Tutorial za brisanje metapodataka file system-a sa slike diska

Uvod

Imamo sliku diska na kojemu se između ostaloga nalaze neke obrisane datoteke. Te obrisane datoteke je moguće rekonstruirati na dva načina:

1. "brzo", pomoću metapodataka *file system*-a koji nam olakšavaju pronalazak
2. "sporo", pretraživajući cijelu sliku za otiscima (*file signature*) traženih datoteka (obično povezanih uz format datoteke)

Ta druga metoda je poznata pod nazivom *file carving*. Mi želimo sa slike izbrisati sve podatke osim čistih podataka obrisanih datoteka kako bi samo taj način rekonstrukcije bio moguć.

Postupak

Tutorial je objašnjen na primjeru u kojem imamo:

- Sliku diska (*slika_sa_metapodacima.img*)
- Tražene obrisane datoteke (*dokument1.docx*, *dokument2.pdf*, *slika.jpeg*, *tekst.txt*)

Postupak se provodi na *Windows* OS-u uz hex editor *HxD*, no sličan je i na drugim sustavima sa drugim hex editorom. Pretpostavljeno je osnovno znanje korištenja hex editora.

Ovaj postupak pretpostavlja da datoteke nisu fragmentirane. U slučaju da postoje fragmentirane datoteke, potrebno je naći njene fragmente u slici i tretirati ih kao odvojene datoteke u ovom postupku.

1. Otvori sliku i sve datoteke u hex editoru

slika

2. Pronađi koje byte-ove na slici zauzimaju datoteke

1. Otvori prvu datoteku u hex editoru
2. Označi i kopiraj cijeli njen hex sadržaj
3. Otvori sliku u hex editoru
4. Pretraži ju pomoću upravo kopiranog hex sadržaja. Za *HxD*:
    1. Pozicioniraj se na početak slike
    2. Odaberi Search → Find
    3. Zaljepi kopiran hex sadržaj u "Search for" polje (ako je sadržaj prevelik polje će izgledati prazno no sve će normalno funkcionirati)
    4. Odaberi "Hex-values" u "Datatype" polju
    5. Odaberi "Forward" u "Search direction" polju
    6. Stisni "OK"

5. Zapiši koje *byte*-ove zauzima ta datoteka u slici, i ponovi postupak od koraka 1 sa sljedećom datotekom
    1. U *HxD*-u je to označeno u donjem dijelu prozora (prikazano na slici)

slika

U mojem slučaju, datoteke sadržavaju ove *byte*-ove na slici:

Ime datoteke	**Prvi byte**	**Zadnji byte**
dokument1.docx	24000	25295
dokument2.pdf	28A6000	28AC304
slika.jpg	28AD000	28C3C7C
tekst.txt	295E920	295E982

=== 3.

From:
http://studentski-izvjestaji.zesoi.fer.hr/ - **Studentski izvještaji**

Permanent link:
http://studentski-izvjestaji.zesoi.fer.hr/doku.php?id=studenti:zad_deljkic:tutorial_brisanja_metapodataka&rev=1423178887

Last update: **2023/06/19 16:20**