МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет прикладной математики и информатики

Кафедра ТПИ

Дисциплина: «Сетевые информационные технологии»

Лабораторная работа №2

АНАЛИЗ ТРАФИКА КОМПЬЮТЕРНОЙ СЕТИ

Факультет: ФПМИ

Группа: ПМИМ-31

Студенты: Тарулин М. А., Холодова В.С.

Преподаватель: Кобылянский В.Г.

Дата выполнения:

Отметка о защите:

Новосибирск, 2024 г.

1. Цель работы

Целями работы является изучение программного обеспечения, предназначенного для контроля и анализа сетевого трафика, а также получение практических навыков работы с программой WireShark.

2. Задание

2.1. Запустить захват сетевого трафика в WireShark, проходящего через интерфейс, подключенный к локальной или внешней сети. Эмулировать сетевую активность в течение 10 минут выполнением указанных действий:

- посетить различные сайты, просмотреть текстовый и видеоконтент;
- выполнить пинг и трассировку любых узлов сети Интернет;
- с помощью браузера подключиться к серверу ftp.intel.com и скачать из корневого каталога файл readme.txt;
- отключить перехват и сохранить сеанс в файле с расширением .pcapng.

2.2. Выполнить фильтрацию трафика по протоколам HTTP, ICMP, ARP, FTP. Для FTP выполнить перехват команд и данных.

2.3.Заполнить таблицу используя данные из отчета Статистика/Свойства файла. При заполнении таблицы обратите внимание на соблюдение размерности величин (Кбайт, Мбайт, Мбит).

2.4. По данным отчета Статистика/Иерархия Протоколов заполнить таблицу распределения трафика по протоколам и сделать выводы о соотношении прикладных и служебных протоколов.

2.5. Заполнить таблицу 2.4 распределения Ethernet-трафика по узлам сети. Исходные данные для заполнения таблицы получить из отчета Статистика/Конечные точки. Определить, какие из узлов наиболее загружены с учетом направления трафика (исходящий, входящий, общий).

2.6. По данным табл. 2.2 определить относительную загрузку сети (в %) за контрольный период времени по формуле:

$$Загрузка = \frac{(Трафик, Мбит / Время, сек) \cdot 100}{(Пропускная\ способность, Мбит / сек)}$$

3. Ход работы

3.1. Запустим захват сетевого трафика в WireShark. Совершим эмуляцию сетевой активности в течении 10 минут.

