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 №3

ПРОТОКОЛЫ СТЕКА TCP/IP

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

Целью работы является изучение структуры передаваемых по сети кадров и пакетов, работающих на канальном и сетевом уровне.

2. Задание

2.1. Запустить перехват пакетов в WireShark.

2.2. Определить с помощью утилиты **ping** доступность заданных узлов в соответствии с вариантом задания (таблица 1), выполнить трассировку к одному из узлов.

2.3. С помощью браузера просмотреть несколько страниц на сайте **nstu.ru**; подключиться к системе Moodle и просмотреть файлы с календарным планом выполнения лабораторных работ и рейтинговой системой по курсу «Сетевые информационные технологии».

2.4. С помощью клиента WinSCP подключиться по протоколу FTP к серверу fpm2.ami.nstu.ru и выполнить копирование на сервер в Ваш домашний каталог текстового файла согласно варианту из таблицы 1. Архив с файлами можно скачать из системы Moodle.

2.5. Остановить перехват пакетов и сохранить результаты в файл с расширением .pcapng.

2.6. С помощью WireShark определить внутреннюю структуру кадров и пакетов, передаваемых по сети; сравнить ее со структурами, описанными в протоколах Ethernet, IP и TCP.

2.7. Определить последовательность прохождения запросов, реализующих алгоритм трассировки одного из заданных в таблице 1 узлов.

2.8. Восстановить сеанс обмена данными по протоколу HTTP между браузером и сервером при выполнении п.3.

2.9. Восстановить сеанс обмена данными по протоколу FTP при выполнении п.4, найти перехваченные логин и пароль, а также восстановить содержимое переданного файла.

2.10. Определить последовательность прохождения запросов, реализующих один из протоколов в соответствии с вариантом из таблицы 1 (ICMP, DNS или ARP). Построить схему работы протокола и формат пакетов.

2.11. Найти в перехваченном трафике пакеты, передаваемые по протоколу в соответствии с вариантом задания (см. таблицу 1), определить назначение данного протокола.

2.12. Найти в перехваченном трафике широковещательные запросы по протоколам DHCP, ARP и ответы на них. Определить структуру передаваемых по этим протоколам кадров.

2.13. Определить значение поля «Тип данных» для кадра Ethernet при передаче пакетов IP, ARP, ICMP, DNS, DHCP.

2.14. Построить статистику по используемым за время сеанса протоколам.

2.15. Изучить процесс установления соединения по протоколу TCP.

3. Вариант

Таблица 1

Вариант	Номер пункта и задание
7	2. Утилита ping: asutp.ru, ohranatruda.ru,volgaweb.ru, toolsmart.ru, sviazist.nnov.ru, dogma.su , sec.ru
	4. test6.txt
	10. ICMP
	11. SSH

4. Ход работы

4.1. Запустим перехват пакетов в WireShark.

4.2. С помощью утилиты ping определим доступность узлов, указанных в таблице 1. Выполним трассировку узла asutp.ru.

```
C:\Users\evils>ping dogma.su

Обмен пакетами с dogma.su [91.201.52.217] с 32 байтами данных:
Ответ от 91.201.52.217: число байт=32 время=24мс TTL=59
Ответ от 91.201.52.217: число байт=32 время=27мс TTL=59
Ответ от 91.201.52.217: число байт=32 время=23мс TTL=59
Ответ от 91.201.52.217: число байт=32 время=24мс TTL=59

Статистика Ping для 91.201.52.217:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 23мсек, Максимальное = 27 мсек, Среднее = 24 мсек

C:\Users\evils>ping sec.ru

Обмен пакетами с sec.ru [185.114.247.107] с 32 байтами данных:
Ответ от 185.114.247.107: число байт=32 время=56мс TTL=60
Ответ от 185.114.247.107: число байт=32 время=59мс TTL=60
Ответ от 185.114.247.107: число байт=32 время=61мс TTL=60
Ответ от 185.114.247.107: число байт=32 время=55мс TTL=60

Статистика Ping для 185.114.247.107:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 55мсек, Максимальное = 61 мсек, Среднее = 57 мсек

C:\Users\evils>trace asutp.ru
"trace" не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\Users\evils>tracert asutp.ru

Трассировка маршрута к asutp.ru [81.177.140.55]
с максимальным числом прыжков 30:

  1    <1 мс    <1 мс    <1 мс  Eltex.Home [192.168.1.1]
  2     3 ms     2 ms     2 ms  100.81.64.1
  3     4 ms     1 ms     2 ms  217.107.118.221
  4     6 ms     5 ms     2 ms  95.167.93.75
  5     *        *        *     Превышен интервал ожидания для запроса.
  6    48 ms    48 ms    44 ms  89.191.239.165
  7    44 ms    45 ms    46 ms  msk-bgw1-xe-0-2-0-0.rt-comm.ru [217.106.6.166]
  8    49 ms    46 ms    46 ms  msk-bgw1-xe-0-2-0-0.rt-comm.ru [217.106.6.166]
  9    50 ms    46 ms    46 ms  srv201-h-st.jino.ru [81.177.140.55]

Трассировка завершена.
```

Рисунок 1 – Проверка доступности и трассировка заданных узлов.

