Министерство образования республики Молдова

Технический Университет Молдовы

Департамент Программной Инженерии и Автоматики

Отчёт

Лабораторная работа №1

По предмету: Infractiuni informatice si tehnici de investigare

Выполнил студ. гр. SI-202 Абабий Эдуард

Проверил Масютин Максим

Кишинёв – 2023

**Scopul** acestui laborator este de a-i învăța pe studenți să determine dacă un fișier are o extensie de fișier necorespunzătoare, aceasta fiind o metodă folosită frecvent de atacatori pentru a transmite cu succes programe malware prin firewall-uri și de a le ascunde de utilizatorul tipic.

**Sarcina:**

1. Completați cîmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierelor!

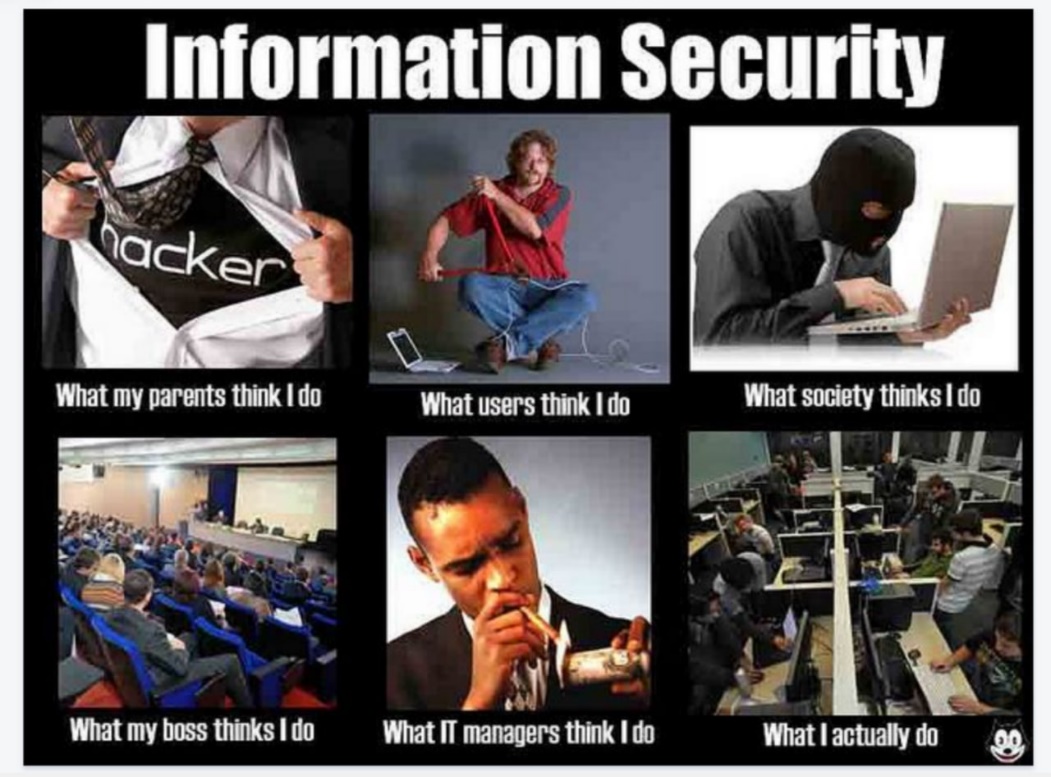
2. Alegeți un fișier la dorință și pentru acest fișier creați un writeup (descrieți pe pași cum ați rezolvat exercițiul și ați obținut informația necesară, obligatoriu includeți și capturi de ecran).

