CARNET

File carving

CERT.hr-PUBDOC-2019-4-377

CERT.hr

Sadržaj

1 Uvod

Pojam „*file carving*“ u užem smislu predstavlja proces obnove (rekonstrukcije) datoteka s digitalnog medija za pohranu podataka bez korištenja metapodataka datotečnog sustava. Popularnim jezikom rečeno radi se o spašavanju datoteka koje su obrisane, izgubljene, oštećene ili sakrivene. Isti proces u širem smislu naziva se „*data carving*“ i označava „izrezivanje“ manjeg skupa podataka (npr. datoteka) iz određenog šireg skupa podataka. Taj širi skup podataka, osim na tvrdim diskovima, može biti zapisan na bilo kojem mediju za pohranu podataka, npr. u memoriji računala, prijenosnim medijima, sustavima za pohranu podataka u oblaku ili u snimci mrežnog prometa.

File carving se koristi kada uobičajene metode obnove podataka ne daju rezultate, npr. kada razni „*undelete*“ programi ne uspijevaju obnoviti izbrisane datoteke jer nisu dostupni metapodaci datotečnog sustava. Proces se može koristiti za spašavanje podataka nakon nezgode ili kao dio računalne forenzike kada je potrebno obnoviti obrisane podatke koji mogu poslužiti kao dokazni materijal.

1.1 Datotečni sustavi

O organizaciji datoteka na medijima za pohranu podataka brinu se datotečni sustavi. Svaki datotečni sustav na svoj način organizira podatke koji se zapisuju u alokacijske tablice (eng. *allocation tables*). Navedeni metapodaci služe operacijskom sustavu kao upute kako doći do pojedinih datoteka. Datotečni sustavi osiguravaju podršku i za mnoga druga svojstva direktorija i datoteka kao što su npr. šifriranje podataka, kontrola pristupa, integritet podataka itd.

U tablici 1 prikazani su različiti operacijski sustavi te odgovarajući datotečni sustavi koje oni koriste.

Operacijski sustav	Datotečni sustav
Windows Me, 98, 95 i stariji	FAT12, FAT16, FAT32, VFAT, exFAT
Windows NT, XP, Server 2003, Vista, Server 2008, 7, 8, Server 2012, 10, Server 2016	NTFS (eng. *New Technology File System*)
Mac OS	HFS, HFS+, APFS
Linux	ext2/ext3/ext4 i brojni drugi

Tablica 1 – različiti operacijski sustavi s pripadajućim datotečnim sustavima

U nastavku je dan kratki pregled najčešće korištenih datotečnih sustava kod operacijskih sustava Windows, Linux i MacOS.

Datotečni sustavi operacijskog sustava Microsoft Windows

Datotečni sustavi koji se najčešće koriste kod Windows operacijskih sustava su FAT (eng. *File Allocation Table*), NTFS (eng. *New Technology File System*) i exFAT.

Datotečni sustav FAT sastoji se od početnog (eng. *boot*) sektora, alokacijske tablice i prostora za spremanje direktorija i datoteka.

Naziv datoteke može imati do osam znakova, a nastavak tri. Datoteka nema oznaku vlasnika. Mogu joj se definirati prava čitanja i pisanja. Iz datotečnog sustava FAT nastali su datotečni sustavi FAT12, FAT16 i FAT32.

Uvođenjem operacijskog sustava Windows NT 1993. godine počeo se koristiti datotečni sustav NTFS kojim su uvedene brojne funkcionalnosti koje nisu bile podržane u datotečnim sustavima FAT.

Datotečni ustav exFAT zaštićen je patentnim pravima i ima neke prednosti u odnosu na NTFS, ali nije kompatibilan s ranijim inačicama datotečnih sustava FAT.

Datotečni sustavi operacijskih sustava Linux

Operacijski sustavi Linux su nastali u zajednici slobodnog softvera (eng. *free and open source software*). Razvijani su za niz različitih primjena tako da podržavaju različite datotečne sustave. Primjeri podržanih datotečnih sustava su:

- ext2, ext3, ext4 – osnovni Linux datotečni sustavi. Naziv datoteke može imati 254 znaka, datoteka ima oznaku vlasnika i pripadnost grupi. Mogu se definirati prava izvođenja, čitanja i pisanja. Pored datoteka, datotečni sustav omogućuje zapisivanje uređaja (eng. *device*) i cjevovoda (eng. *pipes*). Unaprjeđenjem ext2 datotečnog sustava nastao je ext3, koji koristi transakcijski način zapisivanja datoteka, a daljnjim unaprjeđenjem ext3 nastao je ext4 koji ima podršku za optimiran način zapisa dodijeljenih sektora i svojstava datoteka;

- ReiserFS – datotečni sustav razvijen za pohranu velike količine malih datoteka. Ima dobru mogućnost pretraživanja datoteka i omogućava zapisivanje malih datoteka na način da sprema krajeve datoteka zajedno s njihovim metapodacima, kako se ne bi koristili veliki blokovi za ovu namjenu;

- XFS – datotečni sustav se koristi kod IRIX poslužitelja, a razvijen je u tvrtki SGI. Sustav ima dobre performanse i široko se koristi kod pohrane velike količine podataka;

- JFS – datotečni sustav razvijen u IBM-u kao podrška za rad snažnih računalnih sustava.

Datotečni sustavi operacijskog sustava MacOS

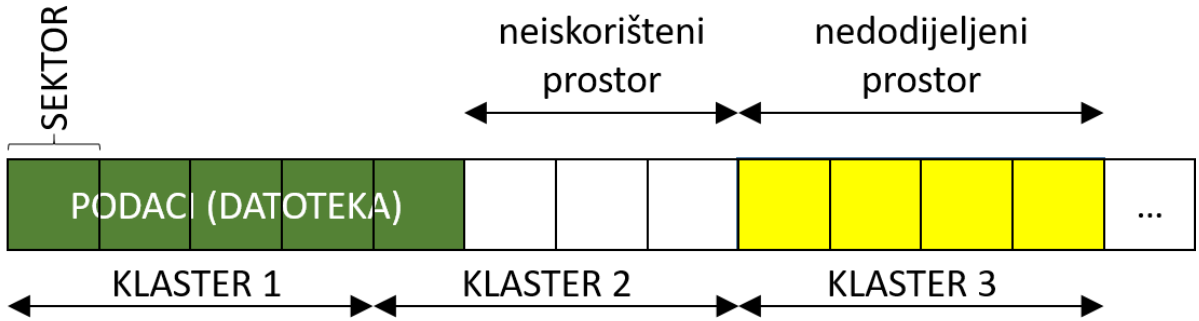
MacOS (prijašnji OS X) koristi datotečni sustav Apple File System (APFS) koji je zamijenio datotečni sustav HFS+, dok je HFS+ nastao iz prijašnjeg datotečnog sustava HFS. Datotečni sustavi APFS se koristi na velikom broju različitih proizvoda tvrtke Apple (Mac računala, iPhone pametni telefoni, iPod medijski uređaji i Apple X poslužitelji). Osim podataka o direktorijima i datotekama, datotečni sustavi pohranjuju i zapise o izgledu direktorija, poziciji prozora itd.