4.3. С помощью браузера просмотрим несколько страниц на сайте **nstu.ru**; подключимся к системе Moodle и просмотрим файлы с календарным планом выполнения лабораторных работ и рейтинговой системой по курсу «Сетевые информационные технологии».

4.4. С помощью клиента WinSCP подключимся по протоколу FTP к серверу fpm2.ami.nstu.ru и выполним копирование на сервер в домашний каталог текстового файла согласно варианту из таблицы 1.

4.5. Определим внутреннюю структуру кадров и пакетов, передаваемых по сети.

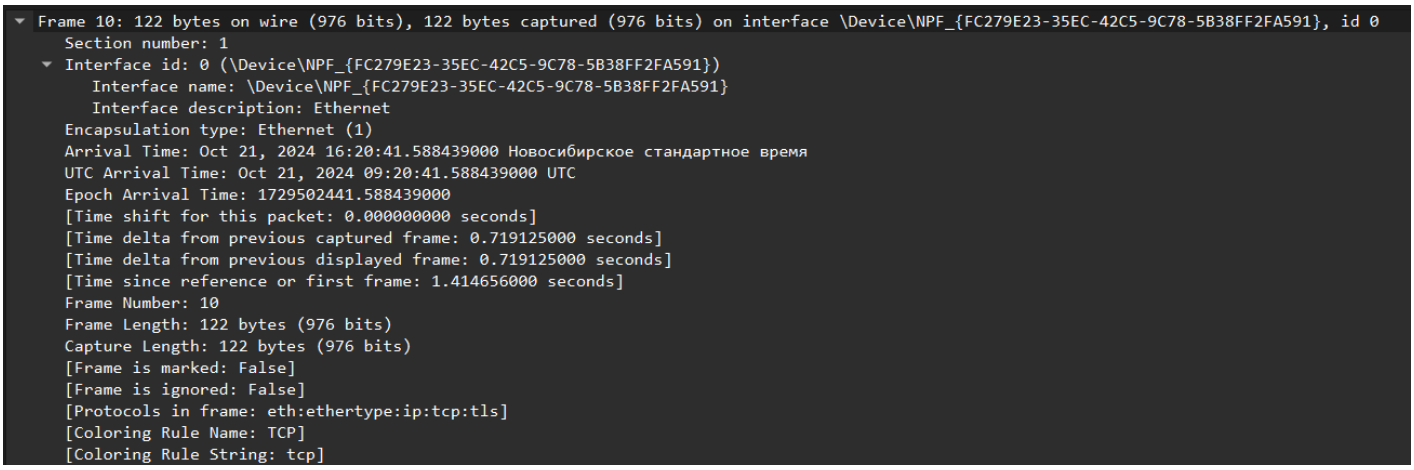


Рисунок 2 – Внутренняя структура кадра.