**Решение задач:**

1. file1

Первые 4 байта: **FF D8 FF 67**

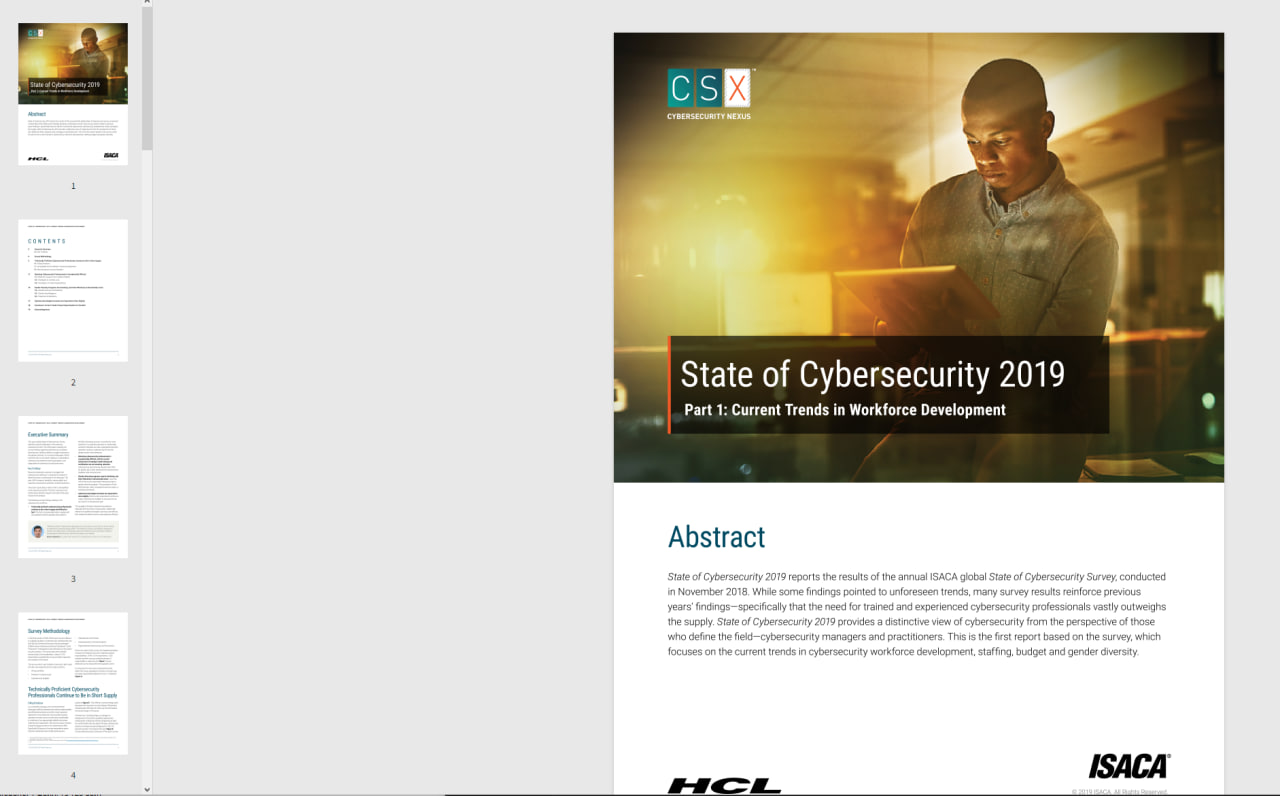
Расширение, тип файла: **JPEG/JFIF graphics file**



1. file2

Первые 4 байта: **25 50 44 6F**

Расширение, тип файла: **PDF, FDF, AI Adobe Portable Document Format, Forms Document Format, and Illustrator graphics files**



1. file3

Первые 4 байта: **50 4B 03 6F**

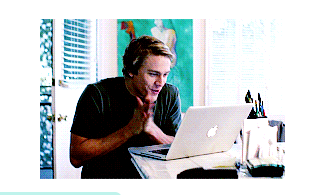
Расширение, тип файла: **ODT, ODP, OTT OpenDocument text document, presentation, and text document template, respectively.**



1. file4

Первые 4 байта: **47 49 46 38**

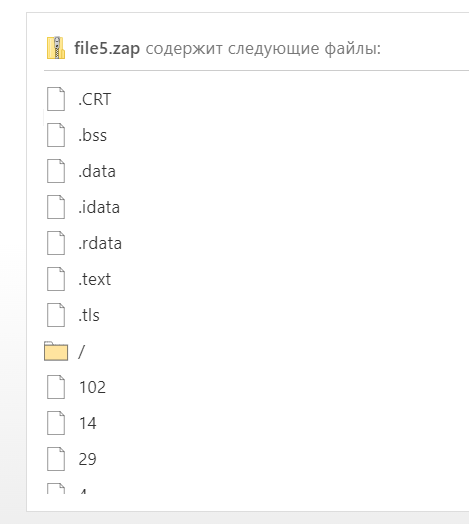
Расширение, тип файла: **GIF Graphics interchange format file**



