

Анализ трафика в Wireshark

Лабораторная работа №3

Суннатилло Махмудов

02 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Изучение и анализ сетевых протоколов на разных уровнях модели OSI с помощью анализатора трафика **Wireshark**.

1. Определить параметры сетевых интерфейсов и изучить структуру MAC-адреса.
2. Проанализировать кадры канального уровня (ARP, ICMP).
3. Исследовать транспортные протоколы (**TCP, UDP, QUIC**) и их особенности.
4. Рассмотреть механизм установления соединения TCP (*three-way handshake*).

Теоретическая часть

- **MAC-адресация** — уникальная идентификация сетевого интерфейса.
- **ARP** — сопоставление IP и MAC-адресов.
- **ICMP** — служебные сообщения, диагностика (ping).
- **TCP** — надёжная передача данных, трёхстороннее рукопожатие.
- **UDP** — простой протокол без установления соединения.
- **QUIC** — работает поверх UDP, обеспечивает шифрование и ускорение.
- **Wireshark** — анализатор пакетов для исследования уровней модели OSI.

Выполнение работы

- Получение параметров интерфейса с помощью `ipconfig`.
- Определение MAC-адреса устройства.
- Разбор структуры адреса: OUI (производитель), уникальный идентификатор, тип (unicast/global).

Адаптер Ethernet Ethernet:

```
DNS-суффикс подключения . . . . . :  
Локальный IPv6-адрес канала . . . : fe80::b707:d865:dc39:d9f5%17  
IPv4-адрес. . . . . : 192.168.1.10  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз. . . . . : 192.168.1.1
```

Адаптер Ethernet Ethernet 2:

```
DNS-суффикс подключения . . . . . :  
Локальный IPv6-адрес канала . . . : fe80::bae0:cc2e:9d1e:b2d4%19  
IPv4-адрес. . . . . : 192.168.56.1  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз. . . . . :
```

Рис. 1: Вывод команды `ipconfig`

Анализ ARP и ICMP

- Ping шлюза по умолчанию.
- Фильтрация трафика в Wireshark: **arp or icmp**.
- Анализ эхо-запросов и эхо-ответов.
- Изучение ARP-запросов и ответов.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Файл', 'Правка', 'Вид', 'Запуск', 'Захват', 'Анализ', 'Статистика', 'Телефония', 'Беспроводная связь', 'Инструменты', and 'Справка'. The toolbar contains icons for file operations, packet list, packet details, packet bytes, and packet capture. The packet list pane shows a filtered view of traffic with the filter 'arp or icmp'. The packet details pane shows the selected packet (No. 572) with its structure: Ethernet II, Internet Protocol Version 4, and ICMP Echo (ping) request. The packet bytes pane shows the raw data of the packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
17	3.119065	192.168.1.10	192.168.1.1	ICMP	302	Destination unreachable (Port unreachable)
572	27.649926	192.168.1.10	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 573)
573	27.650418	192.168.1.1	192.168.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 572)
574	28.655284	192.168.1.10	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 575)
575	28.655863	192.168.1.1	192.168.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 574)
580	29.667912	192.168.1.10	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 581)
581	29.668543	192.168.1.1	192.168.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 580)
583	30.682341	192.168.1.10	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 584)
584	30.682967	192.168.1.1	192.168.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 583)
585	31.252917	ASUSTekCOMPU_78:b6:...	GigaByteTech_21:d6:...	ARP	60	Who has 192.168.1.10? Tell 192.168.1.1
586	31.252947	GigaByteTech_21:d6:...	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.10 is at 10:ff:e0:21:d6:b4

Packet 572 details:

- Frame 572: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on Ethernet II, Src: GigaByteTech_21:d6:b4 (10:ff:e0:21:d6:b4), Dst: ASUS10000:01:08:00:4d:5a (08:00:01:01:08:00:4d:5a)
- Destination: ASUS10000:01:08:00:4d:5a (08:00:01:01:08:00:4d:5a)
- Source: GigaByteTech_21:d6:b4 (10:ff:e0:21:d6:b4)
- Type: IPv4 (0x0800)
- [Stream index: 3]
- Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 60
 - Identification: 0x0000 (00000000)

Packet 572 bytes:

```
0000 c8 7f 54 78 b6 f2 10 ff e0 21 d6 b4 08 00 45 00 ..Tx....!...E-
0010 00 3c ab fa 00 00 80 01 00 00 c0 a8 01 0a c0 a8 ...<.....
0020 01 01 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66 ....MZ...-abcde
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdegh hi
```

Анализ транспортных протоколов

- HTTP-трафик (TCP): запросы GET, ответы 200 OK.
- DNS-трафик (UDP): запросы A/HTTPS-записей.
- QUIC-трафик (UDP+TLS 1.3): зашифрованные сегменты и Handshake.

