



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 № 2**

Студент группы

*ИВБО-07-21, Стока Иван Павлович*

(подпись)

Преподаватель

*Рогов И.Е.*

(подпись)

Отчет представлен

«\_\_\_»\_\_\_\_\_2023 г.

Москва 2023 г.

# СОДЕРЖАНИЕ

ХОД РАБОТЫ .....	3
Шаг 1 UgraCTF .....	3
Шаг 2 UgraCTF .....	4
Шаг 3 FreeHackQuest .....	4
Шаг 4 FreeHackQuest .....	5
Шаг 5 PicoCTF .....	6
ЗАКЛЮЧЕНИЕ .....	8
СПИСОК ИСТОЧНИКОВ.....	9

# ХОД РАБОТЫ

## Шаг 1 UgraCTF

Для нахождения ключа необходимо отфильтровать все протоколы HTTP, после чего отследить путь протоколов, где в последнем запросе находим ячейку с данными (data). Там представлен код в системе HEX. Рассматриваем байт пакеты данной ячейки и получаем необходимый ключ (Рисунок 1).

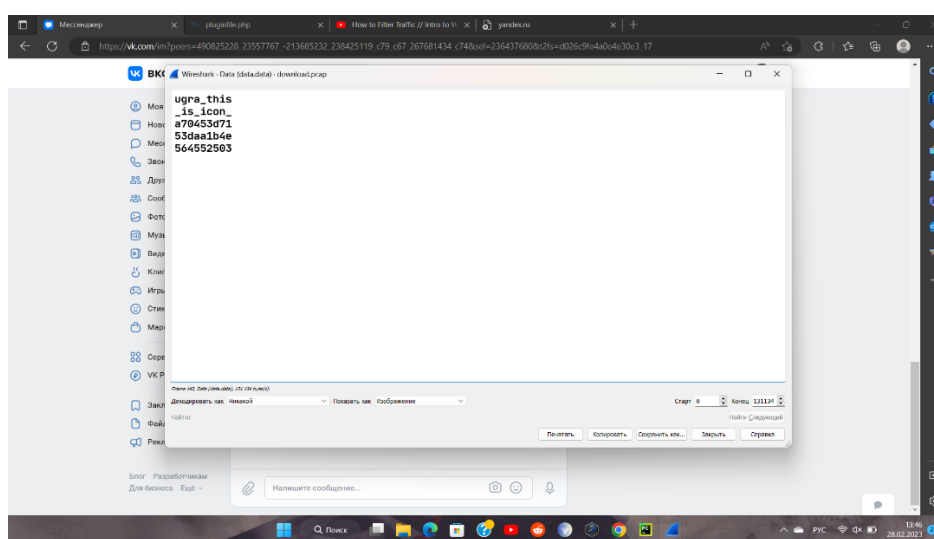


Рисунок 1 – Ключ

Проводится проверка правильности ключа (Рисунок 2).

