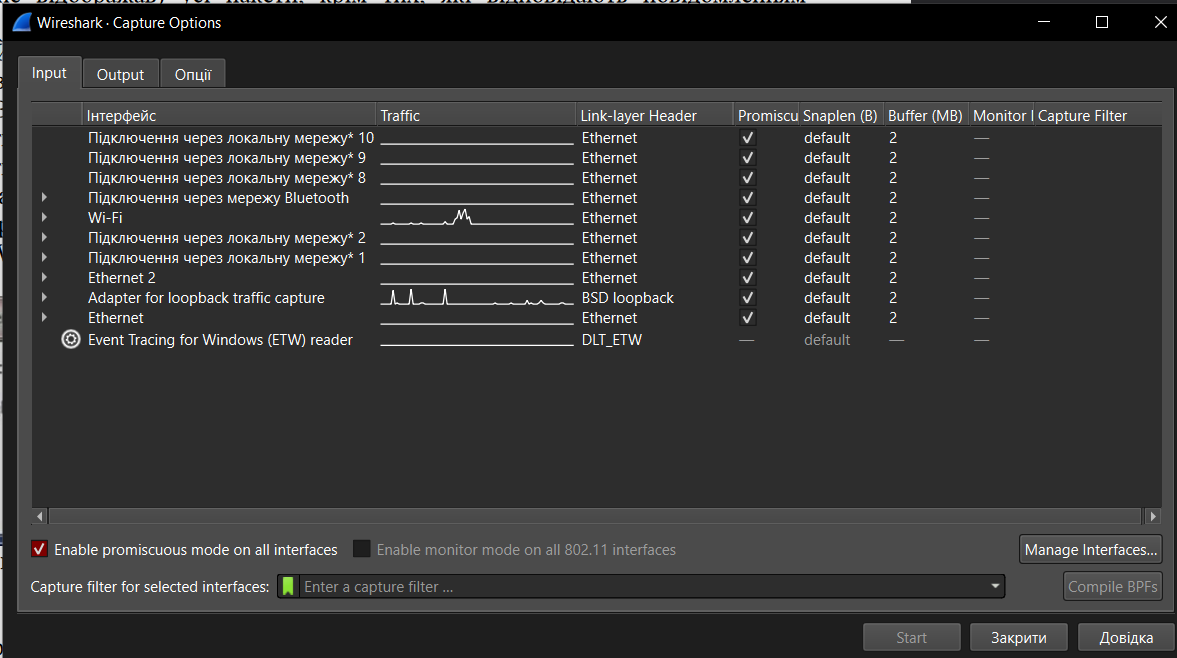


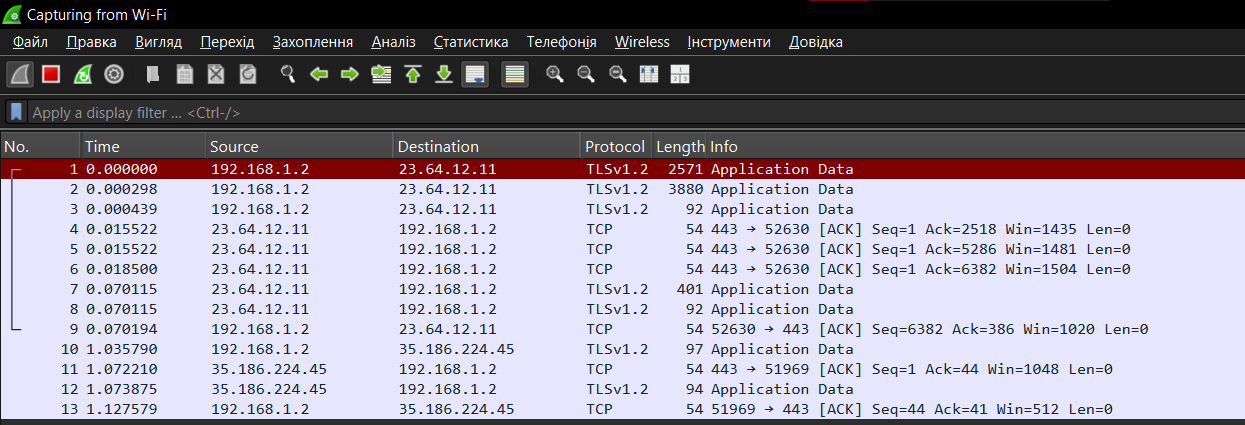


1. Запуск Wireshark.

