

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІІСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 1
З дисципліни: Комп'ютерні мережі

Основи захоплення та аналізу пакетів

Виконав:
Студент III курсу
Групи КА-74
Джалаганія Б.І.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

Хід виконання роботи

The screenshot displays the Wireshark network traffic analysis tool. The main packet list shows several HTTP requests from 192.168.1.57 to 128.119.245.12. The selected packet (No. 84) is an HTTP POST request to /api. The packet details pane shows the structure of the frame, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

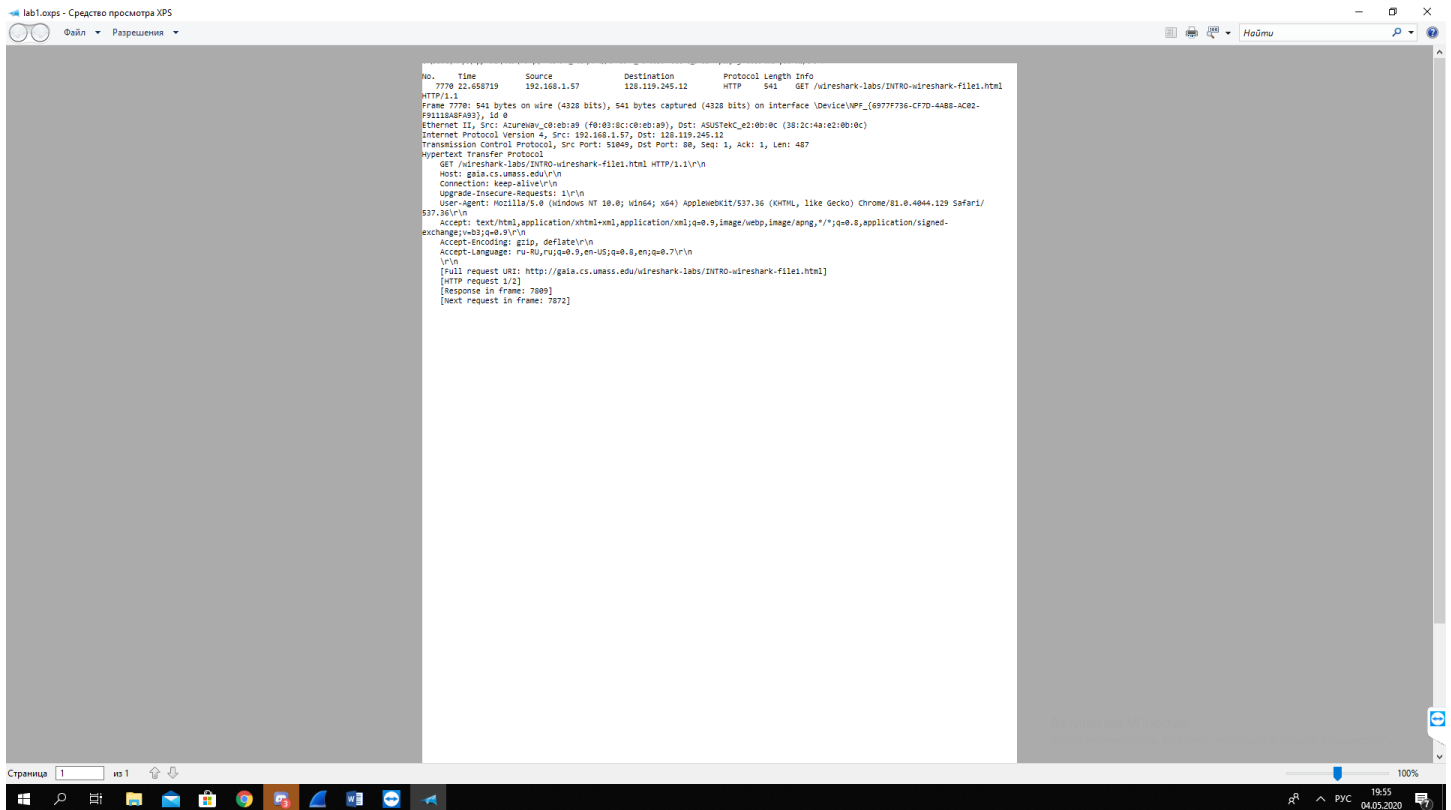
No.	Time	Source	Destination	Protocol	Length	Info
77...	22.658719	192.168.1.57	128.119.245.12	HTTP	541	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
78...	22.784645	128.119.245.12	192.168.1.57	HTTP	492	HTTP/1.1 200 OK (text/html)
78...	22.950515	192.168.1.57	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
78...	23.073594	128.119.245.12	192.168.1.57	HTTP	538	HTTP/1.1 404 Not Found (text/html)
84...	25.016499	192.168.1.57	149.154.167.1...	HTTP	94	POST /api HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 7770: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface \Device\NPF_{6977F736-CF7D-4AB8-AC02-F91118A8FA93}, id 0
> Ethernet II, Src: AzureWav_c0:eb:a9 (f0:03:8c:c0:eb:a9), Dst: ASUSTekC_e2:0b:0c (38:2c:4a:e2:0b:0c)
> Internet Protocol Version 4, Src: 192.168.1.57, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51049, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
> Hypertext Transfer Protocol

0000 38 2c 4a e2 0b 0c f0 03 8c c0 eb a9 08 00 45 00 8, J.....E..
0010 02 0f 47 41 40 00 80 06 7a 42 c0 a8 01 39 80 77 ..GA@...zB...9.w
0020 f5 0c c7 69 00 50 9a 58 8f 3d 6b 8b e2 36 50 18 ...i.P.X=k..6P..
0030 00 44 9b a0 00 00 47 45 54 20 2f 77 69 72 65 73 ..D....GE T/wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO..
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1..

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Profile: Default
Packets: 10638 · Displayed: 5 (0.0%) · Dropped: 0 (0.0%)
19:30 04.05.2020



Контрольні питання

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
TCP, RTCP, UDP, TLS, DNS, HTTP.
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
ICP, Ethernet II, HTTP, TCP.
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Пройшло 0.125926 с.

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

Запит:

Вихідна: 192.168.1.57

Цільова: 128.119.245.12

Відповідь:

Вихідний: 128.119.245.12

Цільовий: 192.168.1.57

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

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

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

HTTP/1.1 200 OK (text/html)

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Було проаналізовано час за який було відправлено перший запит та отримано першу відповідь, а також було розглянуто протоколи HTTP.