



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

## **Лабораторна робота №1**

**З дисципліни: «Комп'ютерні мережі»**

**На тему: «Основи захоплення та аналізу пакетів»**

**Виконала:**

Студентка III курсу

Групи КА-74

Горюшкіна К.Г.

**Перевірив:**

Кухарев С.О.

**Київ 2020**

## Хід виконання роботи

1. Після запуску Wireshark та введення відповідного запиту у браузері отримали захоплені пакети:

Wireshark interface showing a packet capture. The packet list on the left shows several TCP and TLSv1 packets. The packet details pane on the right shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and Transport Layer Security. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	17.248.147.83	192.168.1.117	TLSv1...	Ignored Unknown Record
2	0.000110	192.168.1.117	17.248.147.83	TCP	58076 → 443 [ACK] Seq=1 Ack=4294965849 Win=2048 Len=0 TSval=1257699846 TSecr=38734...
3	0.142193	17.248.147.83	192.168.1.117	TCP	[TCP Retransmission] 443 → 58076 [ACK] Seq=4294965849 Ack=1 Win=3283 Len=1448 TSva...
4	0.142294	192.168.1.117	17.248.147.83	TCP	58076 → 443 [ACK] Seq=1 Ack=1123 Win=2007 Len=0 TSval=1257699988 TSecr=3873493326
5	0.193892	192.168.1.117	17.248.147.83	TLSv1...	Application Data
6	0.193893	192.168.1.117	17.248.147.83	TLSv1...	Application Data
7	0.689888	17.248.147.83	192.168.1.117	TLSv1...	[TCP Previous segment not captured] , Ignored Unknown Record
8	0.689972	192.168.1.117	17.248.147.83	TCP	[TCP Dup ACK #1] 58076 → 443 [ACK] Seq=680 Ack=1123 Win=2048 Len=0 TSval=12577005...
9	0.710510	17.248.147.83	192.168.1.117	TCP	[TCP Retransmission] 443 → 58076 [PSH, ACK] Seq=2571 Ack=680 Win=3325 Len=1122 TSv...
10	0.710591	192.168.1.117	17.248.147.83	TCP	[TCP Dup ACK #2] 58076 → 443 [ACK] Seq=680 Ack=1123 Win=2048 Len=0 TSval=12577005...
11	1.012237	17.248.147.83	192.168.1.117	TCP	[TCP Retransmission] 443 → 58076 [ACK] Seq=1123 Ack=680 Win=3325 Len=1448 TSval=38...
12	1.012341	192.168.1.117	17.248.147.83	TCP	58076 → 443 [ACK] Seq=680 Ack=3693 Win=2007 Len=0 TSval=1257700856 TSecr=3873494166
13	4.056470	ASUSTekC_92:2d...	Spanning-tree-...	STP	Conf. Root = 32768/0/c8:60:00:92:2d:1a Cost = 0 Port = 0x8002
14	4.056475	192.168.1.169	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
15	4.058574	192.168.1.117	17.248.147.83	TLSv1...	Application Data
16	4.058575	192.168.1.117	17.248.147.83	TLSv1...	Application Data
17	4.062901	192.168.1.117	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
18	4.367397	192.168.1.117	17.248.147.83	TCP	[TCP Retransmission] 58076 → 443 [PSH, ACK] Seq=680 Ack=3693 Win=2048 Len=679 TSva...
19	4.422545	17.248.147.83	192.168.1.117	TCP	[TCP Previous segment not captured] 443 → 58076 [ACK] Seq=6263 Ack=1359 Win=3367 L...
20	4.463580	17.248.147.83	192.168.1.117	TCP	[TCP Retransmission] 443 → 58076 [PSH, ACK] Seq=5141 Ack=1359 Win=3367 Len=1122 TSv...
21	4.463676	192.168.1.117	17.248.147.83	TCP	[TCP Dup ACK 12#1] 58076 → 443 [ACK] Seq=1359 Ack=3693 Win=2048 Len=0 TSval=125770...
22	4.504642	17.248.147.83	192.168.1.117	TCP	[TCP Retransmission] 443 → 58076 [ACK] Seq=3693 Ack=1359 Win=3367 Len=1448 TSval=3...

