

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 ІІІ курсу
Групи КА-74
Соболь Н. О.
Перевірив: Кухарєв С. О.

Київ 2020

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

Хід виконання роботи

The image shows a Wireshark network traffic analysis interface. At the top, the title bar reads 'Lab1.pcapng'. Below it is a menu bar with options: Файл, Правка, Видял, Перехід, Захоплення, Аналіз, Статистика, Телефонія, Wireless, Tools, Довідка. A toolbar with various icons is positioned below the menu. The main window is divided into three panes. The top pane, 'Packet List', displays a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 219 is highlighted. The middle pane, 'Packet Details', shows the hierarchical structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The bottom pane, 'Packet Bytes', displays the raw data of the selected packet in hexadecimal and ASCII. The status bar at the bottom indicates 'Lab1.pcapng', 'Packets: 38484', 'Displayed: 38484 (100.0%)', 'Dropped: 0 (0.0%)', and 'Profile: Default'.

Lab1.psranag

Файл Правка Видяг Перехід Захоплення Аналіз Статистика Телефонія Wireless Tools Довідка

http

No.	Time	Source	Destination	Protocol	Length	Info
153	16.827744	77.47.196.251	128.119.245.12	HTTP	520	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
219	17.359438	128.119.245.12	77.47.196.251	HTTP	492	HTTP/1.1 200 OK (text/html)
237	17.799138	77.47.196.251	128.119.245.12	HTTP	452	GET /favicon.ico HTTP/1.1
259	18.893283	128.119.245.12	77.47.196.251	HTTP	538	HTTP/1.1 200 Not Found (text/html)
305	21.445095	5.45.62.116	77.47.196.251	HTTP	753	HTTP/1.1 404 OK
306	21.475249	77.47.196.251	5.45.62.116	HTTP	356	GET /R/A3gKIGUzN2fLZGwOtU4YzRiOWQ4NTMxNDlkHjRiTc2YmVhEgQC3AIgGkCigH_KgcIBBCG39Z6KgCIXaxCiIdvMgoIBBdG39Z6GIAKONmSoJgBQiCKR-U...
1984	147.221684	77.47.196.251	5.45.58.178	HTTP	1084	POST /v1/touch HTTP/1.1 (application/x-enc)
1991	147.349407	5.45.58.178	77.47.196.251	HTTP	326	HTTP/1.1 200 OK
2804	231.525220	5.45.62.116	77.47.196.251	HTTP	1450	HTTP/1.1 200 OK
2805	231.538510	77.47.196.251	5.45.62.116	HTTP	356	GET /R/A3gKIGUzN2fLZGwOtU4YzRiOWQ4NTMxNDlkHjRiTc2YmVhEgQC3AIgGkCigH_KgcIBBDq4NZ6KgCIXaxCiIdvMgoIBBDq4NZ6GIAKONmSoJgBQiCKR-U...
3037	257.503775	77.47.196.251	104.75.72.24	HTTP	267	GET /ru-RU/livefile/preinstall?region=UA&appid=C98A580842DBB9405BBF071EAD76512D21FE368FORM=Threshold HTTP/1.1
3043	257.566940	104.75.72.24	77.47.196.251	HTTP/X..	366	HTTP/1.1 200 OK

> Frame 219: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface VDeviceWPF_ {6FA3E7CE-A519-455D-821F-4AF69DA9A9BD}, id 0
 Ethernet II, Src: Hangzhou_9d:38:c8 (00:0f:e2:9d:38:c8), Dst: AzureWav_0a:a3:f7 (80:c5:f2:0a:a3:f7)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 77.47.196.251
 Transmission Control Protocol, Src Port: 80, Dst Port: 50311, Seq: 1, Ack: 467, Len: 438

Hypertext Transfer Protocol

```
> HTTP/1.1 200 OK\r\n
Date: Tue, 25 Feb 2020 16:55:55 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, 25 Feb 2020 06:59:03 GMT\r\n
ETag: "51-59f6105e8c5ac"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
```