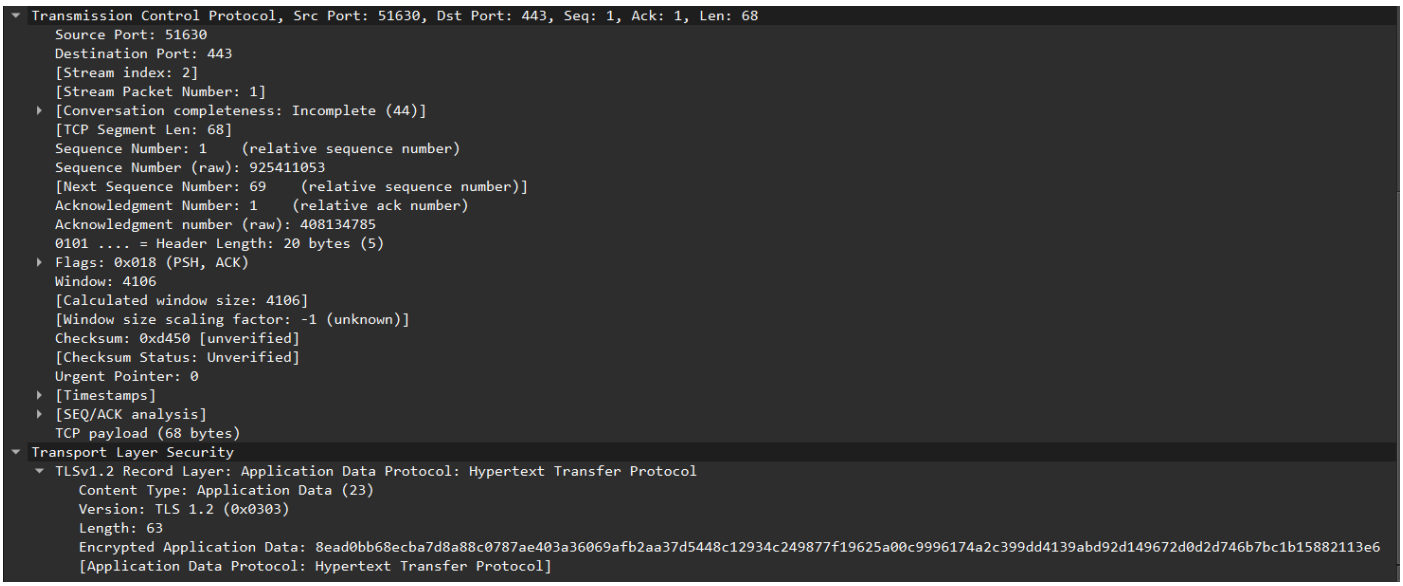


Рисунок 3 – Внутренняя структура пакета.

Внутренняя структура кадров и пакетов, захваченных с помощью Wireshark, точно соответствует описаниям протоколов Ethernet, IP и TCP. Ethernet-кадр включает MAC-адреса источника и назначения, тип кадра и другие поля. IP-пакет содержит заголовок, длину, TTL, IP-адреса и другие параметры. TCP-сегмент показывает порты источника и назначения, номера последовательности и подтверждения, флаги и размер окна. Wireshark позволяет детально анализировать эти структуры, подтверждая правильность передачи данных.

4.6. Выведем последовательность прохождения запросов, реализующих алгоритм трассировки заданного узла.

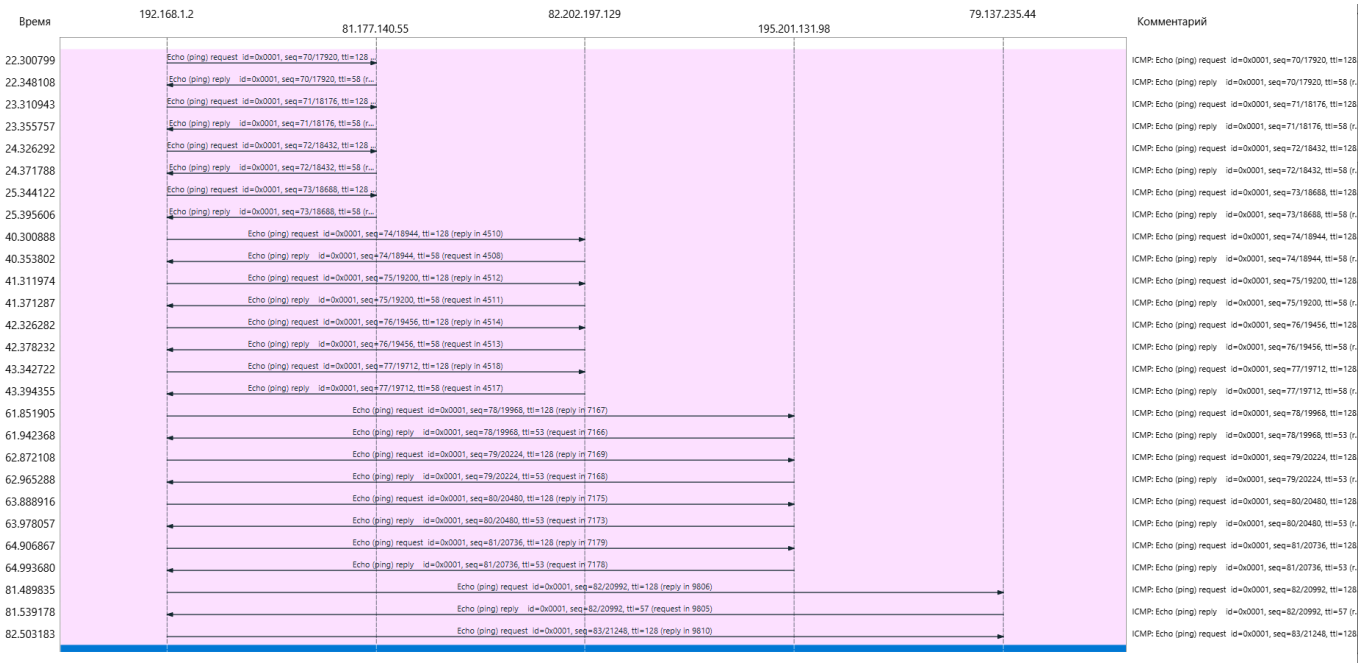


Рисунок 4 – Последовательность прохождения запросов, реализующих алгоритм трассировки заданного узла.

