МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС

«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»

НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №1

з курсу «Комп’ютерні мережі»

тема: «Захоплення та аналіз пакетів»

Виконала: студентка 3 курсу

групи КА-77

Пересунько М.О.

Прийняв: Кухарєв С.О.

Київ – 2020р.

Frame 57: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF\_{76D97BE3-AF50-4EAD-B5FD-B0FEFF15522F}, id 0

Ethernet II, Src: HonHaiPr\_39:d9:49 (40:b8:9a:39:d9:49), Dst: Cisco-Li\_60:14:45 (20:aa:4b:60:14:45)

Internet Protocol Version 4, Src: 10.186.199.12, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 41273, Dst Port: 80, Seq: 1, Ack: 1, Len: 496

Hypertext Transfer Protocol

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

[Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/INTRO-wireshark-file1.html

Request Version: HTTP/1.1

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/79.0.3945.130 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

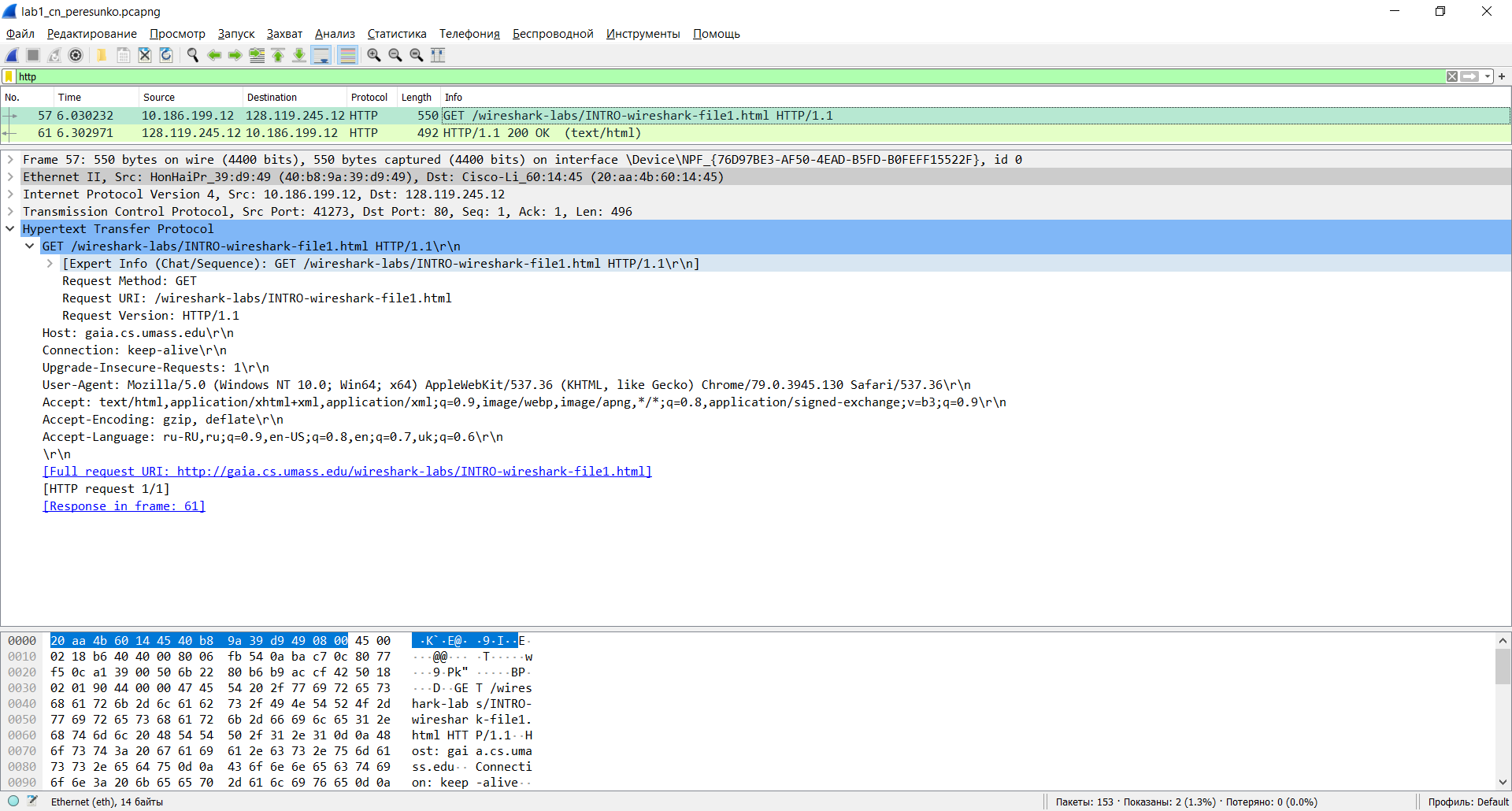
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/1]

[Response in frame: 61]



Frame 61: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF\_{76D97BE3-AF50-4EAD-B5FD-B0FEFF15522F}, id 0

Ethernet II, Src: Cisco-Li\_60:14:45 (20:aa:4b:60:14:45), Dst: HonHaiPr\_39:d9:49 (40:b8:9a:39:d9:49)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.186.199.12

