Российский университет дружбы народов

Лабораторная работа №3

АНАЛИЗ ТРАФИКА В WIRESHARK

Российский университет дружбы народов

- Титульная страница
- Структура
- Представление выступающего
- Прагматика
- Цель выполнения лаб. работы
- Задача выполнения лаб. работы
- Результат выполнения лаб. работы

Российский университет дружбы народов

Выполнил: Юсупов Шухратджон Фирдавсович
Факультет: Физико-математических и естественных наук
Направление: Прикладная информатика (09.03.03)
Группа: НПИбд-02-20
Ст. Номер: 1032205329
Почта Outlook: 1032205329@rudn.ru

Цель:

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

```
C:\Users\user>ipconfig

Настройка протокола IP для Windows


Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::10b2:f593:3336:c7cd%17
   IPv4-адрес. . . . . . . . . . . . : 172.16.16.138
   Маска подсети . . . . . . . . . . : 255.255.254.0
   Основной шлюз. . . . . . . . . . : 172.16.16.1

C:\Users\user>
```

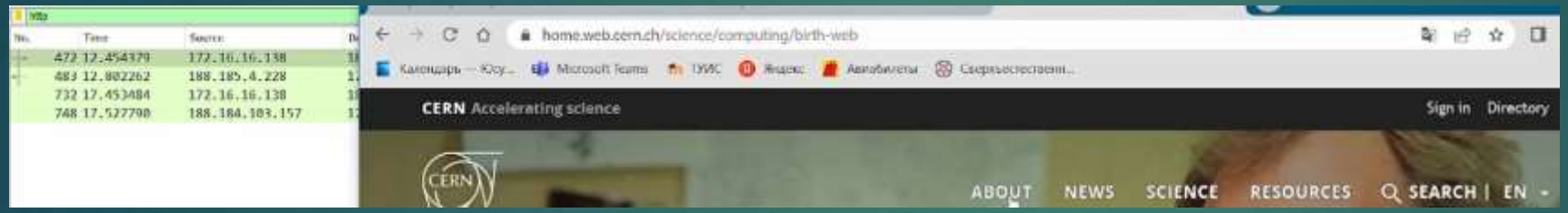
```
C:\Users\user>ping 172.16.16.1

Обмен пакетами с 172.16.16.1 по с 32 байтами данных:
Ответ от 172.16.16.1: число байт=32 время=8мс TTL=254
Ответ от 172.16.16.1: число байт=32 время=2мс TTL=254
Ответ от 172.16.16.1: число байт=32 время=2мс TTL=254
Ответ от 172.16.16.1: число байт=32 время=2мс TTL=254

Статистика Ping для 172.16.16.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 8 мсек, Среднее = 3 мсек

C:\Users\user>
```

