МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра ИИТ

Отчёт

о лабораторной работе №6

по дисциплине «Компьютерные системы и сети»

Тема: «Анализ сетевого трафика и протоколов

(на базе WireShark)»

Выполнил студент 2 курса

группы ПО-11 Сымоник И.А.

Номер зачетной книжки: 220220

Проверил: Савицкий Ю.В.

**Цель работы**: приобретение навыков анализа сетевого трафика компьютерных сетей; изучение структуры сетевых протоколов различных уровней

**Вариант 6**

**Ход работы**

|  |  |
| --- | --- |
| **Вариант** | **Адрес url** |
| 6 | https://ria.ru/ |

1. Остановить и сохранить захват. Для захваченных пакетов определить

статистические данные:

- процентное соотношение трафика разных протоколов в сети;

- среднюю скорость кадров/сек;

- среднюю скорость байт/сек;

- минимальный, максимальный и средний размеры пакета;

- степень использования полосы пропускания канала (загрузку сети)

Изображение выглядит как текст, число, Шрифт, снимок экрана

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

2. Отфильтровать в захвате IP пакеты. Определить статистические данные:

- процентное соотношение трафика разных протоколов стека tcp/ip в сети;

- средний, минимальный, максимальный размеры пакета.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

3. На примере третьего захваченного IP-пакета указать структуры протокола канального уровня (протокола Ethernet 802.3, Wi-Fi 802.11, либо другого, используемого в вашей конфигурации) и протокола IPv4. Отметить поля заголовков и описать их и интерпретировать их значения.

Захваченный пакет:



Протокол канального уровня(Ethernet 802.3):

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

MAC-адрес назначения (Destination MAC Address): 6 байт (30:03:c8:10:1a:57), адрес устройства-получателя.

MAC-адрес источника (Source MAC Address): 6 байт (80:7d:14:81:4a:77), адрес устройства-отправителя.

Тип или длина (Type/Length): 2 байта (0x0800), указывает на то, что это IPv4-пакет.

Протокол IPv4:

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Версия (Version): 4, указывает на версию протокола IPv4.

Длина заголовка (Header Length): 4 бита, что соответствует 20 байтам (5 слов по 32 бита), так как это стандартный размер заголовка IPv4.

Тип сервиса (Type of Service): 8 бит, предназначен для определения приоритета обработки пакета.

Длина пакета (Total Length): 16 бит, указывает на общую длину пакета в байтах (включая заголовок и данные). Значение - 44

Идентификатор (Identification): 16 бит, идентифицирует фрагменты, связанные с одним и тем же исходным пакетом. Значение - 12800

Флаги (Flags): 3 бита, используются для управления фрагментацией. Значение – 010 (Установлен бит запрета фрагментирования)

Смещение фрагмента (Fragment Offset): 13 бит, указывает на смещение фрагмента в пакете. Значение – 0

Время жизни (Time to Live): 8 бит, определяет количество переходов, которое пакет может сделать через маршрутизаторы, прежде чем он будет отброшен. Значение – 52