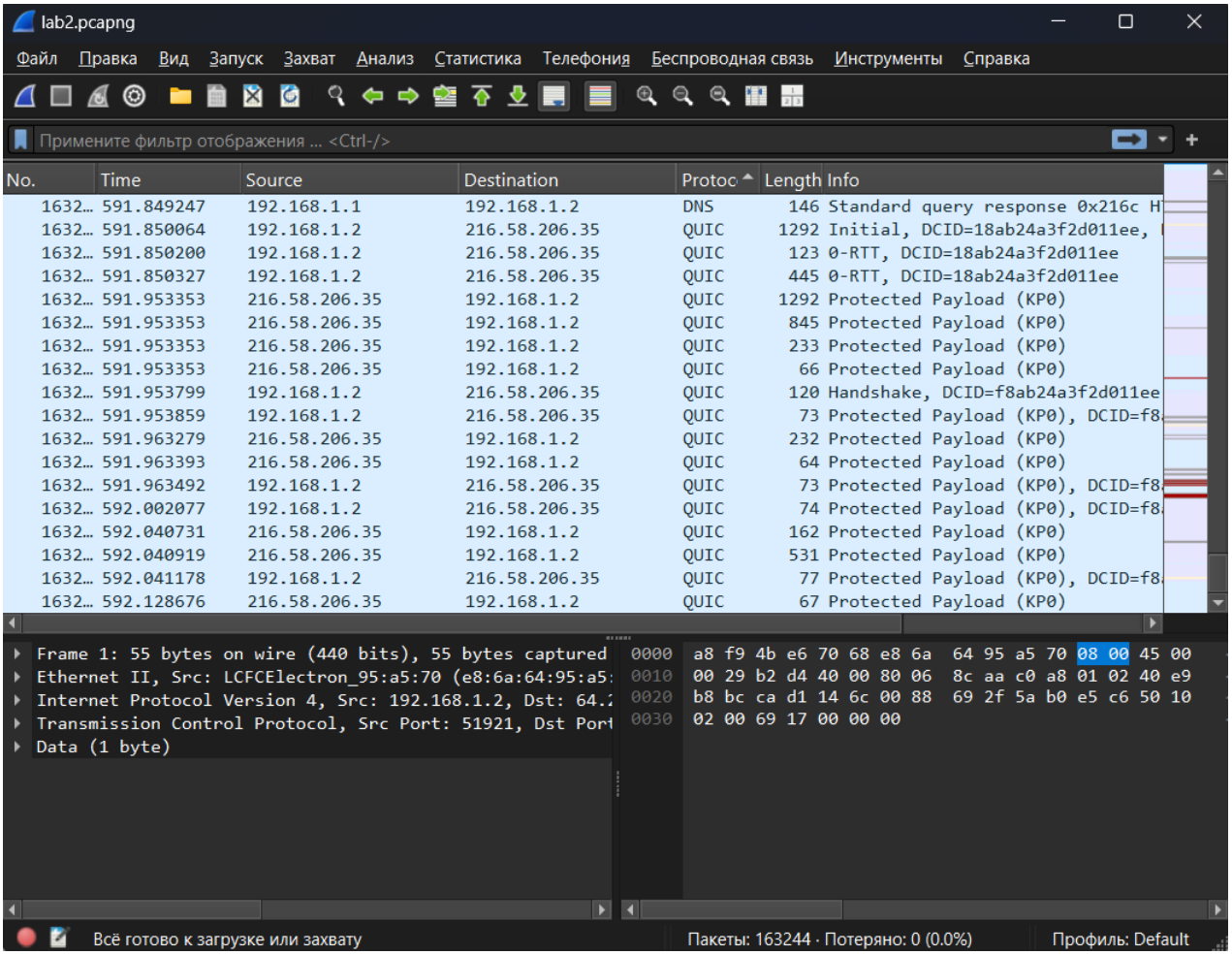

Рисунок 1 – Захват сетевого трафика в WireShark.

3.2. Выполним фильтрацию трафика по протоколам HTTP, ICMP, ARP, FTP. Для FTP выполнить перехват команд и данных.