1.2 Zapisivanje podataka

Prilikom zapisa podataka na digitalne medije, podaci se obično ne zapisuju bajt po bajt, već se grupiraju u tzv. sektore ili blokove koji su obično veličine 512, 1024, 2048, 4096 ili više bajtova. Primjerice, ako se koriste sektori/blokovi veličine 512 bajtova, a neka

datoteka je veličine 800 bajtova, ona će zauzeti dva sektora/bloka od 512 bajtova, odnosno 1024 bajtova sveukupno.

Neki datotečni sustavi grupiraju sektore u jedinice koje se nazivaju klasteri. Klasteri sadržavaju jedan ili više uzastopnih sektora. Broj sektora u klasteru ovisi o karakteristikama računala i operacijskih sustava te je uvijek potencija broja 2 (npr. 2^0=1, 2^1=2, 2^2=4, 2^3=8, 2^4=16 itd.). Taj se broj određuje kod formatiranja datotečnog sustava i uvijek je konstantan broj. Kod zapisivanja podataka, datotečni sustav će datotekama dodijeliti cijeli broj klastera, čak i ako su podaci manji od ukupne veličine dodijeljenog prostora. Ako primjerice neki podaci zauzimaju 5 sektora, uz klastere veličine 4 sektora, za njihovu pohranu dodijelit će im se 2 klastera, kako je prikazano na slici 1.



Slika 1 – pohranjivanje datoteka u klastere

Iskorišteni dio prostora naziva se dodijeljeni prostor (eng. *allocated space*), dok se dio prostora koji ostaje prazan naziva neiskorišteni prostor (eng. *slack space*). On može biti prazan ili može sadržavati podatke od obrisanih datoteka. Prostor koji nije dodijeljen niti jednoj datoteci naziva se nedodijeljeni prostor (eng. *unallocated space*). On isto tako može biti prazan ili može sadržavati podatke od obrisanih datoteka.

Postoje tri osnovne strukture zapisa koje se koriste kod datotečnih sustava:

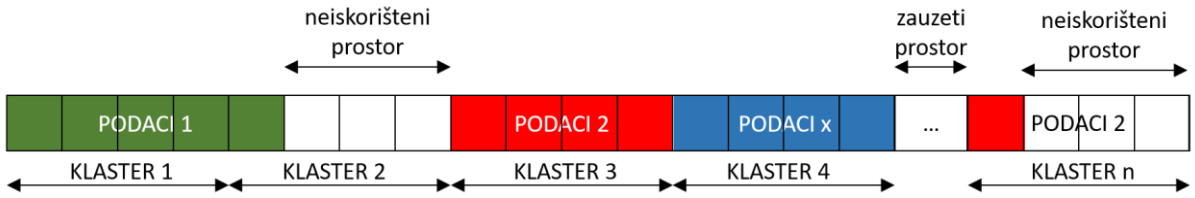
- kontinuirana (svi podaci se pohranjuju kontinuirano, u blokovima koji slijede jedan iza drugog);
- povezana (svaki blok podataka sadrži pokazivač na sljedeći blok podataka);
- indeksirana (indeksni blok sadrži pokazivače na blokove u kojima je datoteka zapisana).

Moderni datotečni sustavi nastoje podatke zapisivati kontinuirano. Međutim, ponekad zapisi ipak budu fragmentirani tj. razbacani u klastere/blokove podataka koji nisu susjedni. Do fragmentarnog zapisa podataka dolazi se u slučajevima:

- kada je malo slobodnog prostora na disku
- ili zbog brisanja, skraćivanja ili proširenja postojećih datoteka.

S porastom kapaciteta digitalnih medija poput diskovnih pogona i memorijskih kartica, smanjuje se vjerojatnost da će zapisi datoteka biti fragmentirani. Ipak, ta vjerojatnost raste s povećanjem veličina datoteka. Nedostatak fragmentarnosti zapisa očituje se i u

dodatnom vremenu potrebnom za pretraživanje i pomicanja glava za čitanje na tvrdim diskovima kako bi došli do pozicije na kojem se nalaze različiti dijelovi datoteke koje je potrebno sklopiti u jedinstveni skup podataka. Novi operacijski sustavi nastoje izbjeći fragmentarnost zapisa, što je relativno jednostavno uz veliki dostupni prostor za zapisivanje, ali u nekim slučajevima to ipak nije moguće. Na slici 2 prikazani su kontinuirani i fragmentirani zapis podataka. Primjerice, želimo pohraniti dvije datoteke veličine 5 sektora, dok su klasteri veličine 4 sektora. Tada, zauzeće diska neće biti 10 sektora, već 16 sektora, zato što će svaka datoteka zauzeti 2 cijela klastera (tj. ukupno 8 + 8 = 16 sektora). Na slici 2, datoteka označena „PODACI 1“ zapisana je kontinuirano (u klasterima 1 i 2), dok je datoteka označena „PODACI 2“ fragmentirano zapisana (u klasterima 4 i *n*).



Slika 2 – primjer kontinuiranog i fragmentiranog zapisa datoteka

Neki od pojmova s kojima se susrećemo kod zapisivanja podataka su sljedeći:

- Zaglavlje (eng. *header*) – blok podataka koji sadrži početni dio datoteke.
- Podnožje (eng. *footer*) – blok podataka koji sadrži završni dio datoteke.
- Fragment (eng. *fragment*) – jedan blok ili niz blokova koji pripadaju jednoj datoteci. Jedna datoteka može biti zapisana u više različitih fragmenata koji nisu međusobno povezani, a čak ne moraju biti posloženi po nekom redoslijedu. Udaljenost između pojedinih fragmenata nije poznata, a moguće je da dio fragmenata ni ne postoji na mediju jer su preko njih zapisani drugi podaci.
- Osnovni fragment (eng. *base fragment*) – početni fragment u zapisu datoteke. Sadrži zaglavlje (ako je dostupno).
- Točka fragmentacije (eng. *fragmentation point*) – zadnji blok podataka u zapisu datoteke poslije kojega nastupa fragmentacija. Kako postoji mogućnost da je datoteka zapisana u više fragmenata, tako za jednu datoteku može postojati i više točaka fragmentacije.
- Područje fragmentacije (eng. *fragmentation area*) – uzastopni blokovi podataka koji su grupirani u skup koji sadrži točku fragmentacije.