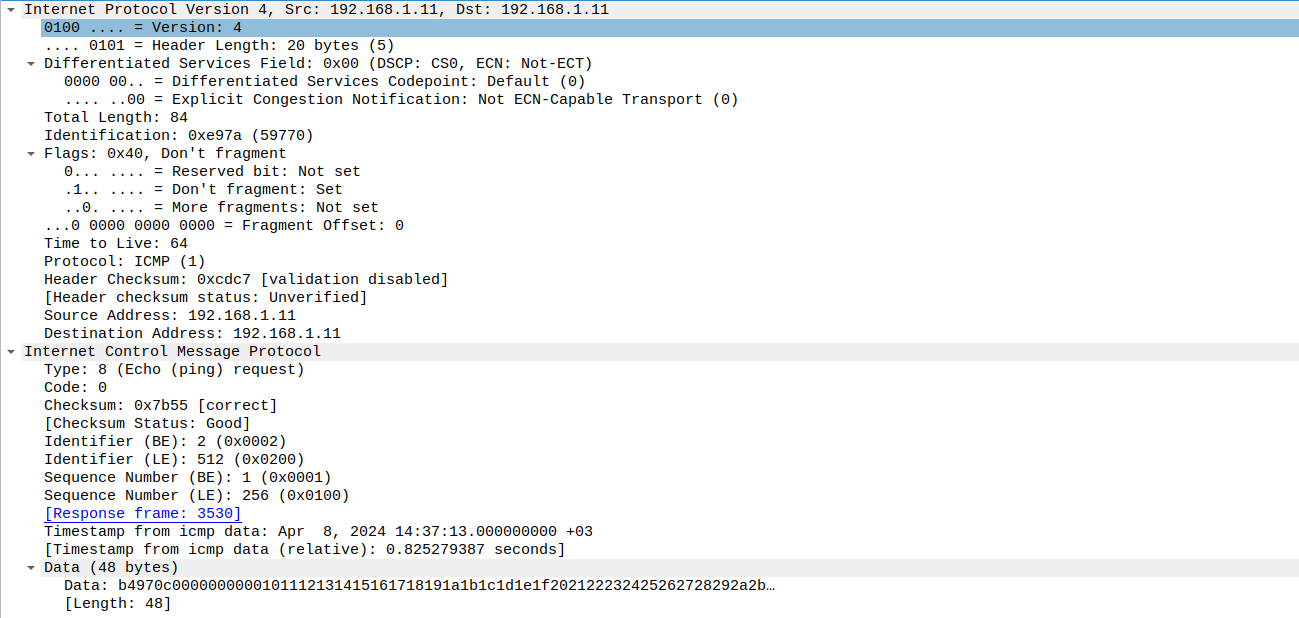
Протокол (Protocol): 8 бит, указывает на протокол верхнего уровня. Значение – TCP

Контрольная сумма заголовка (Header Checksum): 16 бит, используется для проверки целостности заголовка IPv4. Значение – 0xb53b

IP-адрес источника (Source IP Address): 32 бита (192.168.1.100), IP-адрес устройства-отправителя. Значение – 178.248.234.228

IP-адрес назначения (Destination IP Address): 32 бита (10.0.0.1), IP-адрес устройства-получателя. Значение – 192.168.1.11

4. Запустив Wireshark на захват, выполнить команду ping для IP адреса компьютера (предварительно определив его адрес с помощью ipconfig; пример команды: ping 172.17.20.246). Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты, относящиеся к выполнению команды ping. На базе полученных пакетов и значений их полей интерпретировать результат работы утилиты ping. Описать все протоколы, используемые утилитой.Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

В утилите ping используется протокол ICMP. В этом протоколе следующие поля:

Тип сообщения (Type): Определяет тип сообщения ICMP. Например, тип 8 соответствует эхо-запросу, а тип 0 - эхо-ответу. Значение – 8

Код (Code): Код, который обычно используется для более детальной классификации типа сообщения. Значение - 0

