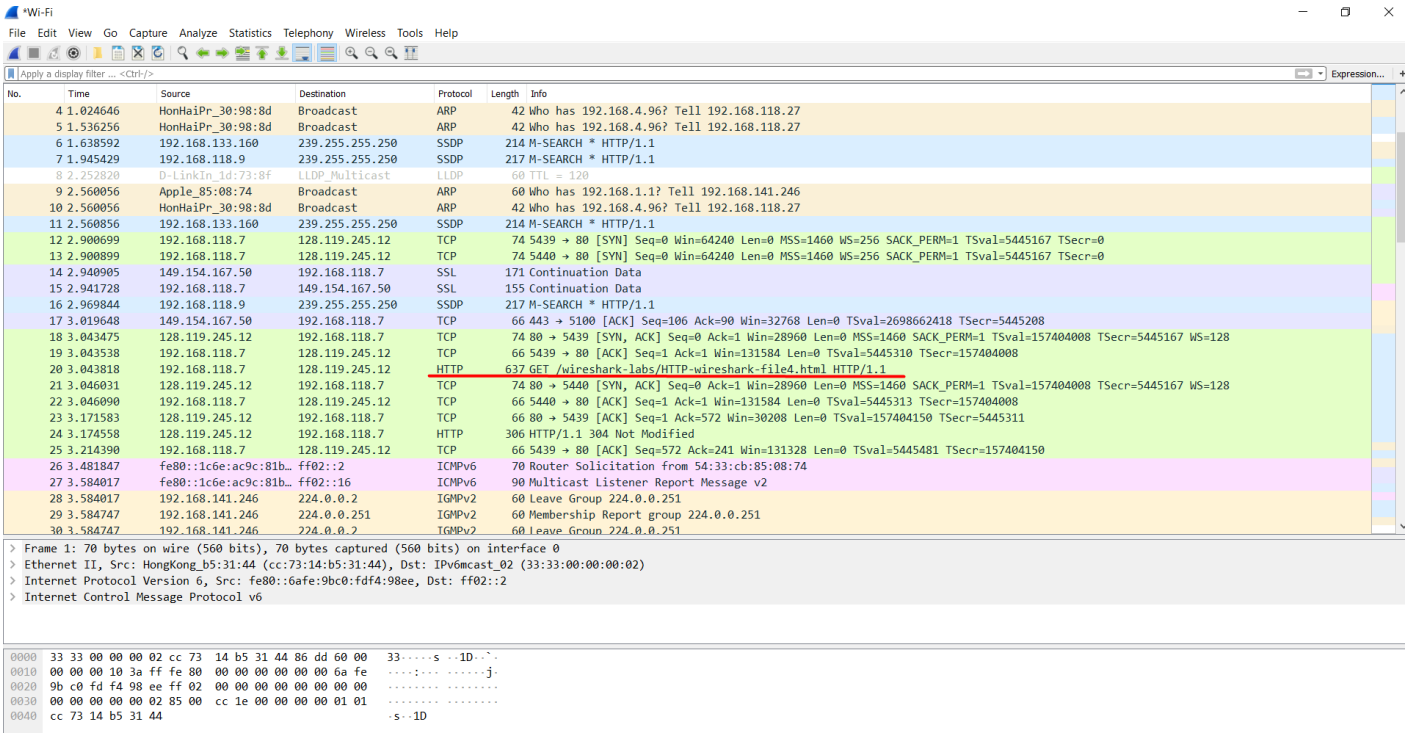
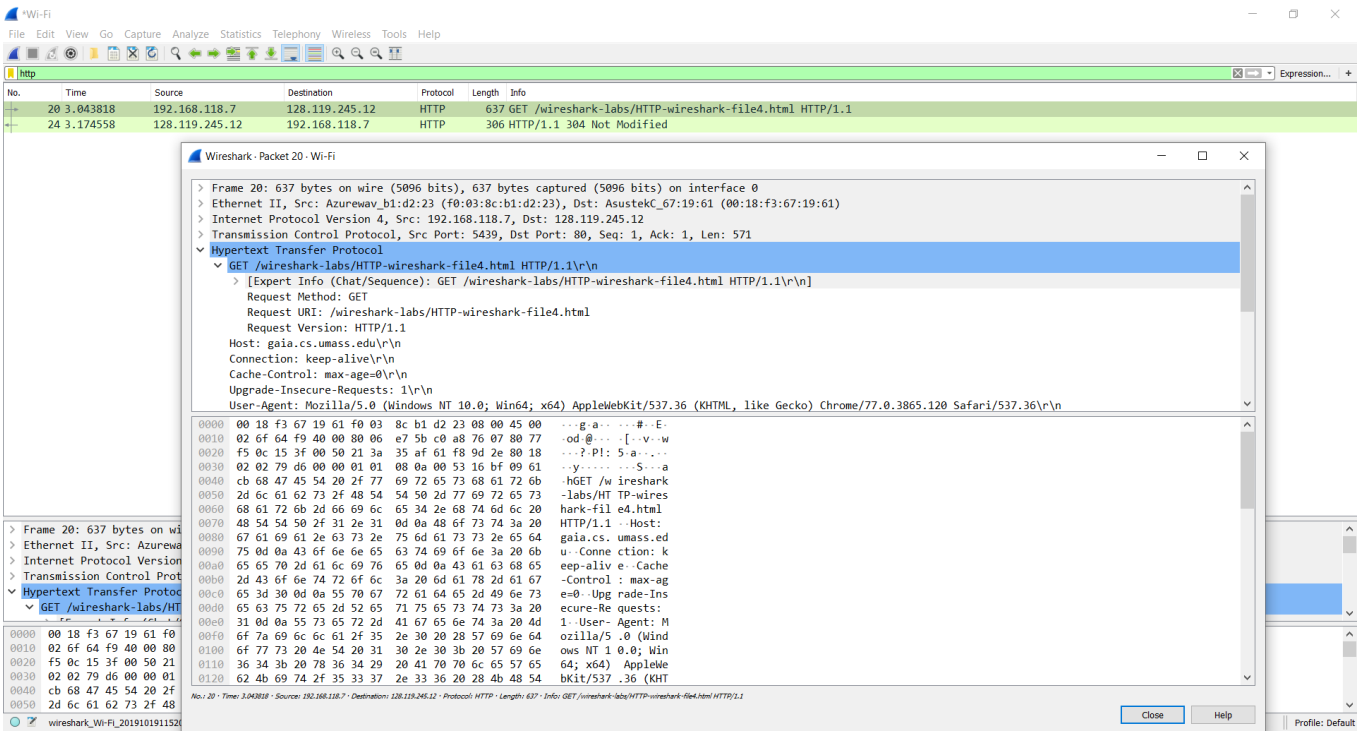
Task 1

