Лабораторная №3

Сетевые технологии - Комягин А.Н.

Российский университет дружбы народов, Москва, Россия

Цель

Цель работы

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

MAC-адресация

С помощью команды ipconfig определить основные параметры сетевого соединения.

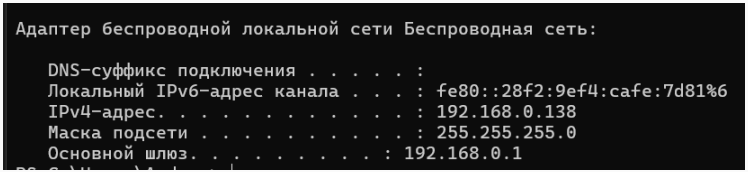


Рис. 1: ipconfig

Анализ кадров канального уровня в Wireshark

Захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня (Ethernet II).

Для генерации трафика была выполнена команда ping 192.168.0.1 (ping основного шлюза). В Wireshark был применен фильтр **arp or icmp**.

Анализ ICMP-трафика

На скриншоте ниже виден обмен ICMP-пакетами (эхо-запросы и эхо-ответы).

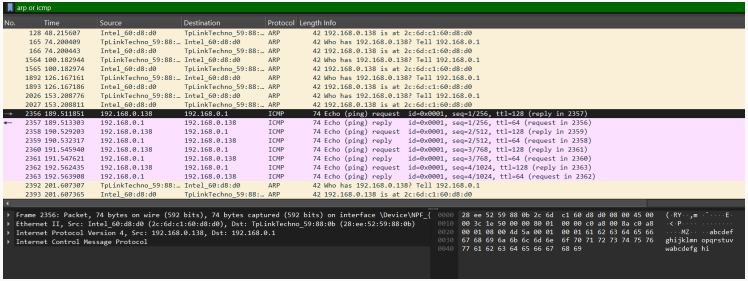


Рис. 2: ICMP 2356

Анализ ICMP-трафика

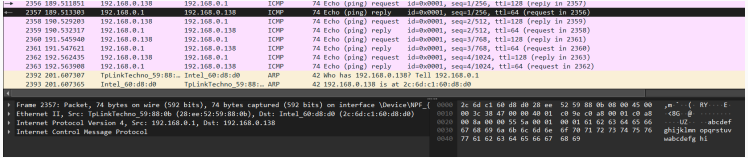


Рис. 3: ICMP 2357

Анализ ARP-трафика

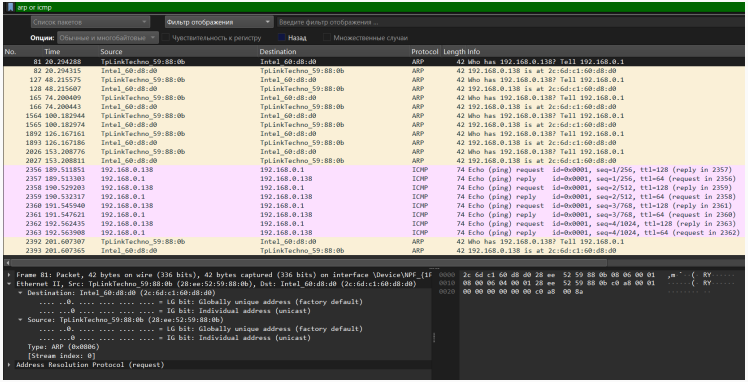


Рис. 4: ARP 81

Анализ ARP-трафика

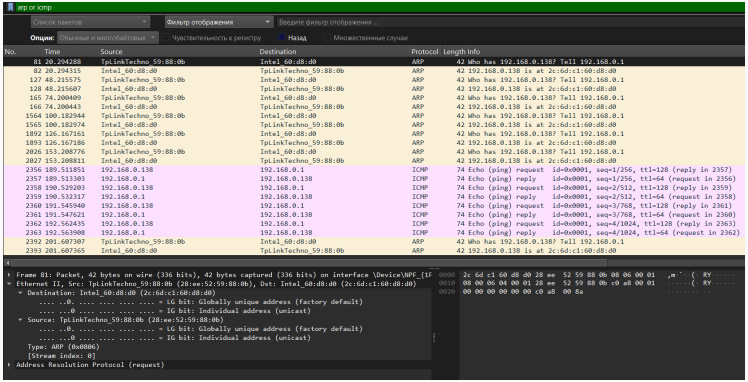
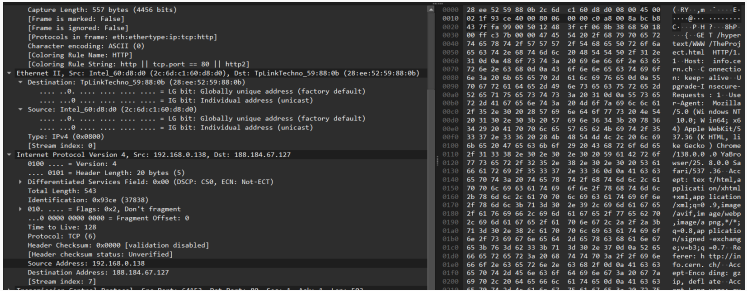


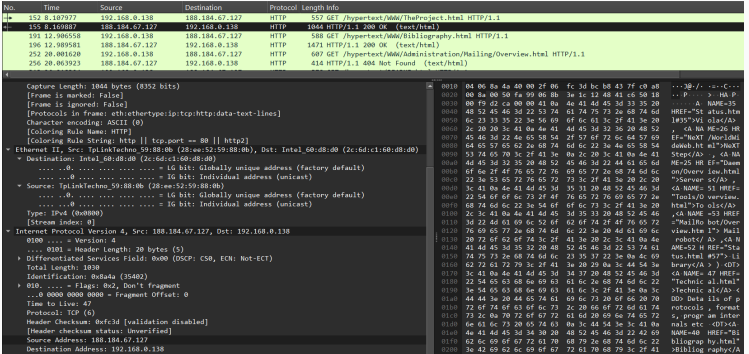
Рис. 5: ARP 82

Анализ протоколов транспортного уровня

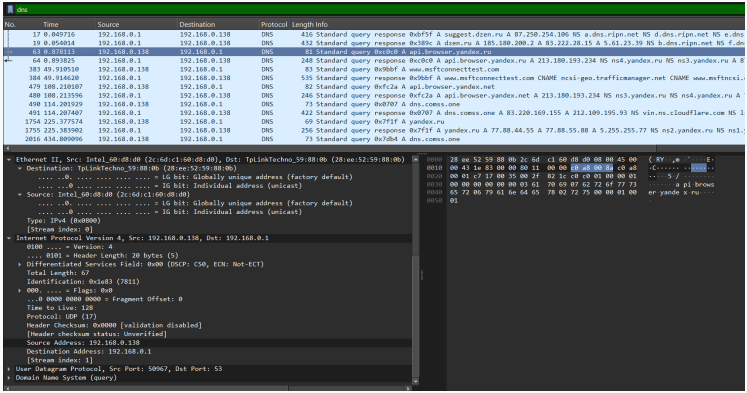
HTTP GET Request (пакет №152)



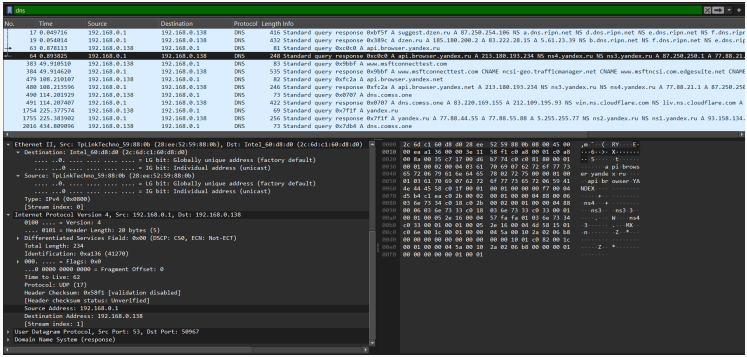
HTTP 200 OK Response (пакет №191)