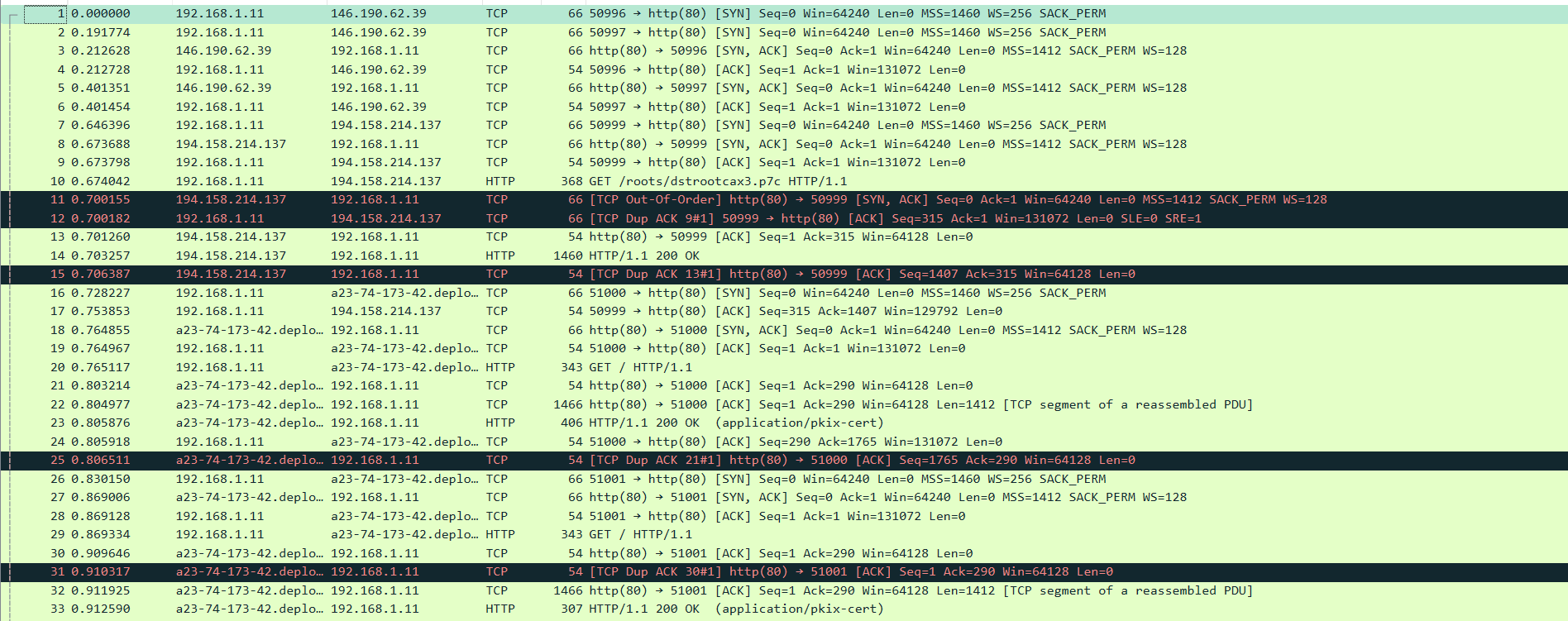
Контрольная сумма (Checksum): Проверка целостности пакета. Значение – 0х7b55

Идентификатор (Identifier) и последовательный номер (Sequence Number): Идентификатор и последовательный номер, которые помогают установить соответствие между эхо-запросами и эхо-ответами. Значения – 0x0002 и 0х0001 (порядок от старшего к младшему), . Значения – 0x0200 и 0х0100 (порядок от младшего к старшему).