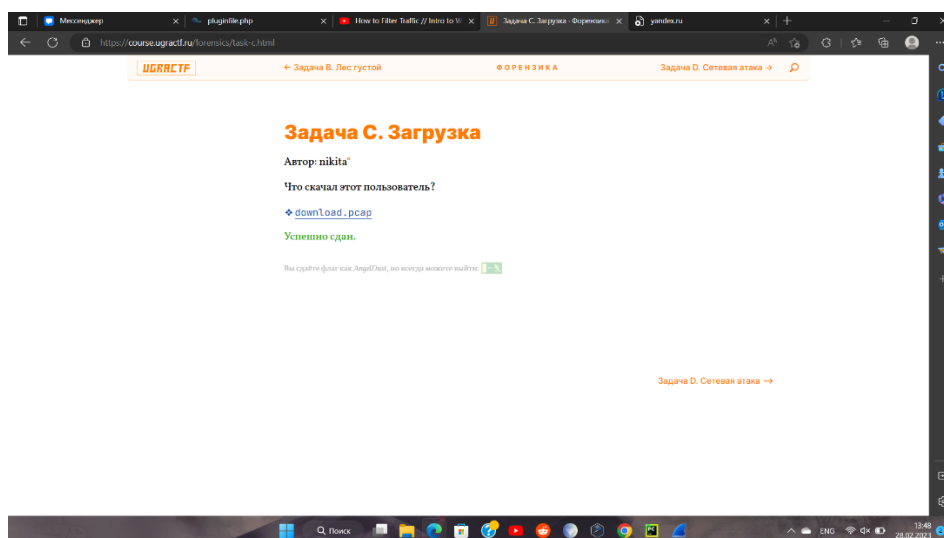


Рисунок 2 – Проверка правильности ключа

## Шаг 2 UgraCTF

Необходимо сделать фильтр по HTTP протоколам, далее извлекаются по одной букве данные, приносившиеся запросами с text/html информацией. По итогу получаем ключ: ugra\_pcap\_with\_trash\_beebc1fec68e6db. Проводится проверка правильности ключа (Рисунок 3).

## Задача D. Сетевая атака

Автор: nikita°

Наш сайт взломали! Кто виноват и что делать?

❖ [attack.pcap](#)

Успешно сдан.

Вы сдаёте флаг как *AngelDust*, но всегда можете выйти: 

Рисунок 3 – Проверка правильности ключа

## Шаг 3 FreeHackQuest

Проводится фильтрация TELNET протоколов. При проходе по запросам находится логин, пароль, а также ключ (Рисунок 4).

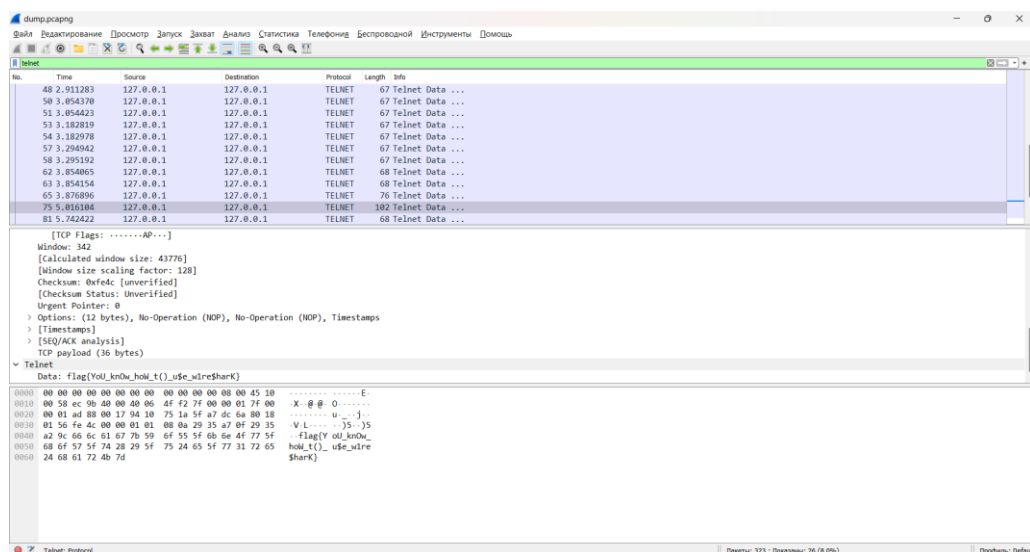


Рисунок 4 – Ключ

## Проводится проверка правильности ключа (Рисунок 5).

Название: Find Me

Статус: решена (2023-03-01T07:31:01.000)

Авторские права:

Раздел: UFO CTF School 2016 / forensics

Состояние: Доступен

Решили: 200 users

Очки: +100

Автор: AfftaR (afftar.589@gmail.com, vk.com/afftarx)

Сообщить об ошибке

RU: У нас в конторе админ работает с удаленной машиной как-то странно, попробуй понять как он это делает и найди пароль!