1.2.1 Metapodaci

Da bismo znali što se događa s datotekama kada se obrišu, moramo znati kako pojedini datotečni sustavi funkcioniraju. Iako *file carving* alati rade na temelju poznate strukture datoteke, a ne na temelju metapodataka iz datotečnog sustava, poznavanje kako pojedini datotečni sustavi funkcioniraju i zapisuju datoteke može biti prilično korisno.

Kada se datoteka obriše, metapodaci o datoteci (npr. naziv datoteke, veličina, lokacija prvog bloka podataka/klastera itd.) mijenjaju se na sljedeći način:

- kod operacijskih sustava Windows, prvo slovo u nazivu datoteke mijenja se u binarni zapis koji odgovara heksadekadskoj vrijednosti E5; na datotečnim sustavima kod operacijskih sustava Linux naziv datoteke ostaje i dalje dostupan, ali se briše adresa prvog bloka s metapodacima;

- briše se zapis datoteke iz alokacijske tablice, čime se operacijskom sustavu daje do znanja da se lokacije obrisane datoteke mogu dodijeliti novoj datoteci;

- podaci sadržaja datoteke ostaju i dalje fizički zapisani na istom mjestu, ali samo do trenutka dok se djelomično ili u potpunosti oni ne prepišu novim podacima.

1.3 Datoteke

Datoteke su imenovane zbirke podataka (binarnih znamenki). Danas postoji veliki broj različitih vrsta datoteka kao što su npr. dokumenti (nastavci .pdf, .doc, .docx, .xls, .xslx, .ppt, .pptx …), fotografije (nastavci .jpg, .gif, .png, .bmp, .tif …), video datoteke (nastavci .mp4, .avi, .mov, .mkv …), audio datoteke (nastavci .mp3, .wav, .ogg …), arhive (nastavci .zip, .rar,. .7z, .tar …) i brojni drugi tipovi datoteka i njihov broj se neprestano povećava. Posebne vrste datoteka su direktoriji i simboličke veze.

Datoteke se mogu stvoriti, čitati, zapisivati, preimenovati, izmijeniti (smanjiti, povećati), premještati, kopirati ili izbrisati. To je moguće korištenjem različitih programa, uz znanje i radnju korisnika ili na temelju posebnih algoritama. Operacijski sustavi obično koriste nastavke u nazivu datoteka radi identifikacije vrste datoteke (npr. nastavak .txt označava tekstualne datoteke). Ovi nastavci su uvedeni kako bi se olakšalo operacijskim sustavima da ispravno otvaraju datoteke, odnosno da povežu datoteku s odgovarajućim programima. Više informacija o nastavcima datoteka dostupno je ovdje i ovdje.

No, ne oslanjaju se svi operacijski sustavi na nastavke datoteka. Jedan od razloga je i što se nastavci datoteka mogu lako promijeniti, što će rezultirati u pogrešnom prepoznavanju vrste datoteke. Stoga neki operacijski sustavi danas analiziraju strukturu datoteke, i ako je prepoznaju, izvršava se tražena operacija nad tom datotekom. Kako bi se olakšala ovakva analiza strukture datoteke, za svaku vrstu datoteke je uveden jedinstveni uzorak bajtova koji nazivamo potpis datoteke (eng. *file signature*) ili „čarobni broj“ (eng. *magic number*).

1.4 Potpisi datoteka

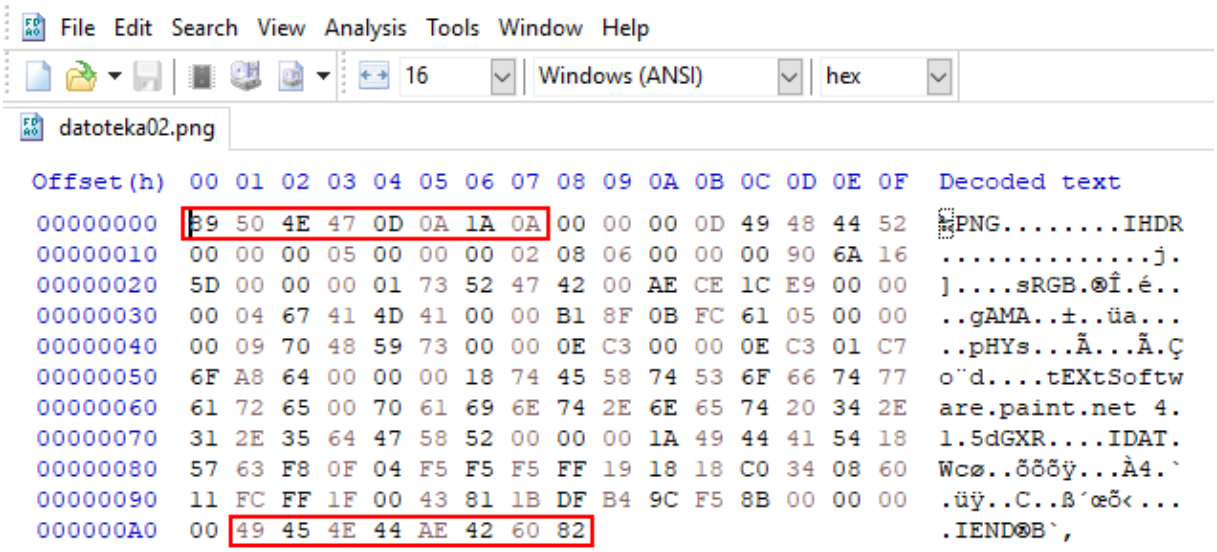
Potpis datoteke ili čarobni broj je pojam, koji kada se odnosi na datoteke, označava uzorak koji se dodaje u zapis svake datoteke i koji se koristi za identifikaciju njenog formata. Potpis datoteke dodaje se u zaglavlju i/ili podnožju i omogućava operacijskom sustavu da identificira formate različitih datoteka. U tablici 2 prikazani su primjeri potpisa nekih datoteka u heksadekadskom zapisu.

format	zaglavlje	podnožje
.pdf	25 50 44 46	Više mogućih potpisa na kraju: 0A 25 25 45 4F 46 0A 25 25 45 4F 46 0A 0D 0A 25 25 45 4F 46 0D 0A 0D 25 25 45 4F 46 0D
.jpg	FF D8	FF D9
.png	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44 AE 42 60 82
.rtf	7B 5C 72 74 66	7D

Tablica 2 – primjeri potpisa nekih formata datoteka u heksadekadskom zapisu

Više informacija o potpisima datoteka dostupno je ovdje i ovdje.