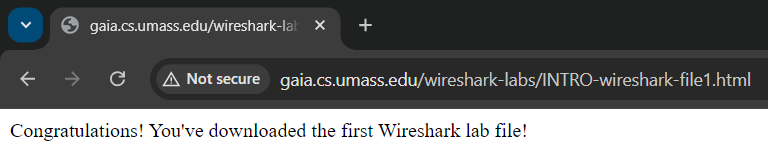


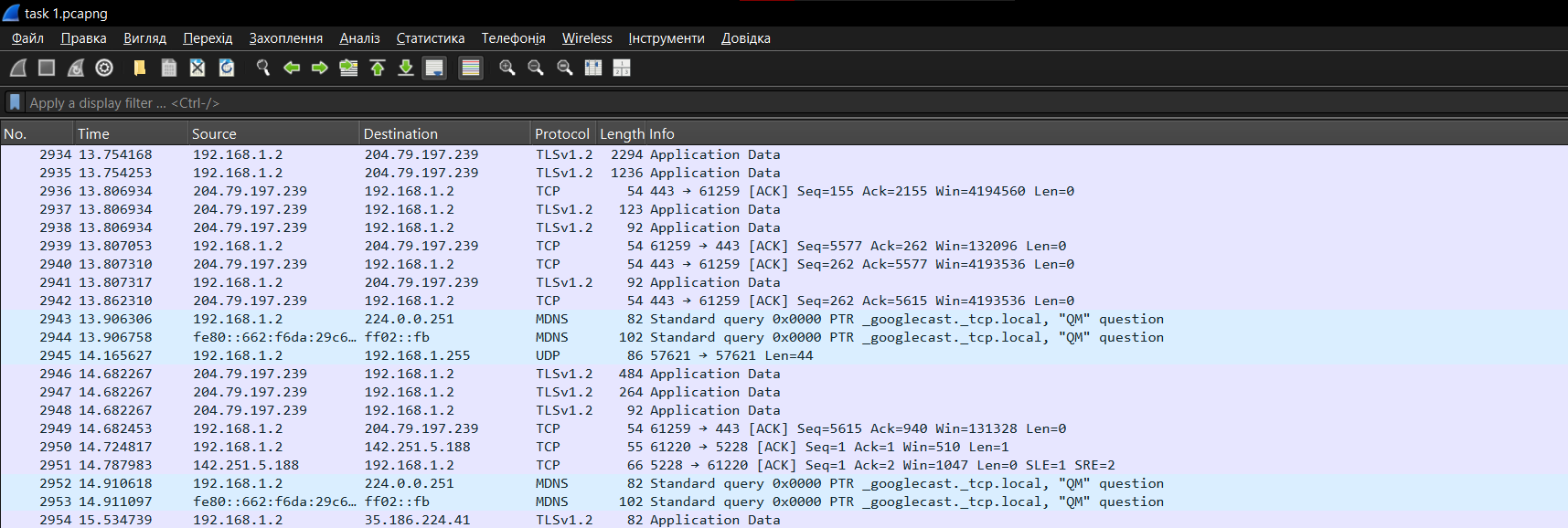


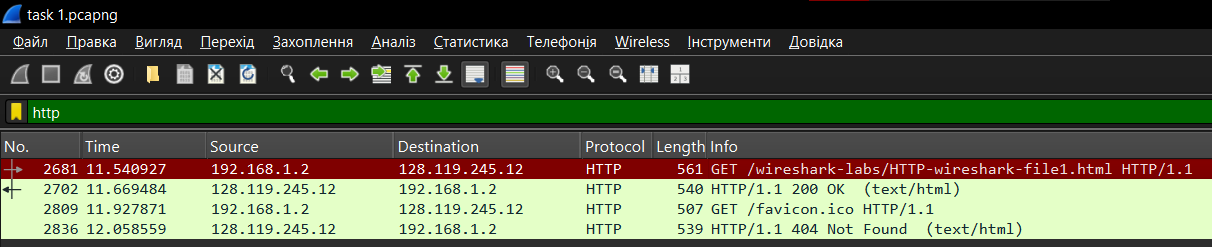


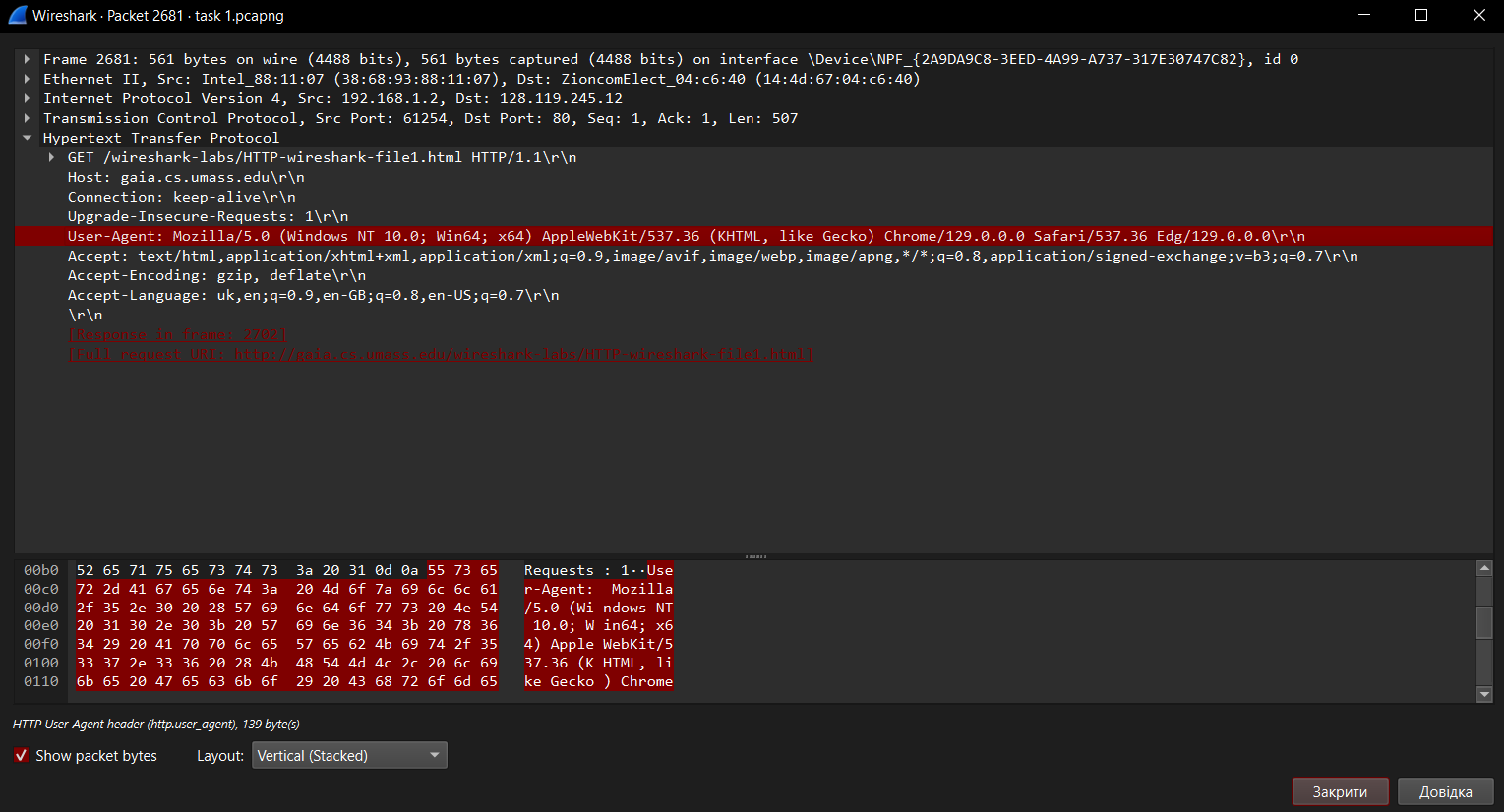


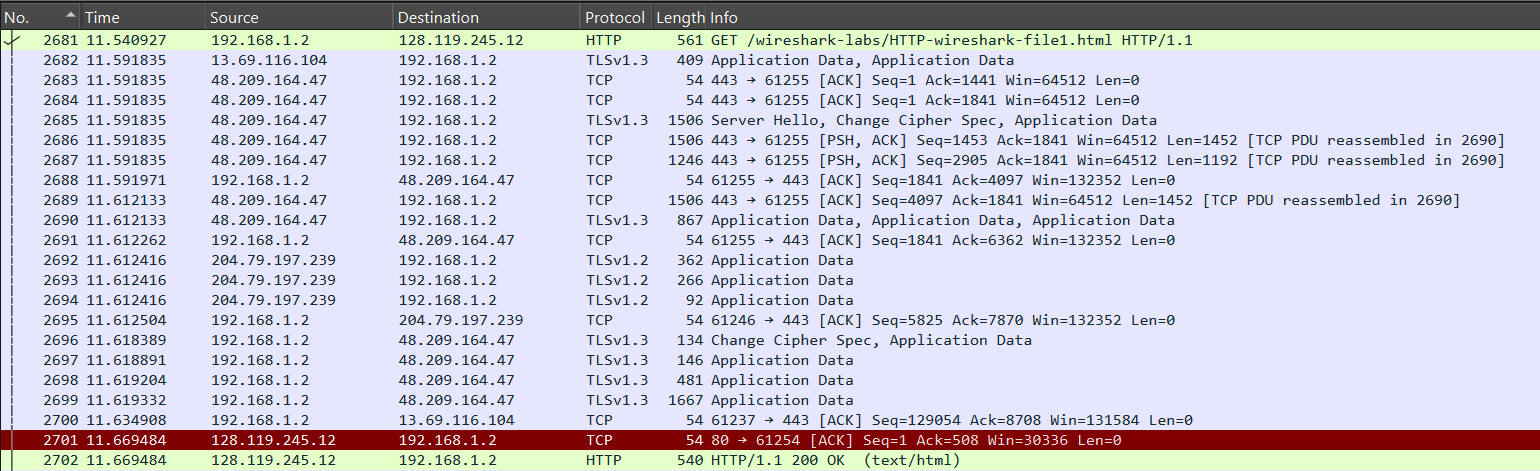
1. Аналіз HTTP-запиту з сайту: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>









