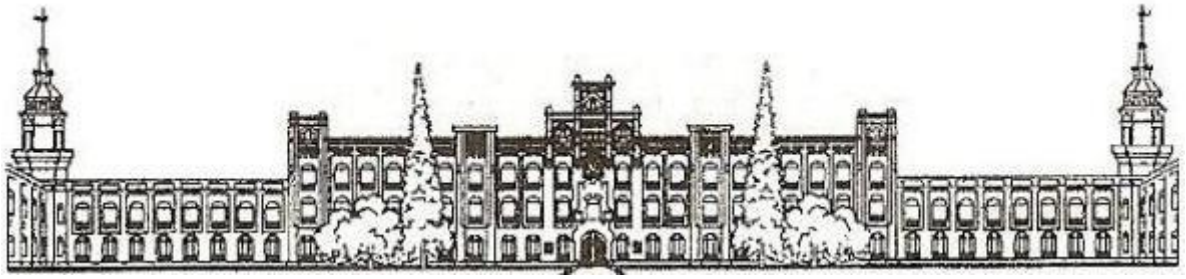

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА ММСА

Практична робота № 1

З курсу: «Комп'ютерні мережі»

Виконала:

Студентка III курсу

Групи КА-73

Ярошенко В. О.

Прийняв: Кухарєв С.О.

Київ 2020

Запит

No. Time Source Destination Protocol Length Info 61 13.295709 192.168.43.41 128.119.245.12 HTTP 574 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 Frame 61: 574 bytes on wire (4592 bits), 574 bytes captured (4592 bits) on interface \Device\NPF_{E1E68F3E-92A6-43A9-9B40-8B93E4B61CD4}, id 0 Interface id: 0 (\Device\NPF_{E1E68F3E-92A6-43A9-9B40-8B93E4B61CD4}) Encapsulation type: Ethernet (1) Arrival Time: Mar 11, 2020 12:43:28.069510000 Финляндия (зима) [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1583923408.069510000 seconds [Time delta from previous captured frame: 0.001324000 seconds] [Time delta from previous displayed frame: 0.000000000 seconds] [Time since reference or first frame: 13.295709000 seconds] Frame Number: 61 Frame Length: 574 bytes (4592 bits) Capture Length: 574 bytes (4592 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: LiteonTe_df:2b:9a (2c:d0:5a:df:2b:9a), Dst: be:a5:8b:83:c2:2f (be:a5:8b:83:c2:2f) Destination: be:a5:8b:83:c2:2f (be:a5:8b:83:c2:2f) Address: be:a5:8b:83:c2:2f (be:a5:8b:83:c2:2f) .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default) ....0 .... = IG bit: Individual address (unicast) Source: LiteonTe_df:2b:9a (2c:d0:5a:df:2b:9a) Address: LiteonTe_df:2b:9a (2c:d0:5a:df:2b:9a) .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 192.168.43.41, Dst: 128.119.245.12 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) 0000 00.. = Differentiated Services Codepoint: Default (0) .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 560 Identification: 0x1987 (6535) Flags: 0x4000, Don't fragment 0... .... = Reserved bit: Not set .1.. .... = Don't fragment: Set ..0. .... = More fragments: Not set ...0 0000 0000 0000 = Fragment offset: 0 Time to live: 128 Protocol: TCP (6) Header checksum: 0x7deb [validation disabled] [Header checksum status: Unverified] Source: 192.168.43.41 Destination: 128.119.245.12 Transmission Control Protocol, Src Port: 50468, Dst Port: 80, Seq: 1, Ack: 1, Len: 520 Source Port: 50468 Destination Port: 80 [Stream index: 11] [TCP Segment Len: 520] Sequence number: 1 (relative sequence number) Sequence number (raw): 4014273241 [Next sequence number: 521 (relative sequence number)] Acknowledgment number: 1 (relative ack number) Acknowledgment number (raw): 372194294 0101 .... = Header Length: 20 bytes (5) Flags: 0x018 (PSH, ACK) 000. .... = Reserved: Not set ...0 .... = Nonce: Not set .... 0... .... = Congestion Window Reduced (CWR): Not set .... .0.. .... = ECN-Echo: Not set .... ..0. .... = Urgent:

Not set ....1 .... = Acknowledgment: Set .... 1... = Push: Set .... .0.. = Reset: Not set ....0. = Syn: Not set ....0 = Fin: Not set [TCP Flags: ·····AP···] Window size value: 514 [Calculated window size: 131584] [Window size scaling factor: 256] Checksum: 0xb097 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 [SEQ/ACK analysis] [iRTT: 0.174088000 seconds] [Bytes in flight: 520] [Bytes sent since last PSH flag: 520] [Timestamps] [Time since first frame in this TCP stream: 0.175412000 seconds] [Time since previous frame in this TCP stream: 0.001324000 seconds] TCP payload (520 bytes) Hypertext Transfer Protocol GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\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/80.0.3987.132 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 C:\Users\872B~1\AppData\Local\Temp\wireshark_Беспроводная сеть 2_20200311124311_a13392.pcapng 102 total packets, 2 shown accept-language: ru-UA,ru;q=0.9,uk-UA;q=0.8,uk;q=0.7,ru-RU;q=0.6,en-US;q=0.5,en;q=0.4\r\n Host: gaia.cs.umass.edu\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: 63]

