

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»  
Обнинский институт атомной энергетики  
Отделение интеллектуальных кибернетических систем

**Лабораторная работа №2**

по курсу «Информационные сети»

на тему «Исследование структуры сетевых пакетов с помощью  
анализатора трафика Wireshark»

Вариант №8 — FTP.

Подписи:

Исполнитель

студент гр. ИС-Б17

\_\_\_\_\_

В. Ю. Петренко

Принял

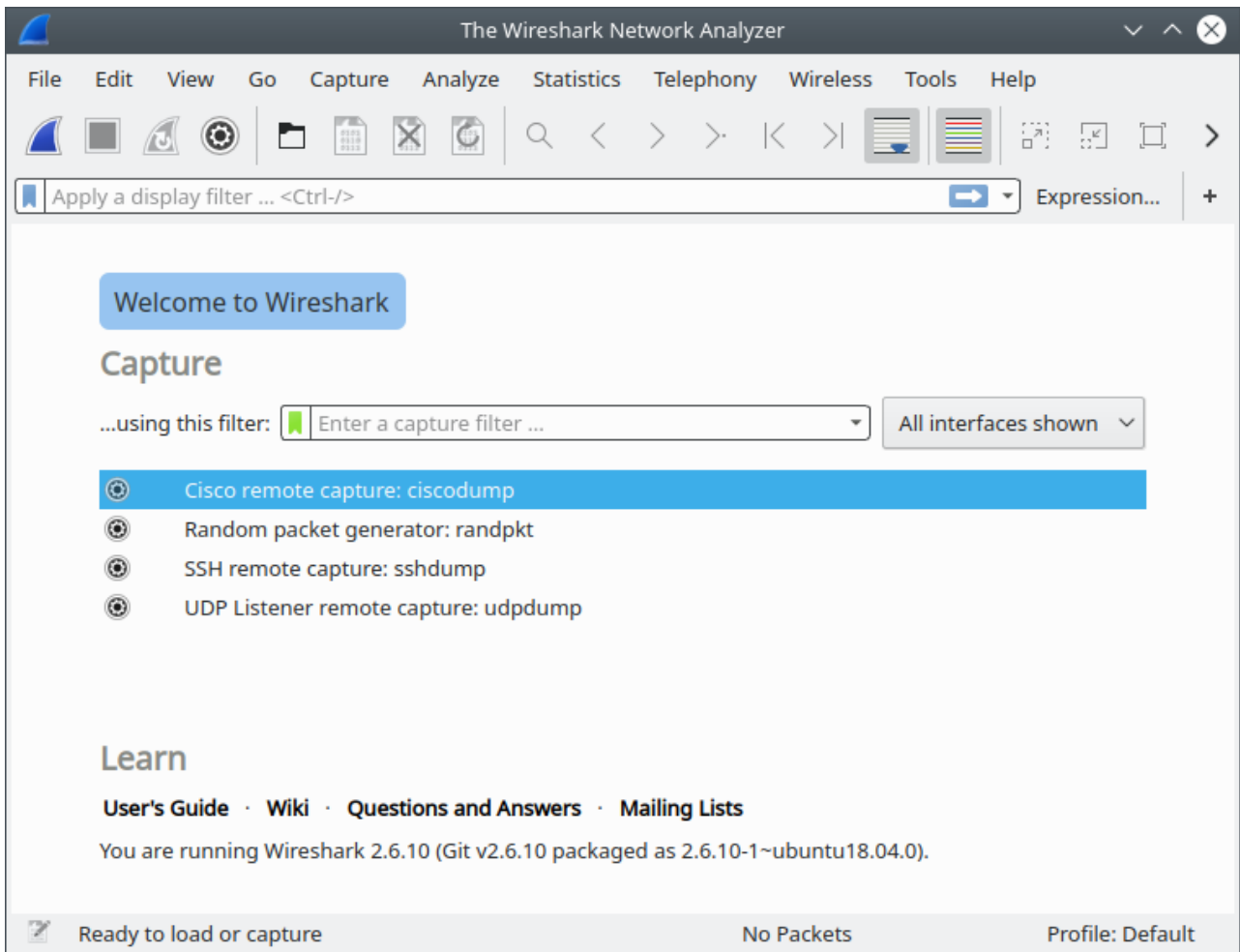
старший преподаватель

\_\_\_\_\_

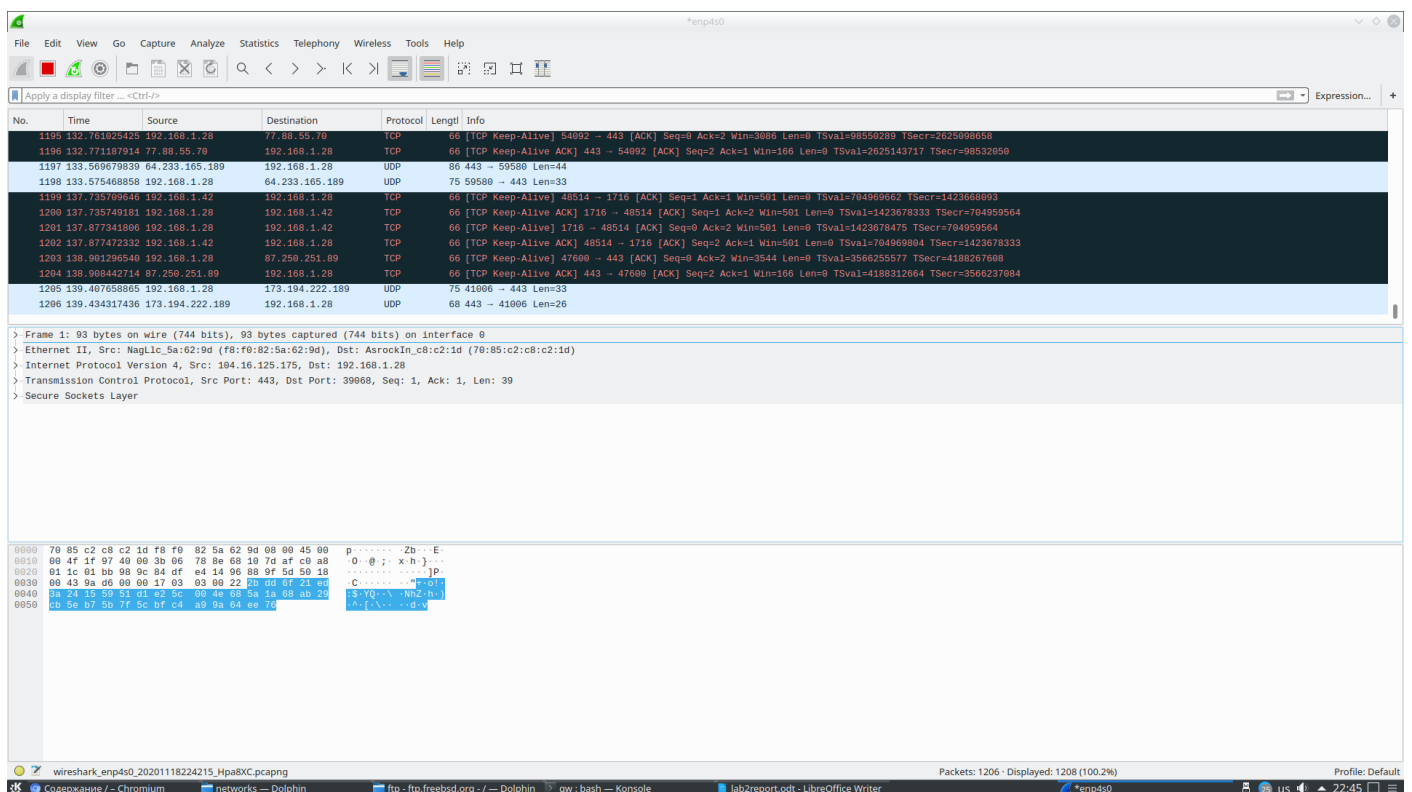
И. В. Охрименко

Обнинск, 2020

## 1) Запустить Wireshark



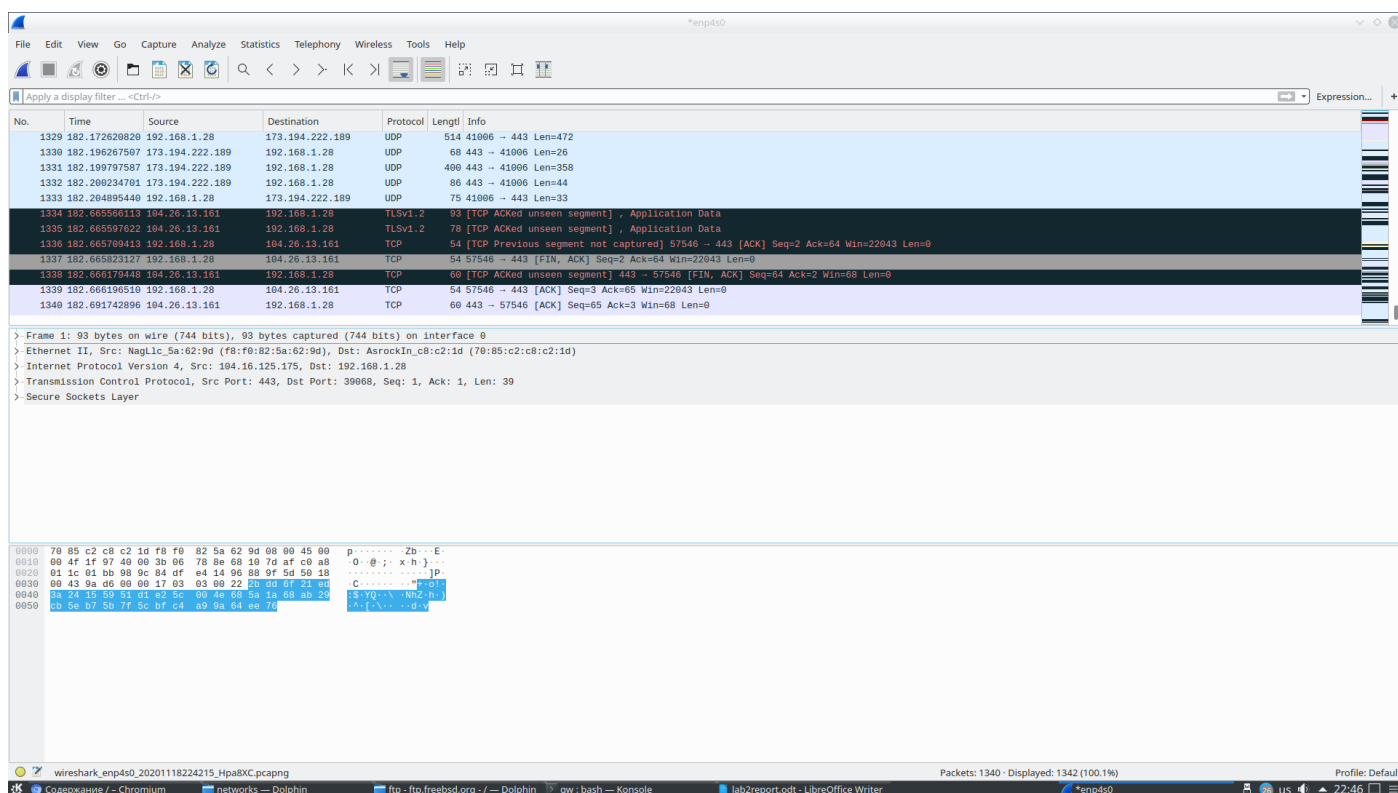
## 2) запустить процесс захвата трафика



3) скачать файл с FTP-сервера (например, <ftp://ftp.freebsd.org/>)

ftp: ftp.freebsd.org	
Имя	Дата изменен
pub	19.07.14 0:00
FreeBSD	18.11.20 19:30
development	18.11.20 19:30
doc	12.11.17 0:00
ports	12.11.17 0:00
releases	18.11.20 19:30
snapshots	12.11.20 15:55
dir.sizes	18.11.20 10:00
README.TXT	07.05.15 0:00
TIMESTAMP	18.11.20 19:30
favicon.ico	19.07.14 0:00
index.html	24.11.14 0:00

4) остановить захват трафика



Захваченный трафик сохранен в ftp+ftp-data.pcapng.

