

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

Лабораторна робота № 1
З дисципліни: Комп'ютерні мережі

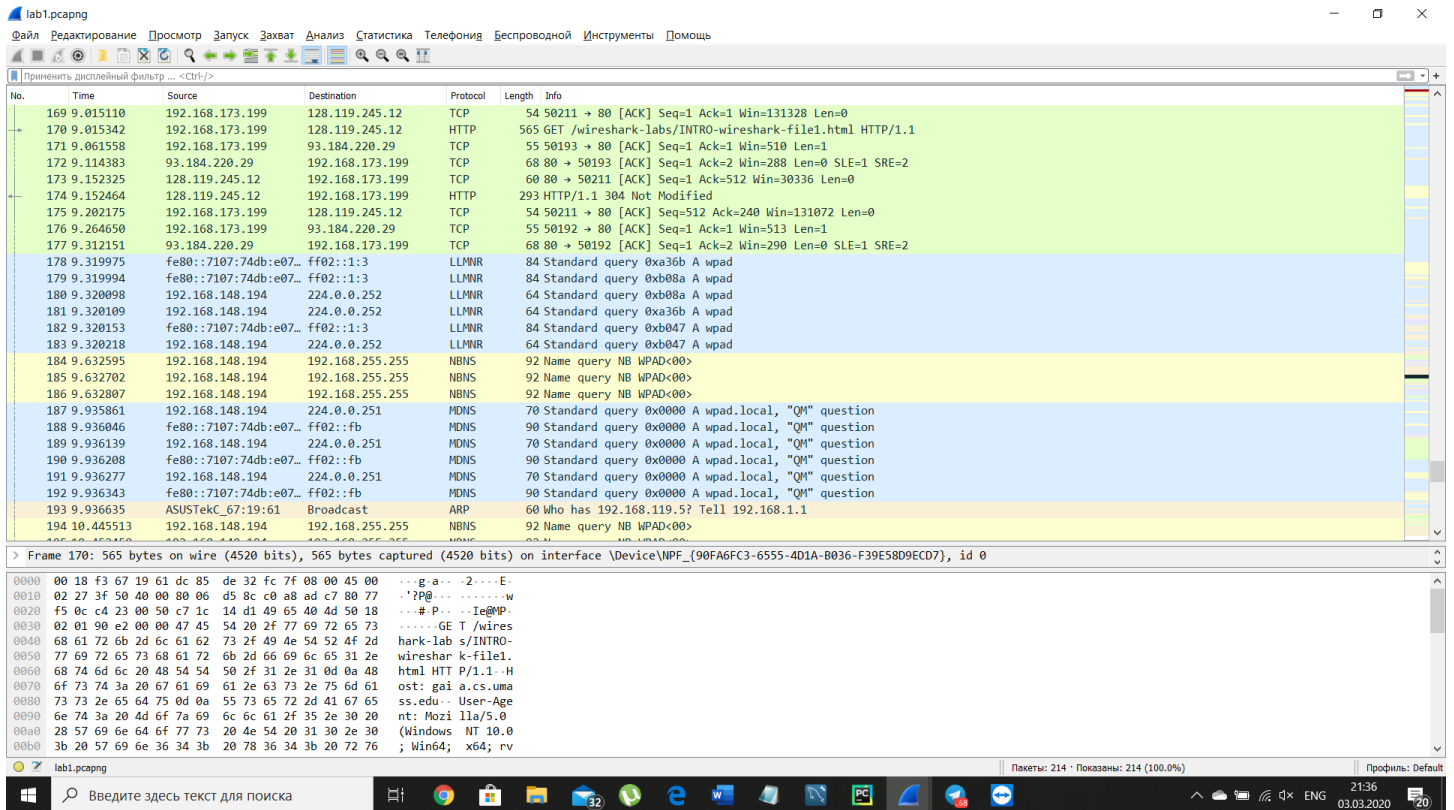
Основи захоплення та аналізу пакетів

Виконала:
Студентка III курсу
Групи КА-77
Д'яченко А.С.
Перевірив: Кухарєв С. О.