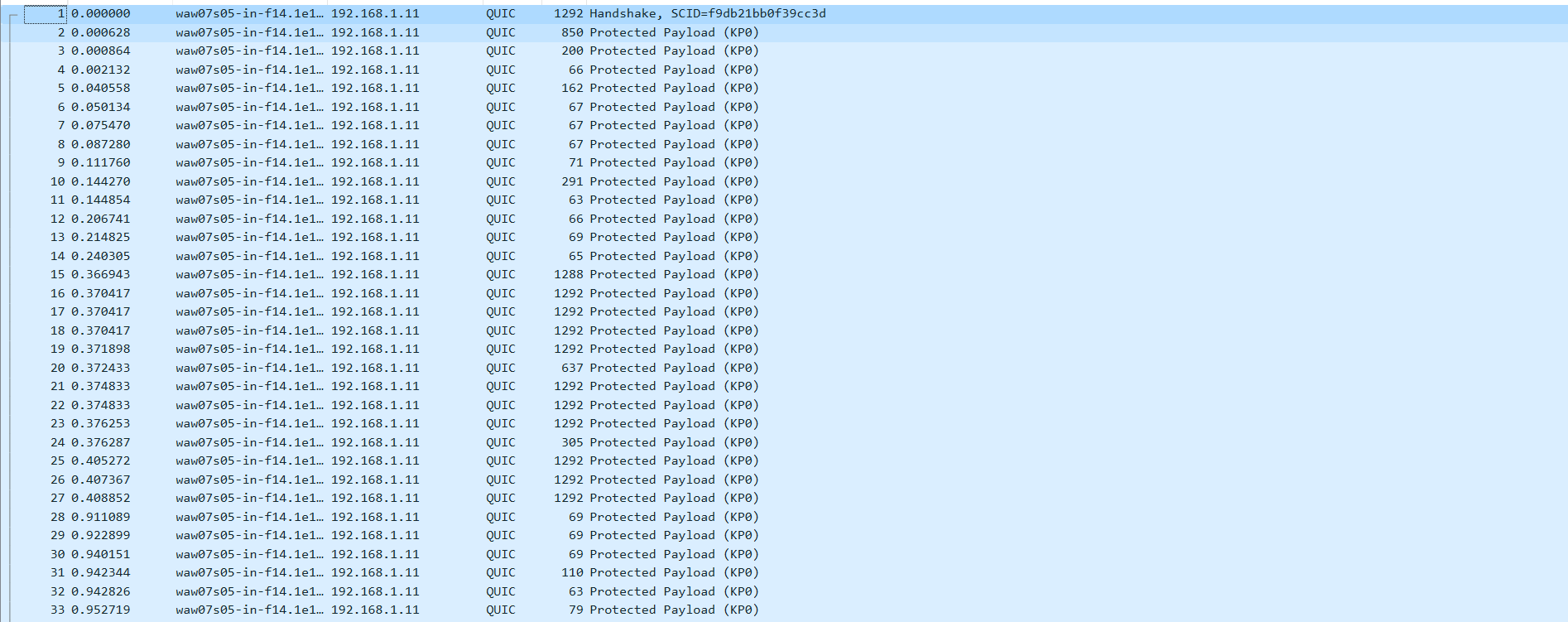
Данные (Data): Сами данные, включая метку времени отправки и приема пакета.

5. Сформировать не менее 3-х сложных фильтров захвата с использованием полей протоколов, операторов сравнения (таблицы 1 и 2 из файла теоретические\_указания4) и логических операторов; каждый раз перезапуская захват, для каждого фильтра захватить соответствующие пакеты.