Відповідь

No. Time Source Destination Protocol Length Info 63 13.500011 128.119.245.12 192.168.43.41 HTTP 492 HTTP/1.1 200 OK (text/html) Frame 63: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{E1E68F3E-92A6-43A9-9B40-8B93E4B61CD4}, id 0 Interface id: 0 (\Device\NPF_{E1E68F3E-92A6-43A9-9B40-8B93E4B61CD4}) Interface name: \Device\NPF_{E1E68F3E-92A6-43A9-9B40-8B93E4B61CD4} Interface description: Беспроводная сеть 2 Encapsulation type: Ethernet (1) Arrival Time: Mar 11, 2020 12:43:28.273812000 Финляндия (зима) [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1583923408.273812000 seconds [Time delta from previous captured frame: 0.006236000 seconds] [Time delta from previous displayed frame: 0.204302000 seconds] [Time since reference or first frame: 13.500011000 seconds] Frame Number: 63 Frame Length: 492 bytes (3936 bits) Capture Length: 492 bytes (3936 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: be:a5:8b:83:c2:2f (be:a5:8b:83:c2:2f), Dst: LiteonTe_df:2b:9a (2c:d0:5a:df:2b:9a) Destination: LiteonTe_df:2b:9a (2c:d0:5a:df:2b:9a) Address: LiteonTe_df:2b:9a (2c:d0:5a:df:2b:9a) .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast) Source: be:a5:8b:83:c2:2f (be:a5:8b:83:c2:2f) Address: be:a5:8b:83:c2:2f (be:a5:8b:83:c2:2f) .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default) ....0 .... = IG bit: Individual address (unicast) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.41 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) 0000 00.. = Differentiated Services Codepoint: Default (0) .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 478 Identification: 0x0092 (146) Flags: 0x4000, Don't fragment 0... .... = Reserved bit: Not set .1.. .... = Don't fragment: Set ..0. .... = More fragments: Not set ...0 0000 0000 0000 = Fragment offset: 0 Time to live: 43 Protocol: TCP (6) Header checksum: 0xec32 [validation disabled] [Header checksum status: Unverified] Source: 128.119.245.12 Destination: 192.168.43.41 Transmission Control Protocol, Src Port: 80, Dst Port: 50468, Seq: 1, Ack: 521, Len: 438 Source Port: 80 Destination Port: 50468 [Stream index: 11] [TCP Segment Len: 438] Sequence number: 1 (relative sequence number) Sequence number (raw): 372194294 [Next sequence number: 439 (relative sequence number)] Acknowledgment number: 521 (relative ack number) Acknowledgment number (raw): 4014273761 0101 .... = Header Length: 20 bytes (5) Flags: 0x018 (PSH, ACK) 000. .... = Reserved: Not set ...0 .... = Nonce: Not set .... 0... .... = Congestion Window Reduced (CWR): Not set .... .0.. .... = ECN-Echo: Not set .... ..0. .... = Urgent: Not set ....1 .... = Acknowledgment: Set .... 1... = Push: Set .... .0.. = Reset: Not set ....0. = Syn: Not set ....0 = Fin: Not set [TCP Flags: ·····AP···] Window size value: 237 [Calculated window size: 30336] [Window size scaling factor: 128] Checksum: 0x5b12 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 [SEQ/ACK analysis] [iRTT: 0.174088000 seconds] [Bytes in flight: 438] [Bytes sent since last PSH flag: 438] [Timestamps] [Time since first frame in this TCP stream: 0.379714000 seconds] [Time since previous frame in this TCP stream: 0.006236000 seconds] TCP payload (438 bytes) Hypertext Transfer Protocol HTTP/1.1 200 OK\r\n Date: Wed, 11 Mar 2020 10:43:24 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: Wed, 11 Mar 2020 05:59:01 GMT\r\n C:\Users\872B~1\AppData\Local\Temp\wireshark_Беспроводная сеть 2_20200311124311_a13392.pcapng 102 total packets, 2 shown ETag: "51-5a08deed5f8b5"\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 1/1] [Time since request: 0.204302000 seconds] [Request in frame: 61] [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)

Контрольні запитання:

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

   NBNS, SSL, TCP, UDP, ARP, HTTP, SSDP.

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

   HTTP

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

   0,204302

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

   Запит:
   Цільова: 128.119.245.12
   Вихідна: 192.168.43.41

   Відповідь:
   Цільова: 192.168.43.41
   Вихідна: 128.119.245.12

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

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

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

   HTTP/1.1 200 OK\r\n

Висновок:

Мені дуже сподобалось працювати у середовищі Wireshark, на жаль зробити лабу нормально вийшло тільки з разу 10, але нічого, це надало мені змогу дізнатись більше про Wireshark та зрозуміти як в ньому працювати. Загалом, ставлю 10/10.