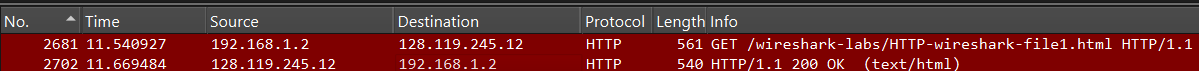


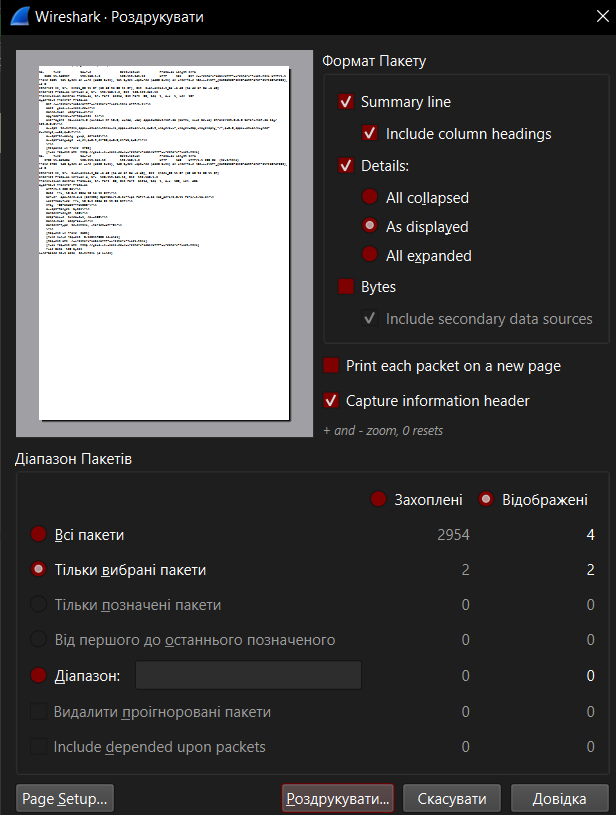
У стовпці Protocol між HTTP-запитами відображені такі протоколи: TLSv1.3, TLSv1.2, TCP. Час що пройшов до одержання HTTP-запита з повідомленням HTTP/1.1 200 OK становить: 11.669484 - 11.54927 = 0.120214 секунд.