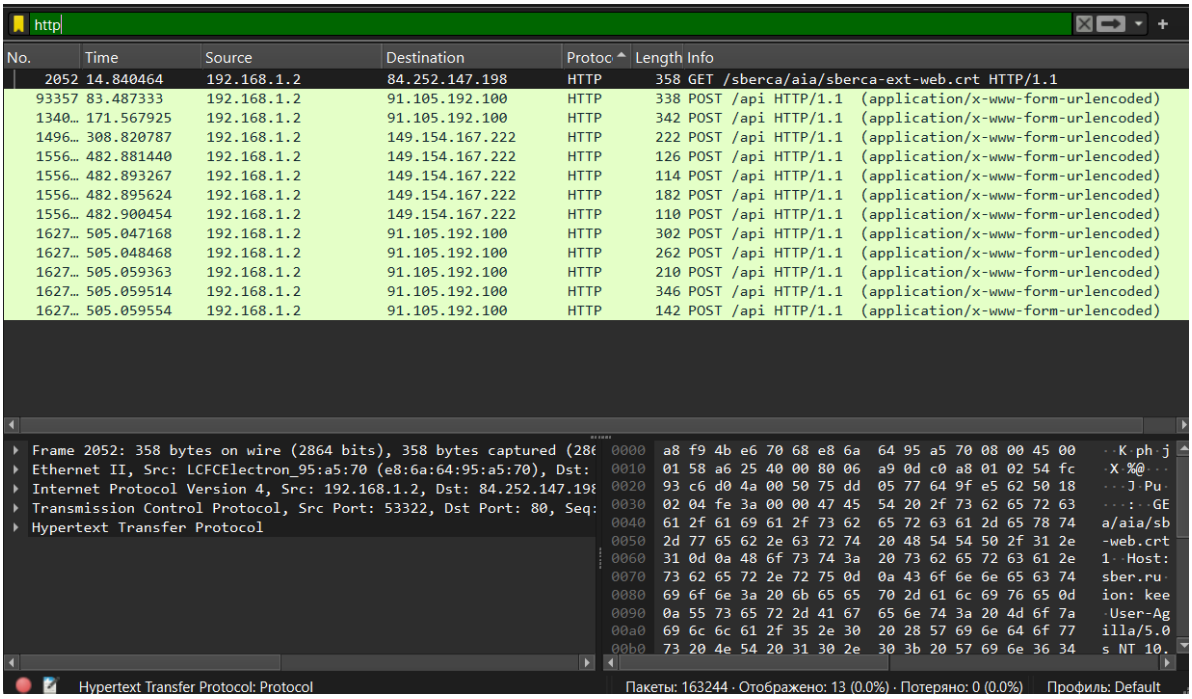

Рисунок 2.1 – Фильтрация трафика по протоколу HTTP.

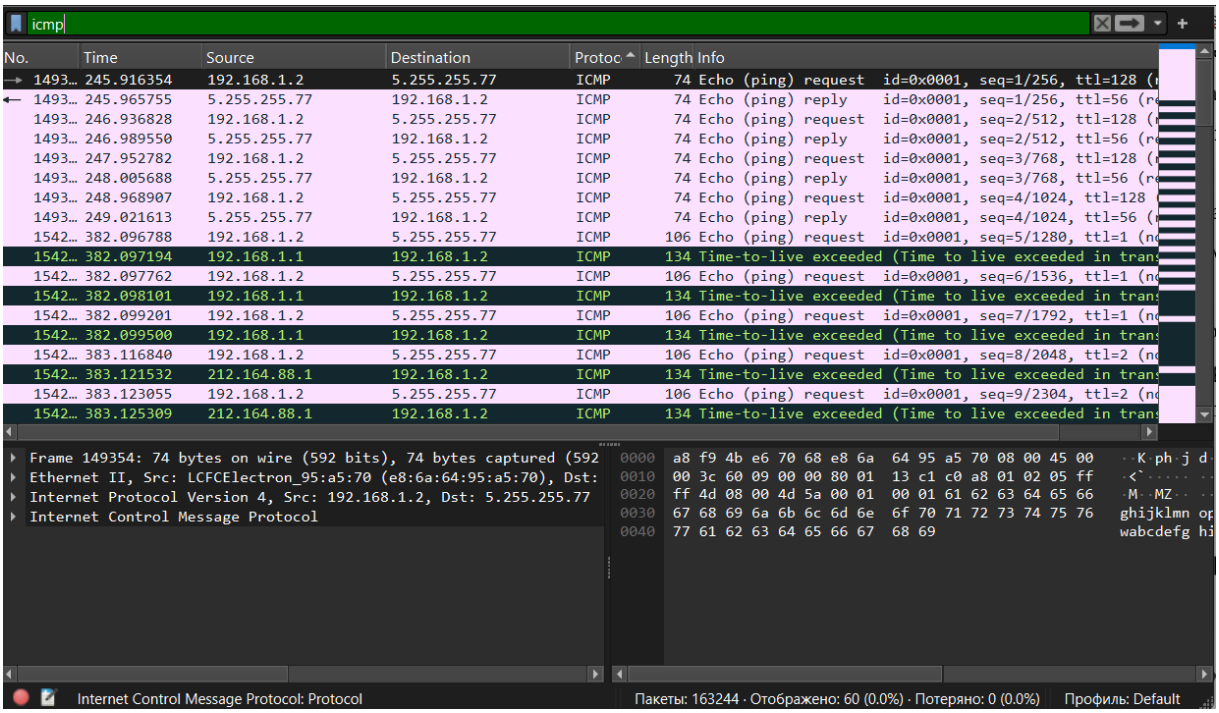

Рисунок 2.2 – Фильтрация трафика по протоколу ICMP.

