Сетевые технологии

Анализ трафика в Wireshark

Хамди Мохаммад

15 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

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

Выполнение лабораторной работы

Анализ кадров канального уровня

```
PS C:\work\hamdimohammad\vagrant> ipconfig

Настройка протокола IP для Windows


Адаптер Ethernet Ethernet:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::52ff:33b6:449a:870f%18
   IPv4-адрес. . . . . . . . . . . . : 192.168.1.35
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . : 192.168.1.1

Адаптер Ethernet Ethernet 2:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::d3f2:8384:1a21:d660%21
   IPv4-адрес. . . . . . . . . . . . : 192.168.56.1
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:
```

Рис. 1: Результат команды ipconfig

```
PS C:\work\hamdimohammad\vagrant>
PS C:\work\hamdimohammad\vagrant> ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
PS C:\work\hamdimohammad\vagrant>
```

Рис. 2: Проверка доступности шлюза

Анализ кадров канального уровня

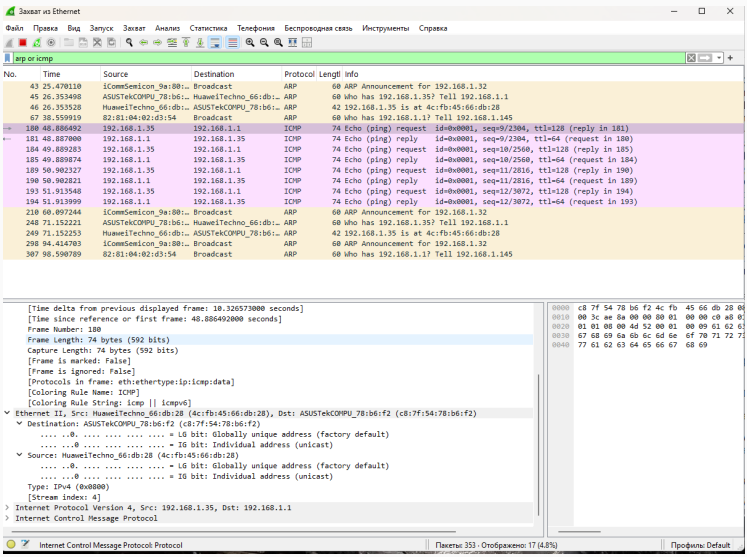


Рис. 2. ICMP запрос и ответ в Wireshark

Анализ кадров канального уровня

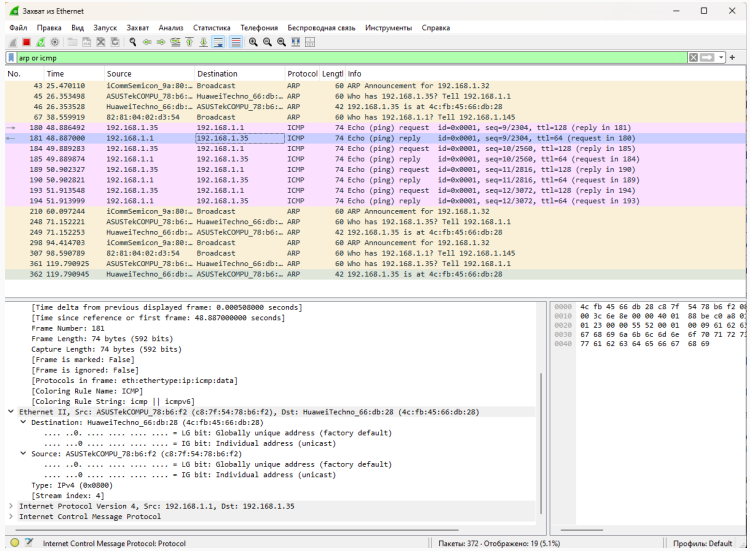


Рис. 4: Детализация ICMP-запроса

Анализ кадров канального уровня

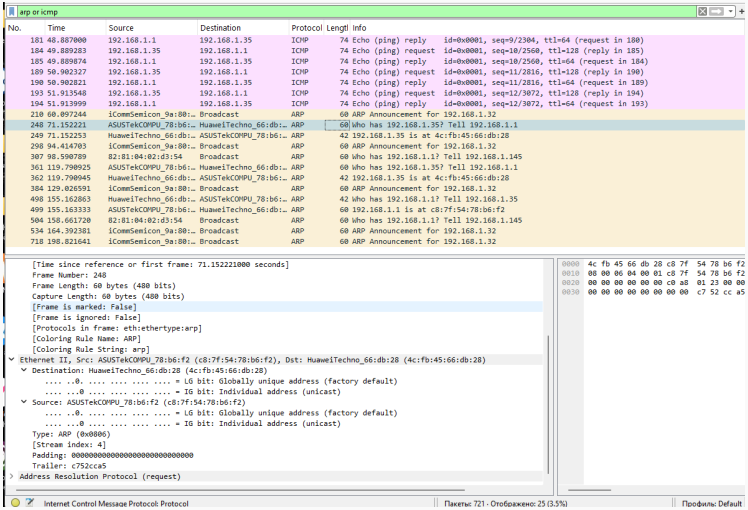


Рис. 5: Детализация ICMP-ответа

Анализ ARP

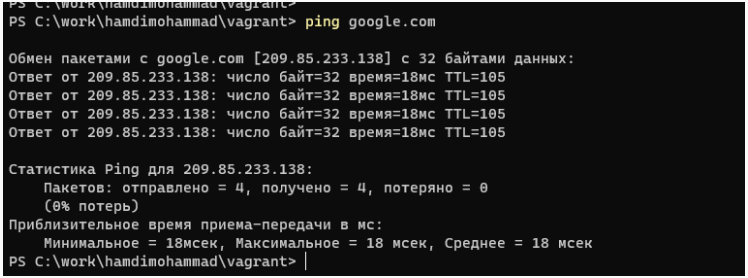
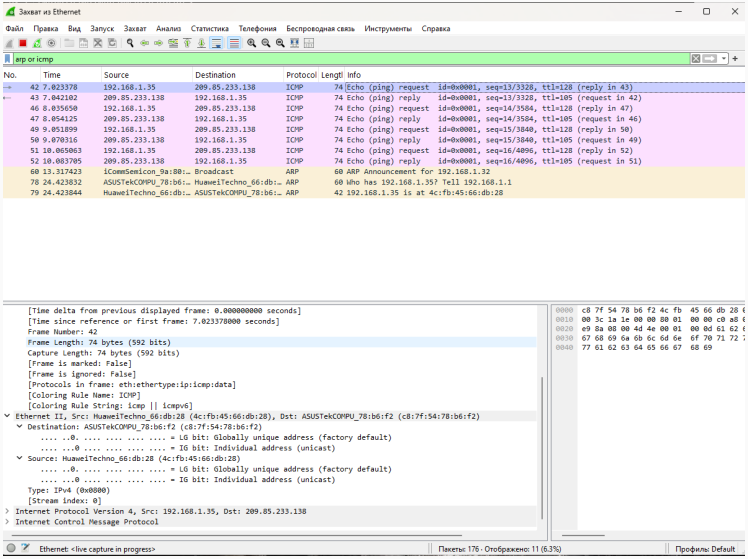
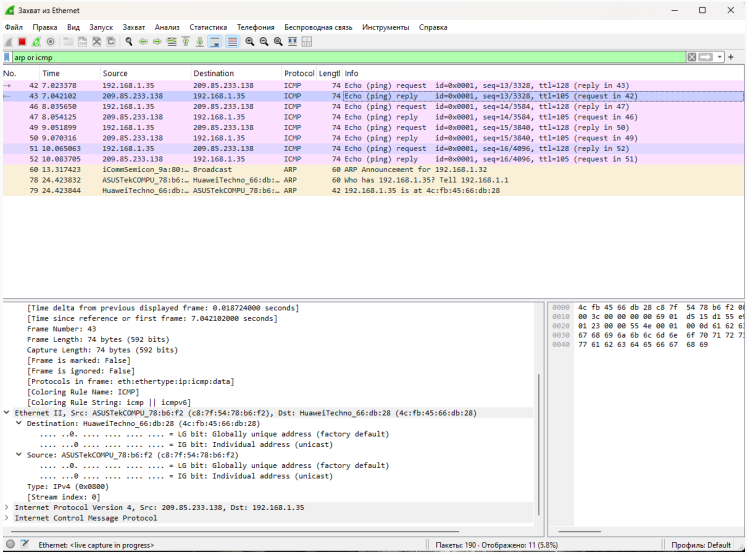


