Usporedba file carving programa

Uvod

Ovaj dokument služi kao kratka usporedba programa za *file carving*. Uspoređena su 3 najčešće korištena *file carving* programa u praktičnim scenarijima: foremost, scalpel i PhotoRec.

Sva tri programa su FOSS (*Free and open-source software*), rade na (između ostaloga) operacijskom sustavu Linux te podržavaju *carving* velikog broja različitih formata datoteka.

Ni jedan od ova tri programa ne pokušava pronaći informacije sakrivene steganografijom ili šifriranjem - drugi programi, posebno namijenjeni za te svrhe, su za to prikladniji.

Foremost

Foremost je jedan od najstarijih *file carving* programa. On koristi konfiguracijsku datoteku u kojoj su zapisani *headeri*, *footeri* i maksimalne duljine različitih vrsta datoteka pomoću kojih identificira datoteke u slobodnom prostoru diska.

Scalpel

Scalpel je *file carving* program napravljen na temelju verzije foremosta verzije 0.69. On je često brži od foremost-a i ostalih programa no uz to donosi i veliki broj beskorisnih (*false postive*) datoteka, čime je konačna veličina njegovog izlaza često i do nekoliko redova veličine veća od izlaza drugih programa. Takvi rezultati su dobiveni jer Scalpel za svaki pronađeni *header* konstruira novu datoteku ni najmanje ne gledajući je li ona ispravna.

PhotoRec

PhotoRec je *file carving* program originalno napravljen za povrat obrisanih slika, no danas podržava sve česte vrste datoteka. On koristi tehnike *carvinga* kao i foremost, no uz nešto sofisticiraniju implementaciju, tražeći više vrsta uzoraka koji uključuju i uzorke iz sredine datoteka a ne samo *headere* i *footere*.

Analize programa

Dva izvora[1][2] su napravila analizu različitih *carving* programa, oba uključujući foremost, scalpel i PhotoRec. Glavna tema analize je preciznost pronađenih datoteka, no analizirano je i vrijeme potrebno za obradu slike diska i ukupna veličina izlaza.

Analiza se vršila pokretanjem programa nad različitim slikama diska te provjeravanjem koliko se pronađenih datoteka poklapa sa originalnim datotekama.

U oba izvora je PhotoRec bio na samom vrhu po preciznošću. Nije bio najbolji jedino u jednoj od četiri

slike diska u drugom izvoru[2] te u prvom izvoru[1] u analizi slike gdje je najbolji program bio specifično napravljen za taj izazov (sliku diska). U oba slučaja je bio drugi po preciznošću, ne daleko od prvog.

Što se tiče relativnog poretka ova tri programa po preciznošću, konzistentno je PhotoRec bio prvi, foremost drugi te scalpel treći.

Gledajući relativan poredak po brzini, scalpel je najčešće bio najbrži, PhotoRec drugi najbrži, a foremost najsporiji.

Osobna iskustva

Koristio sam sva tri programa u praktičnom slučaju na slici diska od 500GB, koristeći operacijski sustav Kali Linux. Ni jedan program nije u potpunosti savršen, no PhotoRec se bez sumnje čini najbolji.

Sva tri programa su bila jednostavna za koristiti. PhotoRec ima najdetaljnije i najjednostavnije sučelje koje vodi korisnika kroz korake, te omogućava jednostavno zaustavljanje i nastavljanje analize.

Foremost je u nekom trenutku zapeo na slici, i nakon više pokretanja je svaki put zapeo na istome mjestu i nije nastavljao. Podaci nađeni do tog trenutka su se činili dobro sastavljeni.

Scalpel je napravio analizu cijelog diska bez stajanja no dao je ~200GB podataka, od kojih je velika većina bila beskorisna.

PhotoRec je obavio analizu cijelog diska bez stajanja, no na kraju analize je samo krenuo ispočetka, i tako nastavio dok ga nisam na trećem pokretanju odpočetka zaustavio. No čini se da to nije utjecalo na analizu diska, broj pronađenih datoteka se nije promijenio od kraja prvog prolaska.

Vremenski su sva tri alata bila relativno slična.

Što se tiče pronađenih datoteka, PhotoRec je pronašao najveći broj datoteka i velika većina se čini u potpunosti ispravna. Foremost je pronašao manji broj datoteka od PhotoRec-a, no to je možda i očekivano jer zbog bug-a nije uspio analizirati sliku do kraja. Scalpel je našao oko 20 puta veću količinu podataka od PhotoRec-a i foremost-a, no i uz to nije pronašao sve datoteke koje su oni pronašli.

Zaključak

Rezultati analize iz dva izvora se poklapaju sa mojim osobnim iskustvom - PhotoRec je jedan od najboljih, ako ne i najbolji alat za generalni *file carving*. Obavlja analizu slike u usporedivom vremenu sa ostalim alatima, te daje najbolje rezultate.

Izvori

1. https://digital-forensics.sans.org/summit-archives/2010/eu-digital-forensics-incident-response-summit-bas-kloet-advanced-file-carving.pdf - “Advanced file carving - How much evidence are you ignoring?”, Bas Kloet, Hoffmann Investigations, rujan 2010.
2. http://www.dtic.mil/dtic/tr/fulltext/u2/a550119.pdf - “A Comparative Analysis Of File Carving -

Software”, Timothy Courrejou, Simson L. Garfinkel, 12.9.2011.
3. http://foremost.sourceforge.net/ - Foremost
4. https://github.com/sleuthkit/scalpel - Scalpel
5. http://www.cgsecurity.org/wiki/PhotoRec - PhotoRec