Запросы ICMP включают последовательные echo request и echo reply пакеты.

4.7. Восстановим сеанс обмена данными по протоколу HTTP.

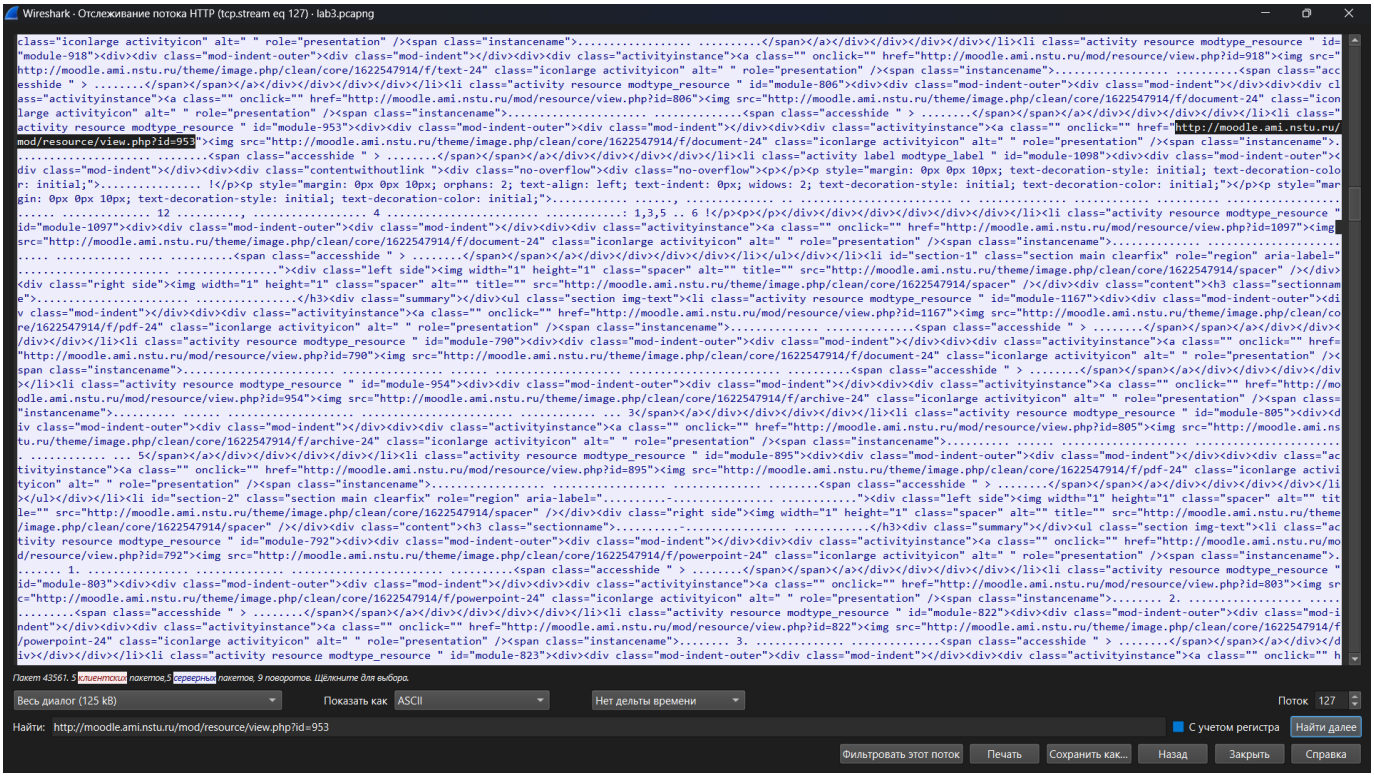


Рисунок 5 – Сеанс обмена данным по протоколу HTTP между браузером и сервером.

4.8. Восстановим сеанс обмена данными по протоколу FTP.

4.9. Последовательность прохождения запросов протокола ICMP отображена в пункте 4.6.

Схема работы протокола ICM: отправитель инициирует запрос, отправляя ICMP Echo Request пакет к цели. Пакет проходит через несколько маршрутизаторов, каждый из которых уменьшает поле TTL и проверяет контрольную сумму. Когда пакет достигает цели, целевое устройство получает Echo Request и отвечает ICMP Echo Reply. Ответный пакет Echo Reply возвращается к отправителю через маршрутизаторы Отправитель получает Echo Reply и завершает цикл.

Байт	0-7	8-15	16-31
[0-3]	Тип	Код	Контрольная сумма

Рисунок 7 – Формат пакета ICMP.