DNS Standard Query (пакет №63)



DNS Standard Query Response (пакет №64)



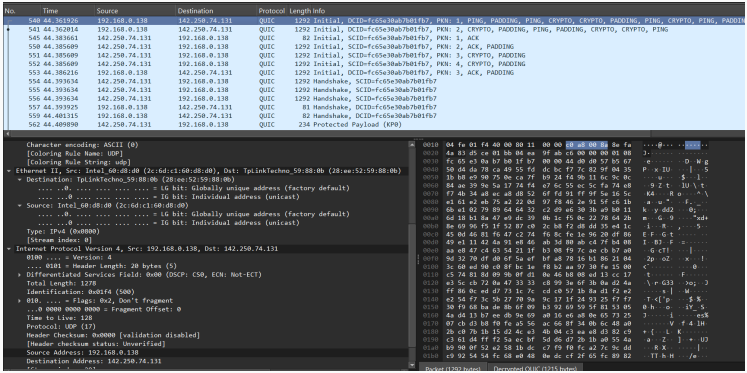
Проанализировать информацию по протоколу QUIC.

Был захвачен трафик к современному веб-ресурсу, использующему протокол QUIC.

Описание: QUIC (Quick UDP Internet Connections) — это транспортный протокол, работающий поверх UDP. Он обеспечивает шифрование по умолчанию и более быстрое установление соединения.

На скриншотах виден обмен пакетами Initial и Handshake, которые служат для установления защищенного соединения между клиентом 192.168.0.138 и сервером 142.250.74.131.

QUIC.


