

Лабораторная работа. Использование программы Wireshark для просмотра сетевого трафика

Цель работы:

Научиться собирать и анализировать данные протокола ICMP в программе Wireshark при передаче данных в локальной сети и при передаче данных в удаленную сеть.

Ход работы:

Часть 1. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в локальной сети.

Определим адреса интерфейсов ПК, с помощью команды `ipconfig /all`

```
DNS-суффикс подключения . . . . . :  
Описание. . . . . : Realtek RTL8723DE 802.11b/g/n PCIe Adapter  
Физический адрес. . . . . : D8-C0-A6-20-CC-6B  
DHCP включен. . . . . : Да  
Автонастройка включена. . . . . : Да  
Локальный IPv6-адрес канала . . . : fe80::3d8a:4da4:bb5c:56eb%10(Основной)  
IPv4-адрес. . . . . : 192.168.1.5(Основной)  
Маска подсети . . . . . : 255.255.255.0
```

Предварительно загрузив и установив, запустим программу Wireshark. Выберем интерфейс и убедившись в его правильности запустим захват данных.

Захват из Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
14635	59.535205	99.181.65.178	192.168.1.5	TLSv1.2	861	Application Data
14636	59.535248	192.168.1.5	99.181.65.178	TCP	54	56137 → 443 [ACK] Seq=71874 Ack=11513935 Win=4106 Len=0
14637	59.684832	192.168.1.5	136.243.19.144	TCP	54	56188 → 80 [FIN, ACK] Seq=146 Ack=285 Win=131072 Len=0
14638	59.756355	136.243.19.144	192.168.1.5	TCP	54	80 → 56188 [FIN, ACK] Seq=285 Ack=147 Win=15744 Len=0
14639	59.756473	192.168.1.5	136.243.19.144	TCP	54	56188 → 80 [ACK] Seq=147 Ack=286 Win=131072 Len=0
14640	59.888438	Proizvod_18:d9:7e	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.1
14641	60.062566	192.168.1.5	74.125.131.101	TCP	66	56198 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
14642	60.111042	74.125.131.101	192.168.1.5	TCP	66	443 → 56198 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460

> Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{79FF168E-C98F-4B7D-B3B1-2E03850F6581}, id 0
> Ethernet II, Src: Proizvod_18:d9:7e (f4:e5:78:18:d9:7e), Dst: AzureWav_20:cc:6b (d8:c0:a6:20:cc:6b)
> Internet Protocol Version 4, Src: 99.181.65.178, Dst: 192.168.1.5
> Transmission Control Protocol, Src Port: 443, Dst Port: 56137, Seq: 1, Ack: 1, Len: 27
> Transport Layer Security

0000 d8 c0 a6 20 cc 6b f4 e5 78 18 d9 7e 08 00 45 00k... x...~E.
0010 00 43 26 91 40 00 33 06 ba 0f 63 b5 41 b2 c0 a8 ...-C&@3...cA...
0020 01 05 01 bb db 49 94 80 99 31 b0 69 4d d0 50 18I...1IM.P
0030 00 7e df 56 00 00 17 03 03 00 16 10 5e ab 1e 8c ...~V...{...^...
0040 cc 6b 9f 08 27 7b 71 54 43 42 91 47 1d 56 27 68 ...k...{qT CB.G.V'h
0050 95 .

Беспроводная сеть: <live capture in progress> | Пакеты: 14660 · Показаны: 14660 (100.0%) | Профиль: Default

Применим фильтр для того, чтобы видеть только единицы данных протокола ICMP. Затем отправим ping на IP-адрес другого компьютера.

The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets, filtered for ICMP. The middle pane shows the details of the selected packet (No. 970), including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP Echo (ping) request). The bottom pane shows the raw packet data in hexadecimal and ASCII. Overlaid on the Wireshark window is a Windows Command Prompt window showing the execution of the command 'ping 192.168.1.4'. The output of the command shows four successful replies from 192.168.1.4, each with 32 bytes of data, a TTL of 128, and varying response times (6ms, 6ms, 3ms, 3ms). The Command Prompt also displays the 'Statistics Ping' for 192.168.1.4, indicating 4 packets sent, 4 received, 0% loss, and average response times.

