SVEUČILIŠTE U SPLITU
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

IZVJEŠTAJ

LABARATORIJSKA VJEŽBA 2

Matea Lebo

Split, lipanj 2021.

Lab 2- Razumijevanje hash funkcija, ekstenzija

VJEŽBA 1

Cilj ove vježbe je razumijeti da datoteke imaju jedinstvena zaglavlja na osnovu tipa datoteke. Pokazat ćemo kako datoteke ne trebaju imati ekstenziju za koje se trenutno prikazuju. Veoma bitno je kod računalne forenzike detektirati datateke koje imaju promijenjenu ekstenziju, jer one mogu ukazivati na potencijalno skrivanje informacije.

Rj.:

```
import magic
import glob

BLOCK_SIZE = 65536
# print("1. file:")
# print(magic.from_file("Lab2_download_1/file1"))
# print(magic.from_buffer(open("Lab2_download_1/file1", "rb").read(2048)))
# print("2. file:")
# print(magic.from_file("Lab2_download_1/file2.txt"))
# print(magic.from_buffer(open("Lab2_download_1/file2.txt", "rb").read(2048)))
# print("3. file:")
# print(magic.from_file("Lab2_download_1/file3"))
# print(magic.from_buffer(open("Lab2_download_1/file3", "rb").read(2048)))

filenames = glob.glob('Lab2_download_1/*', recursive = True)
for filename in filenames :
print(filename)
print(magic.from_file(filename))
```

VJEŽBA 2

Cilj ove vježbe je pokazati kako dvije datoteke kreirane u na različitim uređajima imaju iste hash otiske ukoliko je njihov sadržaj identičan. Također ćemo pokazati iako je sadržaj datoteke identičan (razlikuje se po kapitalizaciji) hash otisak će u tom slučaju biti isti.

Rj.:

```
import glob
import hashlib

BLOCK_SIZE = 65536

filenames = glob.glob('Lab2_download_1/*', recursive = True)
for filename in filenames :
print("---------" + filename + "--------")
sha256_hash = hashlib.sha256()
md5_hash = hashlib.md5()
sha1_hash = hashlib.sha1()
with open(filename, 'rb') as f :
```

```
fb = f.read(BLOCK_SIZE)
while len(fb) > 0:
sha1_hash.update(fb)
sha256_hash.update(fb)
md5_hash.update(fb)
fb = f.read(BLOCK_SIZE)
print("SHA 256")
print(sha256_hash.hexdigest())
print("MD 5")
print(md5_hash.hexdigest())
print("SHA 1")
print(sha1_hash.hexdigest())
```

VJEŽBA 3

a) Kreirajte u Word programu datoteku te u nju upišite neki sadržaj. Sačuvajte dokument u ekstenziji .docx pod nazivom test na računalu (test.docx). Nakon toga, napravite kopiju word dokumenta te joj promijenite naziv i ekstenziju tako da ime bude identično originalnom dokumentu, dok joj je ekstenzija jednaka ekstenziji slike .jpg (test.jpg). Hoće li hash otisak (MD5 i SHA1) obaju dokumenata biti isti.

b) Pretpostavimo da je tvrtka prijavila problem korporativne špijunaže u kojem smatraju da im je ukraden/kopiran tekstualni dokument u PDF-u iznimne važnosti. Budući da tvrtka ne želi otkriti sadržaj dokumenta, forenzični istražitelj dobiva u uvid hash otisak dokumenta:

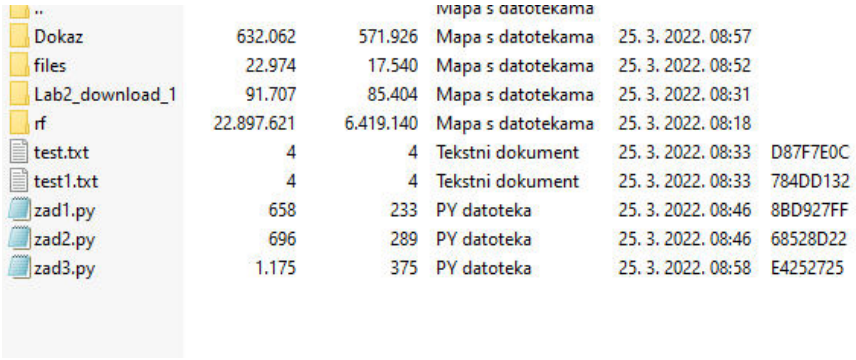
c15e32d27635f248c1c8b66bb012850e5b342119

Također, sa računala osumnjičene osobe ste izuzeli niz dokumenata koji bi mogli ukazivati na potencijalni dokaz. Dokumente u datoteci Dokaz.zip možete preuzeti iz direktorija Download. Raspakirajte dokumente i napravite analizu te navedite o kojem se dokumentu radi.

Rj:

```
import glob
import hashlib

BLOCK_SIZE = 65536

filenames = glob.glob('files/test.*', recursive = True)
for filename in filenames :
print("---------" + filename + "--------")
sha256_hash = hashlib.sha256()
md5_hash = hashlib.md5()
sha1_hash = hashlib.sha1()
with open(filename, 'rb') as f :
fb = f.read(BLOCK_SIZE)
```

```
while len(fb) > 0:
sha1_hash.update(fb)
sha256_hash.update(fb)
md5_hash.update(fb)
fb = f.read(BLOCK_SIZE)
print("MD 5")
print(md5_hash.hexdigest())
print("SHA 1")
print(sha1_hash.hexdigest())



print("------------------------------------------------")
filenames = glob.glob('Dokaz/*', recursive = True)
for filename in filenames :
sha1_hash = hashlib.sha1()
with open(filename, 'rb') as f :
fb = f.read(BLOCK_SIZE)
while len(fb) > 0:
sha1_hash.update(fb)
fb = f.read(BLOCK_SIZE)
if sha1_hash.hexdigest() == "c15e32d27635f248c1c8b66bb012850e5b342119" :
    print(f"\nFound: {filename}")
    print(sha1_hash.hexdigest())
    print("c15e32d27635f248c1c8b66bb012850e5b342119")
```



..			Mapa s datotekama		
Dokaz	632.062	571.926	Mapa s datotekama	25. 3. 2022. 08:57	
files	22.974	17.540	Mapa s datotekama	25. 3. 2022. 08:52	
Lab2_download_1	91.707	85.404	Mapa s datotekama	25. 3. 2022. 08:31	
rf	22.897.621	6.419.140	Mapa s datotekama	25. 3. 2022. 08:18	
test.txt	4	4	Tekstni dokument	25. 3. 2022. 08:33	D87F7E0C
test1.txt	4	4	Tekstni dokument	25. 3. 2022. 08:33	784DD132
zad1.py	658	233	PY datoteka	25. 3. 2022. 08:46	8BD927FF
zad2.py	696	289	PY datoteka	25. 3. 2022. 08:46	68528D22
zad3.py	1.175	375	PY datoteka	25. 3. 2022. 08:58	E4252725