1. Запустили Wireshark и перешли по ссылке http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html :



2. Отфильтровали пакеты и открыли для просмотра содержимого:



3. Открыли содержимое пакета:

Frame 23: 637 bytes on wire (5096 bits), 637 bytes captured (5096 bits) on interface 0

Interface id: 0 (\Device\NPF_{7E76D05C-62D5-4861-9984-7D585BD35844})

Interface name: \Device\NPF_{7E76D05C-62D5-4861-9984-7D585BD35844}

Interface description: Wi-Fi

Encapsulation type: Ethernet (1)

Arrival Time: Oct 19, 2019 12:01:34.025576000 FLE Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1571475694.025576000 seconds

[Time delta from previous captured frame: 0.000296000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 2.751673000 seconds]

Frame Number: 23

Frame Length: 637 bytes (5096 bits)

Capture Length: 637 bytes (5096 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: Azurewav_b1:d2:23 (f0:03:8c:b1:d2:23), Dst: AsustekC_67:19:61 (00:18:f3:67:19:61)

Destination: AsustekC_67:19:61 (00:18:f3:67:19:61)

Address: AsustekC_67:19:61 (00:18:f3:67:19:61)

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

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

Source: Azurewav_b1:d2:23 (f0:03:8c:b1:d2:23)

Address: Azurewav_b1:d2:23 (f0:03:8c:b1:d2:23)

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

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

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.118.7, 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: 623

Identification: 0x6511 (25873)

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: 0xe743 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.118.7

Destination: 128.119.245.12

Transmission Control Protocol, Src Port: 5518, Dst Port: 80, Seq: 1, Ack: 1, Len: 571