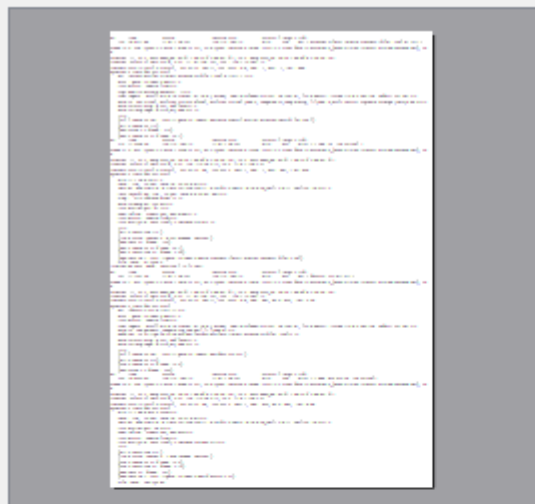
0000 80 c5 f2 0a a3 f7 00 0f e2 9d 38 c8 00 00 45 00 :B...E.
 0010 01 de 98 23 40 00 30 06 29 48 80 77 f5 0c 4d 2f ...#0.)H w-M/
 0020 c4 fb 00 50 c4 87 0f 3f 7b 1e 0d c5 5d 06 50 18 ...P...? {...] P.
 0030 00 ed 00 70 00 00 48 54 54 50 2f 31 2e 31 20 32 ...p-H T/1.1 2
 0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 00 OK.-D ate: Tue
 0050 2c 20 32 35 20 46 65 62 20 32 30 32 30 21 31 36 , 25 Feb 2020 16
 0060 3a 35 35 3a 35 35 20 47 4d 54 0d 0a 53 65 72 fe :55:55 G MT--Serv
 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
 0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
 00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per
 00b0 6e 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 1/2.0.11 Perl/v5
 00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3-.L ast-Modi
 00d0 66 69 65 64 3a 20 54 75 65 2c 20 32 35 20 46 65 fied: Tu e, 25 Fe

Packets: 38494 · Displayed: 166 (0.4%) · Drooped: 0 (0.0%) Profile: Default

< >

No.: 153 · Time: 16.827744 · Source: 77.47.196.251 · Destination: 128.119....nqth: 520 · Info: GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Help



Формат Пакету

- ☒ Summary line
- ☒ Include column headings
- ☒ Details:
- ☐ All collapsed
- ☒ As displayed
- ☐ All expanded
- ☐ Байтів
- ☐ Print each packet on a new page

+ and - zoom, 0 resets

Діапазон Пакетів

☐ Захоплені ☒ Відображені

- | | | |
|---|-------|-----|
| <input checked="" type="radio"/> Всі пакети | 38484 | 166 |
| <input type="radio"/> Тільки <u>в</u> ибрані пакети | 1 | 1 |
| <input type="radio"/> Тільки <u>п</u> означені пакети | 0 | 0 |
| <input type="radio"/> Від першого до <u>о</u> станнього позначеного | 0 | 0 |
| <input type="radio"/> Діапазон: <input type="text"/> | 0 | 0 |
| <input type="checkbox"/> Видалити <u>п</u> роігноровані пакети | 0 | 0 |

Page Setup...

Print...

Cancel

Help

```

No.      Time      Source      Destination      Protocol Length Info
153 16.827744  77.47.196.251 128.119.245.12  HTTP 520 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 153: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{6FA3E7CE-A519-455D-821F-4AF69DA9A9BD}, id 0
Ethernet II, Src: AzureWav_0a:a3:f7 (80:c5:f2:0a:a3:f7), Dst: Hangzhou_9d:38:c8 (00:0f:e2:9d:38:c8)
Internet Protocol Version 4, Src: 77.47.196.251, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50311, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
  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: en-US,en;q=0.9\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: 219]
  [Next request in frame: 237]

```

Контрольні питання

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
ARP, HTTP, IGMPv2, NBNS, MDNS, LLMNR, LOOP, TCP, TLSv1.2, BROWSER, DNS, TLSv1.3
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
ARP, HTTP, IGMPv2, NBNS, MDNS, LLMNR, LOOP, TCP, TLSv1.2, BROWSER, DNS, TLSv1.3
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?
Пройшло 0,531698 с.
4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?
Запит:
Вихідна: 77.47.196.251
Цільова: 128.119.245.12
Відповідь:
Вихідний: 128.119.245.12
Цільовий: 77.47.196.251
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)

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.