SVEUČILIŠTE U SPLITU
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

IZVJEŠTAJ

LABARATORIJSKA VJEŽBA 3

Matea Lebo

Split, lipanj 2021.

Lab 3- Forenzika USB uređaja

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.

```
__version__ = 0.01


def main():

    file_path = 'setupapi.dev.log'

    # Print version information when the script is run
    print('='*22)
    print('SetupAPI Parser, ', __version__)
    print('='*22)

    parseSetupapi(file_path)


def parseSetupapi(setup_file):
    """
    Interpret the file
    :param setup_file: path to the setupapi.dev.log
    :return: None
    """
    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 the information discovered
    :param usb_name: String USB Name to print
    :param usb_date: String USB Date to print
    :return: None
    """

    print('Device: {}'.format(usb_name))
    print('First Install: {}'.format(usb_date))


if __name__ == '__main__':
    # Run the program
    main()
```