5) настроить фильтр (ftp || ftp-data)

Wireshark capture of an FTP session. The packet list shows an FTP session with various commands and responses. Packet 258 is selected, showing details of an FTP response. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
258	76.495942150	213.138.116.78	192.168.1.28	FTP	127	Response: 220 This is ftp0.bme.freebsd.org - hosted at Bytemark.co.uk
260	76.566817823	192.168.1.28	213.138.116.78	FTP	82	Request: USER anonymous
261	76.633340039	213.138.116.78	192.168.1.28	FTP	100	Response: 331 Please specify the password.
263	76.633492276	192.168.1.28	213.138.116.78	FTP	83	Request: PASS anonymous@
264	76.702976556	213.138.116.78	192.168.1.28	FTP	72	Response: 230-
266	76.703140525	213.138.116.78	192.168.1.28	FTP	132	Response: 230-This is ftp0.bme.FreeBSD.org, graciously hosted by Bytemark.
268	76.703522586	213.138.116.78	192.168.1.28	FTP	72	Response: 230-
270	76.704359814	213.138.116.78	192.168.1.28	FTP	129	Response: 230-FreeBSD files can be found in the /pub/FreeBSD directory.
272	76.704974273	213.138.116.78	192.168.1.28	FTP	72	Response: 230-
274	76.705244312	213.138.116.78	192.168.1.28	FTP	89	Response: 230 Login successful.
276	76.705358217	192.168.1.28	213.138.116.78	FTP	72	Request: SYST

Frame 258: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0  
 Ethernet II, Src: NagLlc\_5a:62:9d (f8:f0:82:5a:62:9d), Dst: AsrockIn\_c8:c2:1d (70:85:c2:c8:c2:1d)  
 Internet Protocol Version 4, Src: 213.138.116.78, Dst: 192.168.1.28  
 Transmission Control Protocol, Src Port: 21, Dst Port: 45224, Seq: 1, Ack: 1, Len: 61  
 File Transfer Protocol (FTP)  
 [Current working directory: ]

0000 70 85 c2 c8 c2 1d f8 f0 82 5a 62 9d 08 00 45 00 p.....Zb...E  
 0010 00 71 00 00 40 00 32 06 3c ea d5 8a 74 4e c0 a8 q...@.2.<...tN..  
 0020 01 1c 00 15 b0 a8 33 8a 5b ca 20 67 e4 53 80 18 .....3...g.S..  
 0030 02 00 72 c4 00 00 01 01 08 0a d7 04 bf b6 21 45 .....!E  
 0040 fc 01 32 32 30 20 54 68 69 73 20 69 73 20 66 74 ..220 Th is is ft  
 0050 70 30 2e 62 6d 65 2e 66 72 65 65 62 73 64 2e 6f p0.bme.f reebsd.o  
 0060 72 67 20 2d 20 68 6f 73 74 65 64 20 61 74 20 42 rg - hos ted at B  
 0070 79 74 65 6d 61 72 6b 2e 63 6f 2e 75 6b 0d 0a ytemark. co.uk..

Вопросы:

1. Сколько байт данных содержится в пакете FTP-DATA?

Ответ: 20.

2. Укажите IP-адреса FTP-сервера и вашего компьютера.

Ответ: IP-адрес ПК — 192.168.1.28, FTP-сервера 212.138.116.78.

3. Укажите MAC-адрес FTP-сервера.

Ответ: f8:f0:82:5a:62:9d.

4. Укажите протокол транспортного уровня, который использует протокол FTP.

Ответ: TCP.

5. Укажите порт, который используется при передаче данных по протоколу FTP.

Ответ: 21.

6. Поясните, чем отличаются пакеты FTP и FTP-DATA.

Ответ: Процесс, использующий TCP, определяется числом - номером порта (сокета). Номер порта для ftp data=20, используется для передачи данных по протоколу ftp; для ftp=21, используется для передачи управляющих команд по протоколу ftp.