Рис. 6: Анализ ARP-запроса

Анализ ARP


Захват из Ethernet
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка
arp or icmp
No. Time Source Destination Protocol Lengt Info
42 7.023378 192.168.1.35 209.85.233.138 ICMP 74 Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 43)
43 7.042102 209.85.233.138 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=13/3328, ttl=105 (request in 42)
46 8.035650 192.168.1.35 209.85.233.138 ICMP 74 Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 47)
47 8.054125 209.85.233.138 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=14/3584, ttl=105 (request in 46)
49 9.051899 192.168.1.35 209.85.233.138 ICMP 74 Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 50)
50 9.070316 209.85.233.138 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=15/3840, ttl=105 (request in 49)
51 10.065063 192.168.1.35 209.85.233.138 ICMP 74 Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 52)
52 10.083705 209.85.233.138 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=16/4096, ttl=105 (request in 51)
60 13.317423 iCommSemicon_9a:80:… Broadcast ARP 60 ARP Announcement for 192.168.1.32
78 24.423832 ASUSTekCOMPU_78:b6:… HuaweiTechno_66:db:… ARP 60 Who has 192.168.1.35? Tell 192.168.1.1
79 24.423844 HuaweiTechno_66:db:… ASUSTekCOMPU_78:b6:… ARP 42 192.168.1.35 is at 4c:fb:45:66:db:28
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 7.023378000 seconds]
Frame Number: 42
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
Destination: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
.... ..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: 192.168.1.35, Dst: 209.85.233.138
Internet Control Message Protocol
0000 c8 7f 54 78 b6 f2 4c fb 45 66 db 28
0010 00 3c 1a 1e 00 00 80 01 00 00 c0 a8
0020 e9 8a 08 00 4d 4e 00 01 00 0d 61 62
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72
0040 77 61 62 63 64 65 66 67 68 69
Ethernet: <live capture in progress>
Пакеты: 176 · Отображено: 11 (6.3%)
Профиль: Default