Transmission Control Protocol, Src Port: 80, Dst Port: 41273, Seq: 1, Ack: 497, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Tue, 18 Feb 2020 14:36:32 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Tue, 18 Feb 2020 06:59:01 GMT\r\n

ETag: "51-59ed434ef8587"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

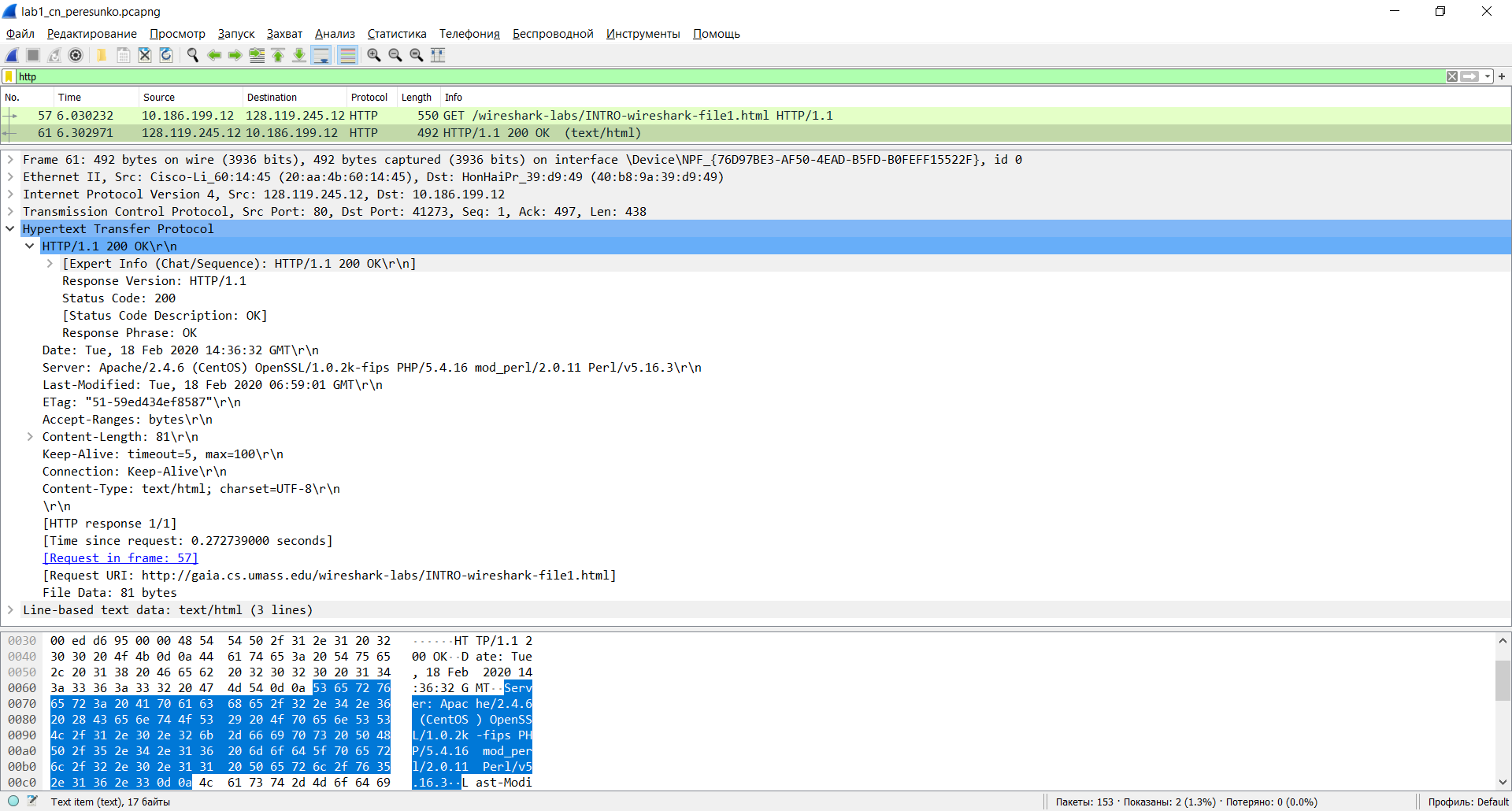
[Time since request: 0.272739000 seconds]

[Request in frame: 57]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

File Data: 81 bytes

Line-based text data: text/html (3 lines)



1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?

DNS, HTTP, LLMNR, MNDS, NBNS, SSDP, SSL, SSLv3, TCP, TLSv1, UDP.

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

TCP, IP, Ethernet, HTTP

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

0.272739 c

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

Із запитом:

Вихідна адреса: 10.186.199.12

Цільова адреса: 128. 119. 245. 12.

Із відповіддю:

Цільова адреса: 10.186.199.12

Вихідна адреса: 128. 119. 245. 12.

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

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

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

HTTP/1.1 200 OK\r\n

**Висновок:** Набуто базові навички роботи з wireshark, деяка інформація про протоколи, навички захоплення пакетів.