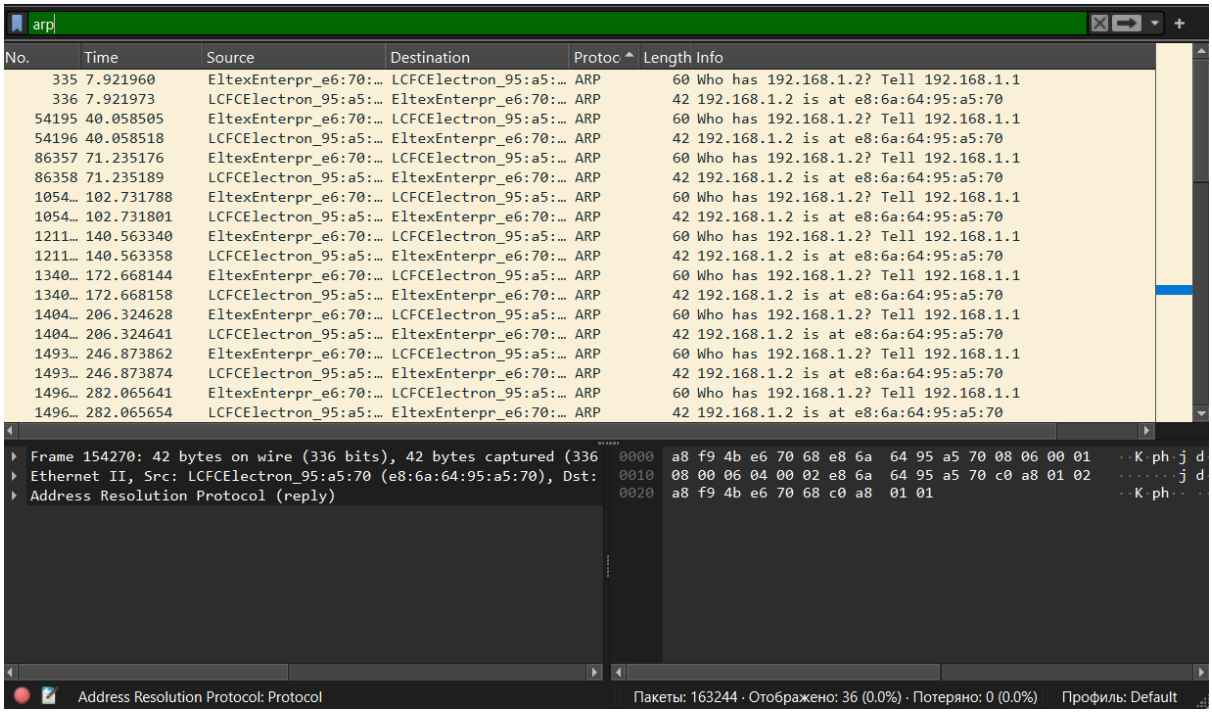

Рисунок 2.3 – Фильтрация трафика по протоколу ARP.

