

Министерство образования республики Молдова
Технический Университет Молдовы
Департамент Программной Инженерии и Автоматики

О т ч ё т

Лабораторная работа №1

По предмету: Infractioni 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:

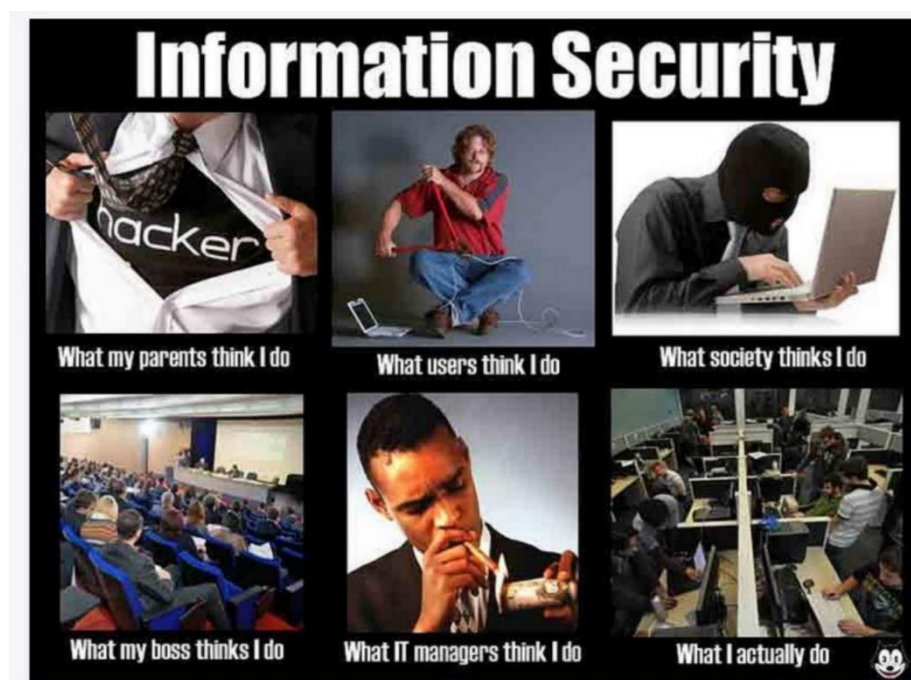
1. Completați câmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierelor!
2. Alegeți un fișier la dorință și pentru acest fișier creați un writeup (descrieți pe pași cum ați rezolvat exercițiul și ați obținut informația necesară, obligatoriu includeți și capturi de ecran).

Решение задач:

1. file1

Первые 4 байта: **FF D8 FF 67**

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



2. 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**



3. file3

Первые 4 байта: **50 4B 03 6F**

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

HACKERMAN



4. file4

Первые 4 байта: **47 49 46 38**

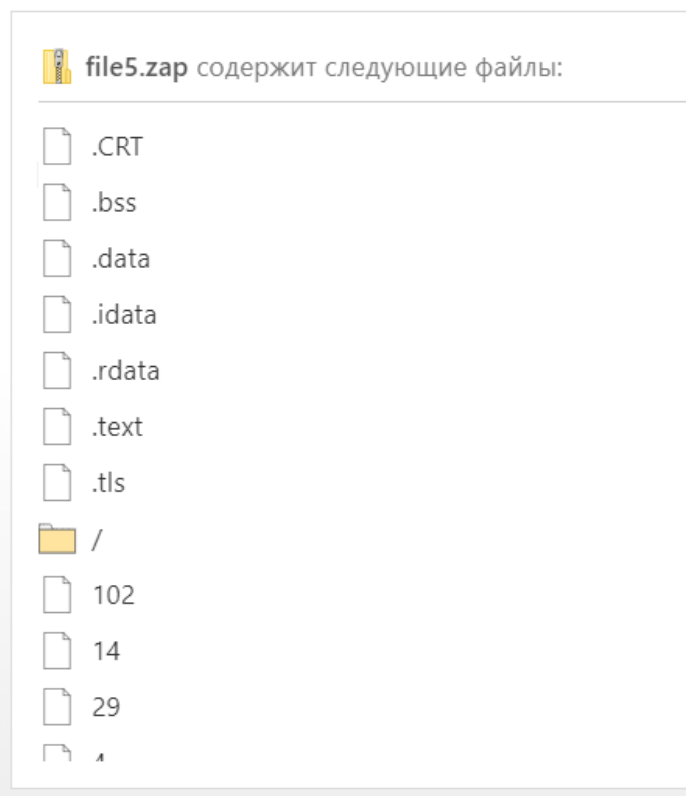
Расширение, тип файла: **GIF Graphics interchange format file**



