

Лабораторная работа №3

Анализ трафика в Wireshark

Газизянов Владислав Альбертович

2025-10-10

Содержание I

1 Цели работы

Изучение посредством Wireshark кадров Ethernet

Анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP

Освоение методов захвата и анализа сетевого трафика

2 Установка и настройка Wireshark

Wireshark - анализатор трафика сетей на базе Ethernet
Использует библиотеку Pcap/WinPcap для захвата пакетов
Требуется административных прав для работы
Поддерживает фильтрацию трафика по протоколам

3 Анализ MAC-адресации

Команда `ipconfig /all` показывает сетевые интерфейсы

Определены MAC-адреса всех адаптеров

Основной интерфейс: Беспроводная сеть

MAC-адрес: C0-BF-BE-CF-C4-CE

```
C:\Windows\System32>ipconfig /all
```

```
Настройка протокола IP для Windows
```

```
Имя компьютера . . . . . : Ony
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
```

```
Адаптер Ethernet Ethernet 2:
```

```
DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet Adapter
Физический адрес. . . . . : 0A-00-27-00-00-0C
```

4 Структура MAC-адреса

C0-BF-BE-CF-C4-CE

OUI: C0-BF-BE (MediaTek Inc.)

Идентификатор интерфейса: CF-C4-CE

Тип: индивидуальный (unicast)

Администрирование: глобальное

5 Захват ICMP трафика

Запущен захват на интерфейсе «Беспроводная сеть»

Выполнен ping шлюза: `ping 192.168.0.1`

Применен фильтр: `arp or icmp`



Рисунок 2: Фильтрация ARP и ICMP

6 Анализ ICMP-запроса

Echo request от 192.168.0.101 к 192.168.0.1

Длина кадра: 74 байта

MAC назначения: TPLink_15:a1:6c (шлюз)

MAC источника: AzureWaveTec_cf:c4:ce (компьютер)

Тип: Ethernet II

```
Frame 41926: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface  
Ethernet II, Src: AzureWaveTec_cf:c4:ce (c0:bf:be:cf:c4:ce), Dst: TPLink_15:a1:6c (5c:62:8b:15:a1:6c)  
  Destination: TPLink_15:a1:6c (5c:62:8b:15:a1:6c)  
    .... ..0. .... = LG bit: Globally unique address (factory default)  
    .... ...0 .... = IG bit: Individual address (unicast)  
  Source: AzureWaveTec_cf:c4:ce (c0:bf:be:cf:c4:ce)  
    .... ..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: 192.168.0.101, Dst: 192.168.0.1
```


7 Анализ ICMP-ответа

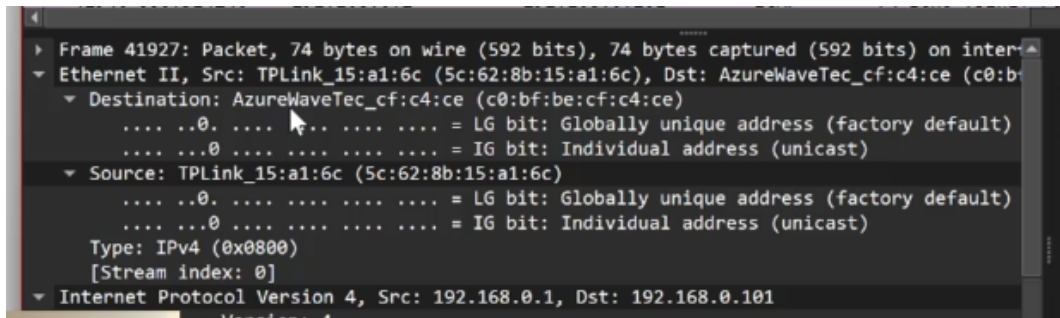
Echo reply от 192.168.0.1 к 192.168.0.101

Длина кадра: 74 байта

MAC назначения: AzureWaveTec_cf:c4:ce (компьютер)

MAC источника: TPLink_15:a1:6c (шлюз)

Тип: Ethernet II



```
▶ Frame 41927: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▼ Ethernet II, Src: TPLink_15:a1:6c (5c:62:8b:15:a1:6c), Dst: AzureWaveTec_cf:c4:ce (c0:b0:00:00:c0:b0)
  ▼ Destination: AzureWaveTec_cf:c4:ce (c0:b0:00:00:c0:b0)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: TPLink_15:a1:6c (5c:62:8b:15:a1:6c)
    .... ..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: 192.168.0.1, Dst: 192.168.0.101
```

8 Анализ ARP пакетов

ARP запрос:

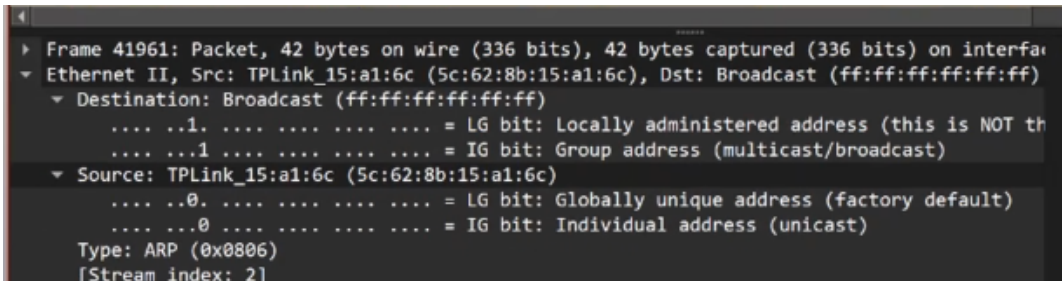
«Who has 192.168.0.101?» от шлюза

MAC назначения: Broadcast (ff:ff:ff:ff:ff:ff)