4.10. Отобразим пакеты протокола SSH в перехваченном трафике.

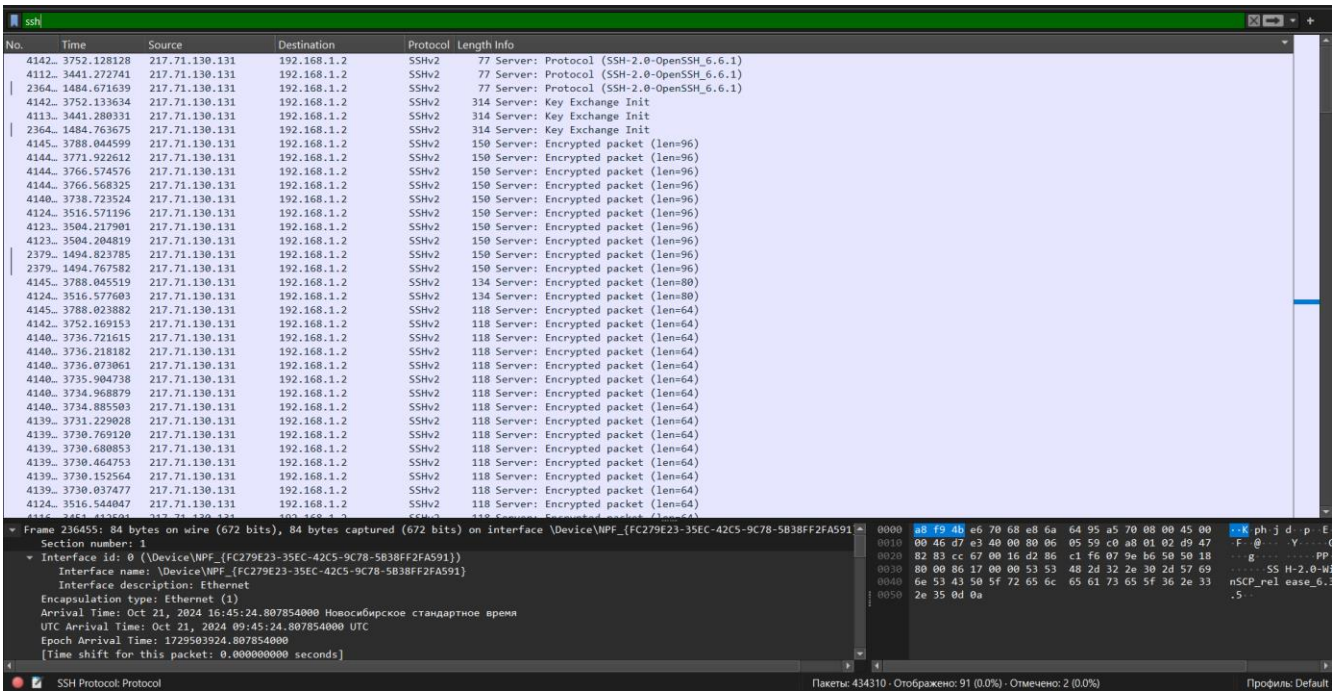


Рисунок 8 – Пакеты протокола SSH.

4.11. Найдем в перехваченном трафике широковещательные запросы по протоколам DHCP, ARP и ответы на них.

Структура кадра DHCP включает в себя Ethernet-заголовок, IP-заголовок, UDP-заголовок и полезную нагрузку DHCP, где содержатся поля для опроса и передачи настроек IP-адреса. Кадр ARP содержит Ethernet-заголовок, за которым следует ARP-

заголовок и полезная нагрузка, включающая MAC и IP-адреса отправителя и получателя.