EN:

[Download dump.pcapng](#)

Имя файла	Размер файла	Счетчик загрузок
<a href="#">dump.pcapng</a>	64KB	67

(md5: 8fb8c2ae1fa3290e2db73c57f3f9afc9)

Мои ответы

Wed Mar 01 2023 10:31:01 GMT+0300 (Москва, стандартное время):  
flag[YoU\_knOw\_hoW\_t()\_u\$e\_wtresharK] (levenshtein: 0)

Рисунок 5 – Проверка правильности ключа

## Шаг 4 FreeHackQuest

Проверяется через фильтр, существование в данных протоколов строки FLAG, используя команду data contains “FLAG”. По данному запросу выдаётся протокол типа ICMP с флагом, записанном в HEX системе (Рисунок 6).

Wireshark packet capture showing ICMP Echo (ping) replies. The selected packet (No. 2898) is an Echo (ping) reply from 172.29.255.46 to 172.29.255.11. The packet details show the ICMP type as 0 (Echo (ping) reply), code as 0, and a data field containing a hex string: 464c4177b3863363066326231666132313439383936396663376231653733362653432. The packet bytes pane shows the raw data in hex and ASCII, with the ASCII part displaying '.\*.g.. 'D...E' and 'C...@: \$. ....' followed by '.....i...FLAG(8' and 'c60f2b1f a2149896' and '9fc7b1e7 33be42e)' and '0a'.

Рисунок 6 – Ключ

Проводится проверка правильности ключа (Рисунок 7).

Имя файла	Размер файла	Счетчик загрузок
<a href="#">dump_pcap_tgz</a> (md5: 511b57b32781ecbfd68716c47f469003)	2MB	44
<a href="#">проxy.jpg</a> (md5: a13dd0c42b3ed688c652e4e1d75dfc9c)	42KB	39

Мои ответы

Wed Mar 01 2023 12:21:38 GMT+0300 (Москва, стандартное время):  
**8c60f2b1fa21498969fc7b1e733be42e** (levenshtein: 0)

Wed Mar 01 2023 12:21:28 GMT+0300 (Москва, стандартное время):  
**FLAG{8c60f2b1fa21498969fc7b1e733be42e}** (levenshtein: 6)

Рисунок 7 – Проверка правильности ключа

## Шаг 5 PicoCTF

Делается фильтр по HTTP протоколам, выделяются запросы, возвращающие данные в text/html формате, по итогу находится закодированный флаг, который надо декодировать, в конечном итоге находится нужный ключ (Рисунок 8-9).