Анализ ICMP и ARP при ping внешнего ресурса



Анализ ICMP и ARP при ping внешнего ресурса

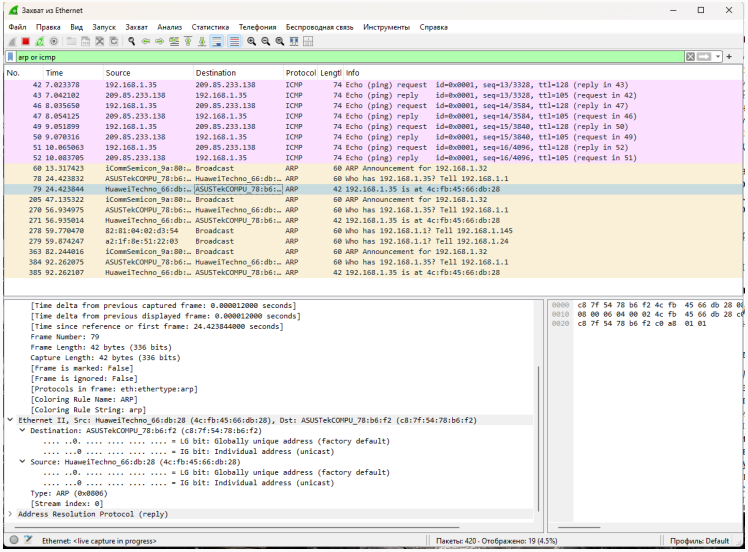


Рис. 2. Анализ ICMP-трафика при ping google.com

Анализ транспортного уровня: HTTP

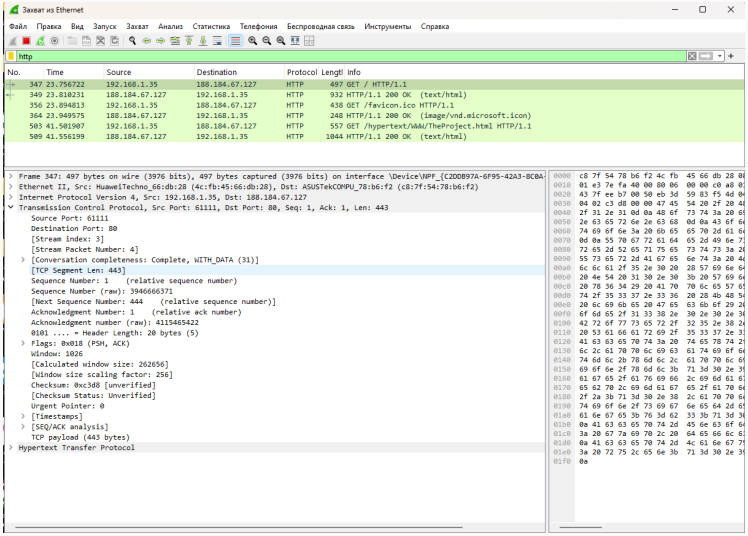


Рис. 10: HTTP-запрос в Wireshark

Анализ транспортного уровня: HTTP

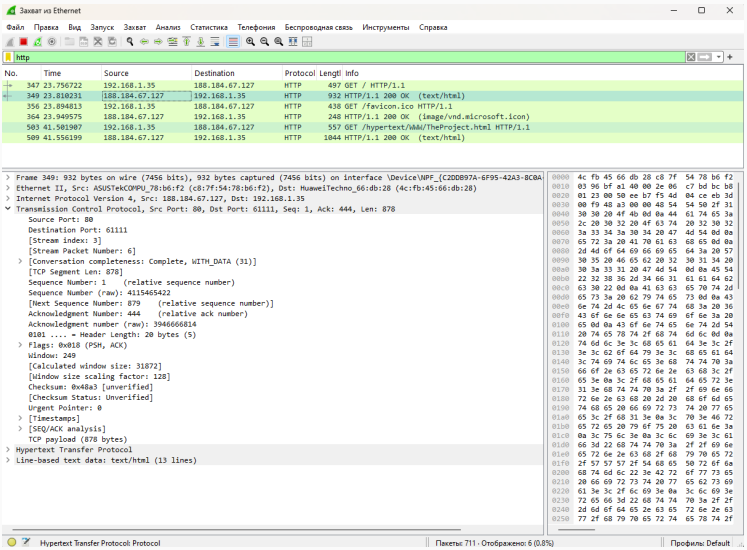


Рис. 11: HTTP-ответ в Wireshark

Анализ транспортного уровня: DNS

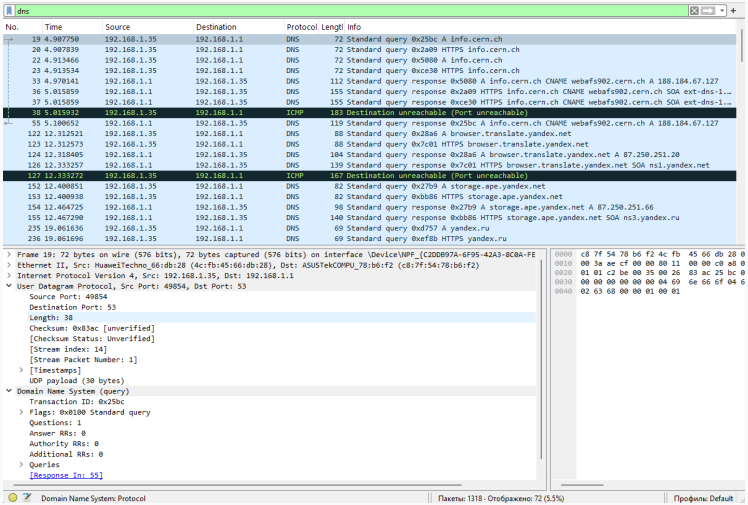
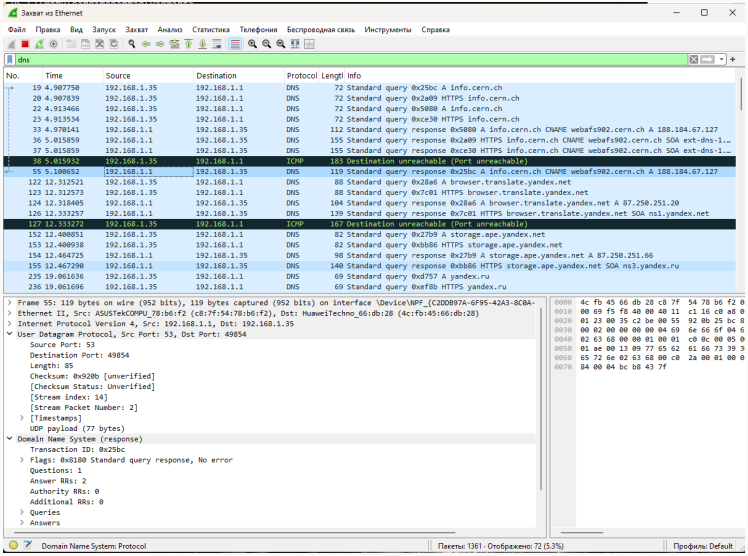