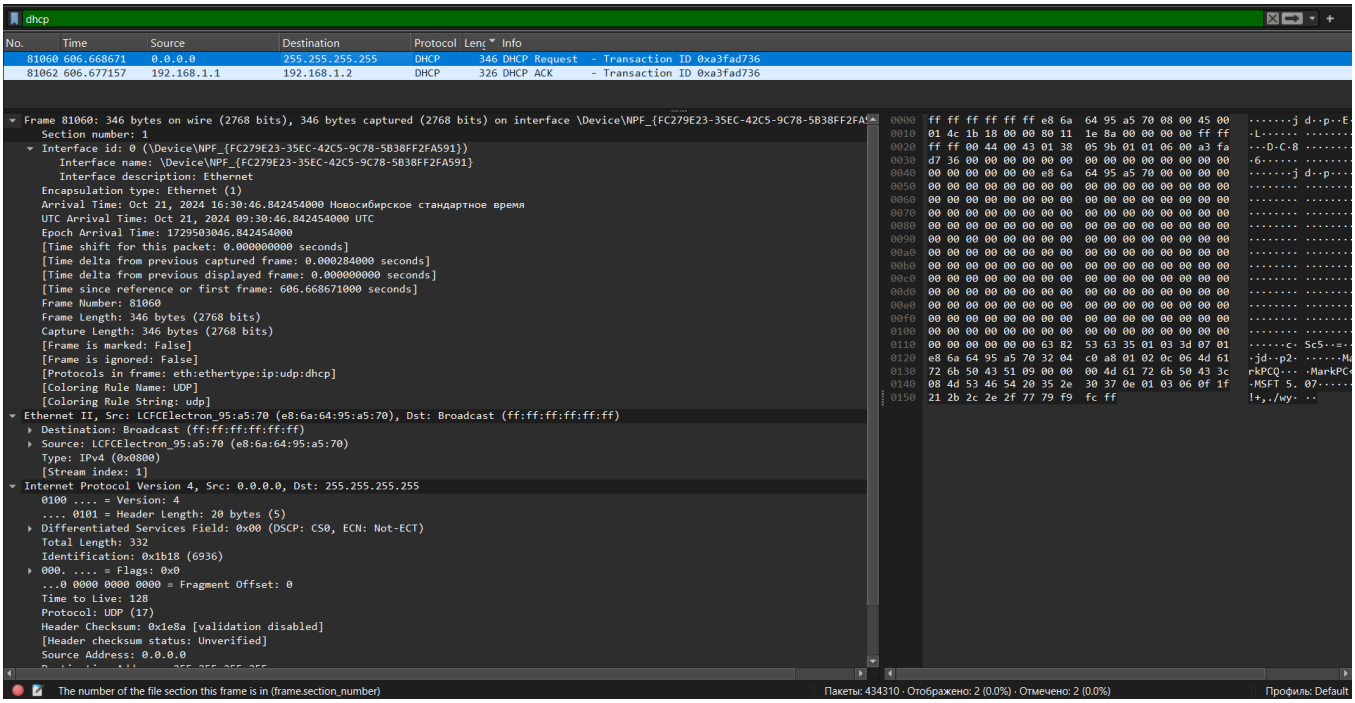


Рисунок 9 – Широковещательные запросы по протоколу DHCP.