Na slici 3 prikazan je heksadekadski zapis jedne PNG datoteke s karakterističnim potpisom datoteke u zaglavlju i podnožju.



Slika 3 – heksadekadski zapis jedne .png datoteke

Na operacijskim sustavima iz Unix obitelji se za provjeru vrste datoteke koristi program zvan „**file**“ koji čita i interpretira datoteku „/usr/share/file/magic.mgc“ ili „/usr/share/file/magic“ kako bi povezao magični broj s vrstom datoteke.

Na operacijskom sustavu Microsoft Windows se može koristiti isti program kao dio **cgywin** paketa ili se može koristiti program **TrID**.

2 *File carving* tehnike

File carving tehnike dijele se na osnovne i napredne tehnike.

2.1 Osnovne *file carving* tehnike

Kod osnovnih procesa polazi se od sljedećih pretpostavki:

- početak datoteke nije prepisan,
- zapis datoteke nije fragmentiran,
- datoteka nije komprimirana (npr. uporabom NTFS kompresije).

U ovom slučaju *file carving* alati koriste podatke o zaglavlju i podnožju datoteka na temelju kojih rade pretraživanje većeg skupa podataka.

2.2 Napredne *file carving* tehnike

U slučajevima kad su zapisi datoteka fragmentirani, potrebno je koristiti napredne tehnike *file carvinga*. Pri tome pojedini fragmenti mogu biti zapisani van redoslijeda ili mogu čak i nedostajati.

Ako je zapis datoteke fragmentiran, alati za *file carving* moraju se oslanjati na poznavanje unutarnje strukture datoteka. Novi operacijski sustavi nastoje izbjeći fragmentaciju zapisa kako bi se ubrzalo čitanje i zapisivanje datoteka, no u pojedinim uvjetima to se ipak ne da izbjeći, npr. ako nema dostupnih kontinuiranih sektora za zapis datoteke, ili ako se dodaju novi podaci, čime se povećava veličina datoteke, a nema slobodnih sektora koji bi omogućili kontinuirani zapis. Nadalje, zlonamjerni korisnici mogu utjecati na zapis datoteke tako da on namjerno bude fragmentiran, kako bi se otežala obnova datoteke nakon njenog brisanja. Kod osnovnih *file carving* tehnika koje se temelje na pronalaženju zaglavlja i podnožja datoteke, ne vodi se briga o strukturi datoteke, što znači da se ne razmatra mogućnost da neki sektori mogu biti umetnuti, izbrisani ili izmijenjeni. Nadalje, neke datoteke mogu imati zaglavlje ili SOF (eng. *Start Of File*), ali nemaju podnožje ili EOF (eng. *End Of File*). U takvim slučajevima dobro poznavanje strukture datoteke je ključno za ispravnu rekonstrukciju, pa se stoga novi algoritmi za *file carving* temelje upravo na poznavanju strukture datoteka.

2.2.1 *File carving* tehnika zaglavlje-podnožje

File carving tehnika „zaglavlje-podnožje“ ili „zaglavlje-maksimalna veličina datoteke“ temelji se na poznavanju zaglavlja i podnožja datoteke ili na poznavanju zaglavlja i maksimalne veličine datoteke. Neki od alata koji koriste ovu tehniku su *Scalpel*, *Foremost* i *File finder* (*EnCase*).

2.2.2 *File carving* tehnika temeljena na strukturi datoteke

File carving tehnika temeljena na strukturi datoteke koristi unutrašnji raspored elemenata datoteke. Elementi koji se pri tome koriste su: zaglavlje, podnožje, identifikacijski nizovi i informacija o veličini datoteke. Neki od alata koji koriste ovu tehniku su *Foremost* i *PhotoRec*.

2.2.3 *File carving* tehnika temeljena na sadržaju

Sadržaj datoteka najčešće je slabo definiran. Stoga *file carving* tehnike temeljene na sadržaju rekonstrukciju datoteke rade na temelju:

- broja znakova,
- prepoznavanja teksta odnosno jezika,
- uporabe filtera,
- statističkih svojstva podataka,
- entropije podataka (velike promjene u entropiji obično označavaju da podaci zapisani u bloku pripadaju drugoj datoteci).

3 *File carving* alati

Postoji veći broj alata koji se mogu koristiti za *file carving*. Neki su slobodni (eng. *free and open source*) i besplatni, dok se drugi prodaju kao komercijalni softver. Različiti alati obično daju i različite rezultate, tj. jedan *file carving* alat će možda uspjeti rekonstruirati datoteke koje neki drugi alat neće, i obrnuto. Zato je u temeljitom postupku rekonstrukcije datoteka korisno koristiti niz različitih alata.

Za testiranje pojedinih alata mogu se koristiti različite forenzičke testne slike ili slike koje sadrže forenzičke izazove. I jedne i druge mogu se koristiti za vježbu i isprobavanje alata. Primjerice, takve slike moguće je preuzeti ovdje i ovdje.

Češće korišteni slobodni i besplatni *file carivng* alati su:

- Scalpel
- Foremost
- PhotoRec
- ReviveIT
- F-Engrave

Neki od komercijalnih *file carving* alata:

- WinHex (proizvod tvrtke *X-Ways AG*)
- FTK – Forensic Toolkit (proizvod tvrtke *AccessData*)
- EnCase (proizvod tvrtke *GuidanceSoftware*, danas *Opentext*)

U nastavku je dan pregled nekih od *file carving* alata.

