



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА — Российский технологический университет»

РТУ МИРЭА

Институт информационных технологий (ИИТ)
Кафедра инструментального и прикладного программного обеспечения
(ИиППО)

ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ по
дисциплине «Технологии передачи данных»

Лабораторная работа № 3

Студент группы

ИВБО-07-21, Стока Иван Павлович

(подпись)

Преподаватель

Рогов И.Е.

(подпись)

Отчет представлен « _____ » _____ 2023г.

Москва 2023 г.

СОДЕРЖАНИЕ

ХОД РАБОТЫ	3
Шаг 1. Получение информации об интерфейсах	3
Шаг 2. Захват пакетов службы DNS.....	3
Шаг 3. Анализ датаграмм UDP	4
Шаг 4. Анализ TCP-сегментов	6
ЗАКЛЮЧЕНИЕ	7
СПИСОК ИСТОЧНИКОВ	8

ХОД РАБОТЫ

Шаг 1. Получение информации об интерфейсах

Для нахождения необходимых значений конфигурации используется команда `ipconfig /all`. Из выведенной конфигурации берется IP-адрес, MAC-адрес (физический адрес), основной шлюз и DNS-серверы (Таблица 1).

Таблица 1 – Данные сетевого интерфейса (адаптер беспроводной локальной сети)

IP-адрес устройства	192.168.188.31
MAC-адрес устройства	4C-D5-77-A0-EC-FB
IP-адрес шлюза по умолчанию	192.168.188.128
IP-адрес DNS-сервера	192.168.188.128

Шаг 2. Захват пакетов службы DNS

Необходимо воспользоваться диагностической службой `nslookup`, чтобы сделать несколько запросов для заполнения Таблицы 2.

Таблица 2 – Данные соответствия доменных имен IP-адресам

Доменное имя	IP-адреса
Learn.microsoft.com	2a02:26f0:5200:39e::3544 2a02:26f0:5200:3aa::3544 23.64.239.181
Google.com	2a00:1450:4010:c0d::8b 2a00:1450:4010:c0d::64 2a00:1450:4010:c0d::65 2a00:1450:4010:c0d::71 173.194.73.138 173.194.73.101 173.194.73.102 173.194.73.100 173.194.73.113 173.194.73.139

Продолжение Таблицы 2

Vk.com	87.240.132.78 87.240.129.133 93.186.225.194 87.240.132.67 87.240.132.72 87.240.137.164
Yandex.ru	2a02:6b8:a::a 5.255.255.77 5.255.255.70
	77.88.55.88 77.88.55.60

Далее в Wireshark проходит захват пакетов по фильтру dns, где рассматриваются пакеты, которые были отправлены при поиске домена google.com. Требуется изучить запросы и ответы для записей типа A и AAAA (Таблица 3).

Таблица 3 – Информация по запросу DNS для google.com

Тип сообщения	Идентификатор транзакции	Значения поля флаги	Количество вопросов	Содержание
Запрос	0x0002	0x8180	1	Домен: google.com Тип: A
Ответ				Ответы: 6 Домен: google.com Тип: A (Host address) Адрес: 173.194.73.101 Время жизни: 3 seconds
Запрос	0x0003	0x8180	1	Домен: google.com Тип: AAAA
Ответ				Ответы: 4 Домен: google.com Тип: AAAA Адрес: 2a00:1450:4010:c0d::64 Время жизни: 289 seconds

Шаг 3. Анализ датаграмм UDP

Необходимо проанализировать UDP и заполнить необходимую информацию в Таблицы 4-7.

Таблица 4 – Данные заголовка транспортного уровня запрос A google.com

Порт источника	52530
Порт назначения	53
Длина	36
Контрольная сумма	0x2492
Объем полезной нагрузки для транспортного уровня	28 bytes

Таблица 5 – Данные заголовка транспортного уровня ответ A google.com

Порт источника	53
Порт назначения	52530
Длина	132
Контрольная сумма	0xc121
Объем полезной нагрузки для транспортного уровня	124 bytes

Таблица 6 – Данные заголовка транспортного уровня запрос AAAA google.com

Порт источника	52531
Порт назначения	53
Длина	36
Контрольная сумма	0x2475
Объем полезной нагрузки для транспортного уровня	28 bytes

Таблица 7 – Данные заголовка транспортного уровня ответ AAAA google.com

Порт источника	53
Порт назначения	52531

Продолжение Таблицы 7

Длина	148
Контрольная сумма	0x7283
Объем полезной нагрузки для транспортного уровня	140 bytes

UDP будет быстрее, так как не тратит время на установление соединения и не занимается контролем доставки данных.

Шаг 4. Анализ ТСП-сегментов

Проводится анализ процессов трехстороннего квитирования и четырехстороннего квитирования при обращении к ресурсу www.huawei.com.

Проводится фильтрация пакетов по запросу: ip.addr == 104.91.49.115 and tcp.port == 54153.

Далее находятся открытия и закрытия логических соединений (Рисунок 1-2).

139 4.986594	192.168.188.31	104.91.49.115	TCP	66 54152 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
153 5.171468	104.91.49.115	192.168.188.31	TCP	66 443 → 54152 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300 SACK_PERM=1 WS=128
162 5.171860	192.168.188.31	104.91.49.115	TCP	54 54152 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0

Рисунок 5 – обозначение открытия логического соединения

193 5.471737	192.168.188.31	104.91.49.115	TCP	54 54152 → 443 [ACK] Seq=518 Ack=6410 Win=66048 Len=0
196 5.479302	192.168.188.31	104.91.49.115	TLSv1.2	100 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
197 5.479422	192.168.188.31	104.91.49.115	TCP	54 54152 → 443 [FIN, ACK] Seq=644 Ack=6410 Win=66048 Len=0
205 5.635677	104.91.49.115	192.168.188.31	TCP	66 [TCP Dup ACK 17001] 443 → 54152 [ACK] Seq=6410 Ack=518 Win=64128 Len=0 SLE=644 SRE=645
206 5.635677	104.91.49.115	192.168.188.31	TCP	54 443 → 54152 [ACK] Seq=6410 Ack=645 Win=64128 Len=0
210 5.635677	104.91.49.115	192.168.188.31	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
212 5.635784	192.168.188.31	104.91.49.115	TCP	54 54152 → 443 [RST, ACK] Seq=645 Ack=6668 Win=0 Len=0
215 5.635966	104.91.49.115	192.168.188.31	TLSv1.2	100 Application Data
216 5.635966	104.91.49.115	192.168.188.31	TLSv1.2	85 Encrypted Alert
218 5.635966	104.91.49.115	192.168.188.31	TCP	54 443 → 54152 [FIN, ACK] Seq=6745 Ack=645 Win=64128 Len=0

Рисунок 6 – обозначение закрытия логического соединения

ЗАКЛЮЧЕНИЕ

В работе были исследованы службы DNS, а также протоколы транспортного уровня TCP и UDP.

СПИСОК ИСТОЧНИКОВ

1. Олифер В.Г., Олифер В.А. Компьютерной сети. – 2-е изд. – СанктПетербург: Питер, 2021. – 1008 с.
2. Мастер класс по использованию Wireshark // youtube URL: <https://www.youtube.com/watch?v=OU-A2EmVrKQ&list=PLW8bTPfXNGdC5Co0VnBK1yVzAwSSphzpJ> (дата обращения: 07.03.2023).