Остановим захват и проанализируем данные.

Выбрав кадр отправки пакета (request) и открыв вкладку Ethernet II и ответим на поставленные вопросы.

Совпадает ли MAC-адрес источника с интерфейсом вашего компьютера? Да

Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого учащегося? Да

Как ваш ПК определил MAC-адрес другого ПК, на который был отправлен эхо-запрос с помощью команды ping? При помощи протокола ARP. Для того, чтобы обмениваться данными по сети Ethernet компьютерам нужно знать MAC адрес друг друга, так как сеть Ethernet не работает с IP-адресами. При запросе компьютер №1 обращается по IP к компьютеру №2, сообщает свой MAC-адрес и запрашивает MAC-адрес компьютера №2.

Часть 2. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в удаленную сеть

Активируем захват данных и отправим эхо-запрос с помощью команды ping на три URL-адреса, указанных веб-сайтов:

- 1) www.yahoo.com
- 2) www.cisco.com
- 3) www.google.com

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Oleg>ping www.yahoo.com

Обмен пакетами с new-fp-shed.wg1.b.yahoo.com [87.248.100.216] с 32 байтами данных:
Ответ от 87.248.100.216: число байт=32 время=105мс TTL=49
Ответ от 87.248.100.216: число байт=32 время=104мс TTL=49
Ответ от 87.248.100.216: число байт=32 время=97мс TTL=49
Ответ от 87.248.100.216: число байт=32 время=104мс TTL=49

Статистика Ping для 87.248.100.216:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 97мсек, Максимальное = 105 мсек, Среднее = 102 мсек

C:\Users\Oleg>ping www.cisco.com

Обмен пакетами с e2867.dsca.akamaiedge.net [23.43.131.231] с 32 байтами данных:
Ответ от 23.43.131.231: число байт=32 время=59мс TTL=48
Ответ от 23.43.131.231: число байт=32 время=67мс TTL=48
Ответ от 23.43.131.231: число байт=32 время=62мс TTL=48
Ответ от 23.43.131.231: число байт=32 время=67мс TTL=48

Статистика Ping для 23.43.131.231:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 59мсек, Максимальное = 67 мсек, Среднее = 63 мсек

C:\Users\Oleg>ping www.google.com

Обмен пакетами с www.google.com [142.251.1.104] с 32 байтами данных:
Ответ от 142.251.1.104: число байт=32 время=55мс TTL=105
Ответ от 142.251.1.104: число байт=32 время=55мс TTL=105
Ответ от 142.251.1.104: число байт=32 время=55мс TTL=105
Ответ от 142.251.1.104: число байт=32 время=55мс TTL=105

Статистика Ping для 142.251.1.104:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 55мсек, Максимальное = 55 мсек, Среднее = 55 мсек

C:\Users\Oleg>
```

Остановим захват данных, проанализируем и ответим на поставленные вопросы:

а. Указать IP- и MAC-адреса для трех веб-сайтов:

- 1) IP: 87.248.100.216 MAC: f4:e5:78:18:d9:7e
- 2) IP: 23.43.131.231 MAC: f4:e5:78:18:d9:7e
- 3) IP: 142.251.1.104 MAC: f4:e5:78:18:d9:7e

б. Какова существенная особенность этих данных?

Все адреса имеют одинаковый MAC-адрес.

с. Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 1?

В первой части показывается MAC-адрес компьютера находящегося в локальной сети, во второй части отображается MAC-адрес сетевого шлюза.

d. Почему программа Wireshark показывает фактические MAC-адреса локальных узлов, но не показывает фактические MAC-адреса удаленных узлов?

Потому что IP-адрес на который отправляется ping находится в другой сети доступ к которой осуществляется через локальный узел.