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 svi koraci su slični 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 kopiju slike i sve datoteke u hex editoru

- 1. Napravi kopiju slike (slika_bez_metapodataka.img)
- 2. Otvori nju 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 \rightarrow 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. Popuni prostor između datoteka sa nulama

- 1. Pronađi prvi prostor između datoteka
 - 1. On se nalazi između 0. byte-a i početka prve datoteke na slici
 - 2. U mojem slučaju prva datoteka je dokument1.docx (prvi byte se nalazi na 24000. poziciji)
 - 3. Dakle prvi prostor mi se nalazi od 0. do 23FFF. byte-a
- 2. Prebriši taj prostor nulama. U HxD-u:
 - 1. "Edit" \rightarrow "Select block"
 - 2. Provjeri da je odabran "Hex" na kraju prozora
 - 3. "Start-offset" početak prostora (za moj prvi prostor 0)
 - 4. "End-offset" kraj prostora (za moj prvi prostor 23FFF)
 - 5. Stisni "OK", sad je prostor označen
 - 6. Desni klik bilogdje na označenom prostoru → "Fill Selection"
 - 7. "Passes" → izbriši sve osim "1. pass" tipkom "Delete"
 - 8. Stisni "Zerobytes"
 - 9. Stisni "OK", označeni prostor je prebrisan nulama
- 3. Pronađi novi prostor između datoteka i ponovi prošli korak
 - 1. Sljedeći prostor počinje nakon kraja trenutne datoteke do početka sljedeće

slika

4. Slika je gotova

Spremi sliku pritiskom na "File" → "Save".