► Frame 1: 1188 bytes on wire (9504 bits), 1188 bytes captured (9504 bits) on interface en0, id 0

► Ethernet II, Src: ASUSTekC\_92:2d:1a (c8:60:00:92:2d:1a), Dst: Apple\_ef:19:a4 (48:bf:6b:ef:19:a4)

► Internet Protocol Version 4, Src: 17.248.147.83, Dst: 192.168.1.117

► Transmission Control Protocol, Src Port: 443, Dst Port: 58076, Seq: 1, Ack: 1, Len: 1122

► Transport Layer Security

0000 48 bf 6b ef 19 a4 c8 60 00 92 2d 1a 08 00 45 00 H-k...-...E

0010 04 96 ef 25 40 00 39 06 e6 d3 11 f8 93 53 c0 a8 ...%@:9: ...S-

0020 01 75 01 bb e2 dc 13 c5 8c 14 01 9a d4 47 80 18 -u.....G-

Ready to load or capture

Packets: 188 · Displayed: 188 (100.0%)

Profile: Default

## 2. Серед них обираємо лише ті пакети, які створені протоколом HTTP і розкриваємо деталі, пов'язані з цим протоколом:

(для першого запиту)

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows four packets: a GET request (No. 75), a 200 OK response (No. 98), a GET request for a favicon (No. 135), and a 404 Not Found response (No. 136). The selected packet (No. 75) is expanded to show the Hypertext Transfer Protocol details. The request method is GET, and the URI is /wireshark-labs/INTRO-wireshark-file1.html. The host is gaia.cs.umass.edu. The status bar at the bottom indicates 188 packets displayed.

No.	Time	Source	Destination	Protocol	Info	Length
75	7.862914	192.168.1.117	128.119.245.12	HTTP	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	64
98	8.198424	128.119.245.12	192.168.1.117	HTTP	HTTP/1.1 200 OK (text/html)	50
135	11.817424	192.168.1.117	128.119.245.12	HTTP	GET /favicon.ico HTTP/1.1	49
136	12.197419	128.119.245.12	192.168.1.117	HTTP	HTTP/1.1 404 Not Found (text/html)	55

Frame 75: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface en0, id 0  
Ethernet II, Src: Apple\_ef:19:a4 (48:bf:6b:ef:19:a4), Dst: ASUSTekC\_92:2d:1a (c8:60:00:92:2d:1a)  
Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 58168, Dst Port: 80, Seq: 1, Ack: 1, Len: 578  
Hypertext Transfer Protocol  
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1  
[Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1  
Request Method: GET  
Request URI: /wireshark-labs/INTRO-wireshark-file1.html  
Request Version: HTTP/1.1  
Host: gaia.cs.umass.edu  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36  
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  
Accept-Encoding: gzip, deflate  
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7  
If-None-Match: "51-5a50893dfa37e"  
If-Modified-Since: Thu, 07 May 2020 05:59:02 GMT  
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]  
[HTTP request 1/2]  
[Response in frame: 98]  
[Next request in frame: 135]

0070 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1..Host:  
0080 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 gaia.cs.umass.e  
0090 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 du..Conn ection:

(для другого запиту-відповіді)

The screenshot shows a Wireshark packet capture of an HTTP 200 OK response. The packet list on the left shows the same four packets as the first image. The selected packet (No. 98) is expanded to show the Hypertext Transfer Protocol details. The response status is 200 OK, and the content type is text/html. The server is Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod\_perl/2.0.11 Perl/v5.16.3. The status bar at the bottom indicates 188 packets displayed.

No.	Time	Source	Destination	Protocol	Info	Length
75	7.862914	192.168.1.117	128.119.245.12	HTTP	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	64
98	8.198424	128.119.245.12	192.168.1.117	HTTP	HTTP/1.1 200 OK (text/html)	50
135	11.817424	192.168.1.117	128.119.245.12	HTTP	GET /favicon.ico HTTP/1.1	49
136	12.197419	128.119.245.12	192.168.1.117	HTTP	HTTP/1.1 404 Not Found (text/html)	55

Frame 98: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0  
Ethernet II, Src: ASUSTekC\_92:2d:1a (c8:60:00:92:2d:1a), Dst: Apple\_ef:19:a4 (48:bf:6b:ef:19:a4)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.117  
Transmission Control Protocol, Src Port: 80, Dst Port: 58168, Seq: 1, Ack: 579, Len: 438  
Hypertext Transfer Protocol  
HTTP/1.1 200 OK  
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK  
Response Version: HTTP/1.1  
Status Code: 200  
[Status Code Description: OK]  
Response Phrase: OK  
Date: Fri, 08 May 2020 10:09:53 GMT  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod\_perl/2.0.11 Perl/v5.16.3  
Last-Modified: Fri, 08 May 2020 05:59:01 GMT  
ETag: "51-5a51cb1aaf3e9"  
Accept-Ranges: bytes  
Content-Length: 81  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8  
[HTTP response 1/2]  
[Time since request: 0.335510000 seconds]  
[Request in frame: 75]  
[Next request in frame: 135]  
[Next response in frame: 136]  
[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)

0000 48 bf 6b ef 19 a4 c8 60 00 92 2d 1a 08 00 45 00 H.k.....E.  
0010 01 ea c9 61 40 00 30 06 28 0b 80 77 f5 0c c0 a8 ..a@. (.w..  
0020 01 75 00 50 e3 38 63 fd 8a 44 fd 08 90 7c 08 18 -u.P.8c.-D...|..