3.1 PhotoRec

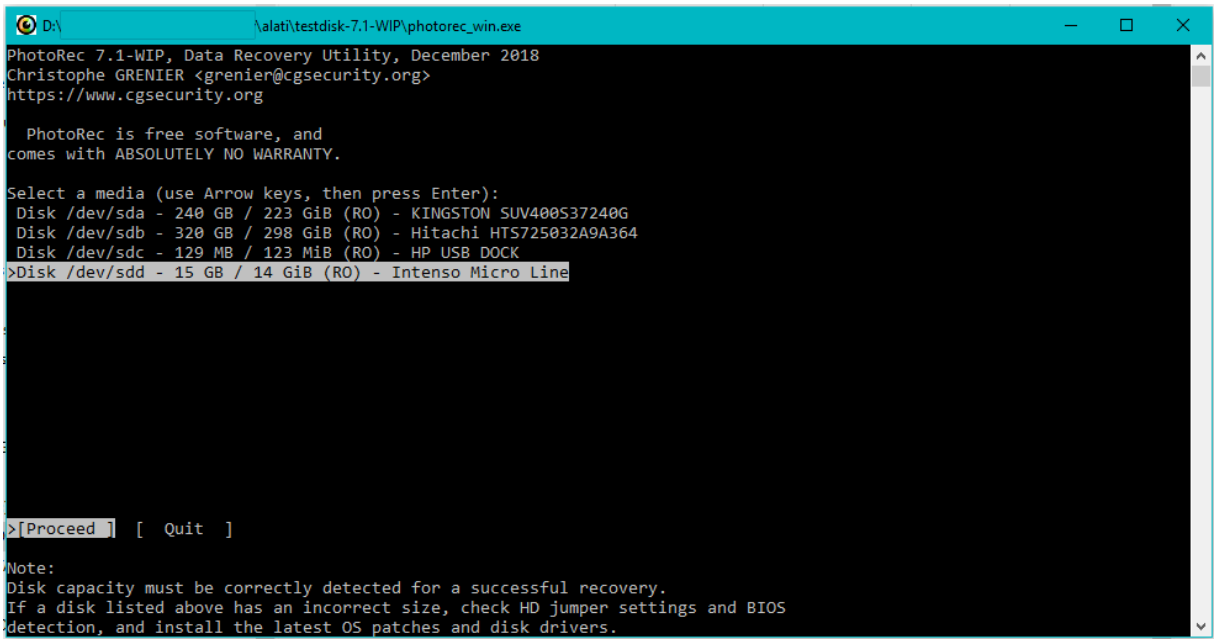
PhotoRec je jedan od najboljih slobodnih i besplatnih *file carving* programa koji se može koristiti zasebno ili kao dio složenijeg forenzičkog alata *Autopsy*. *PhotoRec* je između ostaloga dostupan na operacijskim sustavima Microsoft Windows, Mac OS i Linux.

PhotoRec je prvotno dizajniran za obnovu različitih slikovnih, audio i video datoteka na digitalnim kamerama, mobilnim uređajima, memorijskim karticama i drugim medijima za pohranu podataka uključujući i diskove na računalima i CD-ROM-ove. Daljnjim razvojem programa dodana je podrška i za druge vrste datoteka. *PhotoRec* sveukupno podržava oko 480 različitih vrsta datoteka. Osim različitih multimedijskih formata program podržava rad i s različitim vrstama dokumenata, arhiva i baza podataka. Potpuni popis podržanih vrsta datoteka dostupan je ovdje.

Za povratak izgubljenih datoteka, *PhotoRec* prvo pokušava pronaći veličinu podatkovnog bloka (ili klastera). Ako datotečni sustav nije oštećen, ova se vrijednost može očitati iz superbloka (ext3, ext3, ext4) ili početnog (eng. *boot*) sektora medija (FAT, NTFS,…). Ako taj podatak ne postoji, *PhotoRec* čita medij, sektor po sektor, traži prvih 10 datoteka, te na temelju otkrivenih podataka izračunava veličinu bloka podataka / klastera. Nakon što je izračunata veličina bloka, *PhotoRec* čita medij blok po blok (ili klaster po klaster). Svaki blok se provjerava na temelju potpisa iz baze podataka koja dolazi s programom.

Za rad s programom potrebno je imati odgovarajuće (administratorske) ovlasti ako želite izravno analizirati fizički medij za pohranu podataka (npr. disk ili USB *stick*). Za analizu datoteke koja sadrži presliku nekog medija nisu potrebne administratorske ovlasti.

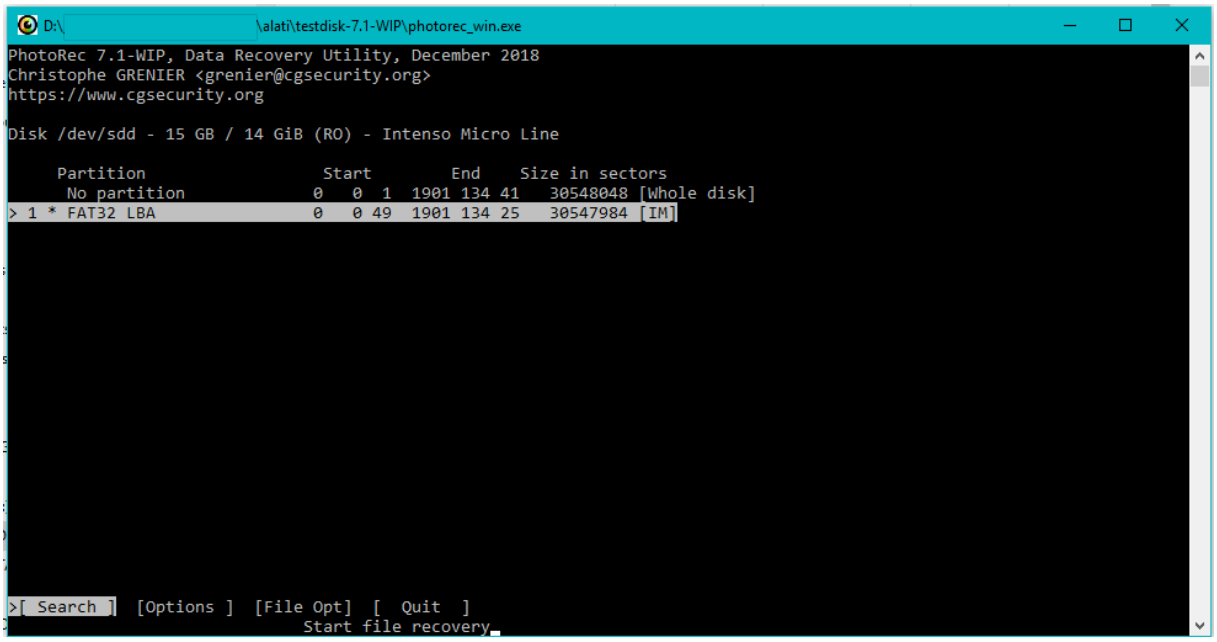
Kao primjer, bit će prikazan izravni *file carving* fizičkog medija za pohranu podataka. Prvo je potrebno odabrati fizički medij za pohranu podataka s kojeg se želi izvršiti obnova datoteka. Odabir se radi na temelju dostupnih medija kao što je prikazano na slici 4.



Slika 4 – odabir medija na kojem će se provoditi *file carving* u alatu *PhotoRec*

Nakon toga, kao što je prikazano na slici 5, moguće je odabrati:

- *Search* – nakon odabira particije i datotečnog sustava započinje s pretraživanjem,
- *Options* – za odabir naprednih postavki programa,
- *File Opt* – za odabir vrsta datoteka za koje je potrebno provesti postupak obnove,
- *Quit* – za izlazak iz programa.