Рис. 12: DNS-запрос

Анализ транспортного уровня: DNS



Анализ транспортного уровня: QUIC

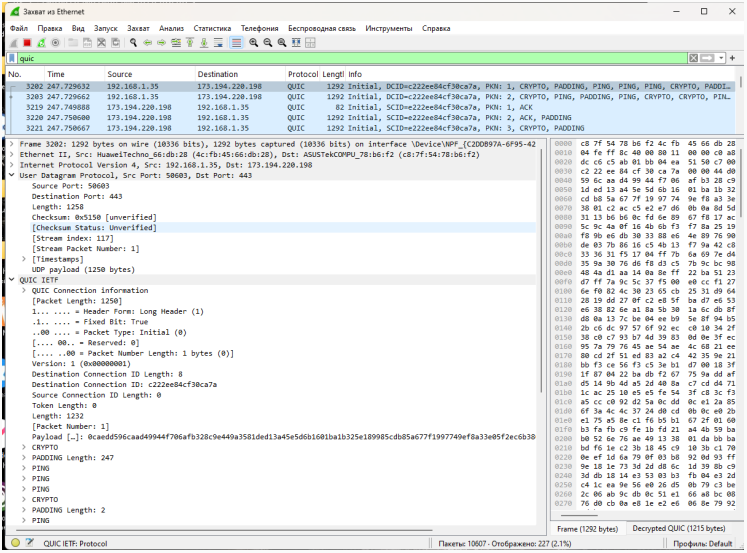
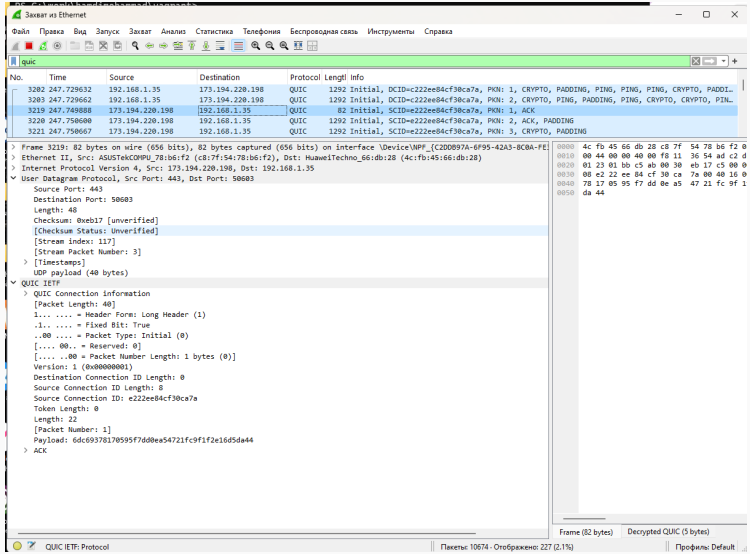
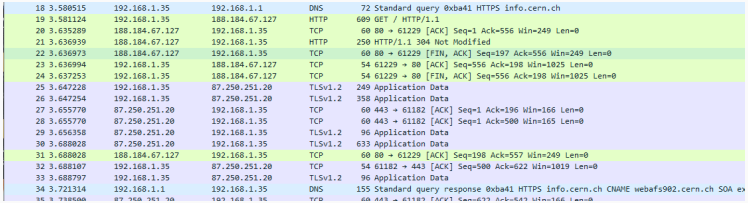