Київ 2020

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

Хід виконання роботи



lab1.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
169	9.015110	192.168.173.199	128.119.245.12	TCP	54	50211 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
170	9.015342	192.168.173.199	128.119.245.12	HTTP	565	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
171	9.061558	192.168.173.199	93.184.220.29	TCP	55	50193 → 80 [ACK] Seq=1 Ack=1 Win=510 Len=1
172	9.114383	93.184.220.29	192.168.173.199	TCP	68	80 → 50193 [ACK] Seq=1 Ack=2 Win=288 Len=0 SLE=2
173	9.152325	128.119.245.12	192.168.173.199	TCP	60	80 → 50211 [ACK] Seq=1 Ack=512 Win=30336 Len=0
174	9.152464	128.119.245.12	192.168.173.199	HTTP	293	HTTP/1.1 304 Not Modified
175	9.202175	192.168.173.199	128.119.245.12	TCP	54	50211 → 80 [ACK] Seq=512 Ack=240 Win=131072 Len=0
176	9.264650	192.168.173.199	93.184.220.29	TCP	55	50192 → 80 [ACK] Seq=1 Ack=1 Win=513 Len=1
177	9.312151	93.184.220.29	192.168.173.199	TCP	68	80 → 50192 [ACK] Seq=1 Ack=2 Win=290 Len=0 SLE=1 SRE=2
178	9.319975	fe80::7107:74db:e07...	ff02::1:3	LLMNR	84	Standard query 0xa36b A upad
179	9.319994	fe80::7107:74db:e07...	ff02::1:3	LLMNR	84	Standard query 0xb08a A upad
180	9.320098	192.168.148.194	224.0.0.252	LLMNR	64	Standard query 0xb08a A upad
181	9.320109	192.168.148.194	224.0.0.252	LLMNR	64	Standard query 0xa36b A upad
182	9.320153	fe80::7107:74db:e07...	ff02::1:3	LLMNR	84	Standard query 0xb047 A upad
183	9.320218	192.168.148.194	224.0.0.252	LLMNR	64	Standard query 0xb047 A upad
184	9.632595	192.168.148.194	192.168.255.255	NBNS	92	Name query NB WPAD<00>
185	9.632702	192.168.148.194	192.168.255.255	NBNS	92	Name query NB WPAD<00>
186	9.632807	192.168.148.194	192.168.255.255	NBNS	92	Name query NB WPAD<00>
187	9.935861	192.168.148.194	224.0.0.251	MDNS	70	Standard query 0x0000 A upad.local, "QM" question
188	9.936046	fe80::7107:74db:e07...	ff02::fb	MDNS	90	Standard query 0x0000 A upad.local, "QM" question
189	9.936139	192.168.148.194	224.0.0.251	MDNS	70	Standard query 0x0000 A upad.local, "QM" question
190	9.936208	fe80::7107:74db:e07...	ff02::fb	MDNS	90	Standard query 0x0000 A upad.local, "QM" question
191	9.936277	192.168.148.194	224.0.0.251	MDNS	70	Standard query 0x0000 A upad.local, "QM" question
192	9.936343	fe80::7107:74db:e07...	ff02::fb	MDNS	90	Standard query 0x0000 A upad.local, "QM" question
193	9.936635	ASUSTekC_67:19:61	Broadcast	ARP	60	Who has 192.168.119.5? Tell 192.168.1.1
194	10.445513	192.168.148.194	192.168.255.255	NBNS	92	Name query NB WPAD<00>

> Frame 170: 565 bytes on wire (4520 bits), 565 bytes captured (4520 bits) on interface \Device\NPF_{90FA6FC3-6555-4D1A-B036-F39E5809ECD7}, id 0

0000 00 18 f3 67 19 61 dc 85 de 32 fc 7f 08 00 45 00 ...g a...2....E:
0010 02 27 3f 50 40 00 80 06 d5 8c c0 a8 ad c7 80 77 ...?P@.....w
0020 f5 0c c4 23 00 50 c7 1c 14 d1 49 65 40 4d 50 18 ...# P...Ie@MP
0030 02 01 90 e2 00 00 47 45 54 20 2f 77 69 72 65 73GE 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.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 ...html HTT P/1.1..H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ...ost: gai a.cs.uma
0080 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 ...ss.edu.. User-Age
0090 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 ...nt: Mozi lla/5.0
00a0 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 ... (Windows NT 10.0
00b0 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 ...; Win64; x64; rv