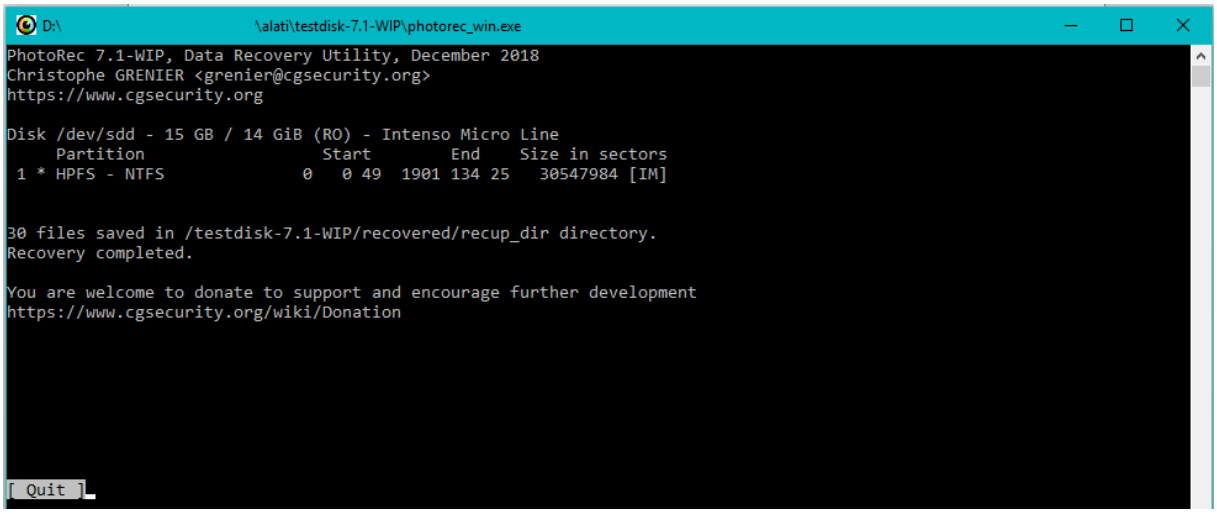


Slika 5 – odabir particije za pretraživanje ili odabir naprednih postavki u alatu *PhotoRec*

Ako se odabere *Search*, u sljedećem koraku potrebno je odabrati:

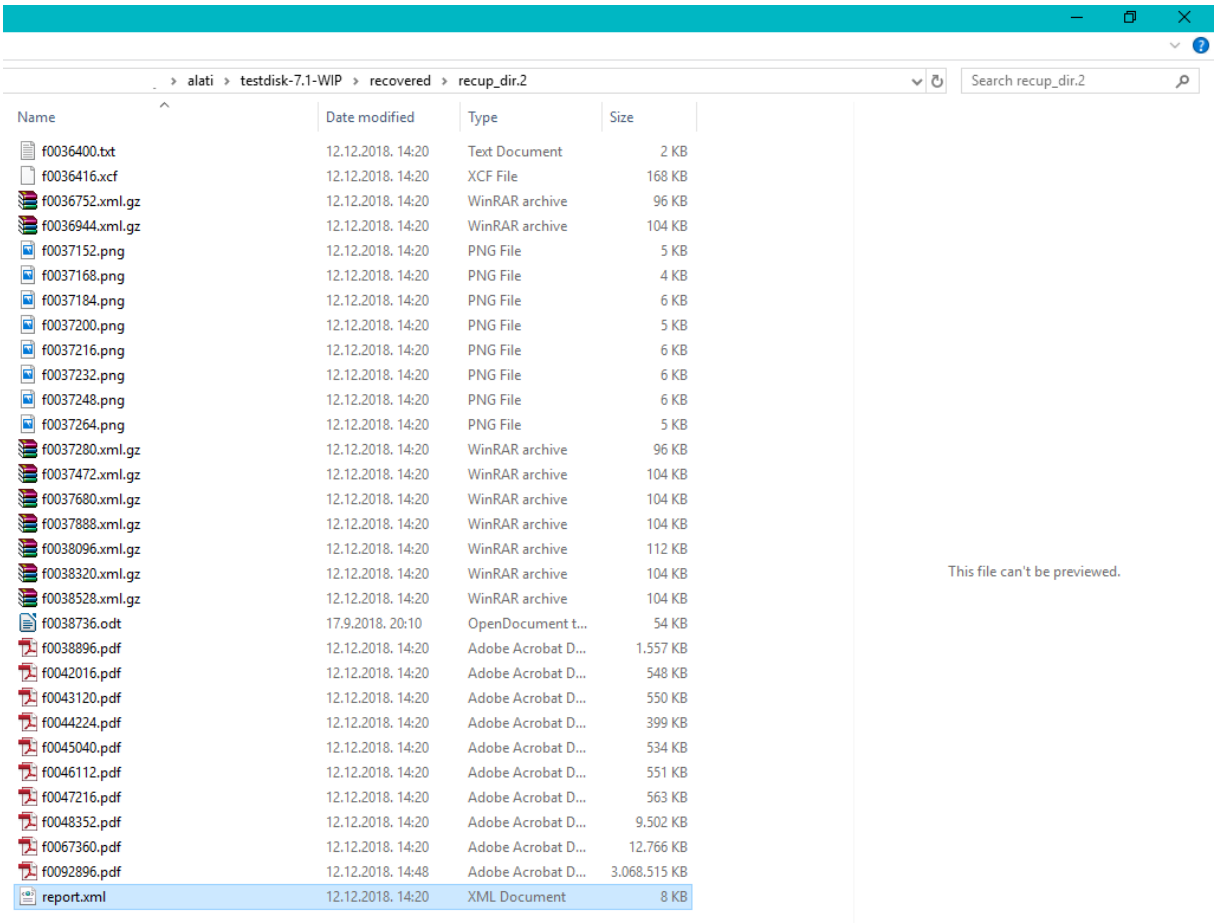
- particiju,
- datotečni sustav (ext2, ext3, ext4 ili FAT, NTFS, HFS+...),
- pretražuje li se samo nedodijeljeni prostor ili cijela particija,
- direktorij u koji će se spremiti obnovljene datoteke (pri tome se ne smije odabrati particija na kojoj se radi *file carving*).

Nakon pokretanja postupka, *PhotoRec* započinje s *file carving postupkom*. Kada postupak završi, *PhotoRec* prikazuje sažetak i zapisuje odgovarajuće izvješće, kao što je prikazano na slici 6.



Slika 6 – prikaz sažetka nakon završetka postupka *file carvinga* u alatu *PhotoRec*

U direktoriju *recup_dirN* spremljene su obnovljene datoteke, gdje se *N* u nazivu direktorija slijedno povećava ako već postoji neka od mapa *recup_dir*, kao što je prikazano na slici 7.