### 3. Друкуємо пакети: (Пакет запиту):

No.	Time	Source	Destination	Protocol	Info
Length	75	7.862914	192.168.1.117	128.119.245.12	HTTP GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 644
Frame 75: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface en0, id 0					
Ethernet II, Src: Apple_ef:19:a4 (48:bf:6b:ef:19:a4), Dst: ASUSTekC_92:2d:1a (c8:60:00:92:2d:1a)					
Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12					
Transmission Control Protocol, Src Port: 58168, Dst Port: 80, Seq: 1, Ack: 1, Len: 578					
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 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 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\r\n					
If-None-Match: "51-5a50893dfa37e"\r\n					
If-Modified-Since: Thu, 07 May 2020 05:59:02 GMT\r\n					
\r\n					
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]					
[HTTP request 1/2]					
[Response in frame: 98]					
[Next request in frame: 135]					

(Пакет відповіді):

No.	Time	Source	Destination	Protocol	Info
Length					
98	8.198424	128.119.245.12	192.168.1.117	HTTP	HTTP/1.1 200 OK
(text/html)					
Frame 98: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0					
Ethernet II, Src: ASUSTekC_92:2d:1a (c8:60:00:92:2d:1a), Dst: Apple_ef:19:a4 (48:bf:6b:ef:19:a4)					
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.117					
Transmission Control Protocol, Src Port: 80, Dst Port: 58168, Seq: 1, Ack: 579, 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: Fri, 08 May 2020 10:09:53 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: Fri, 08 May 2020 05:59:01 GMT\r\n					
ETag: "51-5a51cb1aaf3e9"\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 1/2]					
[Time since request: 0.335510000 seconds]					
[Request in frame: 75]					
[Next request in frame: 135]					
[Next response in frame: 136]					
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]					
File Data: 81 bytes					

## Контрольні запитання:

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

**TLS** (Transport Layer Security)

Захист на транспортному рівні(4); надає можливості безпечної передачі даних в Інтернет для навігації/пошти/спілкування/обміну файлами

**TCP** (Transmission Control Protocol)

Працює на транспортному рівні моделі OSI(4), управляє передачею даних в комп'ютерній мережі

**STP** (Spanning Tree Protocol)

Протокол канального рівня(2), усуває зайві з'єднання (петлі) в топології довільної мережі Ethernet

**UDP** (User Datagram Protocol)

Працює на транспортному рівні(4) моделі OSI як і TCP, але виконує обмін повідомленнями (датаграмами) без підтвердження та гарантії їх доставки

**ARP** (Address Resolution Protocol)

Канальний рівень(2), визначає MAC-адресу по IP-адресі іншого комп'ютера

Наприклад: комп'ютери, з'єднані через Ethernet, не можуть працювати за допомогою IP, тоді один робить запит іншому повідомити номер його MAC-адреси

**DNS** (Domain Name System)

Прикладний рівень(7) (доступ до мережевих служб), перетворює ім'я хоста (комп'ютера/мережевого пристрою) в IP-адресу

**SSDP** (Simple Service Discovery Protocol)

Сеансовий рівень OSI(5), описує механізм, за допомогою якого мережеві клієнти виявляють різні мережеві сервіси

**HTTP** (Hypertext Transfer Protocol)

Прикладний рівень(7), передає веб-сторінки (текстові файли з розміткою HTML), а також зображення і застосунки

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

Ethernet II, Internet Protocol version 4, TCP (Transmission Control Protocol), HTTP

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

$$t = 8.198424 - 7.862914 = 0.33551$$

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

**Пакет із запитом:**

Вихідна адреса: 192.168.1.117

Цільова адреса: 128.119.245.12

**Пакет із відповіддю:**

Вихідна адреса: 128.119.245.12

Цільова адреса: 192.168.1.117

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)

**Висновки:** у ході роботи я ознайомилась з методами роботи в середовищі захоплення та аналізу пакетів Wireshark