Source Port: 5518

Destination Port: 80

[Stream index: 2]

[TCP Segment Len: 571]

Sequence number: 1 (relative sequence number)

[Next sequence number: 572 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

1000 .... = Header Length: 32 bytes (8)

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: 0x7932 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

TCP Option - Timestamps: TSval 6009962, TSecr 157968548

Kind: Time Stamp Option (8)

Length: 10

Timestamp value: 6009962

Timestamp echo reply: 157968548

[SEQ/ACK analysis]

[iRTT: 0.256105000 seconds]

[Bytes in flight: 571]

[Bytes sent since last PSH flag: 571]

[Timestamps]

[Time since first frame in this TCP stream: 0.256401000 seconds]

[Time since previous frame in this TCP stream: 0.000296000 seconds]

TCP payload (571 bytes)

Hypertext Transfer Protocol

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

[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]

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

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file4.html

Request Version: HTTP/1.1

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 10.0; 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: en-US,en;q=0.9\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 1/1]

[Response in frame: 27]

Тут мы можем увидеть все данные о запросе, включая также данные о http запросе, которые были представлены на занятии, то есть структуру пакета и все данные о соединении. Также нам представлена общая информация о данном фрейме, параметры сети, общие данные об IPv4, та TCP IP протоколе. Мы можем узнать порты соединений, destination ip адрес. Если же говорить конкретно о данных http протокола, то мы видим стандартную структуру http пакета, где мы видим метод, версию, host, cache-control, connection.

4. При получении ответа мы видим:

Frame 27: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface 0

Interface id: 0 (\Device\NPF_{7E76D05C-62D5-4861-9984-7D585BD35844})

Interface name: \Device\NPF_{7E76D05C-62D5-4861-9984-7D585BD35844}

Interface description: Wi-Fi

Encapsulation type: Ethernet (1)

Arrival Time: Oct 19, 2019 12:01:34.280961000 FLE Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1571475694.280961000 seconds

[Time delta from previous captured frame: 0.000001000 seconds]

[Time delta from previous displayed frame: 0.255385000 seconds]

[Time since reference or first frame: 3.007058000 seconds]

Frame Number: 27

Frame Length: 306 bytes (2448 bits)

Capture Length: 306 bytes (2448 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: AsustekC_67:19:61 (00:18:f3:67:19:61), Dst: Azurewav_b1:d2:23 (f0:03:8c:b1:d2:23)

Destination: Azurewav_b1:d2:23 (f0:03:8c:b1:d2:23)

Address: Azurewav_b1:d2:23 (f0:03:8c:b1:d2:23)

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

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

Source: AsustekC_67:19:61 (00:18:f3:67:19:61)

Address: AsustekC_67:19:61 (00:18:f3:67:19:61)

.... ..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: 192.168.118.7

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: 292

Identification: 0xf3b2 (62386)

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: 47

Protocol: TCP (6)

Header checksum: 0xaaed [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.118.7

Transmission Control Protocol, Src Port: 80, Dst Port: 5518, Seq: 1, Ack: 572, Len: 240

Source Port: 80

Destination Port: 5518

[Stream index: 2]

[TCP Segment Len: 240]

Sequence number: 1 (relative sequence number)

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

Acknowledgment number: 572 (relative ack number)

1000 .... = Header Length: 32 bytes (8)

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: 236

[Calculated window size: 30208]

[Window size scaling factor: 128]

Checksum: 0x6da4 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

TCP Option - Timestamps: TSval 157968804, TSecr 6009962

Kind: Time Stamp Option (8)

Length: 10

Timestamp value: 157968804

Timestamp echo reply: 6009962

[SEQ/ACK analysis]

[iRTT: 0.256105000 seconds]

[Bytes in flight: 240]

[Bytes sent since last PSH flag: 240]

[Timestamps]

[Time since first frame in this TCP stream: 0.511786000 seconds]

[Time since previous frame in this TCP stream: 0.000001000 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]

[HTTP/1.1 304 Not Modified\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 304

[Status Code Description: Not Modified]

Response Phrase: Not Modified

Date: Sat, 19 Oct 2019 09:01:34 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 1/1]

[Time since request: 0.255385000 seconds]

[Request in frame: 23]

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

Также видим представленную структуру http пакета с кодом выполения 304 (редирект).