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
Фуклєва У. С.
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

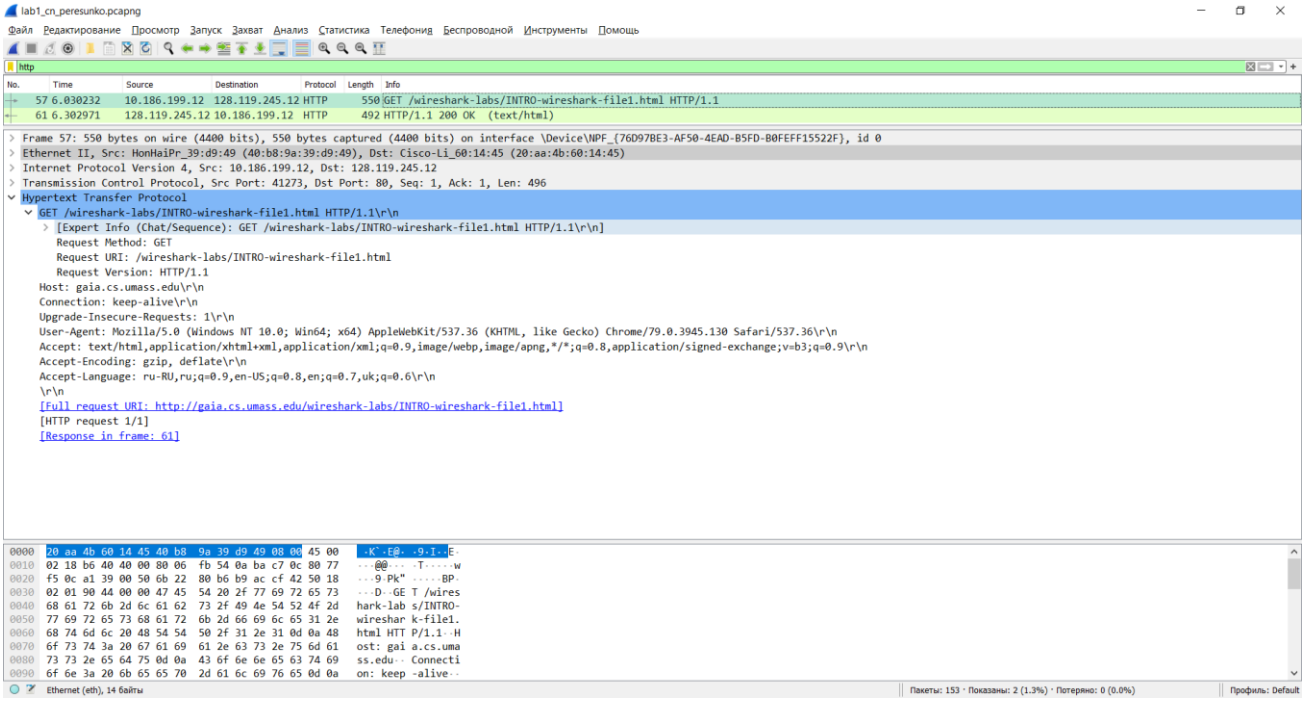
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6\r\n

\r\n

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

[HTTP request 1/1]

[Response in frame: 61]


lab1_cn_peresunko.pcapng
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
http
No. Time Source Destination Protocol Length Info
57 6.030232 10.186.199.12 128.119.245.12 HTTP 550 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
61 6.302971 128.119.245.12 10.186.199.12 HTTP 492 HTTP/1.1 200 OK (text/html)
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]
0000 20 aa 4b 60 14 45 40 b8 9a 39 d9 49 08 00 45 00
0010 02 18 b6 40 40 00 80 06 fb 54 0a ba c7 0c 80 77
0020 f5 0c a1 39 00 50 6b 22 80 b6 b9 ac cf 42 50 18
0030 02 01 90 44 00 00 47 45 54 20 2f 77 69 72 65 73
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a
Ethernet (eth), 14 байты
Пакеты: 153 · Показаны: 2 (1.3%) · Потеряно: 0 (0.0%)
Профиль: Default

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]

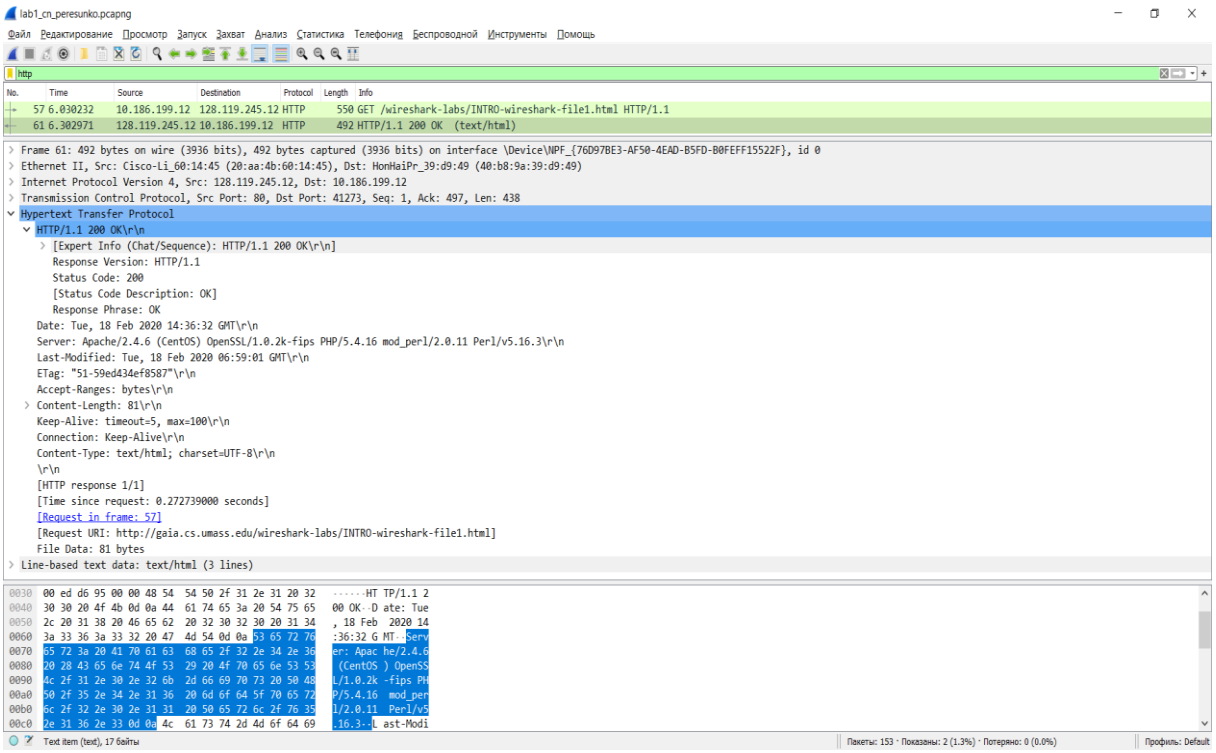
[Time since request: 0.272739000 seconds]

[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

2. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?
   0.272739 с

3. 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.

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

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

5. 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.