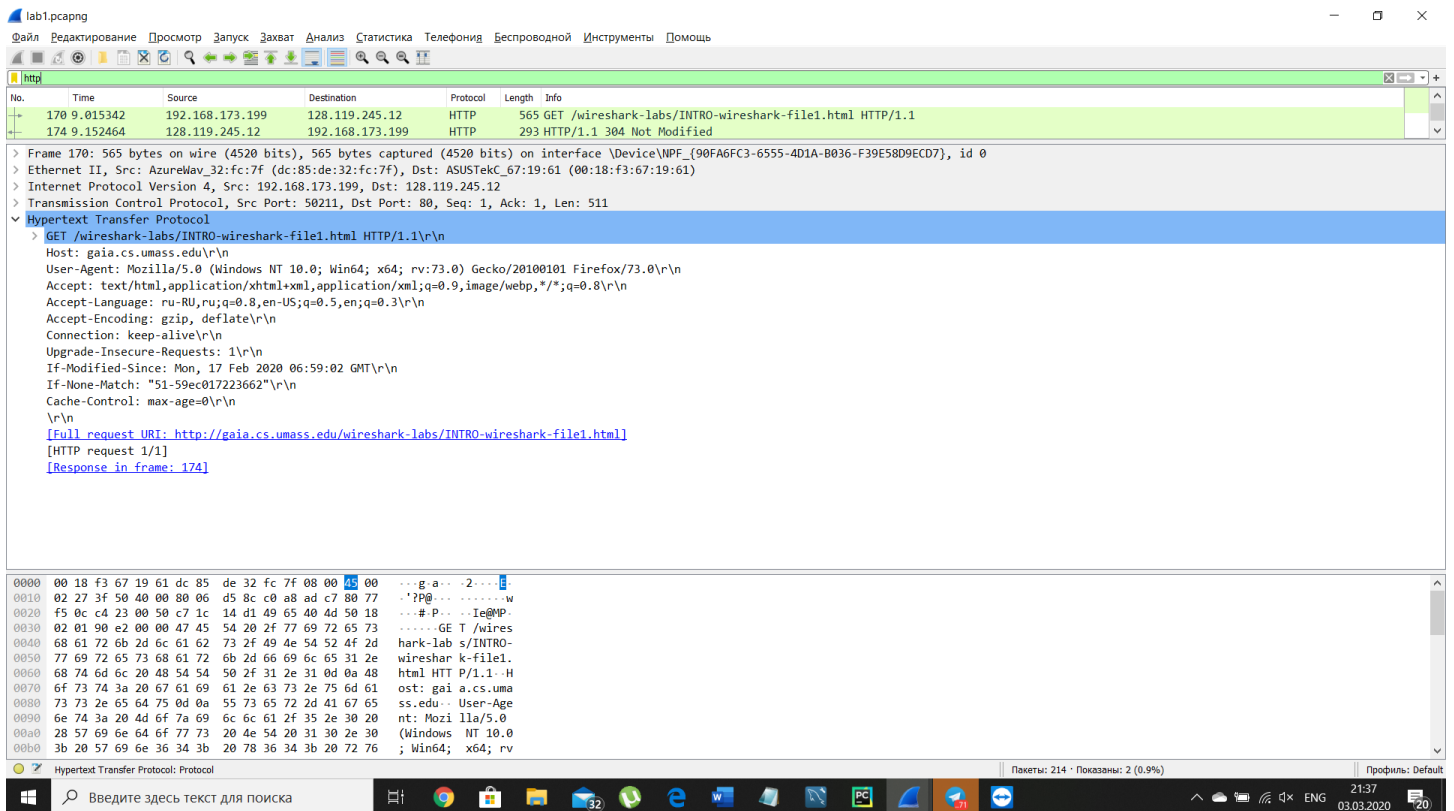
lab1.pcapng

Введите здесь текст для поиска

Пакеты: 214 · Показаны: 214 (100.0%)