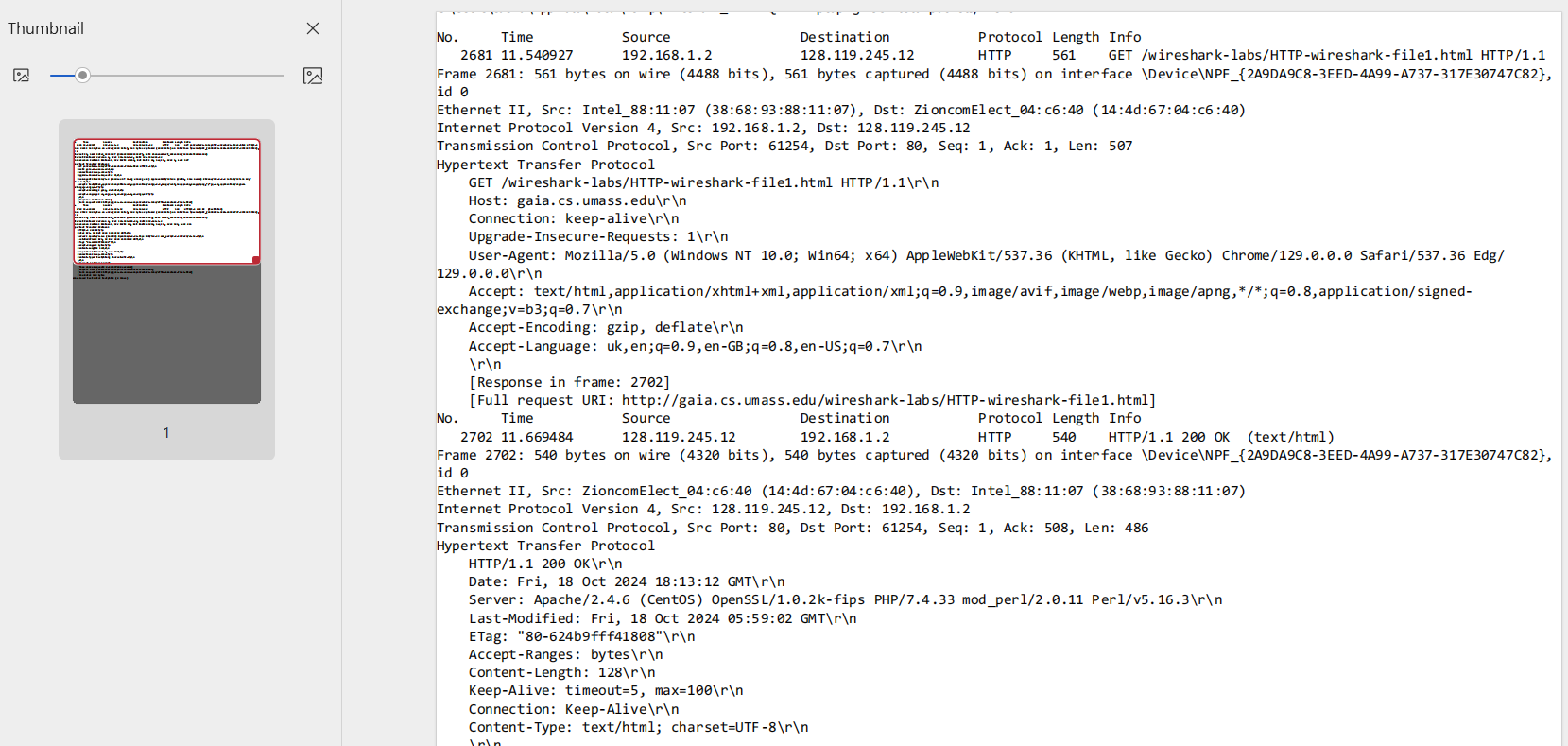


Source - адреса мого комп’ютера яка становить: 192.168.1.2.

Destination - адреса сервера, що становить: 128.119.245.12.









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



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



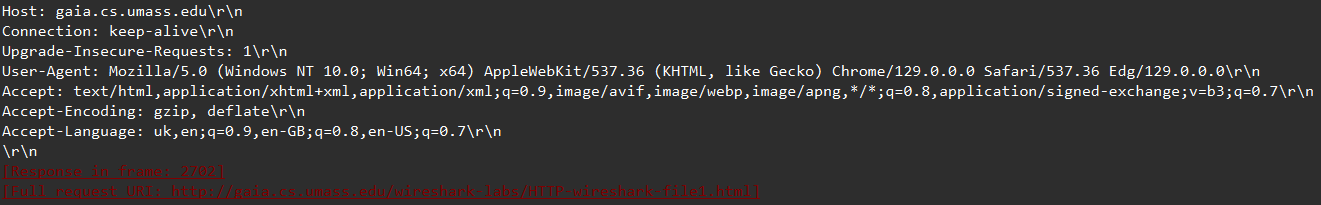
Код стану повернення сервер браузеру становить: 200.



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

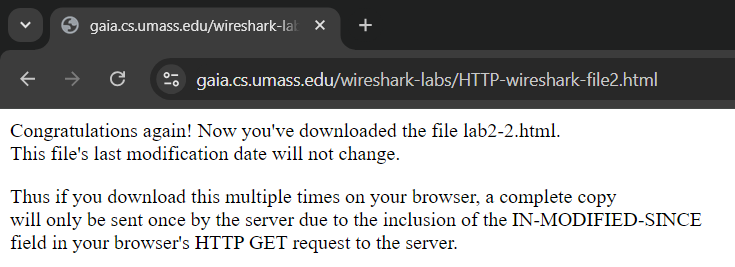


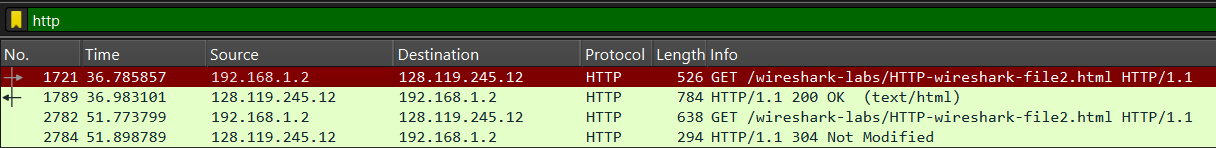
Розмір змісту, що повернув сервер браузеру становить: 128 байт.