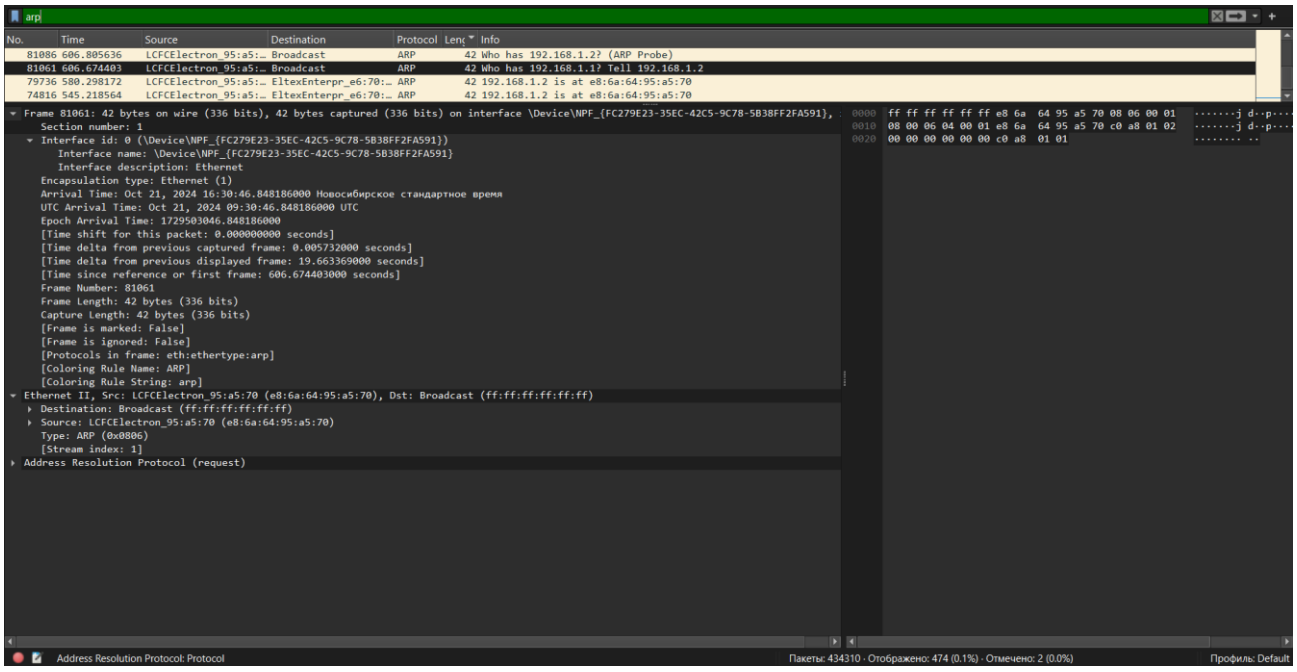
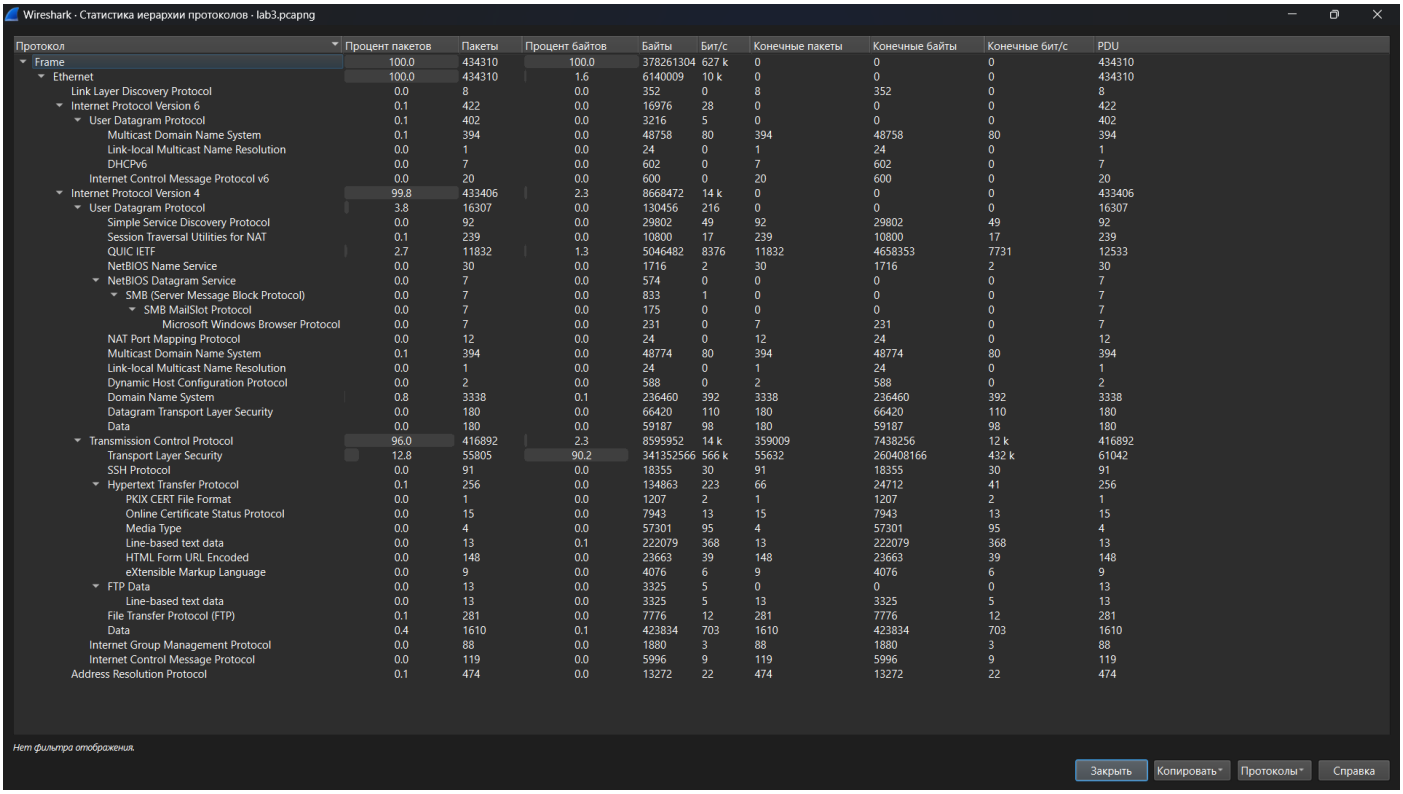


Рисунок 10 – Широковещательные запросы по протоколу ARP.

4.12. Поле «Тип данных» в кадре Ethernet указывает на протокол верхнего уровня, содержащийся в полезной нагрузке кадра. Значения этого поля для различных протоколов следующие: для IP — 0x0800, для ARP — 0x0806, для ICMP — 0x0800, для DNS — 0x0800 и для DHCP — 0x0800.

4.13. Построим статистику по используемым за время сеанса протоколам.