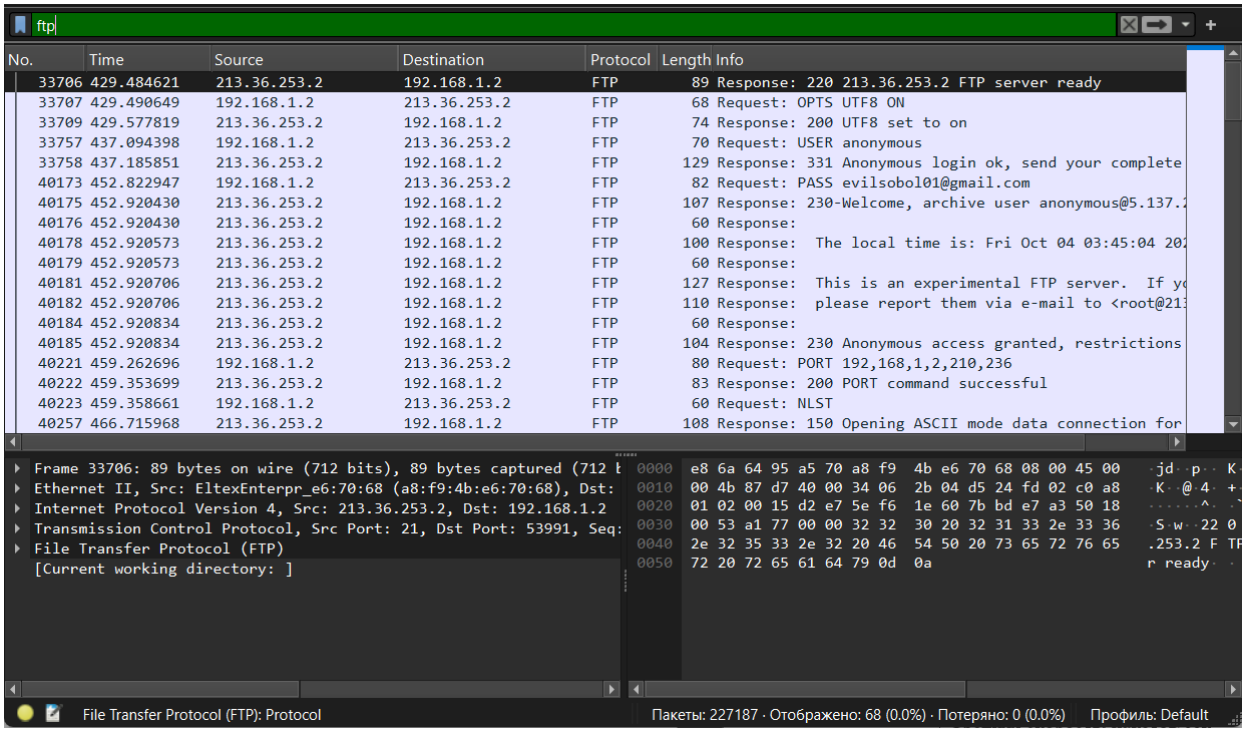

Рисунок 2.4 – Фильтрация трафика по протоколу FTP.

