SVEUČILIŠTE U SPLITU
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

IZVJEŠTAJ

LABORATORIJSKA VJEŽBA 3

Forenzika USB uređaja

Danica Majić

Split, lipanj 2022.

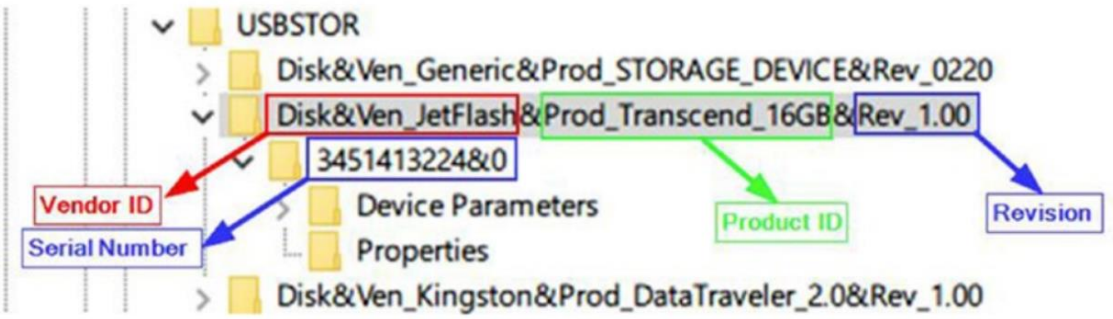
Zamislite sljedeći scenarij: sutradan imate kolokvij iz iznimno kompliciranog kolegija Računalna forenzika. Problem je u tome što nitko ne zna kako će kolokvij izgledati, primjeri kolokvija prošlih godina ne postoje, a skraćene verzije verzija skripti za učenje još nitko nije pripremio.

Međutim, saznalo se da je profesor pripremio kolokvij te ga drži spremljenog na svom računalu. U trenutku neopreznosti profesor, koji ostaje kasno na fakultetu zbog rokova na nekom projektu, odlazi van ureda uzet kavu na aparat, ne zaključava ured, te pri povratku zatekne upaljen ekran računala na kojem se nalazi otvoren direktorij u kojem je kolokvij. Sumnja se da je kolokvij procurio...

1. ZADATAK

Zadatak forenzičara je saznati je li u trenutku neopreznosti bio spojen USB memorijski ključ spojen na računalo na kojeg je mogao biti kopiran kolokvij.

Operacijski sustav Windows 10 sadrži interni log u koji sprema listu (USB) uređaja koji su prvi put bili povezani na računalo. Ime datoteke je setupapi.dev.log koja se nalazi u direktoriju \Windows\inf\. Iz direktorija Download sačuvajte datoteku setupapi.dev.log koju je forenzičar pripremio za vas.
Vaš zadatak je napraviti skriptu u pythonu koja parsira navedenu log datoteku te ispisuje sve USB uređaje koji su bili prvi put povezani na računalo kao i vrijeme u kojem su se prvi put povezali na računalo. Na slici ispod možete vidjeti koji su parametri jedinstveno identificiraju uređaj.



Na ekranu ispod možete vidjeti dio loga u kojem su parametri USB uređaja zapisani u log datoteku:

```
>>>  [Device Install (Hardware initiated) - SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_JetFlash&Prod_Transcend_16GB&Rev_1.00#3451413224&0#{5
>>>  Section start 2021/01/19 11:29:24.146
     dvi: {Build Driver List} 11:29:24.166
```

Poznavajući način na koji se u računalo sprema datoteka, možete parsiranjem veoma brzo izvući listu svih uređaja kao i trenutak u kojem se USB bio prvi put spojen na računalo.

Python kod:

usb_lab3.py

```python
def main():

    file_path = 'setupapi.dev.log'

    parseSetupapi(file_path)


def parseSetupapi(setup_file):

    in_file = open(setup_file)
    data = in_file.readlines()

    for i, line in enumerate(data):
        if 'device install (hardware initiated)' in line.lower():
            device_name = data[i].split('-')[1].strip()
            date = data[i+1].split('start')[1].strip()
            printOutput(device_name, date)

    in_file.close()


def printOutput(usb_name, usb_date):

    print('[Device Install(Hardware Initiated)-: {}'.format(usb_name))
    print('Section Start: {}'.format(usb_date))


if __name__ == '__main__':

    main()