1. file5

Первые 4 байта: **4D 5A 90 00**

Расширение, тип файла: **ZAP ZoneAlam data file**



1. file6

Первые 4 байта: **3C 68 74 60**

Расширение, тип файла: **HTML**



1. file7

Первые 4 байта: **52 61 72 66**

Расширение, тип файла: **RAR(v5) compressed archive file**



1. file8

Первые 4 байта: **50 4B 66 04**

Расширение, тип файла: **ZIP**



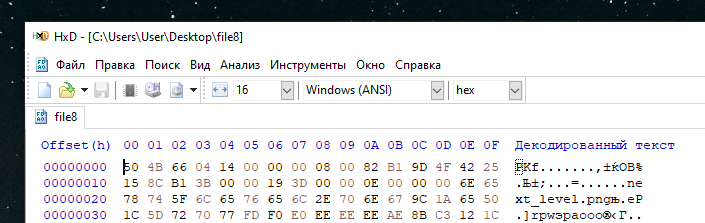
**Задание 2:**  
Write up file8

Рисунок 1 – просмотр hex кода файла

Открыл файл file8 через редактор XxD дабы посмотреть на hex код файла

По первым 4 байтам определил, что это за тип файла

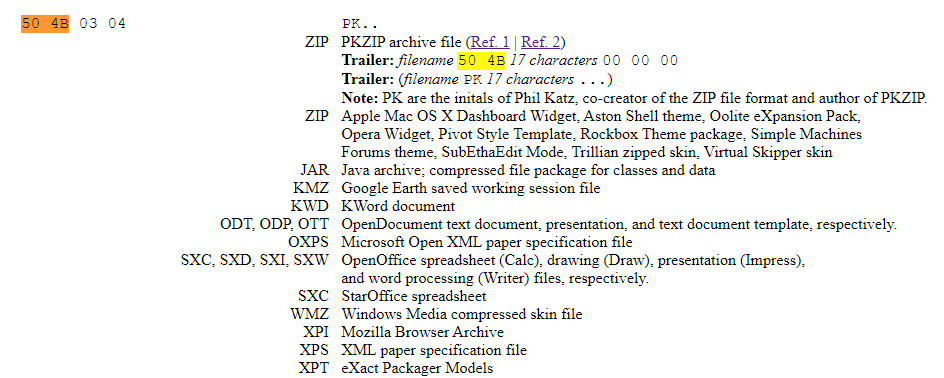


Рисунок 2 – тип файла по коду 50 4B 03 04

Изменив расширение файла на zip я смог открыть файл и увидеть содержимое архива

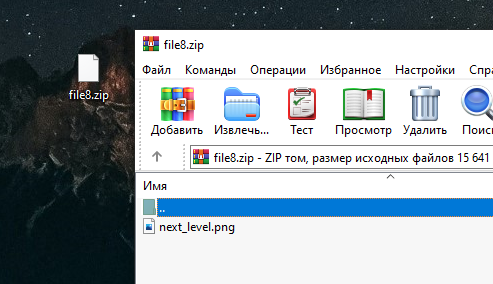


Рисунок 3 – содержимое архива file8.zip

При попытке открыть фотографию мы получаем ошибку о поврежденных данных

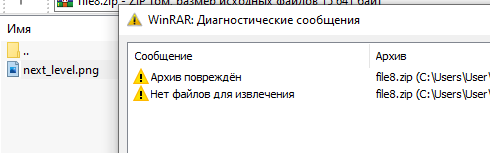


Рисунок 4 – поврежденный архив

Недолго думав и гадав, я увидел, что расширение файла в hex коде было изменено

Код нормального zip архива - 50 4B 03 04  
Код архива file8.zip - 50 4B 66 04

Заменив байты **66** на **03** мы получаем нормальный архив и можем открыть фотографию

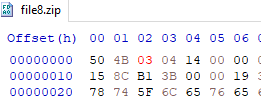


Рисунок 5 – замена байтов



Рисунок 6 – фотография из архива file8

Вывод:  
В данной лабораторной работе я изучил работу с hex редактором, узнал о том, как вычислить расширения файла по первым 4 байтам хекс кода файла.