

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет Программной Инженерии и Компьютерной Техники

Компьютерные сети

Лабораторная работа № 4

«Работа с сетевым анализатором»

Выполнила студентка

Борисова Анастасия Денисовна

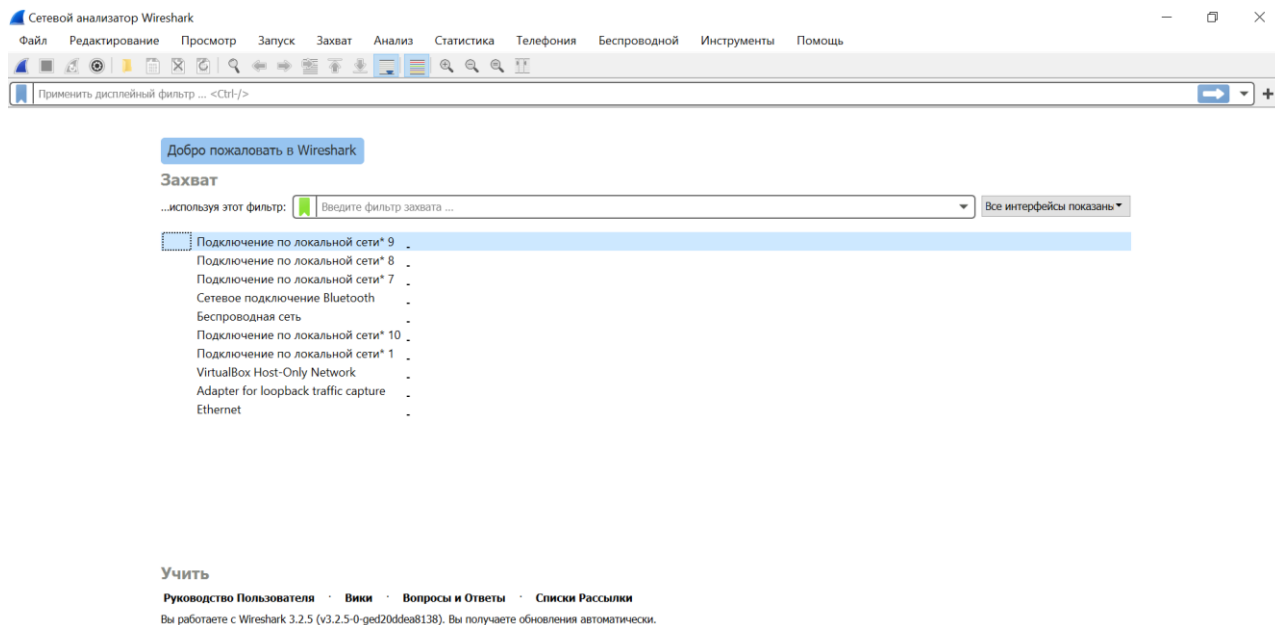
Группа № Р33222

Преподаватель: Маркина Татьяна Анатольевна

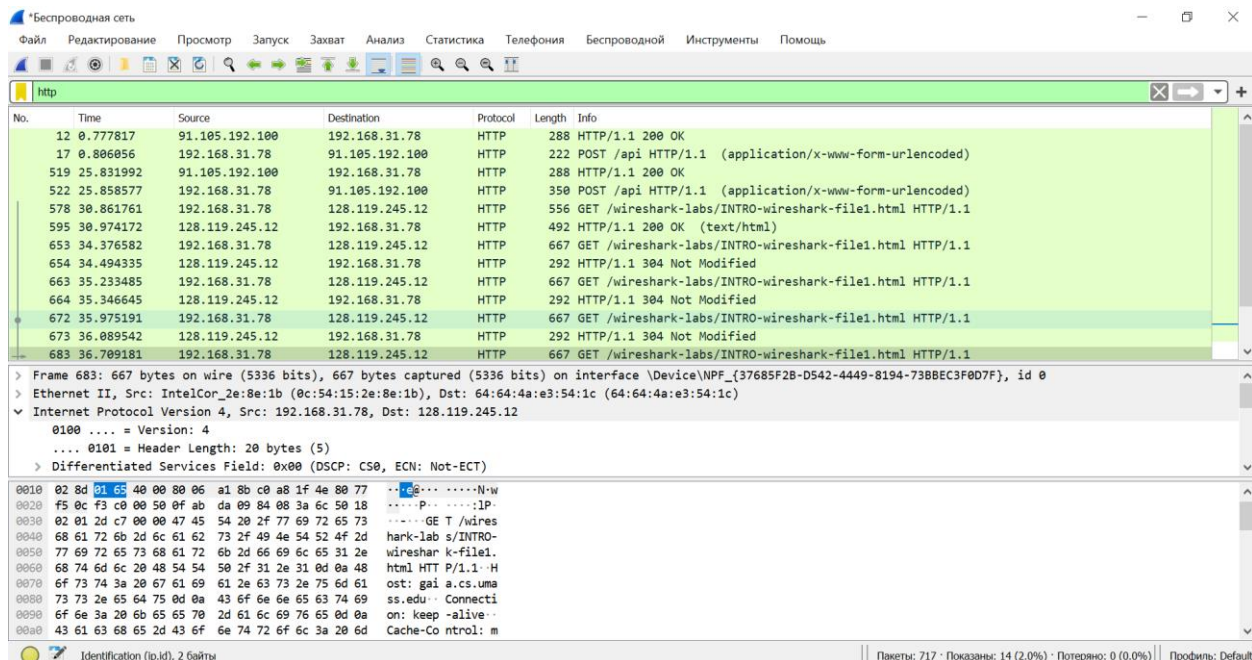
г. Санкт-Петербург

2023

Установила и запустила Wireshark:



После выбора интересующего интерфейса сделала захват пакетов. Для получения необходимого пакета, необходимо перейти в браузере по ссылке <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>. Затем в окне спецификации фильтра отображения в верхней части главного окна Wireshark необходимо ввести «http» и нажать кнопку «Применить» - это приведет к тому, что в списке пакетов будет отображаться только сообщение HTTP:



Для запуска nslookup на Windows я открыла командную строку и запустила nslookup в командной строке:

```
Командная строка - nslookup
Microsoft Windows [Version 10.0.19044.2728]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\nastya>nslookup
ѠѠѠѠ ѠѠ ѠѠѠѠѠѠѠѠ: XiaoQiang
Address: 192.168.31.1

> exit
```

