

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

**Лабораторний практикум № 1**  
**Основи захоплення та аналізу пакетів**

З дисципліни:  
Комп'ютерні мережі

**Виконав:**  
Студент 3 курсу  
Групи –ІС-зп92  
Білозьор О.В.

**Перевірив:**  
Кухарєв С.О.

**Київ 2020**

# Контрольні запитання

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

DNS, HTTP, TCP, TLSv1.2

No.	Time	Source	Destination	Protocol	Length	Info
12	2.522829	192.168.0.104	192.168.0.1	DNS	77	Standard query 0x2023 AA...
13	2.548018	192.168.0.104	192.168.0.1	DNS	77	Standard query 0x2023 AA...
17	2.649789	192.168.0.1	192.168.0.104	DNS	130	Standard query response ...
16	2.649171	192.168.0.104	128.119.245.12	HTTP	462	GET /wireshark-labs/INTR...
19	2.780703	128.119.245.12	192.168.0.104	HTTP	491	HTTP/1.1 200 OK (text/h...
21	2.984182	192.168.0.104	128.119.245.12	HTTP	342	GET /favicon.ico HTTP/1...
22	3.107704	128.119.245.12	192.168.0.104	HTTP	537	HTTP/1.1 404 Not Found ...
2	0.000049	192.168.0.104	64.233.164.189	TCP	54	50039 → 443 [ACK] Seq=1 ...
5	0.900382	172.217.20.163	192.168.0.104	TCP	60	443 → 49989 [ACK] Seq=1 ...
7	0.901264	192.168.0.104	172.217.20.163	TCP	54	49989 → 443 [ACK] Seq=40...
8	0.902012	172.217.20.174	192.168.0.104	TCP	60	443 → 50197 [ACK] Seq=1 ...
10	0.902051	192.168.0.104	172.217.20.174	TCP	54	50197 → 443 [ACK] Seq=40...
11	2.522576	192.168.0.104	128.119.245.12	TCP	66	50199 → 80 [SYN] Seq=0 W...
14	2.648833	128.119.245.12	192.168.0.104	TCP	66	80 → 50199 [SYN, ACK] Se...

No.	Time	Source	Destination	Protocol	Length	Info
14	2.648833	128.119.245.12	192.168.0.104	TCP	66	80 → 50199 [SYN, ACK] Se...
15	2.648967	192.168.0.104	128.119.245.12	TCP	54	50199 → 80 [ACK] Seq=1 A...
18	2.772264	128.119.245.12	192.168.0.104	TCP	60	80 → 50199 [ACK] Seq=1 A...
20	2.780779	192.168.0.104	128.119.245.12	TCP	54	50199 → 80 [ACK] Seq=409...
23	3.107769	192.168.0.104	128.119.245.12	TCP	54	50199 → 80 [ACK] Seq=697...
25	3.827492	192.168.0.104	216.58.215.110	TCP	54	49986 → 443 [ACK] Seq=1 ...
27	5.449146	192.168.0.104	216.58.215.110	TCP	54	49986 → 443 [ACK] Seq=1 ...
1	0.000000	64.233.164.189	192.168.0.104	TLSv1.2	107	Application Data
3	0.878331	192.168.0.104	172.217.20.163	TLSv1.2	93	Application Data
4	0.878447	192.168.0.104	172.217.20.174	TLSv1.2	93	Application Data
6	0.901233	172.217.20.163	192.168.0.104	TLSv1.2	93	Application Data
9	0.902016	172.217.20.174	192.168.0.104	TLSv1.2	93	Application Data
24	3.827429	216.58.215.110	192.168.0.104	TLSv1.2	107	Application Data
26	5.449081	216.58.215.110	192.168.0.104	TLSv1.2	106	Application Data

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

Запит:

eth:ethertype:ip:tcp:http

http						
No.	Time	Source	Destination	Protocol	Length	Info
16	2.649171	192.168.0.104	128.119.245.12	HTTP	462	GET /wireshark-labs/INTRO-wire...
19	2.780703	128.119.245.12	192.168.0.104	HTTP	491	HTTP/1.1 200 OK (text/html)
21	2.984182	192.168.0.104	128.119.245.12	HTTP	342	GET /favicon.ico HTTP/1.1
22	3.107704	128.119.245.12	192.168.0.104	HTTP	537	HTTP/1.1 404 Not Found (text/...

Frame Number: 16  
Frame Length: 462 bytes (3696 bits)  
Capture Length: 462 bytes (3696 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:http]  
[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]  
> Ethernet II, Src: ASUSTekC c7:bb:18 (74:d0:2b:c7:bb:18), Dst: Tp-linkT 93:aa:28 (c4:6e:1f:93:aa:28)

Відповідь:

eth:ethertype:ip:tcp:http:data-text-lines

No.	Time	Source	Destination	Protocol	Length	Info
16	2.649171	192.168.0.104	128.119.245.12	HTTP	462	GET /wireshark-labs/INTRO-wire...
19	2.780703	128.119.245.12	192.168.0.104	HTTP	491	HTTP/1.1 200 OK (text/html)
21	2.984182	192.168.0.104	128.119.245.12	HTTP	342	GET /favicon.ico HTTP/1.1
22	3.107704	128.119.245.12	192.168.0.104	HTTP	537	HTTP/1.1 404 Not Found (text/...