5. file5

Первые 4 байта: **4D 5A 90 00**

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



6. file6

Первые 4 байта: **3C 68 74 60**

Расширение, тип файла: **HTML**

World Wide Web

The WorldWideWeb (W3) is a wide-area [hypermedia](#) information ret

Everything there is online about W3 is linked directly or indirectly to

[What's out there?](#)

Pointers to the world's online information, [subjects](#) , [W3 server Help](#) on the browser you are using

[Software Products](#)

A list of W3 project components and their current state. (e.g. [L: Technical](#)

[Bibliography](#) Details of protocols, formats, program internals etc

[People](#) Paper documentation on W3 and references.

[History](#) A list of some people involved in the project.

[How can I help ?](#) A summary of the history of the project.

[Getting code](#) If you would like to support the web..

Getting the code by [anonymous FTP](#) , etc.

7. file7

Первые 4 байта: **52 61 72 66**

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



8. file8

Первые 4 байта: **50 4B 66 04**

Расширение, тип файла: **ZIP**



Задание 2:

Write up file8

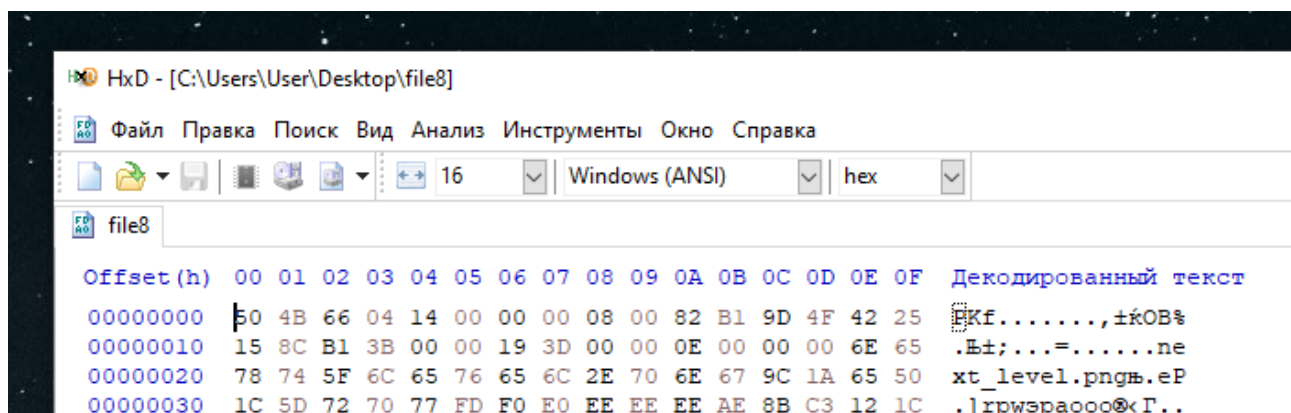


Рисунок 1 – просмотр hex кода файла

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

По первым 4 байтам определил, что это за тип файла

50 4B 03 04	PK..
	ZIP PKZIP archive file (Ref. 1 Ref. 2)
	Trailer: filename 50 4B 17 characters 00 00 00
	Trailer: (filename PK 17 characters ...)