Slika 7 – obnovljene datoteke u mapi *recup_dir2*

3.2 WinHex

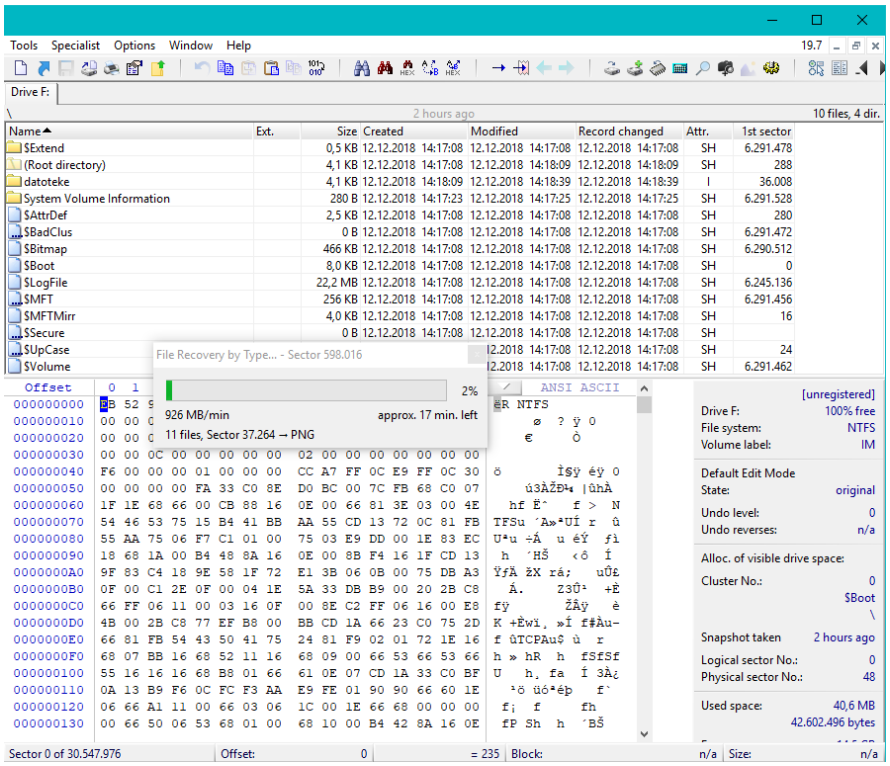
WinHex je alat kojega je razvila njemačka tvrtka *X-Ways Software Technology AG* i koji se koristi za upravljanje datotekama, diskovima i radnom memorijom. *WinHex* je besplatan za evaluaciju u trajanju od 45 dana, a za ostale namjene potrebno je kupiti odgovarajuću licencu. Usporedba funkcionalnosti koje se dobivaju različitim licencama moguće je vidjeti ovdje.

Neke od najbitnijih funkcionalnosti alata *WinHex* su:

- uređivač diskova za tvrde diskove, diskete, CD-ROM i DVD medije, različite memorijske kartice itd.,
- ugrađena podrška za FAT12/16/32, exFAT, NTFS, Ext2/3/4, Next3, CDFS i UDF datotečne sustave,
- ugrađeni interpreter za RAID sustave i dinamičke diskove,
- različite tehnike obnove podataka,
- RAM uređivač (omogućuje pristup fizičkom RAM-u i virtualnoj memoriji),
- intepreter podataka (podrška za 20 tipova podataka),
- uređivanje struktura podataka pomoću predložaka (npr. za popravak tablice particija ili početnih sektora),
- spajanje i dijeljenje datoteka, ujedinjavanje i dijeljenje parnih i neparnih okteta/riječi;
- analiza i usporedba datoteka,
- posebno fleksibilne funkcije pretrage i zamjene,
- kloniranje diskova,
- izrada slika i sigurnosnih kopija medija za pohranu podataka,
- sučelje za programiranje i skripte,
- podrška za 256-bitnu AES enkripciju, kontrolni zbroj, CRC32, kriptografske sažetke (MD5, SHA-1,…),
- sigurno brisanje povjerljivih datoteka i tvrdih diskova radi zaštite privatnosti,
- uvoz svih formata iz privremene memorije,
- prebacivanje između binarnih, heksadekadskih, ASCII, Intel Hex i Motorola S zapisa;
- podrška za znakovne sustave: ANSI ASCII, IBM ASCII, EBCDIC, Unicode;
- prebacivanje između prozora, ispis, generator slučajnih brojeva;
- podrška za datoteke veće od 4 GB, velika brzina rada, jednostavnost uporabe, dostupna mrežna podrška.

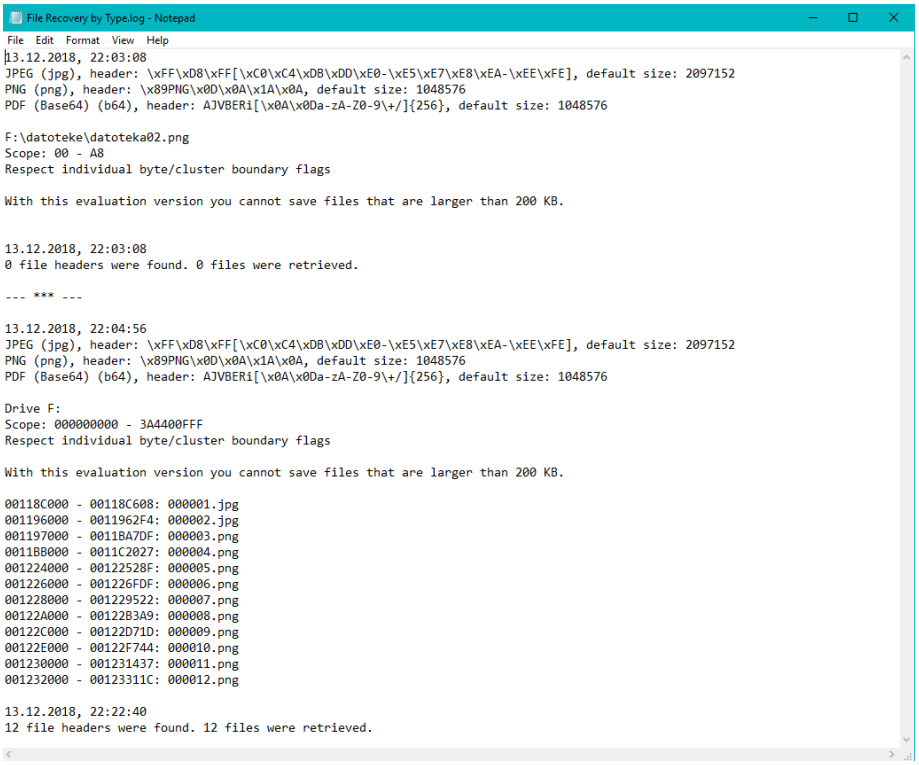
WinHex ima sofisticirane, fleksibilne i brze funkcije simultanog pretraživanja koje se mogu koristiti za pretraživanje čitavog medija za pohranu podataka (ili slike medija), uključujući i neiskorišteni prostor za obrisane datoteke, skrivene podatke i slično te ga je moguće koristiti i u slučajevima kada medij nije vidljiv za operacijski sustav zbog uništenog ili korumpiranog datotečnog sustava.