No. Time Source Destination Protocol Length Info
540 44.361926 192.168.0.138 142.250.74.131 QUIC 1292 Initial, DCID=fc65e30ab7b01fb7, PKN: 1, PING, PADDING, PING, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PING, PADDI
541 44.362014 192.168.0.138 142.250.74.131 QUIC 1292 Initial, DCID=fc65e30ab7b01fb7, PKN: 2, CRYPTO, PADDING, PING, PADDING, CRYPTO, CRYPTO, PING
545 44.383661 142.250.74.131 192.168.0.138 QUIC 82 Initial, SCID=fc65e30ab7b01fb7, PKN: 1, ACK
550 44.385609 142.250.74.131 192.168.0.138 QUIC 1292 Initial, SCID=fc65e30ab7b01fb7, PKN: 2, ACK, PADDING
551 44.385609 142.250.74.131 192.168.0.138 QUIC 1292 Initial, SCID=fc65e30ab7b01fb7, PKN: 3, CRYPTO, PADDING
552 44.385609 142.250.74.131 192.168.0.138 QUIC 1292 Initial, SCID=fc65e30ab7b01fb7, PKN: 4, CRYPTO, PADDING
553 44.386216 192.168.0.138 142.250.74.131 QUIC 1292 Initial, DCID=fc65e30ab7b01fb7, PKN: 3, ACK, PADDING
554 44.393634 142.250.74.131 192.168.0.138 QUIC 1292 Handshake, SCID=fc65e30ab7b01fb7
555 44.393634 142.250.74.131 192.168.0.138 QUIC 1292 Handshake, SCID=fc65e30ab7b01fb7
556 44.393634 142.250.74.131 192.168.0.138 QUIC 1292 Handshake, SCID=fc65e30ab7b01fb7
557 44.393925 192.168.0.138 142.250.74.131 QUIC 81 Handshake, DCID=fc65e30ab7b01fb7
559 44.401315 192.168.0.138 142.250.74.131 QUIC 82 Handshake, DCID=fc65e30ab7b01fb7
562 44.409890 142.250.74.131 192.168.0.138 QUIC 234 Protected Payload (KP0)
Character encoding: ASCII (0)
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0), Dst: TpLinkTechno_59:88:0b (28:ee:52:59:88:0b)
Destination: TpLinkTechno_59:88:0b (28:ee:52:59:88:0b)
.....0..... .... = LG bit: Globally unique address (factory default)
.....0.... .... = IG bit: Individual address (unicast)
Source: Intel_60:d8:d0 (2c:6d:c1:60:d8:d0)
.....0..... .... = LG bit: Globally unique address (factory default)
.....0.... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.0.138, Dst: 142.250.74.131
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1278
Identification: 0x01f4 (500)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.138
Destination Address: 142.250.74.131
0000 2c 6d c1 60 d8 d0 28 ee 52 59 88 0b 08 00 45 00
0010 04 fe 01 f4 40 00 80 11 00 00 c0 a8 00 8a 8e fa
0020 4a 83 d5 ce 01 bb 04 ea 9f ab c6 00 00 00 01 08
0030 fc 65 e3 0a b7 b0 1f b7 00 00 44 d0 d0 57 65 67
0040 50 d4 da 78 ca 49 55 fd dc bc f7 7c 82 9f 04 35
0050 1b b8 e9 98 75 0e ca 7f b9 24 f4 9b 11 6c 9c 8c
0060 84 ae 39 9e 5a 17 74 f4 e7 6c 55 ec 5c fa 74 e8
0070 f7 4b 3a a8 ec a8 d8 52 6f fd 91 ff 9f 5a 16 5c
0080 e1 61 e2 eb 75 a2 22 0d 97 f8 4b 2a 91 5f c6 1b
0090 6b e1 02 79 89 64 64 32 c2 d9 e6 30 3b a9 b0 11
00a0 6d 18 81 8a 47 a9 dc 39 4b 1c f5 0c 22 78 64 2b
00b0 8e 69 96 f5 1f 52 87 c0 2c b8 f2 d8 dd 35 e4 1c
00c0 45 0d 46 81 f6 47 c2 74 f6 8c fe 1e 96 20 ff 86
00d0 49 e1 11 42 4a 91 e8 46 ab 5d 80 ab c4 7f b4 08
00e0 aa e8 47 c4 63 54 21 1f b3 08 f9 7c ae cb b7 a0
00f0 5d 32 70 df d0 6f 5a ef bf ab 78 16 b1 86 21 04
0100 3c 60 ad 90 c0 8f bc 1e f8 b2 aa 97 30 fe 15 00
0110 c5 74 81 6d 09 9e 0f d1 0e 46 b8 b0 ad 13 cc 17
0120 e3 5c cb 72 0a 47 33 33 e8 99 3e 6f 3b 0e d2 4a
0130 ff 36 8c a4 d7 71 1c 7c cd a0 52 1b 8a d1 f2 a2
0140 e2 54 f7 7c 5b 27 70 9a 9c 17 1f 24 93 25 f7 f7
0150 30 f9 68 ba de 8b 6f 09 b3 92 69 59 5f 81 53 05
0160 4a d4 13 b7 ee db 9e 69 a0 16 e6 a8 0e 05 73 25
0170 07 cb d3 b8 f0 fe a5 56 ac 66 8f 34 0b 6c 48 a0
0180 2b c0 7b 1b 15 d2 4c a3 4b 04 c3 ea a8 d3 82 c9
0190 c3 61 d4 ff f2 5a ec bf 5d d6 d7 2b 1b a0 55 4a
01a0 b9 90 0f 52 a2 58 1b dc c7 f9 f0 fc a2 7c 9c dd
01b0 c9 92 54 54 fc 68 e0 48 8e dc cf 2f 65 fc 89 82
Packet (1292 bytes)
Decrypted QUIC (1215 bytes)

Анализ handshake протокола TCP

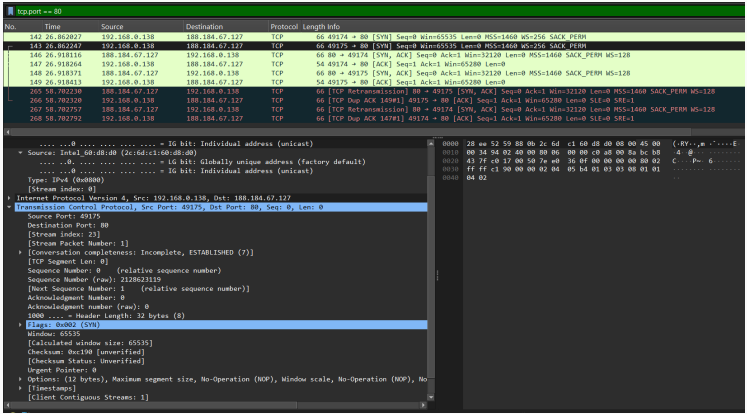
handshake

С помощью Wireshark проанализировать handshake протокола TCP.