The screenshot shows the Wireshark network protocol analyzer interface. The top pane, titled "Захват из Ethernet", displays a list of captured packets. The bottom pane shows the detailed view of a selected packet, identified as a Transmission Control Protocol (TCP) segment.

No.	Time	Source	Destination	Protocol	Length	Info
866	26.319988	192.168.1.10	188.184.67.127	HTTP	497	GET / HTTP/1.1
869	26.374046	188.184.67.127	192.168.1.10	HTTP	932	HTTP/1.1 200 OK (text/html)
892	33.384236	192.168.1.10	188.184.67.127	HTTP	557	GET /hypertext/WWW/TheProject.html HTTP/1.1
897	33.437004	188.184.67.127	192.168.1.10	HTTP	1044	HTTP/1.1 200 OK (text/html)
924	36.443116	192.168.1.10	188.184.67.127	HTTP	580	GET /hypertext/WWW/Help.html HTTP/1.1
928	36.496138	188.184.67.127	192.168.1.10	HTTP	1130	HTTP/1.1 200 OK (text/html)

The detailed view of the selected packet (No. 866) shows the following information:

- Transmission Control Protocol, Src Port: 50094, Dst Port: 80, Seq: 1, Len: 497
- Source Port: 50094
- Destination Port: 80
- [Stream index: 2]
- [Stream Packet Number: 4]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 443]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 2600030513
- [Next Sequence Number: 444 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 2041939721
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 1026

The packet data is displayed in hexadecimal and ASCII format:

```
0000 c8 7f 54 78 b6 f2 10 ff e0 21 d6 b4 08 00 45 00 ..Tx....!...E
0010 01 e3 31 90 40 00 80 06 00 00 c0 a8 01 0a bc b8 --1@.....
0020 43 7f c3 ae 00 50 9a f9 51 31 79 b5 87 09 50 18 C....P...Q1y...P
0030 04 02 c3 bf 00 00 47 45 54 20 2f 20 48 54 54 50 .....GE T / HTT
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 69 6e 66 6f /1.1..Ho st: inf
0050 2e 63 65 72 6e 2e 63 68 0d 0a 43 6f 6e 6e 65 63 .cern.ch ..Conne
0060 74 09 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-aliv
0070 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ..Upgrad e-Insec
0080 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a re-Reque sts: 1-
0090 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Moz
00a0 6c 6c 61 2f 35 2a 30 20 28 57 69 6e 64 6f 77 73 lla/5.0 (Window
00b0 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b NT 10.0 ; Win64
00c0 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 x64) Ap pleWebK
00d0 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c t/537.36 (KHTML
00e0 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 like Ge cko) Ch
00f0 6f 6d 65 2f 31 33 38 2e 30 2e 30 2e 30 20 59 61 ome/138.0.0.0.Y
0100 42 72 6f 77 73 65 72 2f 32 35 2e 38 2e 30 2e 30 Browser/ 25.8.0.
0110 20 53 61 66 61 72 69 7f 35 33 37 2e 33 36 6d 6a Safari/ 537.36.
```

Анализ handshake TCP

- Установление соединения: SYN → SYN+ACK → ACK.
- Визуализация в Wireshark через «График потока».
- Наблюдение последовательности, подтверждений и завершения сеанса.

The image shows a Wireshark packet capture window titled "Захват из Ethernet". The packet list on the left shows a series of HTTP requests. The selected packet is packet 1310, which is an HTTP GET request. The packet details pane on the right shows the structure of the TCP segment and the HTTP request.