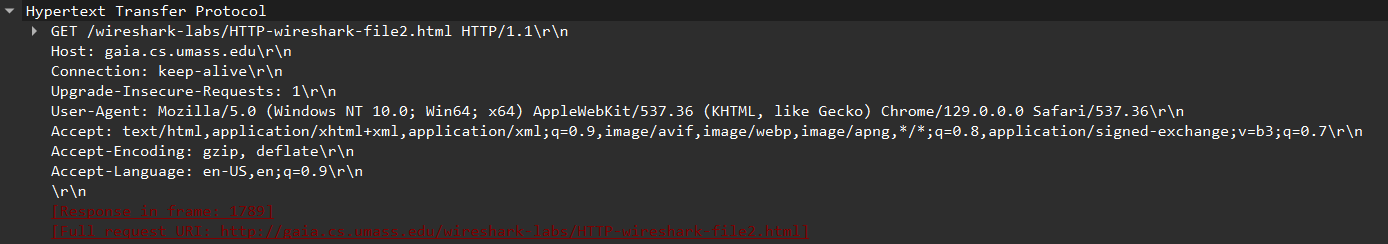


Не відображені у списку пакетів заголовки: Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, Accept-Language.

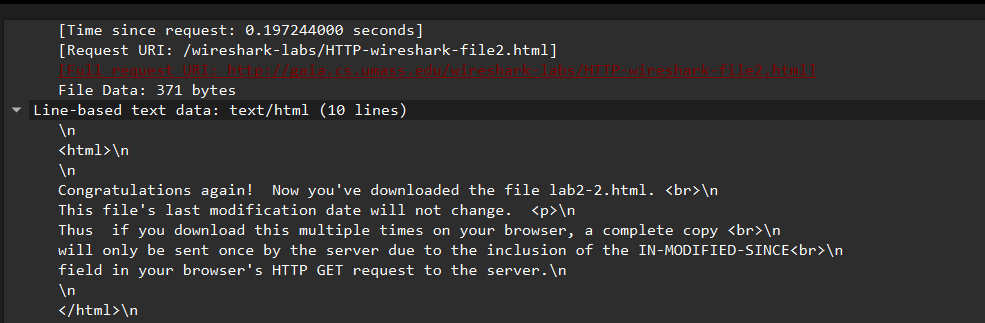
1. Аналіз HTTP-запиту з сайту: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>



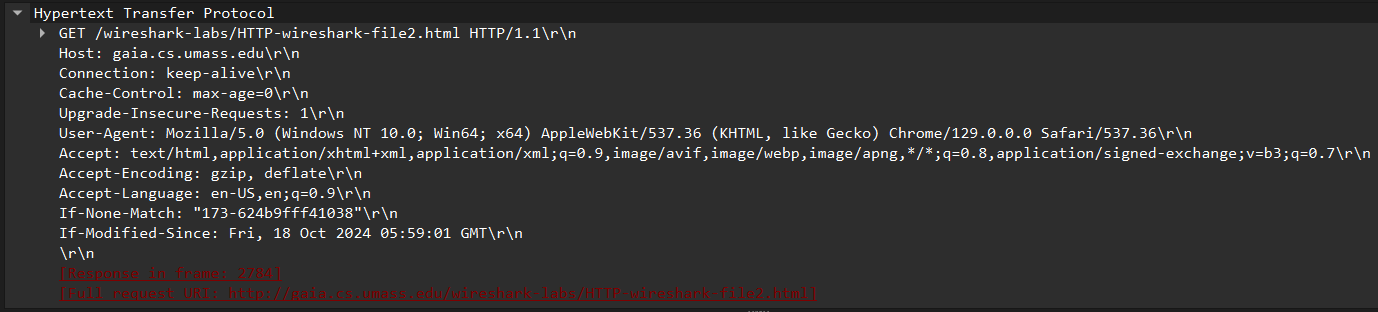


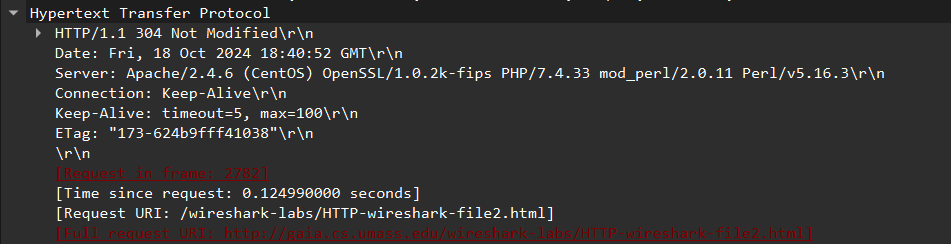


Рядок If-Modifid-Since відсутній у першому GET запиті.