Профиль: Default

2136
03.03.2020



lab1.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

No.	Time	Source	Destination	Protocol	Length	Info
170	9.015342	192.168.173.199	128.119.245.12	HTTP	565	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
174	9.152464	128.119.245.12	192.168.173.199	HTTP	293	HTTP/1.1 304 Not Modified

> Frame 170: 565 bytes on wire (4520 bits), 565 bytes captured (4520 bits) on interface \Device\NPF_{90FA6FC3-6555-4D1A-B036-F39E5809ECD7}, id 0

> Ethernet II, Src: AzureWav_32:fc:7f (dc:85:de:32:fc:7f), Dst: ASUSTekC_67:19:61 (08:18:f3:67:19:61)

> Internet Protocol Version 4, Src: 192.168.173.199, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 50211, Dst Port: 80, Seq: 1, Ack: 1, Len: 511

> 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:73.0) Gecko/20100101 Firefox/73.0\r\n

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

Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

If-Modified-Since: Mon, 17 Feb 2020 06:59:02 GMT\r\n

If-None-Match: "51-59ec017223662"\r\n

Cache-Control: max-age=0\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: 174]

0000 00 18 f3 67 19 61 dc 85 de 32 fc 7f 08 00 45 00 ...g a...2....E:
0010 02 27 3f 50 40 00 80 06 d5 8c c0 a8 ad c7 80 77 ...?P@.....w
0020 f5 0c c4 23 00 50 c7 1c 14 d1 49 65 40 4d 50 18 ...# P...Ie@MP
0030 02 01 90 e2 00 00 47 45 54 20 2f 77 69 72 65 73GE 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.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 ...html HTT P/1.1..H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ...ost: gai a.cs.uma
0080 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 ...ss.edu.. User-Age
0090 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 ...nt: Mozi lla/5.0
00a0 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 ... (Windows NT 10.0
00b0 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 ...; Win64; x64; rv

Hypertext Transfer Protocol: Protocol

Пакеты: 214 · Показаны: 2 (0.9%)

Профиль: Default

2137
03.03.2020

lab1.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

No. Time

170 9.015342

174 9.152464

Wireshark - Файл: lab1.pcapng

Transmission Control Protocol, Src Port: 50211, Dst Port: 80, Seq: 1, Ack: 1, Len: 511

Source Port: 50211

Destination Port: 80

[Stream index: 7]

[TCP Segment Len: 511]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 3340506321

[Next sequence number: 512 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 1231372365

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window size value: 513

[Calculated window size: 131328]

[Window size scaling factor: 256]

0000 00 18 f3 67 19 61 dc 85 de 32 fc 7f 08 00 45 00 ...g.a...2....E-

0010 02 27 3f 50 40 00 80 06 d5 8c c0 a8 ad c7 80 77 ...?P...W

0020 f5 0c c4 23 00 50 c7 1c 14 d1 49 65 40 4d 50 18 ...#P...Ie@MP.

0030 02 01 90 e2 00 00 47 45 54 20 2f 7f 69 72 65 73GE 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.

0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HT P/1.1..H

0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.c.s.uma

0080 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 ss.edu.. User-Age

0090 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 nt: Mozi lla/5.0

00a0 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 (Windows NT 10.0

00b0 3b 20 57 69 6e 6c 3a 3b 20 78 36 34 3b 20 72 76 ; Win64; x64; rv

00c0 3a 37 33 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 :73.0) G ecko/201

00d0 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 37 33 00101 Fi refox/73

00e0 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 .0..Ac ce pt: text

00f0 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio

0100 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xml,appl

0110 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml;q=0.

0000 00 18 f3 67 19 61 dc 85 de 32 fc 7f 08 00 45 00 ...g.a...2....E-

0010 02 27 3f 50 40 00 80 06 d5 8c c0 a8 ad c7 80 77 ...?P...W

0020 f5 0c c4 23 00 50 c7 1c 14 d1 49 65 40 4d 50 18 ...#P...Ie@MP.

0030 02 01 90 e2 00 00 47 45 54 20 2f 7f 69 72 65 73GE 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.