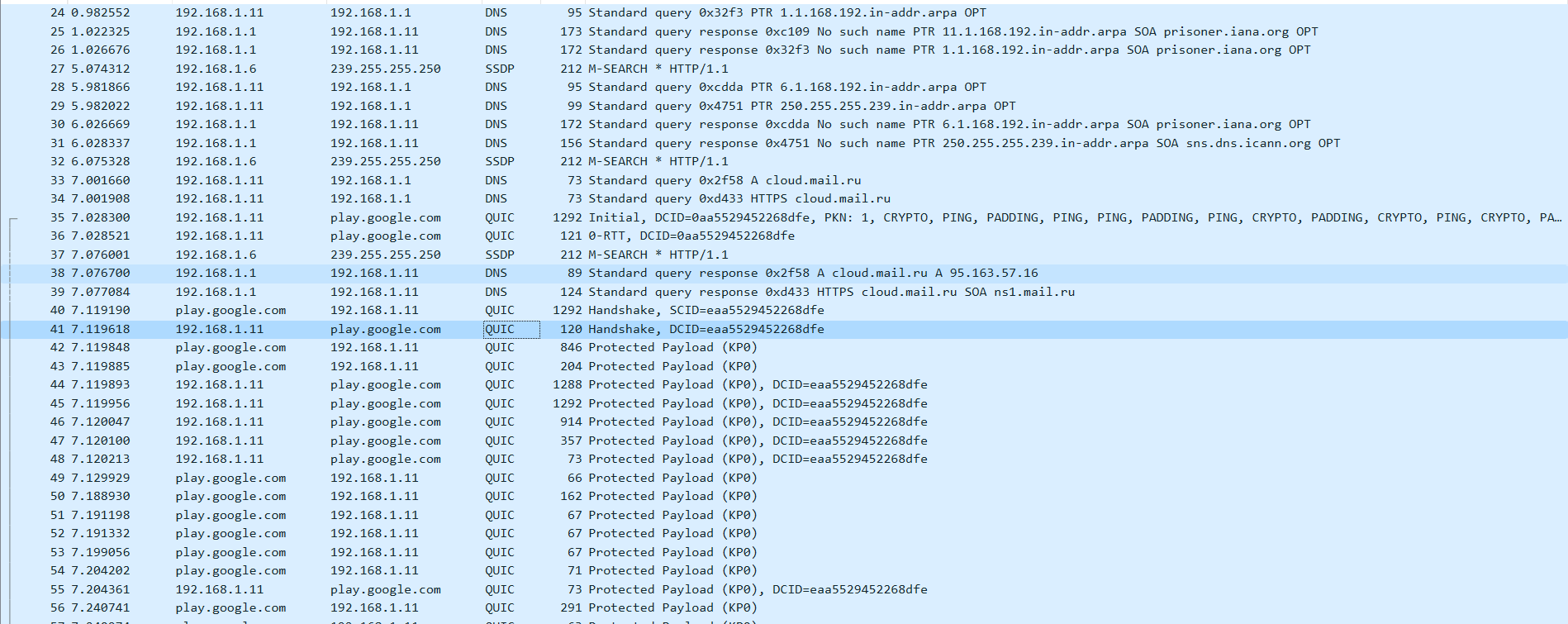
1) tcp port 80 and not arp



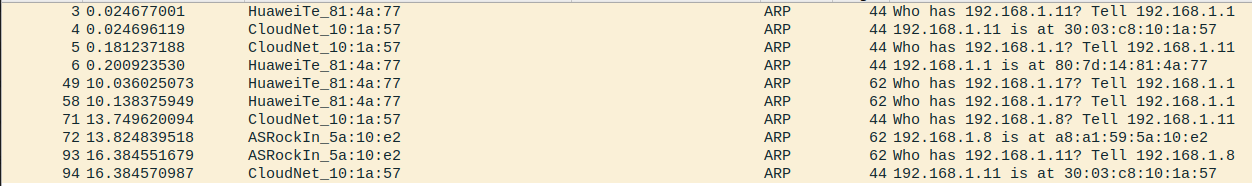
2) src port 443 and udp and not arp

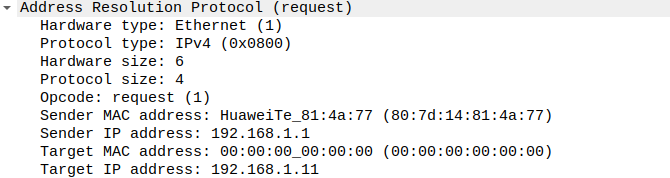


3) udp or icmp and not tcp



6. Выполнить анализ ARP-протокола по примеру из методических указаний.





Hardware Type: Тип сетевого адаптера. Значение - Ethernet(1)

Protocol Type: Тип протокола, для которого выполняется разрешение адресов. Значение - IPv4(0х0800).

Hardware size: Длина аппаратного адреса. Значение - 6.

Protocol size: Длина сетевого адрес. Значение - 4

Opcode: Операция, выполняемая в ARP-запросе или ARP-ответе. Значение – request(запрос).

Sender MAC Address: MAC-адрес отправителя. Значение – 80:7d:14:81:4a:77

Sender IP Address: IP-адрес отправителя. Значение – 192.168.1.1

Target MAC Address: MAC-адрес целевого узла. Значение – отсутствует

Target IP Address: IP-адрес целевого узла. Значение – 192.168.1.11

7. Выполнить анализ TCP-сеансов по примеру из методических указаний

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Первые 3 пакета с флагами (SYN), (SYN,ACK),(ACK) создают TCP сессию. Следующие 7 пакетов отправляют данные. Последние 3 пакета с флагами (FIN,ACK), (FIN,ACK), (ACK) закрывают TCP сессию.

Вывод: приобрели навыки анализа сетевого трафика компьютерных сетей; изучили структуры сетевых протоколов различных уровней