

1. Crack file zip berpassword berikut untuk mendapatkan material UAS. (15)

```
bruteforce.txt - Notepad
File Edit Format View Help
from tqdm import tqdm

import zipfile
import sys


# the password list path you want to use
wordlist = "wordlist.txt"
# the zip file you want to crack its password
zip_file = "UAS.zip"
# initialize the Zip File object
zip_file = zipfile.ZipFile(zip_file)
# count the number of words in this wordlist
n_words = len(list(open(wordlist, "rb")))
# print the total number of passwords
print("Total passwords to test:", n_words)
with open(wordlist, "rb") as wordlist:
    for word in tqdm(wordlist, total=n_words, unit="word"):
        try:
            zip_file.extractall(pwd=word.strip())
        except:
            continue
        else:
            print("[+] Password found:", word.decode().strip())
            exit(0)
print("[!] Password not found, try other wordlist.")

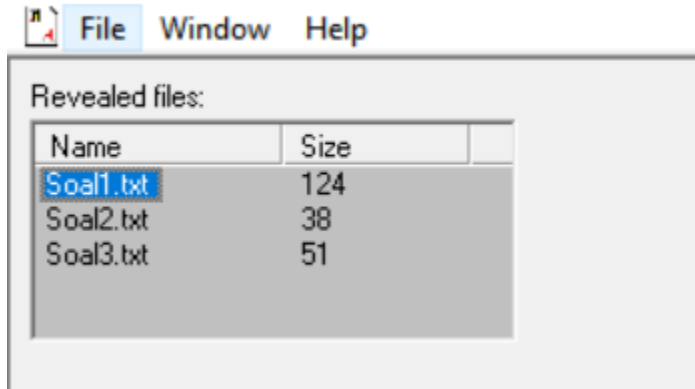
D:\Kuliah\Sistem Forensik Digital>python bruteforce.py
Total passwords to test: 12647
0%|          | 0/12647 [00:00<?, ?word/s][
+] Password found: SFD
0%|          | 0/12647 [00:05<?, ?word/s]

D:\Kuliah\Sistem Forensik Digital>cd UAS
D:\Kuliah\Sistem Forensik Digital\UAS>python bruteforce.py
Total passwords to test: 12647
0%|          | 0/12647 [00:00<?, ?word/s][
+] Password found: DF1
0%|          | 1/12647 [00:01<3:56:27, 1.12s/word]
```

2. Analisa file pcap

- a. Kapan tanggal dan waktu infeksi?(5)  
komputer terinfeksi pada tanggal 2017-01-27
- b. Apa alamat MAC dari komputer Windows yang terinfeksi?(5)
- c. Apa alamat IP dari komputer Windows yang terinfeksi?(5)  
172.16.4.193
- d. Apa nama host dari komputer Windows yang terinfeksi?(5)  
STEWIE-PC
- e. Jenis malware apa yang menginfeksi komputer?(5)

- f. Apa nama malware yang menginfeksi komputer pengguna?(7.5)
  - g. Kit exploit apa yang digunakan untuk menginfeksi komputer pengguna?(7.5)
  - h. Situs web apa yang disusupi sehingga memulai rantai peristiwa infeksi?(7.5)  
Tse1.mm.bing.net
  - i. Sebelum komputer Windows terinfeksi, apa yang dicari pengguna di Bing?(7.5)  
Sebelum terkena infeksi pengguna diketahui mencari berita menggunakan Bing
3. Temukan 3 pertanyaan yang tersembunyi pada gambar dalam file zip.(10)
-  S-Tools - [Revealed Archive]



4. Jawab pertanyaan yang tersembunyi tersebut.
- a. Sebutkan teknik mengamankan data!(apa saja cara yang bisa kita gunakan untuk menghalangi penyusup mendapatkan data kita?)
 

Terdapat banyak cara untuk mengamankan data agar menghalangi penyusup untuk mendapatkan data, diantaranya adalah Enkripsi, Firewall, Cryptography, Secure Socket Layer(SSL), PGP dan Sniffer Packet
  - b. Berikan pandanganmu terhadap UU ITE
 

UU ITE di Indonesia dapat dibilang belum sempurna atau belum mature, karena pada beberapa sisi terdapat UU sehingga kian tahun terjadi peningkatan pelanggaran UU ITE yang padahal seharusnya tidak perlu dilakukan tindak pidana, sering kali juga UU ITE digunakan untuk kepentingan yang tidak semestinya, missal Ketika ada seseorang yang mengkritik sesuatu, jika ada pihak lain yang tidak terima maka bisa menggunakan beberapa pasal UU ITE untuk menjerat orang tersebut, beberapa waktu lalu juga saya mendengar berita bahwa pemerintah akan menerapkan UU ITE seperti RRC dimana hal ini akan menjadikan UU ITE lebih opresif lagi
  - c. Apa yang perlu direvisi/ditambahkan dari UU ITE?
 

Perlu dilakukan kajian dan revisi yang lebih mendalam lagi mengenai UU ITE, salah satu contoh yang aneh dari UU ITE adalah kebocoran data yang terjadi akhir akhir ini, bukannya mengatasi kebocoran data, malah website leakersnya yang di blokir, hal ini tentu tidak menutup kemungkinan oknum untuk melakukan pembobolan data lebih

banyak lagi. mungkin pemerintah Indonesia bisa melihat EU yang sudah menerapkan UU ITE sebagai salah satu UU terpenting, dimana keamanan pengguna menjadi factor utama dalam UU tersebut.