


ПРЕЗЕНТАЦИЯ ЛАБОРАТОРНОЙ РАБОТЫ №3

Анализ трафика в Wireshark

Сетевые технологии

РаботуВыполнил:
Саинт-АмурИзмаэль
Группа:НПИбд-02-20



Цель работы

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

Чтобы отобразить основную конфигурацию ТСП/IP для всех адаптеров, введите `ipconfig` для ОС

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::c11e:88d1:3100:3f9d%14
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::28fd:ba90:d04a:e2a1%15
    IPv4 Address. . . . . : 192.168.0.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

PS C:\Windows\system32>
```

Отображает полную конфигурацию TCP/IP для всех адаптеров. Адаптеры могут представлять физические интерфейсы, такие как установленные сетевые адаптеры, или логические интерфейсы, такие как подключения удаленного доступа. например, Мас-адрес введите `ipconfig /all` для ОС

```
Administrator: Windows PowerShell
/ Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-DHI06N9
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : rudn.ru


Ethernet adapter Ethernet:

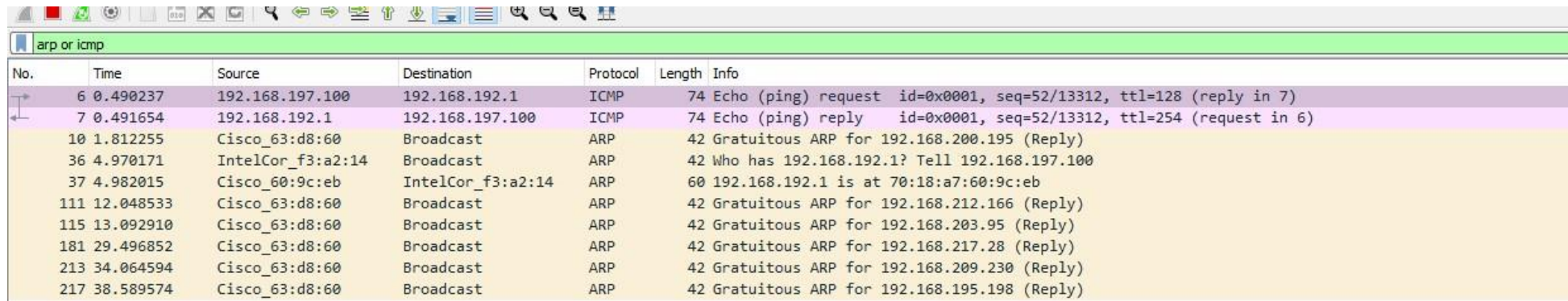
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Ethernet Connection (3) I218-LM
Physical Address. . . . . : F8-CA-B8-3C-33-9B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes


Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-0E
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c11e:88d1:3100:3f9d%14(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 101318695
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-73-CB-2E-F8-CA-B8-3C-33-9B
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled


Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 18-5E-0F-F3-A2-15
DHCP Enabled. . . . . : Yes
```

No.	Time	Source	Destination	Protocol	Length	Info
6	0.490237	192.168.197.100	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=52/13312, ttl=128 (reply in 7)
7	0.491654	192.168.192.1	192.168.197.100	ICMP	74	Echo (ping) reply id=0x0001, seq=52/13312, ttl=254 (request in 6)
10	1.812255	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.200.195 (Reply)
36	4.970171	IntelCor_f3:a2:14	Broadcast	ARP	42	Who has 192.168.192.1? Tell 192.168.197.100
37	4.982015	Cisco_60:9c:eb	IntelCor_f3:a2:14	ARP	60	192.168.192.1 is at 70:18:a7:60:9c:eb
111	12.048533	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.212.166 (Reply)
115	13.092910	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.203.95 (Reply)
181	29.496852	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.217.28 (Reply)
213	34.064594	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.209.230 (Reply)
217	38.589574	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.195.198 (Reply)

Установим на домашнем устройстве Wireshark.

о потом с помощью Wireshark захватим и проанализируем пакеты ARP и ICMP в части кадров канального уровня.

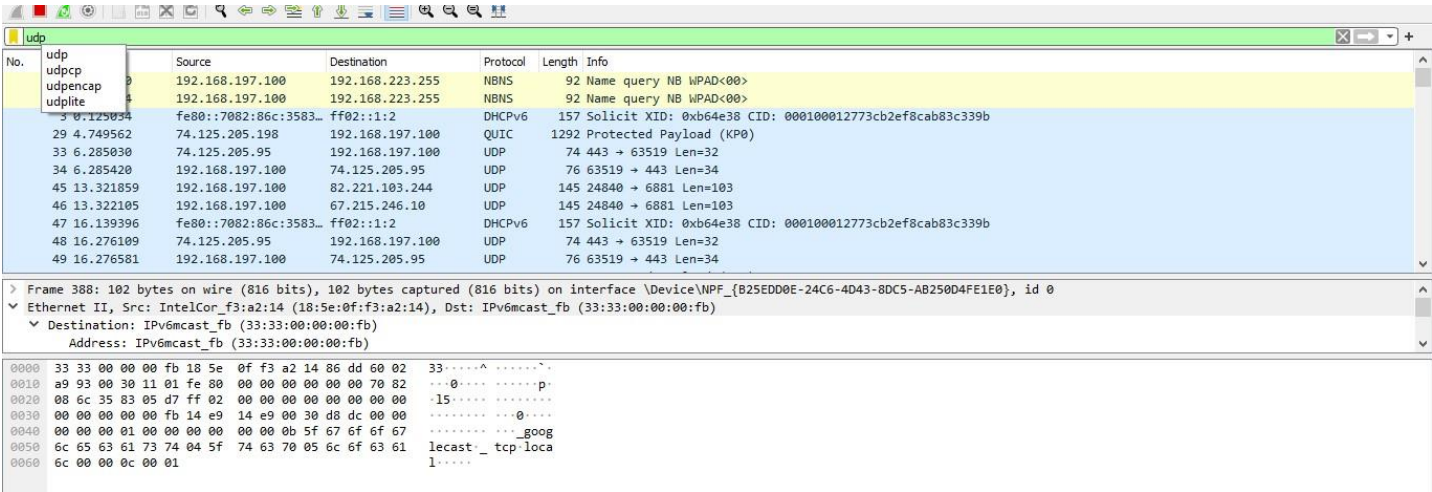
На вашем устройстве в консоли с помощью команды `ping` адрес_шлюза
пропингуйте шлюз по умолчанию,
чтобы знать адрес_шлюза
Запустите консоль с помощью команды `ipconfig` для
типа операционной системы Windows

```
Default gateway : . . . . . 192.168.192.1
PS C:\Windows\system32> ping 192.168.192.1

Pinging 192.168.192.1 with 32 bytes of data:
Reply from 192.168.192.1: bytes=32 time=2ms TTL=254
Reply from 192.168.192.1: bytes=32 time=1ms TTL=254
Reply from 192.168.192.1: bytes=32 time=2ms TTL=254
Reply from 192.168.192.1: bytes=32 time=3ms TTL=254

Ping statistics for 192.168.192.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms
PS C:\Windows\system32>
```

С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC.





ВЫВОДЫ

В этой статье мы рассмотрели, как пользоваться Wireshark для анализа сетевого трафика, а также примеры решения проблем с сетью. Это очень мощная утилита, которая имеет очень много функций.