Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Кафедра математичних методів системного аналізу

ЗВІТ

про виконання лабораторних робіт

з дисципліни “Комп’ютерні мережі”

Лабораторна робота №1 Основи захоплення та аналізу пакетів

Виконав: студент групи ІС-зп91

Бабаркін Владислав Олексійович

Прийняв: Кухарєв С.О.

Київ 2020

**Лабораторна робота №1 Основи захоплення та аналізу пакетів**

|  |
| --- |
|  |
|  |
|  |

|  |
| --- |
| **Запитання 1-6** |
| **No. Time Source Destination Protocol Length Info**  **95 16.120586 192.168.1.108 128.119.245.12 HTTP 541 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1**  Frame 95: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 4, Src: 192.168.1.108, Dst: 128.119.245.12  Transmission Control Protocol, Src Port: 2346, Dst Port: 80, Seq: 1, Ack: 1, Len: 487  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]  [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]  [Severity level: Chat]  [Group: Sequence]  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/81.0.4044.122 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  \r\n  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]  [HTTP request 1/2]  [Response in frame: 101]  [Next request in frame: 103]  **No. Time Source Destination Protocol Length Info**  **101 16.252186 128.119.245.12 192.168.1.108 HTTP 492 HTTP/1.1 200 OK (text/html)**  Frame 101: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.108  Transmission Control Protocol, Src Port: 80, Dst Port: 2346, Seq: 1, Ack: 488, Len: 438  Hypertext Transfer Protocol  HTTP/1.1 200 OK\r\n  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]  [HTTP/1.1 200 OK\r\n]  [Severity level: Chat]  [Group: Sequence]  Response Version: HTTP/1.1  Status Code: 200  [Status Code Description: OK]  Response Phrase: OK  Date: Tue, 28 Apr 2020 05:49:07 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, 28 Apr 2020 05:49:03 GMT\r\n  ETag: "51-5a453639ae143"\r\n  Accept-Ranges: bytes\r\n  Content-Length: 81\r\n  [Content length: 81]  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: 0.131600000 seconds]  [Request in frame: 95]  [Next request in frame: 103]  [Next response in frame: 104]  [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)  <html>\n  Congratulations! You've downloaded the first Wireshark lab file!\n  </html>\n  **No. Time Source Destination Protocol Length Info**  **103 17.021975 192.168.1.108 128.119.245.12 HTTP 473 GET /favicon.ico HTTP/1.1**  Frame 103: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 4, Src: 192.168.1.108, Dst: 128.119.245.12  Transmission Control Protocol, Src Port: 2346, Dst Port: 80, Seq: 488, Ack: 439, Len: 419  Hypertext Transfer Protocol  GET /favicon.ico HTTP/1.1\r\n  [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]  [GET /favicon.ico HTTP/1.1\r\n]  [Severity level: Chat]  [Group: Sequence]  Request Method: GET  Request URI: /favicon.ico  Request Version: HTTP/1.1  Host: gaia.cs.umass.edu\r\n  Connection: keep-alive\r\n  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36\r\n  Accept: image/webp,image/apng,image/\*,\*/\*;q=0.8\r\n  Referer: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html\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  \r\n  [Full request URI: http://gaia.cs.umass.edu/favicon.ico]  [HTTP request 2/2]  [Prev request in frame: 95]  [Response in frame: 104]  **No. Time Source Destination Protocol Length Info**  **104 17.143386 128.119.245.12 192.168.1.108 HTTP 538 HTTP/1.1 404 Not Found (text/html)**  Frame 104: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.108  Transmission Control Protocol, Src Port: 80, Dst Port: 2346, Seq: 439, Ack: 907, Len: 484  Hypertext Transfer Protocol  HTTP/1.1 404 Not Found\r\n  [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]  [HTTP/1.1 404 Not Found\r\n]  [Severity level: Chat]  [Group: Sequence]  Response Version: HTTP/1.1  Status Code: 404  [Status Code Description: Not Found]  Response Phrase: Not Found  Date: Tue, 28 Apr 2020 05:49:08 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  Content-Length: 209\r\n  [Content length: 209]  Keep-Alive: timeout=5, max=99\r\n  Connection: Keep-Alive\r\n  Content-Type: text/html; charset=iso-8859-1\r\n  \r\n  [HTTP response 2/2]  [Time since request: 0.121411000 seconds]  [Prev request in frame: 95]  [Prev response in frame: 101]  [Request in frame: 103]  [Request URI: http://gaia.cs.umass.edu/favicon.ico]  File Data: 209 bytes  Line-based text data: text/html (7 lines)  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n  <html><head>\n  <title>404 Not Found</title>\n  </head><body>\n  <h1>Not Found</h1>\n  <p>The requested URL /favicon.ico was not found on this server.</p>\n  </body></html>\n |

**Контрольні запитання:**

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

HTTP, TCP, ARP, TLSv.1.2, TCP, DNS, TLSv.1.3, ICMP, ICMPv6

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л1\1.png |

Рис. 1.1. Протоколи, які відображалися в вікні лістингу протоколів до включення фільтрації

1. **Які протоколи використовувалися в збережених пакетах запиту та відповіді?**

Протоколи Запиту (рис. 1.2. Протоколи запиту): Ethernet II, Internet Protocol Version 4, Transmission Control Protocol (TCP), Hypertext Transfer Protocol (Http) 1.1

Протоколи відповіді (рис. 1.3. Протоколи відповіді) : Ethernet II, Internet Protocol Version 4, Transmission Control Protocol (TCP), Hypertext Transfer Protocol (Http) 1.1

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л1\2.png |

Рис. 1.2. Протоколи запиту

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л1\3.png |

Рис. 1.3. Протоколи відповіді

1. **Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до**

**отримання першого пакету з відповіддю сервера?**

95 Пакет (Запит) відправлено 16,120586

101 Пакет (Відповідь) отримано 16,252186

Час = 16,252186 - 16,120586 = 0,1316

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

Вихідна адреса запит (Source): 192.168.1.108

Цільова адреса запит (Destination): 128.119.245.12

Вихідна адреса відповідь (Source): 128.119.245.12

Цільова адреса відповідь (Destination): 192.168.1.108

1. **Яким був перший рядок запиту на рівні протоколу HTTP?**

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

1. **Яким був перший рядок відповіді на рівні протоколу HTTP?**

HTTP/1.1 200 OK\r\n