0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HT P/1.1..H

0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.c.s.uma

0080 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 ss.edu.. User-Age

0090 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 nt: Mozi lla/5.0

00a0 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 (Windows NT 10.0

00b0 3b 20 57 69 6e 6c 3a 3b 20 78 36 34 3b 20 72 76 ; Win64; x64; rv

00c0 3a 37 33 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 :73.0) G ecko/201

00d0 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 37 33 00101 Fi refox/73

00e0 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 .0..Ac ce pt: text

00f0 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio

0100 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xml,appl

0110 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml;q=0.

Internet Protocol Version 4 (IP), 20 байты

Пакеты: 214 · Показаны: 2 (0.9%)

Профиль: Default

Введите здесь текст для поиска

2139 03.03.2020

lab1.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

No. Time Source Destination Protocol Length Info

170 9.015342 192.168.173.199 128.119.245.12 HTTP 565 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

174 9.152464 128.119.245.12 192.168.173.199 HTTP 293 HTTP/1.1 304 Not Modified

Window size value: 513

[Calculated window size: 131328]

[Window size scaling factor: 256]

Checksum: 0x90e2 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

[Timestamps]

TCP payload (511 bytes)

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:73.0) Gecko/20100101 Firefox/73.0\r\n

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

Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

If-Modified-Since: Mon, 17 Feb 2020 06:59:02 GMT\r\n

If-None-Match: "51-59ec017223662"\r\n

Cache-Control: max-age=0\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: 174]

0020 f5 0c c4 23 00 50 c7 1c 14 d1 49 65 40 4d 50 18 ...#P...Ie@MP.

0030 02 01 90 e2 00 00 47 45 54 20 2f 7f 69 72 65 73GE 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.

0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HT P/1.1..H

0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.c.s.uma

0080 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 ss.edu.. User-Age

0090 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 nt: Mozi lla/5.0

00a0 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 (Windows NT 10.0

00b0 3b 20 57 69 6e 6c 3a 3b 20 78 36 34 3b 20 72 76 ; Win64; x64; rv

00c0 3a 37 33 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 :73.0) G ecko/201

00d0 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 37 33 00101 Fi refox/73

TCP Segment Len (tcp.len), 1 байт

Пакеты: 214 · Показаны: 2 (0.9%)

Профиль: Default

Введите здесь текст для поиска

2203 03.03.2020

Запит:

No.	Time	Source	Destination	Protocol	Length	Info
170	9.015342	192.168.173.199	128.119.245.12	HTTP	565	GET /wireshark-labs/INTRO-wireshafile1.html HTTP/1.1

Frame 170: 565 bytes on wire (4520 bits), 565 bytes captured (4520 bits) on interface \Device\NPF_{90FA6FC3-6555-4D1F39E58D9ECD7}, id 0
Ethernet II, Src: AzureWav_32:fc:7f (dc:85:de:32:fc:7f), Dst: ASUSTekC_67:19:61 (00:18:f3:67:19:61)
Internet Protocol Version 4, Src: 192.168.173.199, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50211, Dst Port: 80, Seq: 1, Ack: 1, Len: 511

Відповідь:

No.	Time	Source	Destination	Protocol	Length	Info
174	9.152464	128.119.245.12	192.168.173.199	HTTP	293	HTTP/1.1 304 Not Modified

Frame 174: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{90FA6FC3-6555-4D1F39E58D9ECD7}, id 0
Ethernet II, Src: ASUSTekC_67:19:61 (00:18:f3:67:19:61), Dst: AzureWav_32:fc:7f (dc:85:de:32:fc:7f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.173.199
Transmission Control Protocol, Src Port: 80, Dst Port: 50211, Seq: 1, Ack: 512, Len: 239
Hypertext Transfer Protocol

Контрольні питання

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

TCP, HTTP, DNS, SSL, TLSv1.3, ICMPv6, UDP

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 0,137122 с.

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

Запит:

Вихідна: 192.168.173.199

Цільова: 128.119.245.12

Відповідь:

Вихідний: 128.119.245.12

Цільовий: 192.168.173.199

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

GET /wireshark-labs/INTRO-wiresharkfile1.html HTTP/1.1

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

HTTP/1.1 304 Not Modified

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.