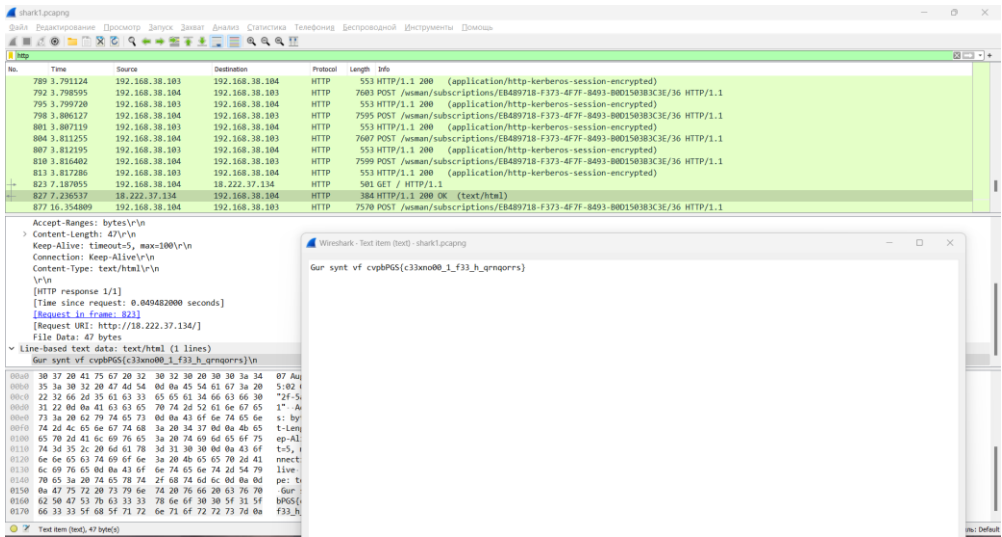


Рисунок 8 – Закодированный ключ

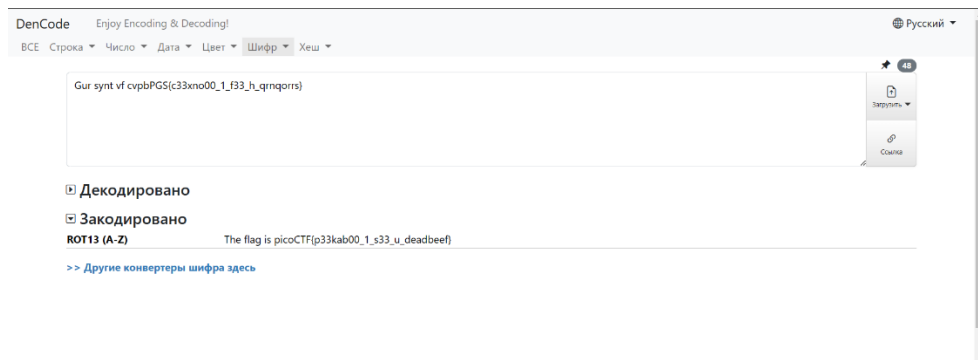


Рисунок 9 – Декодирование ключа

Проводится проверка правильности ключа (Рисунок 10).

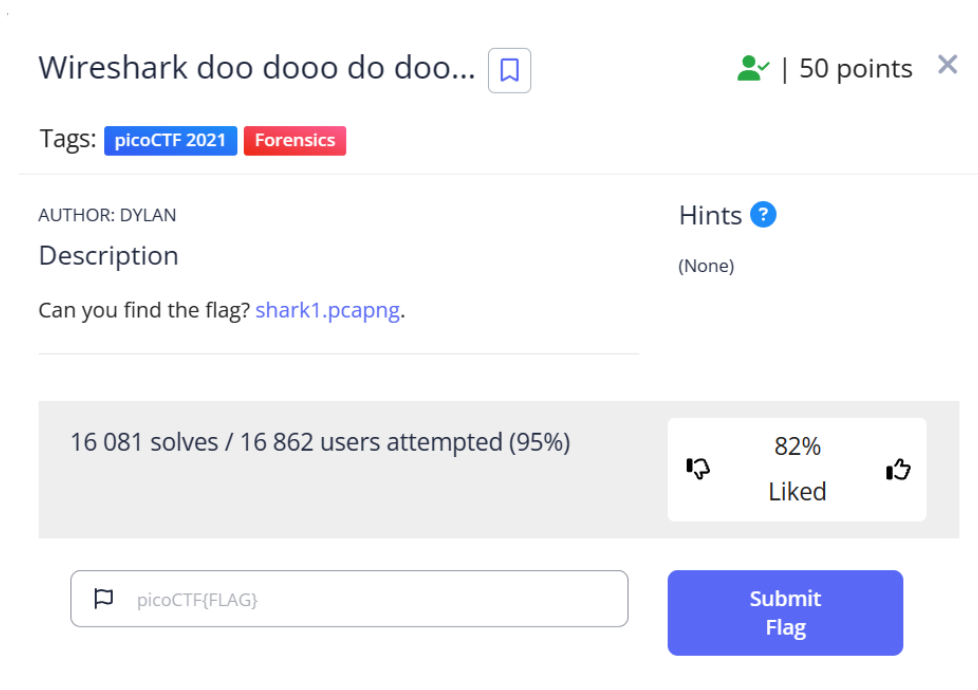


Рисунок 10 – Проверка правильности ключа

## **ЗАКЛЮЧЕНИЕ**

В данной практической работе был изучен функционал программы Wireshark, отслеживающей трафик сети, на примере пентестов.



## СПИСОК ИСТОЧНИКОВ

1. Олифер В.Г., Олифер В.А. Компьютерной сети. – 2-е изд. – Санкт-Петербург: Питер, 2021. – 1008 с.
2. Мастер класс по использованию Wireshark // youtube URL: <https://www.youtube.com/watch?v=OU-A2EmVrKQ&list=PLW8bTPfXNGdC5Co0VnBK1yVzAwSSphzpJ> (дата обращения: 01.03.2023).