Lab 1 Report Digital Forensics

Anton Fluch anf14215 Johan Bäckström jobc5829

21 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:

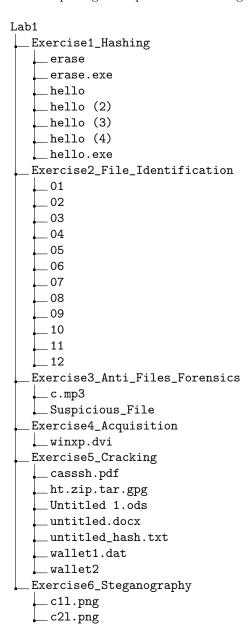
SHA256

 $9 \\c 5 \\d 0 \\b f b e \\c c d \\75858426 \\c f \\c 84345 \\e 0 \\a 68687 \\b 0 \\f \\c 5662 \\b \\715153 \\a a \\88 \\c e \\f \\d 60 \\f \\b a \\a 68687 \\b 0 \\f \\c 5662 \\b \\715153 \\a a \\88 \\c e \\f \\d 60 \\f \\b a \\a \\f \\c e \\f$

MD5

c4a731672747131b8b457a77178ad386

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



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. In Kali Linux ¹ it is possible to calculate the hash sum of a file using the 'file' command

```
sha256sum *
1c4ff4e490b15b2b214f26c5654decccbcbea9eb900f88649dc7b1e42341be56 erase
1316543942a8c6cd754855500cd37068edbbd8b31c4979d2825a4e799fed6102 erase.exe
{\tt fad878bd261840a4ea4a8277c546d4f46e79bbeb60b059cee41f8b50e28d0e88\ hello}
1316543942a8c6cd754855500cd37068edbbd8b31c4979d2825a4e799fed6102 hello (2)
60d13913155644883f130b85eb24d778314014c9479aedb5f6323bf38ad3a451 hello (3)
1c4ff4e490b15b2b214f26c5654decccbcbea9eb900f88649dc7b1e42341be56 hello (4)
60d13913155644883f130b85eb24d778314014c9479aedb5f6323bf38ad3a451 hello.exe
md5sum *
da5c61e1edc0f18337e46418e48c1290 erase
cdc47d670159eef60916ca03a9d4a007 erase.exe
da5c61e1edc0f18337e46418e48c1290 hello
cdc47d670159eef60916ca03a9d4a007 hello (2)
cdc47d670159eef60916ca03a9d4a007 hello (3)
da5c61e1edc0f18337e46418e48c1290 hello (4)
cdc47d670159eef60916ca03a9d4a007 hello.exe}
```

- 3 Exercise 2: File Headers
- 4 Exercise 3: Anti Files Forensics
- 5 Exercise 4: Acquisition
- 6 Exercise 5:
- 7 Exercise 6 Hashing

 $^{^{1} \}rm https://www.kali.org/$