ARP ответ:

«192.168.0.101 is at c0:bf:be:cf:c4:ce»

MAC назначения: индивидуальный



```
▶ Frame 41961: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface  
▼ Ethernet II, Src: TPLink_15:a1:6c (5c:62:8b:15:a1:6c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
  ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)  
    .... ..1. .... = LG bit: Locally administered address (this is NOT the  
    .... ..1 .... = IG bit: Group address (multicast/broadcast)  
  ▼ Source: TPLink_15:a1:6c (5c:62:8b:15:a1:6c)  
    .... ..0. .... = LG bit: Globally unique address (factory default)  
    .... ..0 .... = IG bit: Individual address (unicast)  
Type: ARP (0x0806)  
[Stream index: 2]
```

9 TCP handshake анализ

Трехэтапное рукопожатие:

Пакет 26: [SYN] - инициация (Seq=0)

Пакет 30: [SYN, ACK] - подтверждение (Seq=0, Ack=1)

Пакет 34: [ACK] - завершение (Seq=1, Ack=1)

No.	Time	Source	Destination	Protocol	Length	Info
26	2.760229	192.168.0.101	192.168.0.1	TCP	66	49703 → 53 [SYN] Seq=0 Win=65535 Len=0 MS
30	2.764080	192.168.0.1	192.168.0.101	TCP	66	53 → 49703 [SYN, ACK] Seq=0 Ack=1 Win=292
34	2.764208	192.168.0.101	192.168.0.1	TCP	54	49703 → 53 [ACK] Seq=1 Ack=1 Win=65280 Le
36	2.764281	192.168.0.101	192.168.0.1	TCP	56	49703 → 53 [PSH, ACK] Seq=1 Ack=1 Win=652
37	2.764328	192.168.0.101	192.168.0.1	DNS	88	Standard query 0x8957 A gator.volces.com
40	2.768452	192.168.0.1	192.168.0.101	TCP	54	53 → 49703 [ACK] Seq=1 Ack=3 Win=29312 Le
41	2.768452	192.168.0.1	192.168.0.101	TCP	54	53 → 49703 [ACK] Seq=1 Ack=37 Win=29312 L
44	2.768452	192.168.0.1	192.168.0.101	DNS	1111	Standard query response 0x8957 A gator.vd
46	2.768733	192.168.0.101	192.168.0.1	TCP	54	49703 → 53 [FIN, ACK] Seq=37 Ack=1058 Win
49	2.772888	192.168.0.1	192.168.0.101	TCP	54	53 → 49703 [FIN, ACK] Seq=1058 Ack=38 Win
51	2.772976	192.168.0.101	192.168.0.1	TCP	54	49703 → 53 [ACK] Seq=38 Ack=1059 Win=6425

Рисунок 6: TCP handshake

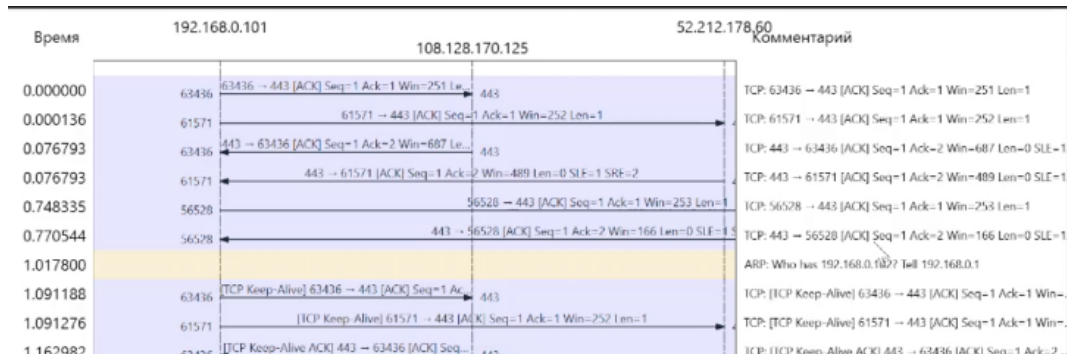
10 График потока TCP

Statistics → Flow Graph → TCP Flow

Наглядно показывает этапы соединения

Видно передачу данных после handshake

Отображение закрытия соединения



11 Сравнение протоколов

Протокол	Уровень	Назначение
ARP	Канальный	Разрешение IP в MAC
ICMP	Сетевой	Диагностика сети
TCP	Транспортный	Надежная передача
UDP	Транспортный	Быстрая передача

12 Ключевые выводы

Wireshark - мощный инструмент анализа трафика

Успешно изучены протоколы канального уровня

Практически подтвержден TCP handshake

Освоены методы фильтрации пакетов

Получены навыки диагностики сетевых соединений