Было инициировано соединение с веб-сервером, трафик был отфильтрован по tcp.port == 80. Были проанализированы первые три пакета, составляющие трёхступенчатое рукопожатие.

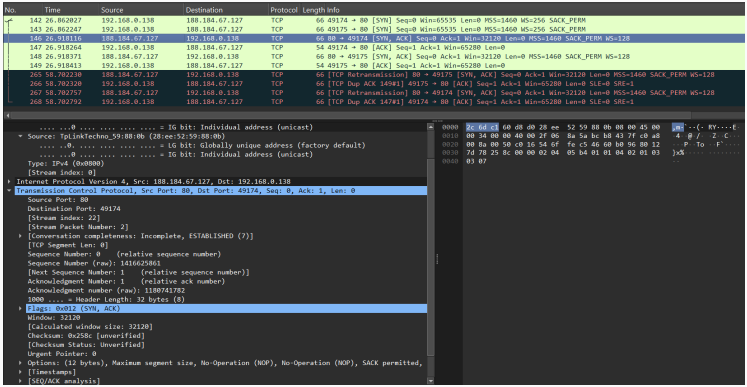
Шаг 1: SYN (пакет №143)

Клиент (192.168.0.138) отправляет серверу (188.184.67.127) сегмент с установленным флагом SYN (Synchronize). Это запрос на установку соединения.



Шаг 2: SYN, ACK (пакет №146)

Сервер отвечает сегментом с двумя флагами: SYN (он также предлагает синхронизировать номер последовательности) и ACK (Acknowledgment - подтверждает получение первого пакета от клиента).



ACK (пакет №147)

Клиент отправляет серверу сегмент с флагом ACK, подтверждая получение пакета SYN, ACK от сервера. На этом рукопожатие завершается, и соединение считается установленным.

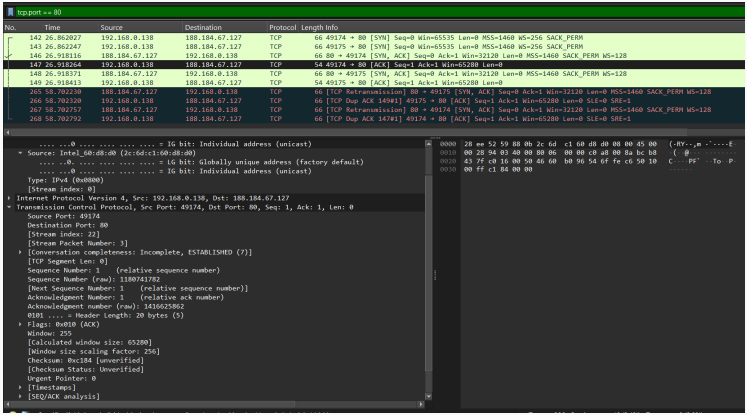


График Потока

Для визуализации обмена был построен график потока, на котором наглядно представлено всё TCP-соединение, включая начальное трёхступенчатое рукопожатие и последующие повторные передачи (Retransmissions).

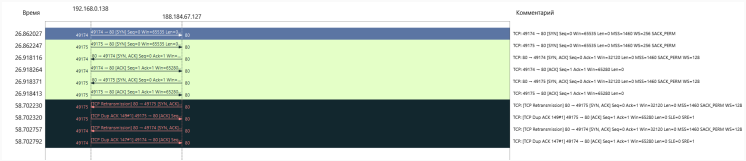


Рис. 6: График Потока

Выводы

Вывод

В ходе работы изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP прошли успешно.