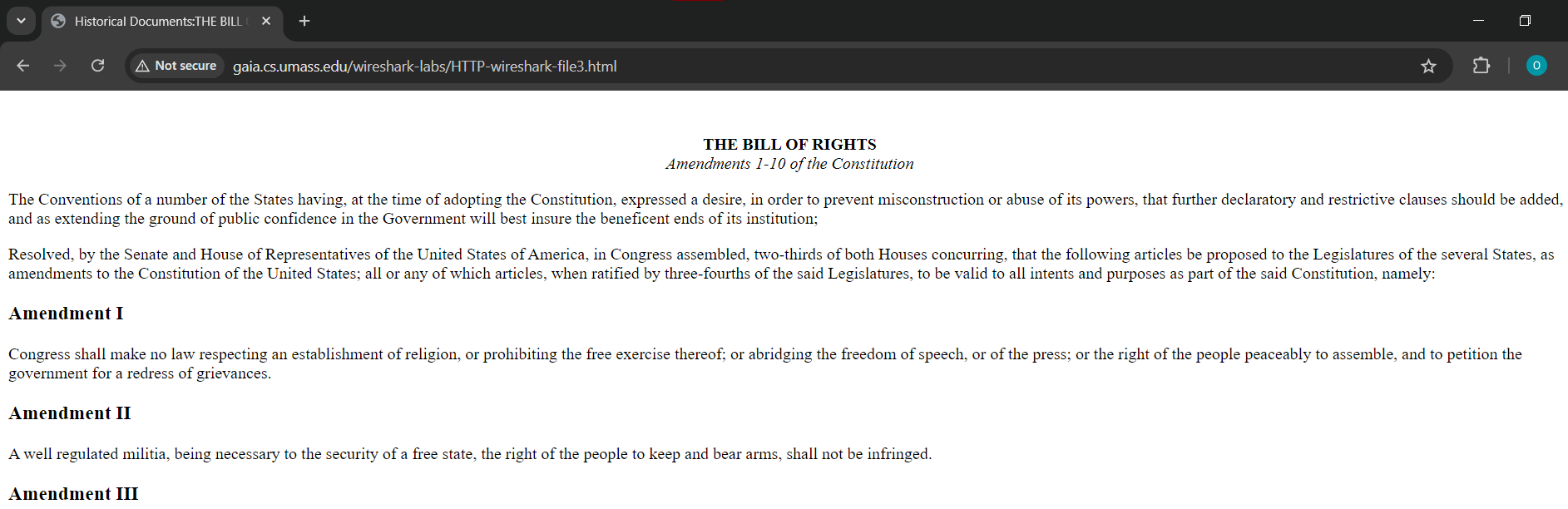
Сервер повертає вміст файлу.

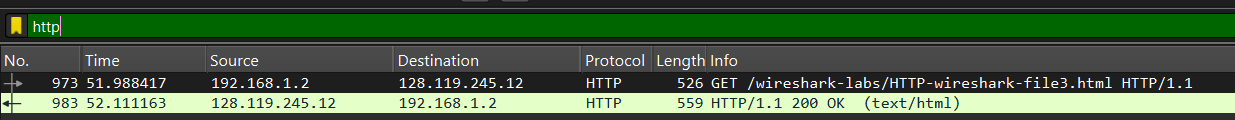
Рядок If-Modified-Sence наявний у другому GET запиті. Інформація цього рядка становить: Fri, 18 Oct 2024 05:59:01 GMT\r\n.

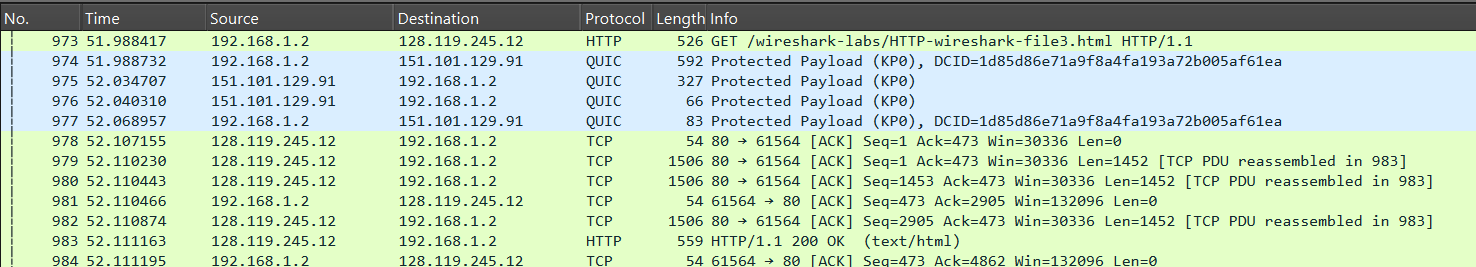


Сервер повертає код 304, фразу Not Modified та він не повертає вміст файлу.