Протокол	Процент пакетов	Пакеты	Процент байтов	Байты	Бит/с	Конечные пакеты	Конечные байты	Конечные бит/с	PDU
Frame	100.0	434310	100.0	378261304	627 k	0	0	0	434310
Ethernet	100.0	434310	1.6	6140009	10 k	0	0	0	434310
Link Layer Discovery Protocol	0.0	8	0.0	352	0	8	352	0	8
Internet Protocol Version 6	0.1	422	0.0	16976	28	0	0	0	422
User Datagram Protocol	0.1	402	0.0	3216	5	0	0	0	402
Multicast Domain Name System	0.1	394	0.0	48758	80	394	48758	80	394
Link-local Multicast Name Resolution	0.0	1	0.0	24	0	1	24	0	1
DHCPv6	0.0	7	0.0	602	0	7	602	0	7
Internet Control Message Protocol v6	0.0	20	0.0	600	0	20	600	0	20
Internet Protocol Version 4	99.8	433406	2.3	8668472	14 k	0	0	0	433406
User Datagram Protocol	3.8	16307	0.0	130456	216	0	0	0	16307
Simple Service Discovery Protocol	0.0	92	0.0	29802	49	92	29802	49	92
Session Traversal Utilities for NAT	0.1	239	0.0	10800	17	239	10800	17	239
QUIC IETF	2.7	11832	1.3	5046482	8376	11832	4658353	7731	12533
NetBIOS Name Service	0.0	30	0.0	1716	2	30	1716	2	30
NetBIOS Datagram Service	0.0	7	0.0	574	0	0	0	0	7
SMB (Server Message Block Protocol)	0.0	7	0.0	833	1	0	0	0	7
SMB MailSlot Protocol	0.0	7	0.0	175	0	0	0	0	7
Microsoft Windows Browser Protocol	0.0	7	0.0	231	0	7	231	0	7
NAT Port Mapping Protocol	0.0	12	0.0	24	0	12	24	0	12
Multicast Domain Name System	0.1	394	0.0	48774	80	394	48774	80	394
Link-local Multicast Name Resolution	0.0	1	0.0	24	0	1	24	0	1
Dynamic Host Configuration Protocol	0.0	2	0.0	588	0	2	588	0	2
Domain Name System	0.8	3338	0.1	236460	392	3338	236460	392	3338
Datagram Transport Layer Security	0.0	180	0.0	66420	110	180	66420	110	180
Data	0.0	180	0.0	59187	98	180	59187	98	180
Transmission Control Protocol	96.0	416892	2.3	8595952	14 k	359009	7438256	12 k	416892
Transport Layer Security	12.8	55805	90.2	341352566	566 k	55632	260408166	432 k	61042
SSH Protocol	0.0	91	0.0	18355	30	91	18355	30	91
Hypertext Transfer Protocol	0.1	256	0.0	134863	223	66	24712	41	256
PKIX CERT File Format	0.0	1	0.0	1207	2	1	1207	2	1
Online Certificate Status Protocol	0.0	15	0.0	7943	13	15	7943	13	15
Media Type	0.0	4	0.0	57301	95	4	57301	95	4
Line-based text data	0.0	13	0.1	222079	368	13	222079	368	13
HTML Form URL Encoded	0.0	148	0.0	23663	39	148	23663	39	148
eXtensible Markup Language	0.0	9	0.0	4076	6	9	4076	6	9
FTP Data	0.0	13	0.0	3325	5	0	0	0	13
Line-based text data	0.0	13	0.0	3325	5	13	3325	5	13
File Transfer Protocol (FTP)	0.1	281	0.0	7776	12	281	7776	12	281
Data	0.4	1610	0.1	423834	703	1610	423834	703	1610
Internet Group Management Protocol	0.0	88	0.0	1880	3	88	1880	3	88
Internet Control Message Protocol	0.0	119	0.0	5996	9	119	5996	9	119
Address Resolution Protocol	0.1	474	0.0	13272	22	474	13272	22	474

Рисунок 11 – Статистика по используемым протоколам.

5. Вывод

В ходе данной работы были изучены и проанализированы структуры передаваемых по сети кадров и пакетов, работающих на канальном и сетевом уровне, с использованием Wireshark. Были запущены перехваты пакетов, выполнены запросы ping и трассировки, а также проведен анализ веб-трафика, FTP соединений и ICMP запросов. Внутренняя структура захваченных кадров и пакетов сравнивалась с описаниями в протоколах Ethernet, IP и TCP, подтверждая их корректность. Также были рассмотрены сеансы обмена данными по протоколам HTTP и FTP, восстановлены логины и пароли, а также содержимое переданных файлов. Определены значения поля «Тип данных» для Ethernet кадров при передаче пакетов IP, ARP, ICMP, DNS и DHCP. Построена статистика по используемым за время сеанса протоколам и изучен процесс установления соединения по протоколу TCP. Проведенный анализ подтвердил правильность передачи данных и дал возможность детально изучить работу различных сетевых протоколов.