  

Frame Number: 19

Frame Length: 491 bytes (3928 bits)

Capture Length: 491 bytes (3928 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

> Ethernet II, Src: Tn-LinkT 93:aa:28 (c4:6e:1f:93:aa:28), Dst: ASUSTekC c7:hh:18 (74:d0:2h:c7:hh:18)

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

Час відправки:

Jun 14, 2020 10:39:12.879394000

No.	Time	Source	Destination	Protocol	Length	Info
16	2.649171	192.168.0.104	128.119.245.12	HTTP	462	GET /wireshark-labs/INTRO-wire...
19	2.780703	128.119.245.12	192.168.0.104	HTTP	491	HTTP/1.1 200 OK (text/html)
21	2.984182	192.168.0.104	128.119.245.12	HTTP	342	GET /favicon.ico HTTP/1.1
22	3.107704	128.119.245.12	192.168.0.104	HTTP	537	HTTP/1.1 404 Not Found (text/...

  

Frame 16: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface \Device\NPF\_{C6EFBD5B-01D6-4564-B1CF-C67A6F318DA3}

> Interface id: 0 (\Device\NPF\_{C6EFBD5B-01D6-4564-B1CF-C67A6F318DA3})

Encapsulation type: Ethernet (1)

Arrival Time: Jun 14, 2020 10:39:12.879394000 Финляндия (лето)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1592120352.879394000 seconds

[Time delta from previous captured frame: 0.000204000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 2.649171000 seconds]

Час відповіді:

Jun 14, 2020 10:39:13.010926000

No.	Time	Source	Destination	Protocol	Length	Info
16	2.649171	192.168.0.104	128.119.245.12	HTTP	462	GET /wireshark-labs/INTRO-wire...
19	2.780703	128.119.245.12	192.168.0.104	HTTP	491	HTTP/1.1 200 OK (text/html)
21	2.984182	192.168.0.104	128.119.245.12	HTTP	342	GET /favicon.ico HTTP/1.1
22	3.107704	128.119.245.12	192.168.0.104	HTTP	537	HTTP/1.1 404 Not Found (text/...

  

Frame 19: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF\_{C6EFBD5B-01D6-4564-B1CF-C67A6F318DA3}

> Interface id: 0 (\Device\NPF\_{C6EFBD5B-01D6-4564-B1CF-C67A6F318DA3})

Encapsulation type: Ethernet (1)

Arrival Time: Jun 14, 2020 10:39:13.010926000 Финляндия (лето)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1592120353.010926000 seconds

[Time delta from previous captured frame: 0.008439000 seconds]

[Time delta from previous displayed frame: 0.131532000 seconds]

[Time since reference or first frame: 2.780703000 seconds]

Різниця: ~ 0.131532 секунди (~ 131,532 мс)



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

Запит:

Source: 192.168.0.104

Destination: 128.119.245.12

Відповідь:

Source: 128.119.245.12

Destination: 192.168.0.104

No.	Time	Source	Destination	Protocol	Length	Info
16	2.649171	192.168.0.104	128.119.245.12	HTTP	462	GET /wireshark-labs/INTRO-wire...
19	2.780703	128.119.245.12	192.168.0.104	HTTP	491	HTTP/1.1 200 OK (text/html)

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

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

No.	Time	Source	Destination	Protocol	Length	Info
16	2.649171	192.168.0.104	128.119.245.12	HTTP	462	GET /wireshark-labs/INTRO-wire...
19	2.780703	128.119.245.12	192.168.0.104	HTTP	491	HTTP/1.1 200 OK (text/html)
21	2.984182	192.168.0.104	128.119.245.12	HTTP	342	GET /favicon.ico HTTP/1.1
22	3.107704	128.119.245.12	192.168.0.104	HTTP	537	HTTP/1.1 404 Not Found (text/...

> Frame 16: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface \Device\NPF\_{C6EFBD5B}

> Ethernet II, Src: ASUSTekC\_c7:bb:18 (74:d0:2b:c7:bb:18), Dst: Tp-LinkT\_93:aa:28 (c4:6e:1f:93:aa:28)

> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 50199, Dst Port: 80, Seq: 1, Ack: 1, Len: 408

> Hypertext Transfer Protocol

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

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n

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

HTTP/1.1 200 OK\r\n

No.	Time	Source	Destination	Protocol	Length	Info
16	2.649171	192.168.0.104	128.119.245.12	HTTP	462	GET /wireshark-labs/INTRO-wire...
19	2.780703	128.119.245.12	192.168.0.104	HTTP	491	HTTP/1.1 200 OK (text/html)
21	2.984182	192.168.0.104	128.119.245.12	HTTP	342	GET /favicon.ico HTTP/1.1
22	3.107704	128.119.245.12	192.168.0.104	HTTP	537	HTTP/1.1 404 Not Found (text/...

> Frame 19: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF\_{C6EFBD5B}

> Ethernet II, Src: Tp-LinkT\_93:aa:28 (c4:6e:1f:93:aa:28), Dst: ASUSTekC\_c7:bb:18 (74:d0:2b:c7:bb:18)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.104

> Transmission Control Protocol, Src Port: 80, Dst Port: 50199, Seq: 1, Ack: 409, Len: 437

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Sun, 14 Jun 2020 07:39:12 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.6 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sun, 14 Jun 2020 05:59:01 GMT\r\n