Рис. 11 - QUIC запрос

Анализ транспортного уровня: QUIC



Анализ TCP handshake



18	3.580515	192.168.1.35	192.168.1.1	DNS	72 Standard query 0xba41 HTTPS info.cern.ch
19	3.581124	192.168.1.35	188.184.67.127	HTTP	609 GET / HTTP/1.1
20	3.635289	188.184.67.127	192.168.1.35	TCP	60 80 → 61229 [ACK] Seq=1 Ack=556 Win=249 Len=0
21	3.636939	188.184.67.127	192.168.1.35	HTTP	250 HTTP/1.1 304 Not Modified
22	3.636973	188.184.67.127	192.168.1.35	TCP	60 80 → 61229 [FIN, ACK] Seq=197 Ack=556 Win=249 Len=0
23	3.636994	192.168.1.35	188.184.67.127	TCP	54 61229 → 80 [ACK] Seq=556 Ack=198 Win=1025 Len=0
24	3.637253	192.168.1.35	188.184.67.127	TCP	54 61229 → 80 [FIN, ACK] Seq=556 Ack=198 Win=1025 Len=0
25	3.647228	192.168.1.35	87.250.251.20	TLSv1.2	249 Application Data
26	3.647254	192.168.1.35	87.250.251.20	TLSv1.2	358 Application Data
27	3.655770	87.250.251.20	192.168.1.35	TCP	60 443 → 61182 [ACK] Seq=1 Ack=196 Win=166 Len=0
28	3.655770	87.250.251.20	192.168.1.35	TCP	60 443 → 61182 [ACK] Seq=1 Ack=500 Win=165 Len=0
29	3.656358	87.250.251.20	192.168.1.35	TLSv1.2	96 Application Data
30	3.688028	87.250.251.20	192.168.1.35	TLSv1.2	633 Application Data
31	3.688028	188.184.67.127	192.168.1.35	TCP	60 80 → 61229 [ACK] Seq=198 Ack=557 Win=249 Len=0
32	3.688107	192.168.1.35	87.250.251.20	TCP	54 61182 → 443 [ACK] Seq=500 Ack=622 Win=1019 Len=0
33	3.688797	192.168.1.35	87.250.251.20	TLSv1.2	96 Application Data
34	3.721314	192.168.1.1	192.168.1.35	DNS	155 Standard query response 0xba41 HTTPS info.cern.ch CNAME webafs902.cern.ch SOA ex
35	3.718599	87.250.251.20	192.168.1.35	TCP	60 443 → 61182 [ACK] Seq=622 Ack=542 Win=166 Len=0

Рис. 16: Анализ TCP-сессии

График потока TCP

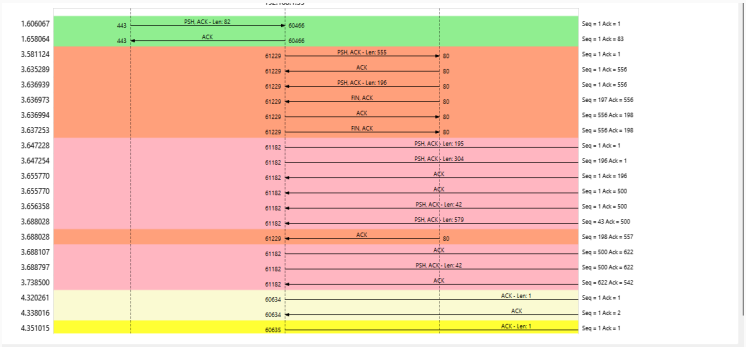


Рис. 17: График потока TCP

Выводы по проделанной работе

Вывод

В ходе работы был проведён анализ установления соединения по протоколу **TCP** с использованием программы **Wireshark**.

Было зафиксировано трёхстороннее рукопожатие (SYN → SYN+ACK → ACK), подтверждающее успешное начало TCP-сессии.

С помощью графика потока были проанализированы этапы установления и завершения соединения, а также последующая передача данных.