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

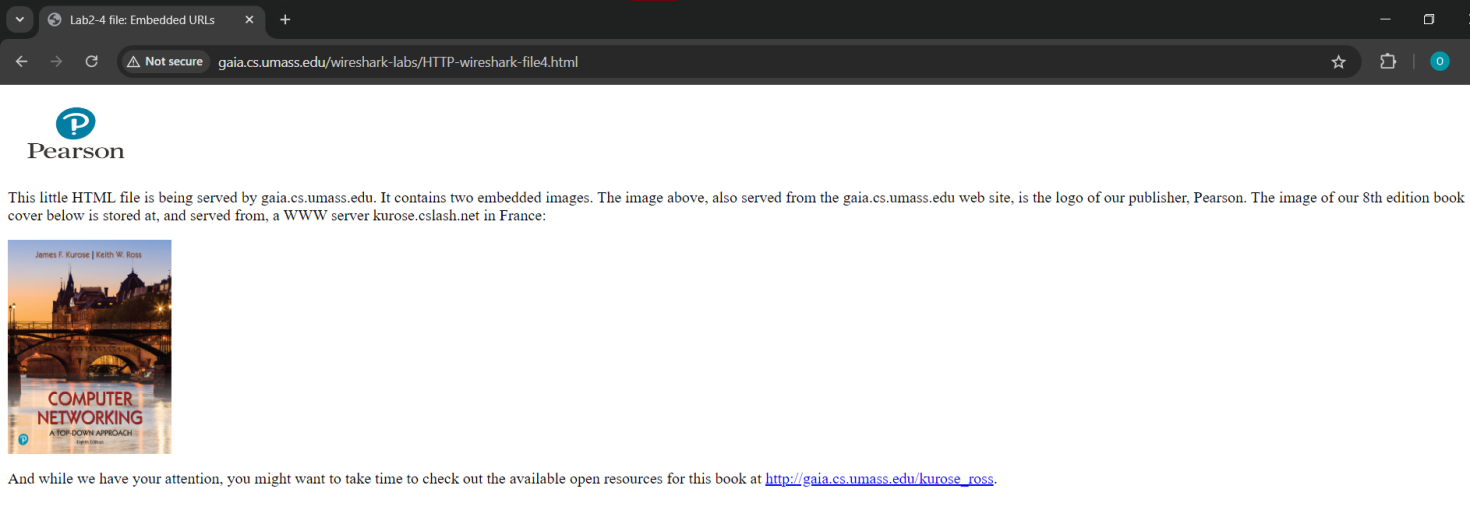


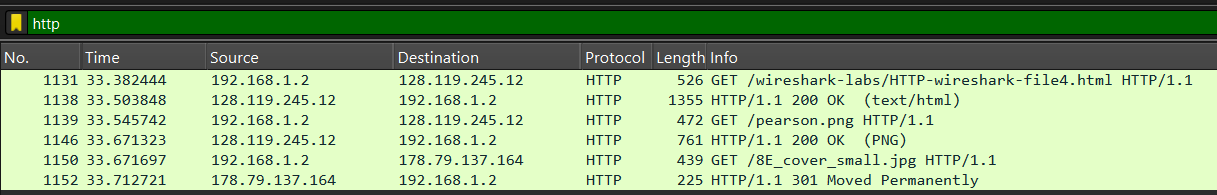




Мій браузер відправив 1 GET запит. У пакеті з номером 973 міститься запит на файл “Білля про права”. Пакет з номером 983 містить відповідь від сервера. Ця відповідь містить код 200 та відповідь OK. Необхідно 5 TCP-сегментів для передачі HTTP-відповіді і файлу “Білля про права”.

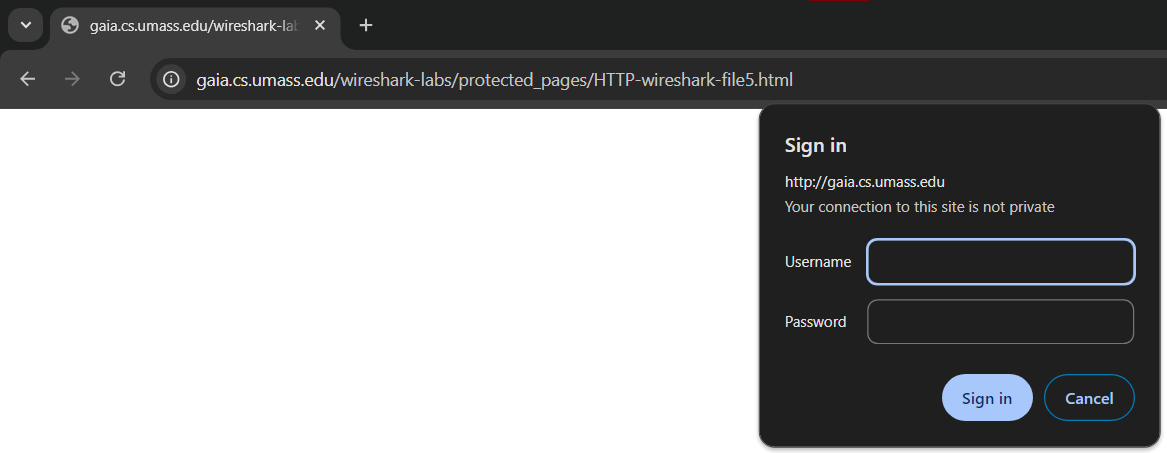
1. Аналіз HTTP-запиту з сайту: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>



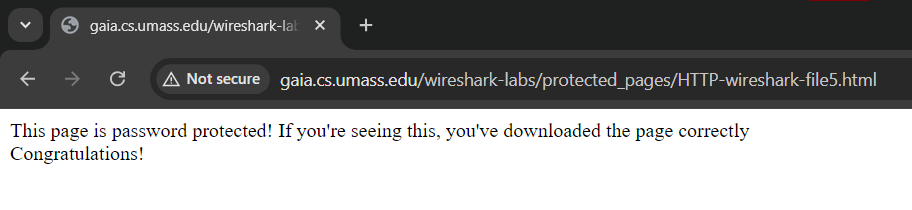


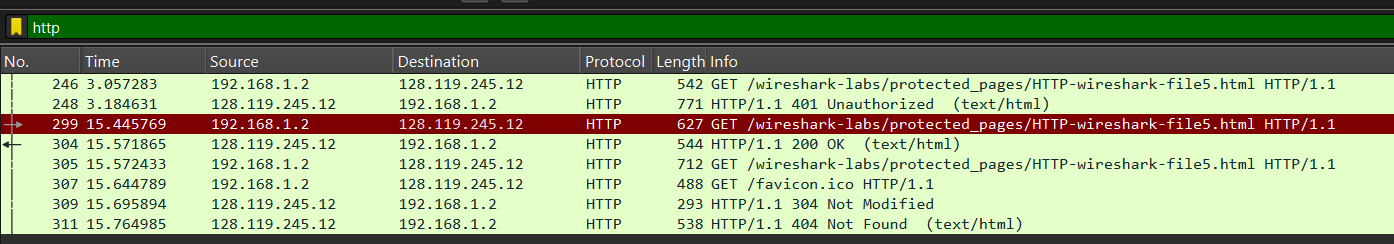
Мій браузер відправив 3 GET запита на такі ip-адреси: 128.119.245.12 та 178.79.137.163. Зображення із обох сайтів мій браузер завантажив послідовно оскільки повідомлення HTTP/1.1 200 OK (PNG) на картнку pearson.png прийшло до GET-запиту на інше зображення.

