Task1

После загрузки страницы мы запускаем wireshark и отловили нужный нам пакет.
Получили запрос на сервер и ответ.

Запрос:

Frame 118: 645 bytes on wire (5160 bits), 645 bytes captured (5160 bits) on interface 0

Interface id: 0 (\Device\NPF_{8DB27C3E-EBB7-4924-AE75-E0A26D3078AF})

Interface name: \Device\NPF_{8DB27C3E-EBB7-4924-AE75-E0A26D3078AF}

Interface description [truncated]: \320\221\320\265\321\201\320\277\321\200\320\276\320\262\320\276\320\264\320\275\320\276\320\265 \321\201\320\265\321\202\320\265\320\262\320\276\320\265 \321\201\320\276\320\265\320\264\320\270\320\275\

Encapsulation type: Ethernet (1)

Arrival Time: Oct 19, 2019 11:39:31.556479000 Финляндия (лето)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1571474371.556479000 seconds

[Time delta from previous captured frame: 0.003647000 seconds]

[Time delta from previous displayed frame: 1.350086000 seconds]

[Time since reference or first frame: 12.287065000 seconds]

Frame Number: 118

Frame Length: 645 bytes (5160 bits)

Capture Length: 645 bytes (5160 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_e4:f5:17 (d0:df:9a:e4:f5:17), Dst: HuaweiTe_77:9b:4a (34:12:f9:77:9b:4a)

Destination: HuaweiTe_77:9b:4a (34:12:f9:77:9b:4a)

Address: HuaweiTe_77:9b:4a (34:12:f9:77:9b:4a)

.... ..0. .... = LG bit: Globally unique address (factory default)

....0 .... = IG bit: Individual address (unicast)

Source: LiteonTe_e4:f5:17 (d0:df:9a:e4:f5:17)

Address: LiteonTe_e4:f5:17 (d0:df:9a:e4:f5:17)

.... ..0. .... = LG bit: Globally unique address (factory default)

....0 .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.43.140, 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: 631

Identification: 0x2ebb (11963)

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: 0x680d [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.43.140

Destination: 128.119.245.12

Transmission Control Protocol, Src Port: 50223, Dst Port: 80, Seq: 1, Ack: 1, Len: 591

Source Port: 50223

Destination Port: 80

[Stream index: 3]

[TCP Segment Len: 591]

Sequence number: 1 (relative sequence number)

[Next sequence number: 592 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

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: 260

[Calculated window size: 66560]

[Window size scaling factor: 256]

Checksum: 0xf03f [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

  [iRTT: 0.178708000 seconds]

  [Bytes in flight: 591]

  [Bytes sent since last PSH flag: 591]

[Timestamps]

  [Time since first frame in this TCP stream: 1.854232000 seconds]

  [Time since previous frame in this TCP stream: 1.675524000 seconds]

TCP payload (591 bytes)

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n

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

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 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\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

If-None-Match: "2ca-5953d25d1970b"\r\n

If-Modified-Since: Sat, 19 Oct 2019 05:59:03 GMT\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]

[HTTP request 1/2]

[Response in frame: 122]

[Next request in frame: 124]

Ответ:

Frame 3: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0

Interface id: 0 (\Device\NPF_{8DB27C3E-EBB7-4924-AE75-E0A26D3078AF})

Interface name: \Device\NPF_{8DB27C3E-EBB7-4924-AE75-E0A26D3078AF}

Interface description [truncated]: \320\221\320\265\321\201\320\277\321\200\320\276\320\262\320\276\320\264\320\275\320\276\320\265 \321\201\320\265\321\202\320\265\320\262\320\276\320\265 \321\201\320\276\320\265\320\264\320\270\320\275\

Encapsulation type: Ethernet (1)

Arrival Time: Oct 19, 2019 12:02:46.702100000 Финляндия (лето)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1571475766.702100000 seconds

[Time delta from previous captured frame: 0.181422000 seconds]

[Time delta from previous displayed frame: 0.181422000 seconds]

[Time since reference or first frame: 0.184439000 seconds]

Frame Number: 3

Frame Length: 294 bytes (2352 bits)

Capture Length: 294 bytes (2352 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: HuaweiTe_77:9b:4a (34:12:f9:77:9b:4a), Dst: LiteonTe_e4:f5:17 (d0:df:9a:e4:f5:17)

Destination: LiteonTe_e4:f5:17 (d0:df:9a:e4:f5:17)

Address: LiteonTe_e4:f5:17 (d0:df:9a:e4:f5:17)

.... ..0. .... = LG bit: Globally unique address (factory default)

....0 .... = IG bit: Individual address (unicast)

Source: HuaweiTe_77:9b:4a (34:12:f9:77:9b:4a)

Address: HuaweiTe_77:9b:4a (34:12:f9:77:9b:4a)

.... ..0. .... = LG bit: Globally unique address (factory default)

....0 .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.140

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: 280

Identification: 0x0180 (384)

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: 49

Protocol: TCP (6)

Header checksum: 0xe5a7 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.43.140

Transmission Control Protocol, Src Port: 80, Dst Port: 50281, Seq: 1, Ack: 592, Len: 240

Source Port: 80

Destination Port: 50281

[Stream index: 1]

[TCP Segment Len: 240]

Sequence number: 1 (relative sequence number)

[Next sequence number: 241 (relative sequence number)]

Acknowledgment number: 592 (relative ack number)

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: 238

[Calculated window size: 238]

[Window size scaling factor: -1 (unknown)]

Checksum: 0xfd5c [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 2]

[The RTT to ACK the segment was: 0.181422000 seconds]

[Bytes in flight: 240]

[Bytes sent since last PSH flag: 240]

[Timestamps]

[Time since first frame in this TCP stream: 0.181422000 seconds]

[Time since previous frame in this TCP stream: 0.181422000 seconds]

TCP payload (240 bytes)

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]

Response Version: HTTP/1.1

Status Code: 304

[Status Code Description: Not Modified]

Response Phrase: Not Modified

Date: Sat, 19 Oct 2019 09:02:41 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Connection: Keep-Alive\r\n

Keep-Alive: timeout=5, max=100\r\n

ETag: "2ca-5953d25d1970b"\r\n

\r\n

[HTTP response 1/2]

[Time since request: 0.181422000 seconds]

[Request in frame: 2]

[Next request in frame: 9]

[Next response in frame: 10]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]