Получила IP-адрес веб-сервера:

```
C:\Users\nastya>nslookup spbu.ru
ѠѠѠѠѠѠѠѠ: XiaoQiang
Address: 192.168.31.1

Не заслуживающий доверия ответ:
ѠѠѠѠ : spbu.ru
Address: 81.89.183.222

C:\Users\nastya>
```

Получила имя и IP-адрес DNS-сервера:

```

C:\Users\nastya>nslookup -type=NS www.spbu.ru
ТхЁтхЁ: XiaoQiang
Address: 192.168.31.1

Не заслуживающий доверия ответ:
www.spbu.ru canonical name = spbu.ru
spbu.ru nameserver = ns2.pu.ru
spbu.ru nameserver = ns.pu.ru

ns.pu.ru internet address = 195.70.196.219
ns2.pu.ru internet address = 195.70.196.210

C:\Users\nastya>nslookup -type=NS spbu.ru
ТхЁтхЁ: XiaoQiang
Address: 192.168.31.1

Не заслуживающий доверия ответ:
spbu.ru nameserver = ns2.pu.ru
spbu.ru nameserver = ns.pu.ru

ns.pu.ru internet address = 195.70.196.219
ns2.pu.ru internet address = 195.70.196.210

C:\Users\nastya>_

```

Отправила запрос на DNS-сервер, так происходит транзакция запроса и ответа происходит непосредственно между нашим запрашивающим хостом и DNS-сервер:

```

C:\Users\nastya>nslookup www.spbu.ru dns.XiaoQiang
ТхЁтхЁ: XiaoQiang
Address: 192.168.31.1

Не заслуживающий доверия ответ:
Ль : spbu.ru
Address: 81.89.183.222
Aliases: www.spbu.ru