1. Аналіз HTTP-запиту з сайту: <http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html>

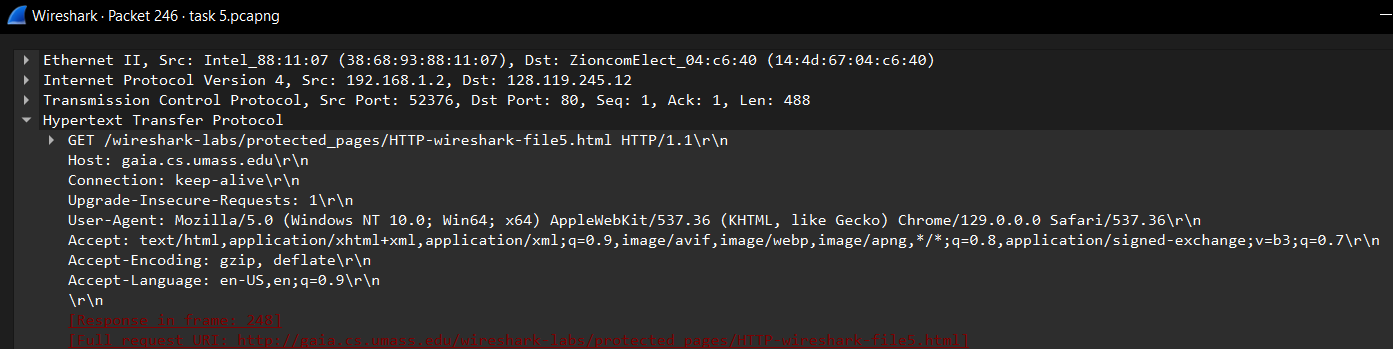


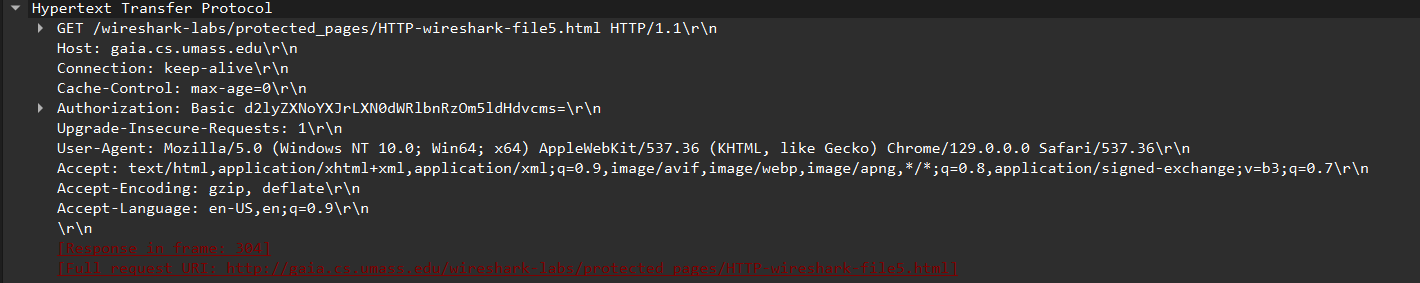
Вводжу логін: wireshark-students, пароль: network.



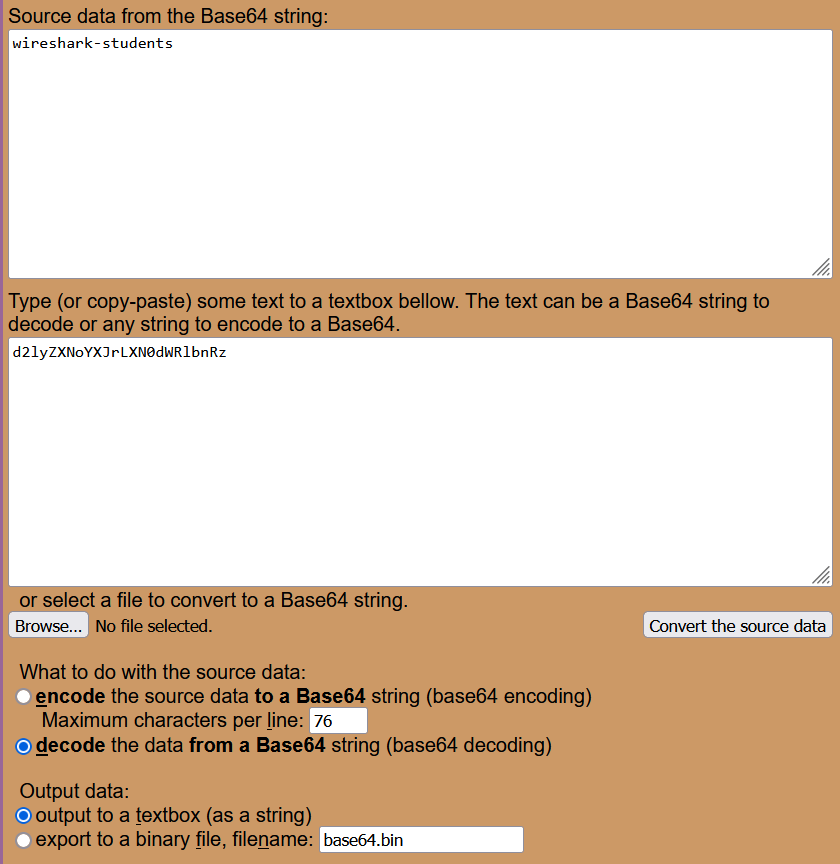


На перший GET запит сервер надсилає код 401 та фразу Unathorized.





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



**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.