No.	Time	Source	Destination	Protocol	Length	Info
1280	126.860316	192.168.1.10	204.79.197.223	HTTP	235	HEAD /pr/1d2d2ea6-1680-4c56-ac58-a441c8c24ff9/Office/Data/16.0.13530.2...
1282	126.893241	204.79.197.223	192.168.1.10	HTTP	220	HTTP/1.1 400 Bad Request
1283	126.897497	192.168.1.10	204.79.197.223	HTTP	252	GET /pr/1d2d2ea6-1680-4c56-ac58-a441c8c24ff9/Office/Data/16.0.13530.20...
1286	126.930514	204.79.197.223	192.168.1.10	HTTP	60	HTTP/1.1 400 Bad Request
1294	127.166432	192.168.1.10	92.123.135.94	HTTP	235	HEAD /pr/1d2d2ea6-1680-4c56-ac58-a441c8c24ff9/Office/Data/16.0.13530.2...
1296	127.197746	92.123.135.94	192.168.1.10	HTTP	439	HTTP/1.1 400 Bad Request
1297	127.200459	192.168.1.10	92.123.135.94	HTTP	252	GET /pr/1d2d2ea6-1680-4c56-ac58-a441c8c24ff9/Office/Data/16.0.13530.20...
1299	127.232051	92.123.135.94	192.168.1.10	HTTP	583	HTTP/1.1 400 Bad Request (text/html)
1301	127.349775	192.168.1.10	2.16.56.87	HTTP	235	HEAD /sg/1d2d2ea6-1680-4c56-ac58-a441c8c24ff9/Office/Data/16.0.13530.2...
1303	127.380729	2.16.56.87	192.168.1.10	HTTP	439	HTTP/1.1 400 Bad Request
1304	127.383105	192.168.1.10	2.16.56.87	HTTP	252	GET /sg/1d2d2ea6-1680-4c56-ac58-a441c8c24ff9/Office/Data/16.0.13530.20...
1305	127.413648	2.16.56.87	192.168.1.10	HTTP/3...	464	HTTP/1.1 400 Bad Request , JSON (application/json)
1307	127.535212	192.168.1.10	2.16.56.87	HTTP	235	HEAD /db/1d2d2ea6-1680-4c56-ac58-a441c8c24ff9/Office/Data/16.0.13530.2...
1308	127.563822	2.16.56.87	192.168.1.10	HTTP	439	HTTP/1.1 400 Bad Request
1309	127.567248	192.168.1.10	2.16.56.87	HTTP	252	GET /db/1d2d2ea6-1680-4c56-ac58-a441c8c24ff9/Office/Data/16.0.13530.20...
1310	127.596085	2.16.56.87	192.168.1.10	HTTP/3...	464	HTTP/1.1 400 Bad Request , JSON (application/json)

[TCP Segment Len: 385]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2534305836
[Next Sequence Number: 386 (relative sequence number)]
Acknowledgment Number: 182 (relative ack number)
Acknowledgment number (raw): 3214181557
0101 = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 501
[Calculated window size: 64128]
[Window size scaling factor: 128]
Checksum: 0xb5d3 [unverified]
[Checksum Offset: 0, Unverified]

0000 10 ff e0 21 d6 b4 c8 7f 54 78 b6 f2 08 00 45 00 ...I... Tx...E
0010 01 a9 f6 30 40 00 34 06 53 05 02 10 38 57 c0 a8 ...@.4. S...BW
0020 01 0a 00 50 c3 c6 97 0a 70 2c bf 94 84 b5 50 18 ...P... p,...P
0030 01 f5 b5 d3 00 00 48 54 54 50 2f 31 2e 31 20 34 ...HT TP/1.1
0040 30 30 20 42 61 64 20 52 65 71 75 65 73 74 0d 0a 00 Bad R equest
0050 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 Content- Type: a
0060 70 6c 69 63 61 74 69 6f 6e 2f 6a 73 6f 6e 0d 0a plicatio n/json
0070 53 65 72 76 65 72 3a 20 4b 65 73 74 72 65 6c 0d Server: Kestrel
0080 0a 58 2d 4d 73 2d 41 70 69 56 65 72 73 69 6f 6e .X-Ms-Ap iVersio
0090 3a 20 44 69 73 74 72 69 62 75 74 65 20 31 2e 32 : Distri bute 1.
00a0 0d 0a 58 2d 4d 73 2d 52 65 67 69 6f 6e 3a 20 70 .X-Ms-R egion:
00b0 72 6f 64 2d 77 65 75 2d 7a 31 0d 0a 58 2d 44 53 rod-wau- z1 .X-D
00c0 47 61 74 65 77 61 79 53 65 72 76 69 63 65 41 50 GatewayS erviceA
00d0 49 2d 05 72 72 6f 72 43 6f 64 65 3a 20 32 30 30 I-ErrorC ode: 20
00e0 31 32 0d 0a 58 2d 44 53 47 61 74 65 77 61 79 53 12 .X-D S Gateway

Вывод

В ходе работы:

- * Изучены MAC-адреса и протоколы ARP/ICMP.
- * Проанализированы транспортные протоколы TCP, UDP, QUIC.
- * Подробно рассмотрен процесс установления TCP-соединения.
- * Использование **Wireshark** позволило наглядно изучить работу сетевых протоколов на разных уровнях модели OSI.