Lab 1 Report
Digital Forensics

Anton Fluch `anfl4215`
Johan Bäckström `jobc5829`

20 september 2017

1 Introduction

The evidence for the case where provided in a .zip file named Lab1.zip. This file produced the following hash sums:

SHA256

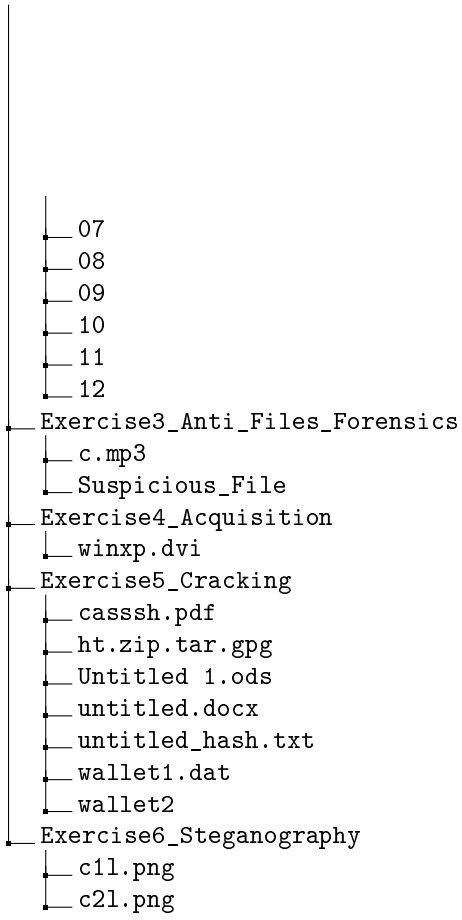
9c5d0bfbeccd75858426cfc84345e0a68687b0fc5662b715153aa88cefd60fba

MD5

c4a731672747131b8b457a77178ad386

When opening the zip file the following folders and files where present:

```
Lab1
├── Exercise1_Hashing
│   ├── erase
│   ├── erase.exe
│   ├── hello
│   ├── hello (2)
│   ├── hello (3)
│   ├── hello (4)
│   └── hello.exe
└── Exercise2_File_Identification
    ├── 01
    ├── 02
    ├── 03
    ├── 04
    ├── 05
    └── 06
```


07
08
09
10
11
12
Exercise3_Anti_Files_Forensics
c.mp3
Suspicious_File
Exercise4_Acquisition
winxp.dvi
Exercise5_Cracking
casssh.pdf
ht.zip.tar.gpg
Untitled 1.ods
untitled.docx
untitled_hash.txt
wallet1.dat
wallet2
Exercise6_Steganography
c1l.png
c2l.png

2 Exercise 1: Hashing

In order to maintain the chain of custody and to uniquely identify all the files, the hash sum where calculated for all the files in the folder Exercise1_Hashing:

SHA256

1c4ff4e490b15b2b214f26c5654decccbcbea9eb900f88649dc7b1e42341be56 erase

1316543942a8c6cd754855500cd37068edbbd8b31c4979d2825a4e799fed6102 erase.exe

fad878bd261840a4ea4a8277c546d4f46e79bbeb60b059cee41f8b50e28d0e88 hello

1316543942a8c6cd754855500cd37068edbbd8b31c4979d2825a4e799fed6102 hello (2)

60d13913155644883f130b85eb24d778314014c9479aedb5f6323bf38ad3a451 hello (3)

1c4ff4e490b15b2b214f26c5654decccbcbea9eb900f88649dc7b1e42341be56 hello (4)

60d13913155644883f130b85eb24d778314014c9479aedb5f6323bf38ad3a451 hello.exe

MD5

da5c61e1edc0f18337e46418e48c1290 erase

cdc47d670159eef60916ca03a9d4a007 erase.exe

da5c61e1edc0f18337e46418e48c1290 hello

cdc47d670159eef60916ca03a9d4a007 hello (2)

cdc47d670159eef60916ca03a9d4a007 hello (3)

da5c61e1edc0f18337e46418e48c1290 hello (4)

cdc47d670159eef60916ca03a9d4a007 hello.exe

In Kali Linux [1]

[1] https://www.kali.org/