	Note: PK are the initials of Phil Katz, co-creator of the ZIP file format and author of PKZIP.
	ZIP Apple Mac OS X Dashboard Widget, Aston Shell theme, Oolite eXpansion Pack, Opera Widget, Pivot Style Template, Rockbox Theme package, Simple Machines Forums theme, SubEthaEdit Mode, Trillian zipped skin, Virtual Skipper skin
	JAR Java archive; compressed file package for classes and data
	KMZ Google Earth saved working session file
	KWD KWord document
	ODT, ODP, OTT OpenDocument text document, presentation, and text document template, respectively.
	OXPS Microsoft Open XML paper specification file
	SXC, SXD, SXI, SXW OpenOffice spreadsheet (Calc), drawing (Draw), presentation (Impress), and word processing (Writer) files, respectively.
	SXC StarOffice spreadsheet
	WMZ Windows Media compressed skin file
	XPI Mozilla Browser Archive
	XPS XML paper specification file
	XPT eXact Packager Models

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

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

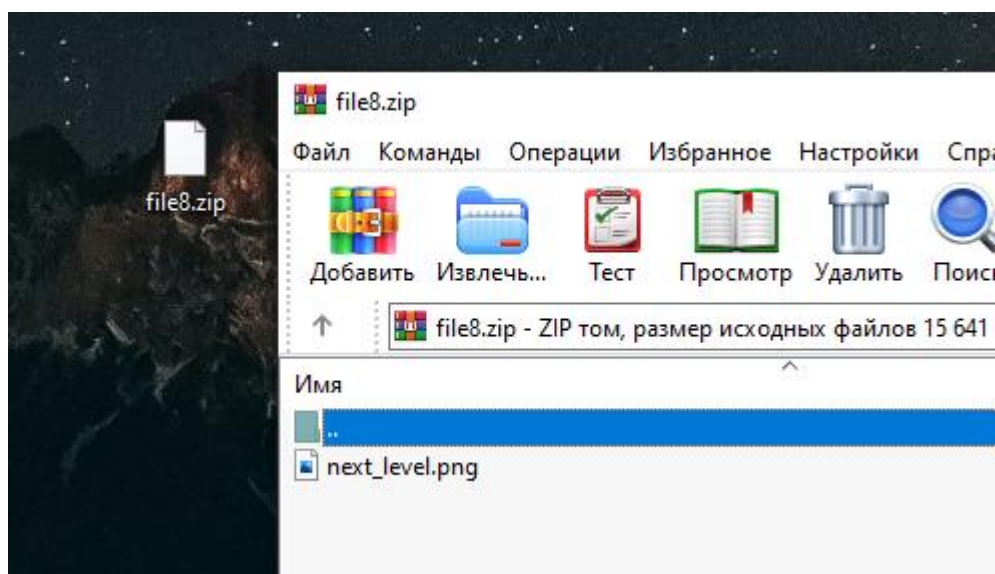


Рисунок 3 – содержимое архива file8.zip

При попытке открыть фотографию мы получаем ошибку о поврежденных данных

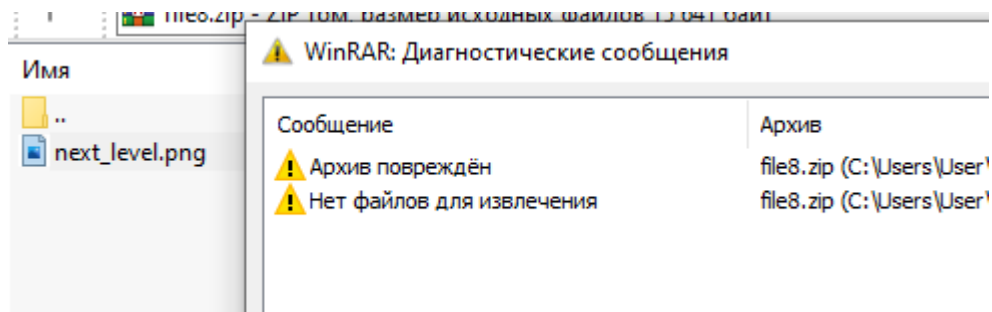


Рисунок 4 – поврежденный архив

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

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


 file8.zip								
Offset (h)	00	01	02	03	04	05	06	07
00000000	50	4B	03	04	14	00	00	00
00000010	15	8C	B1	3B	00	00	19	3
00000020	78	74	5F	6C	65	76	65	6

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.