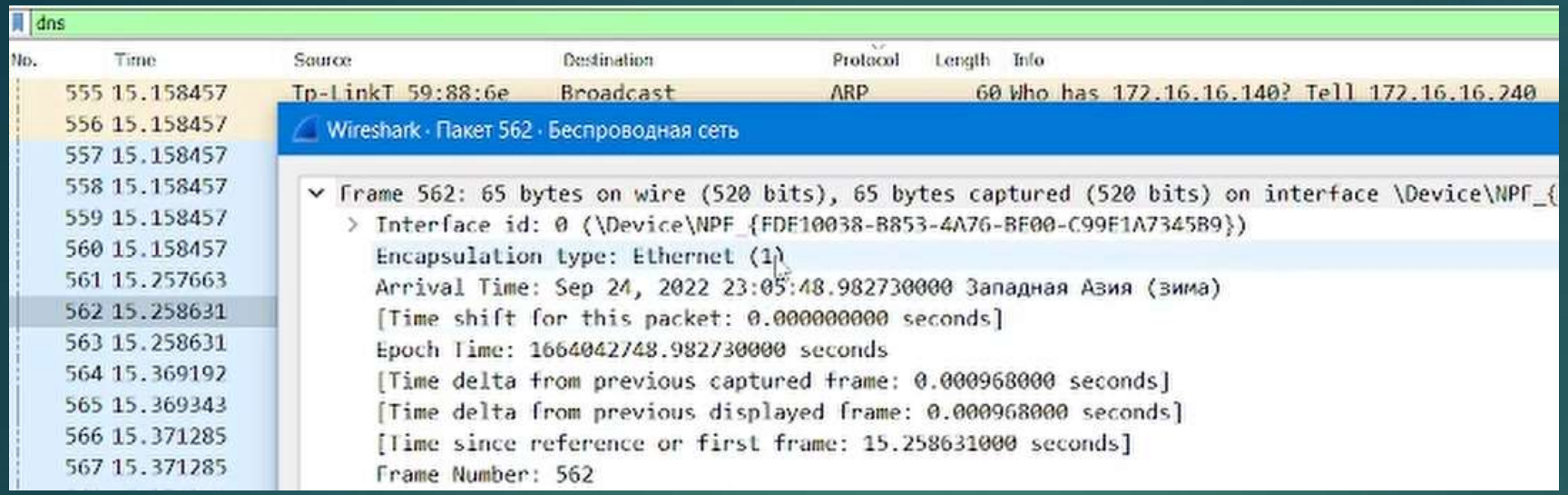
arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
1189	22.959238	172.16.16.1	172.16.16.138	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=254 (request in 1188)
1261	23.969940	172.16.16.138	172.16.16.1	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 1262)
1262	23.972720	172.16.16.1	172.16.16.138	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=254 (request in 1261)
1348	26.318852	Cisco_60:9c:c5	Broadcast	ARP	60	Who has 172.16.16.250? Tell 172.16.16.1
1528	30.008145	Apple_e3:a1:9c	Broadcast	ARP	60	Who has 172.16.17.5? Tell 172.16.16.42
1529	30.008145	IntelCor_e6:91:aa	Broadcast	ARP	60	Who has 172.16.16.1? Tell 172.16.16.68

```
> Frame 1262: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Devic
v Ethernet II, Src: Cisco_60:9c:c5 (70:18:a7:60:9c:c5), Dst: IntelCor_9e:6d:35 (0c:9a:3c:9e
  v Destination: IntelCor_9e:6d:35 (0c:9a:3c:9e:6d:35)
      Address: IntelCor_9e:6d:35 (0c:9a:3c:9e:6d:35)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: Cisco_60:9c:c5 (70:18:a7:60:9c:c5)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.16.16.1, Dst: 172.16.16.138
> Internet Control Message Protocol
```

```
> Frame 3184: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\
v Ethernet II, Src: 6a:d5:17:20:f8:8f (6a:d5:17:20:f8:8f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: 6a:d5:17:20:f8:8f (6a:d5:17:20:f8:8f)
      Address: 6a:d5:17:20:f8:8f (6a:d5:17:20:f8:8f)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
> Address Resolution Protocol (request)
```




dns
No. Time Source Destination Protocol Length Info
555 15.158457 Tp-LinkT_59:88:6e Broadcast ARP 60 Who has 172.16.16.140? Tell 172.16.16.240
556 15.158457
557 15.158457
558 15.158457
559 15.158457
560 15.158457
561 15.257663
562 15.258631
563 15.258631
564 15.369192
565 15.369343
566 15.371285
567 15.371285
Wireshark · Пакет 562 · Беспроводная сеть
Frame 562: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface \Device\NPF_{
Interface id: 0 (\Device\NPF_{FDF10038-B853-4A76-BF00-C99F1A7345B9})
Encapsulation type: Ethernet (1)
Arrival Time: Sep 24, 2022 23:05:48.982730000 Западная Азия (зима)
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1664042748.982730000 seconds
[Time delta from previous captured frame: 0.000968000 seconds]
[Time delta from previous displayed frame: 0.000968000 seconds]
[Time since reference or first frame: 15.258631000 seconds]
Frame Number: 562