```

REZULTAT:

```
PS C:\Users\DanicaMajić\Downloads\danica_lab3\danica_lab3> python usb_lab3.py
[Device Install(Hardware Initiated)-: USB\VID_090C&PID_1000\AA04012900007482]
Section Start: 2021/01/19 11:16:11.471
[Device Install(Hardware Initiated)-: SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_Sharkoon&Prod_Flexi
Section Start: 2021/01/19 11:16:12.248
[Device Install(Hardware Initiated)-: SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP#60A44C3FACC9B161499700B1&0#{53f56307
Section Start: 2021/01/19 11:29:24.146
[Device Install(Hardware Initiated)-: SWD\WPDBUSENUM\{03758bef
Section Start: 2021/03/22 10:50:49.821
[Device Install(Hardware Initiated)-: SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_JetFlash&Prod_TS128MJF2A&Rev_1.00#6&2d97e591&0#{53f56307
Section Start: 2021/03/25 19:54:07.999
[Device Install(Hardware Initiated)-: SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_1100#27A1808450880138&0#{53f56307
Section Start: 2021/04/08 22:31:32.255
PS C:\Users\DanicaMajić\Downloads\danica_lab3\danica_lab3>
```

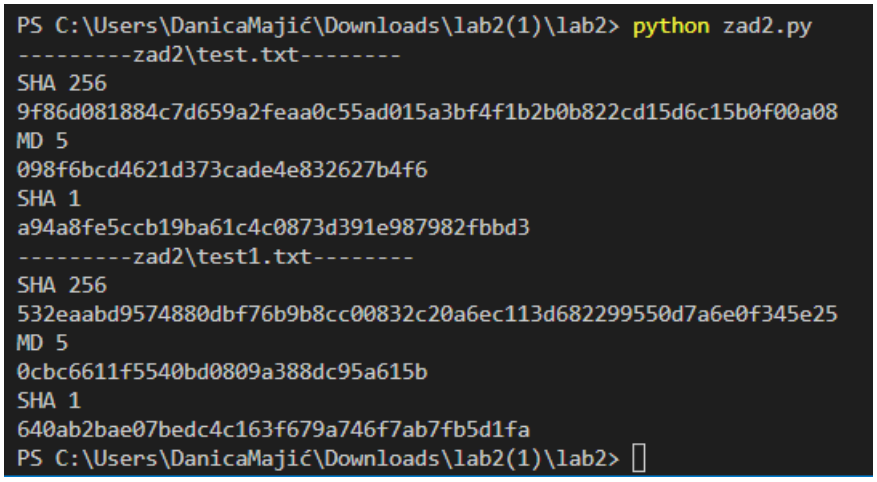
2. ZADATAK

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.

- U Notepad-u kreirajte *text* dokument
- U dokument upišite vrijednost test te sačuvajte datoteku pod nazivom test.txt
- Kreirajte novi dokument te u njega upišite vrijednost Test te ga sačuvajte pod nazivom test1.txt
- korištenjem Python programa izračunajte hash vrijednosti navedenih datoteka
- Trebali biste dobiti ove rezultate:

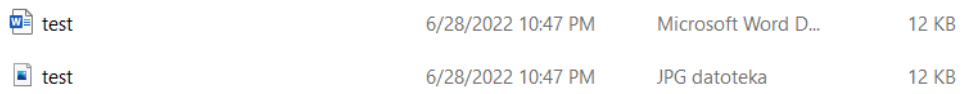
```
--Test.txt--
MD5: 098f6bcd4621d373cade4e832627b4f6
SHA1: a94a8fe5ccb19ba61c4c0873d391e987982fbbd3
SHA256: 9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

--Test1.txt--
MD5: 0cbc6611f5540bd0809a388dc95a615b
SHA1: 640ab2bae07bedc4c163f679a746f7ab7fb5d1fa
SHA256: 532eaabd9574880dbf76b9b8cc00832c20a6ec113d682299550d7a6e0f345e25
```

Dobiveni rezultati:



3. ZADATAK

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.



RIJEŠENJE: Hash otisak (MD5 I SHA1) su isti.

```
PS C:\Users\DanicaMajić\Downloads\lab2(1)\lab2> python zad3.py
---------files\test.docx--------
MD 5
29e29e66fc9636598d28d97ed46c7c1c
SHA 1
78671f9029405fa7956f4a9fedd93b66422f468e
---------files\test.jpg--------
MD 5
29e29e66fc9636598d28d97ed46c7c1c
SHA 1
78671f9029405fa7956f4a9fedd93b66422f468e
------------------------------------------------
```

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

```
Found: Dokaz\Secret_file_52.jpg
c15e32d27635f248c1c8b66bb012850e5b342119
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.

KOD:

```python
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")
```