```

Сделала запрос почтовых серверов DNS-сервером:

```
C:\Users\nastya>nslookup -type=mx spbu.ru
```

```
ТхЁтхЁ: XiaoQiang
```

```
Address: 192.168.31.1
```


Не заслуживающий доверия ответ:

```
spbu.ru MX preference = 5, mail exchanger = ksmg.pu.ru
```

```
spbu.ru MX preference = 10, mail exchanger = ironport2.pu.ru
```

```
C:\Users\nastya>_
```

Получила информацию об отображении моей текущей информации TCP / IP:

 Командная строка

```
C:\Users\nastya>ipconfig /all
```

Настройка протокола IP для Windows

Имя компьютера : DESKTOP-N09T5D7

Основной DNS-суффикс :

Тип узла. : Гибридный

IP-маршрутизация включена : Нет

WINS-прокси включен : Нет

Адаптер Ethernet Ethernet:

Состояние среды. : Среда передачи недоступна.

DNS-суффикс подключения :

Описание. : Intel(R) Ethernet Connection (4) I219-V

Физический адрес. : B4-B6-86-89-A1-07

DHCP включен. : Да

Автонастройка включена. : Да

Адаптер Ethernet VirtualBox Host-Only Network:

DNS-суффикс подключения :

Описание. : VirtualBox Host-Only Ethernet Adapter

Физический адрес. : 0A-00-27-00-00-0E

DHCP включен. : Нет

Автонастройка включена. : Да

Локальный IPv6-адрес канала . . . : fe80::1cae:bb0d:b01a:db1a%14(Основной)

IPv4-адрес. : 192.168.56.1(Основной)

Маска подсети : 255.255.255.0

Основной шлюз. :

IAID DHCPv6 : 688521255

DUID клиента DHCPv6 : 00-01-00-01-29-C6-79-E5-B4-B6-86-89-A1-07

DNS-серверы. : fec0:0:0:ffff::1%1

fec0:0:0:ffff::2%1

fec0:0:0:ffff::3%1

NetBios через TCP/IP. : Включен

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

Состояние среды. : Среда передачи недоступна.

DNS-суффикс подключения :

Посмотрела оставшееся время жизни (TTL) в секундах:

C:\. Командная строка

```
C:\Users\nastya>ipconfig /displaydns
```

Настройка протокола IP для Windows

api.browser.yandex.ru

Имя записи. : api.browser.yandex.ru

Тип записи. : 1

Срок жизни. : 57

Длина данных. : 4

Раздел. : Ответ

А-запись (узла) . . . : 213.180.193.234

play.google.com

Имя записи. : play.google.com

Тип записи. : 1

Срок жизни. : 65

Длина данных. : 4

Раздел. : Ответ

А-запись (узла) . . . : 64.233.164.101

Имя записи. : play.google.com

Тип записи. : 1

Срок жизни. : 65

Длина данных. : 4

Раздел. : Ответ

А-запись (узла) . . . : 64.233.164.138

Имя записи. : play.google.com

Тип записи. : 1

Срок жизни. : 65

Длина данных. : 4

Раздел. : Ответ

А-запись (узла) . . . : 64.233.164.139

Очистила кеш и перезагрузила записи из файла hosts:

```
C:\Users\nastya>ipconfig /flushdns
```

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.

Wireshark ввела в фильтр свой IP-адрес и запустила захват пакетов, посетила веб-страницу и остановила захват пакетов. Посмотрела сообщение DNS-запроса:

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Беспроводная сеть', 'Файл', 'Редактирование', 'Просмотр', 'Запуск', 'Захват', 'Анализ', 'Статистика', 'Телефония', 'Беспроводной', 'Инструменты', and 'Помощь'. The toolbar contains icons for various functions. The main display area is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is 1464, which is a TCP segment of a reassembly.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII.

Below the main display area, there is a status bar showing the number of packets (3014) and the percentage of packets shown (91.2%).