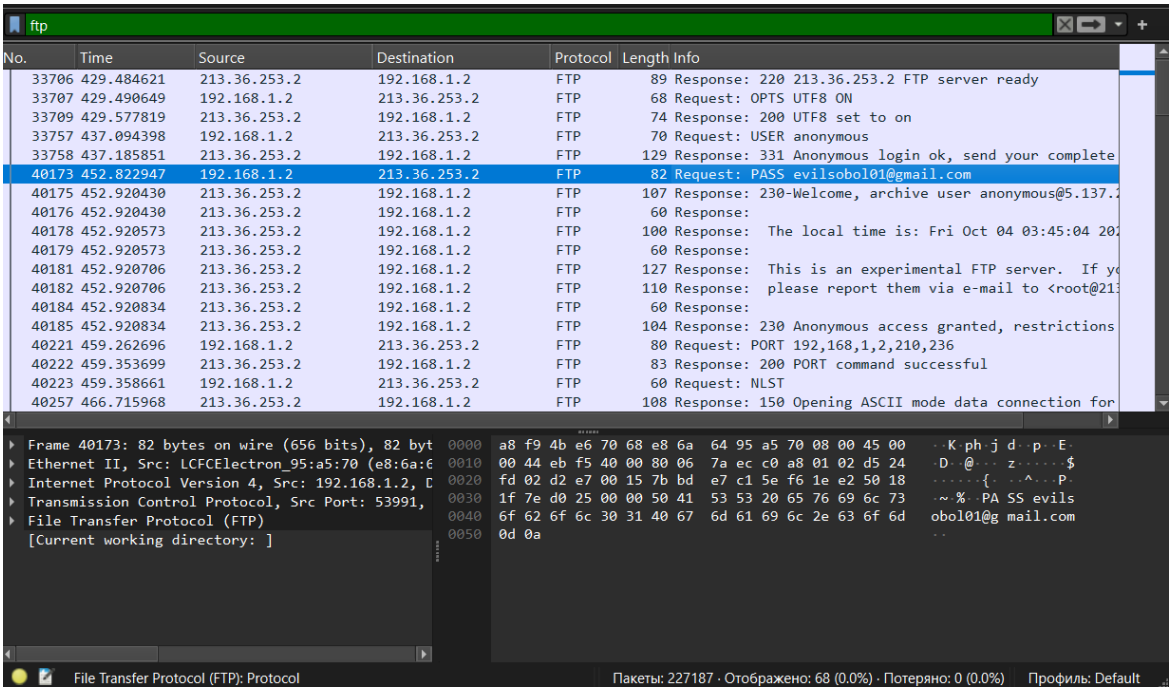

Рисунок 2.5 – Перехват команд и данных по протоколу FTP.

3.3. Заполним таблицу используя данные из отчета Статистика/Свойства файла.

Таблица 1.

Параметр	Значение
Время захвата, мин	8,1
К-во захваченных пакетов	73194
Объем трафика, Мбайт	70,5
Средний размер пакета, Кбайт	0,969
Средняя скорость, пакетов/сек	150,5
Средняя скорость, Мбит/сек	1,166

3.4. По данным отчета Статистика/Иерархия Протоколов заполним таблицу распределения трафика по протоколам.

Таблица 2.

Протокол	Трафик, Мбайт	Трафик, %
IPV6 UDP	0,000296	0,1
IPV4 UDP	0,012744	2,2
TCP	1,45	97,6
ICMP	0,004376	0.1
IGMP	0,000176	>0.1

Итого	1,462	100

Подавляющее большинство трафика приходится на прикладные протоколы (более 98%). Служебные протоколы занимают менее 2% общего объема трафика.

3.5. Заполним таблицу распределения Enternet-трафика по узлам сети.

Таблица 3.

MAC-адрес	Трафик					
	входящий		*исходящий*		*общий*	
	Мбайт	%	Мбайт	%	Мбайт	%
01:00:5e:00:00:01	0,00024	0	0	0	0,00024	0,0002
01:00:5e:00:00:16	0,00028	0	0	0	0,00028	0,0002
01:00:5e:00:00:fb	0,007	0	0	0	0,007	0,0049
01:00:5e:7f:ff:fa	0,002	0	0	0	0,002	0,0014
33:33:00:00:00:fb	0,008	0	0	0	0,008	0,0056
a8:f9:4b:e6:70:68	2	1,41	68	47,88	71	49,9917
e8:6a:64:95:a5:70	68	47,88	2	1,41	71	49,9917
ff:ff:ff:ff:ff:ff	0,006	0	0	0	0,006	0,0042

Узел a8:f9:4b:e6:70:68 наиболее загруженный на исходящий трафик, e8:6a:64:95:a5:70 – на входящий.

3.6.Определим относительную загрузку сети в контрольный период времени:

$$\text{Загрузка} = \frac{\left(\frac{\text{Трафик, Мбит}}{\text{Время, сек}}\right) \cdot 100}{\left(\text{Пропускная способность}, \frac{\text{Мбит}}{\text{сек}}\right)} = \frac{\frac{70{,}5}{4806} \cdot 100}{90} = 0{,}016$$

Где $\text{Пропускная способность} = 90{,}72\ \text{Мбит/сек}$

4. Вывод

В ходе выполнения задания были изучены основы работы с программой Wireshark для анализа сетевого трафика. Была проведена эмуляция сетевой активности путем посещения различных сайтов, просмотра текстового и видеоконтента, выполнения ping и traceroute, подключения к серверу ftp и скачивания файла. Был произведен захват сетевого трафика, который затем был отфильтрован по различным протоколам, включая HTTP, ICMP, ARP и FTP.

По результатам анализа было установлено, что подавляющее большинство трафика приходится на прикладные протоколы, такие как TCP, тогда как служебные протоколы занимают значительно меньший объем трафика. Также были определены

наиболее загруженные узлы сети, где узел a8:f9:4b:e6:70:68 оказался наиболее загруженным на исходящий трафик, а e8:6a:64:95:a5:70 – на входящий. Относительная загрузка сети составила 0,016%, что свидетельствует о том, что сеть использовалась достаточно эффективно в рамках данного периода времени.