Povrat podataka moguće je napraviti odabirom *Tools > Disk Tools > File Recovery by Type*, kao što je prikazano na slici 8. Prije pokretanja postupka potrebno je odabrati postavke pretraživanja (npr. označiti formate datoteka koje se žele pretražiti) i odabrati direktorij za spremanje rezultata postupka.



Slika 8 – postupak traženja .jpg, .png i .pdf datoteka na mediju alatom *WinHex*

Rezultati postupka zajedno s izvješćem (prikazano na slici 9) spremaju se u odabranu mapu.



Slika 9 – izvješće o postupku obnove datoteka u alatu *WinHex*

3.3 Foremost

Foremost je slobodan i besplatan *file carving* alat napravljen za operacijski sustav Linux. Koristi tehniku oporavka podataka pomoću zaglavlja, podnožja i interne strukture datoteka. Iako je prva inačica bila napisana za primjenu u provedbi američkog kaznenog zakona, alat je slobodno dostupan i može se koristiti kao opći alat za vraćanje podataka.

Trenutno dostupna inačica alata *foremost* je 1.5.7. Na većini modernih Linux distribucija *foremost* je dostupan u odgovarajućim softverskim repozitorijima, tako da je primjerice na distribuciji *Ubuntu* alat moguće instalirati naredbom:

```
~$ sudo apt install foremost
```

Obnova izgubljenih datoteka provodi se na temelju zaglavlja i podnožja te je potrebno definirati zaglavlje i podnožje datoteke koju želimo pronaći i spremiti. Ti podaci se definiraju u datoteci „*foremost.conf*“. Ta datoteka je već u pravilu stvorena prilikom instalacije te su u njoj zapisana zaglavlja i podnožja za neke česte vrste datoteka (jpg, gif, png, bmp, avi, exe, mpg, wav, wmv, zip, rar, html, ole i mov). Ako se žele dodati podaci o novoj vrsti datoteke, to se može napraviti uređivanjem konfiguracijske datoteke. Pri tome je potrebno definirati nastavak datoteke, status osjetljivosti na velika i mala slova, maksimalnu veličinu datoteke te zaglavlje i podnožje (ako postoji). Primjer podataka iz konfiguracijske datoteke prikazan je na slici 10.

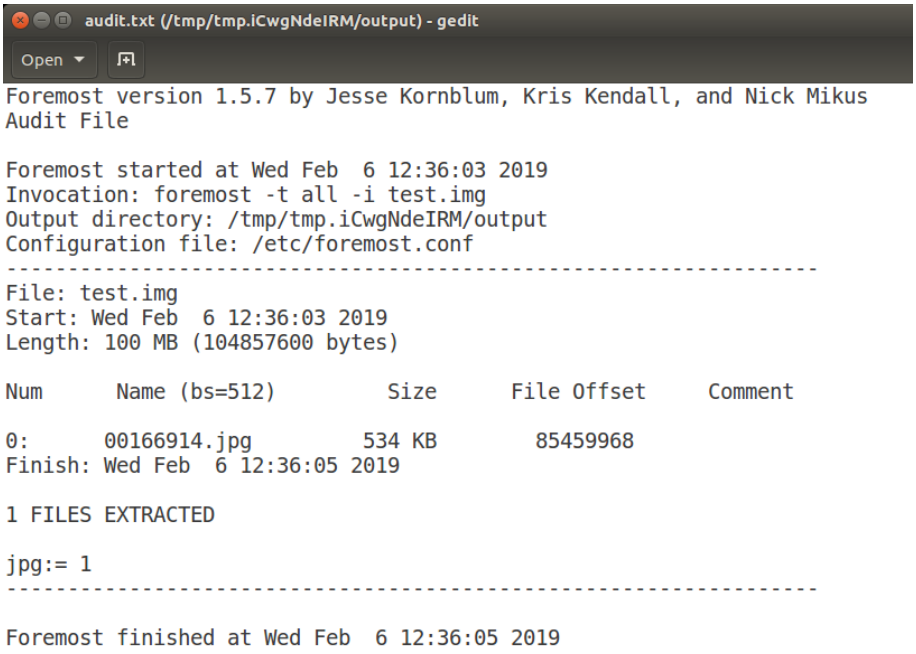
Slika 10 – dio konfiguracijske datoteke za postavke pretraživanja u alatu *foremost*

Pretraživanje datoteka može se raditi na slikama medija (dobivenim alatima kao što su *dd*, *Encase* ili *Safeback*) ili izravno na mediju za pohranu podataka. Program se pokreće iz naredbene linije. Za pretraživanje svih definiranih vrsta datoteka naredba će izgledati:

```
~$ foremost -t all -i test.img
```

Pri pokretanju alata treba voditi računa da se naredbena ljuska nalazi u direktoriju u kojemu prijavljeni korisnik ima dozvolu pisanja te da prijavljeni korisnik ima dozvolu čitanja uređaja ili slike diska na kojoj se provodi *file carving*. Ostale postavke alata *foremost* moguće je pročitati ovdje.

Nakon pokretanja alata, unutar trenutnog direktorija stvara se novi direktorij s pronađenim datotekama. Za svaki od tipova datoteka koji se pretražuju stvara se novi poddirektorij. Nakon završetka postupka *file carvinga*, potrebno je pregledati rezultate i provjeriti nalazi li se među izlaznim datotekama i tražena datoteka. Alat na kraju postupka generira izvješće u datoteci *audit.txt* kao što je prikazano na slici 11.



Slika 11 – Foremost – izvješće na kraju procesa

4 Zaključak

File carving jedan je od temeljnih pristupa vraćanju izgubljenih datoteka (ili podataka općenito), a posebice kada su podaci o datotečnom sustavu korumpirani ili izgubljeni. Iako postoji veći broj alata za *file carving*, osnovni nedostatak im je da nisu sveobuhvatni, pa je najčešće potrebno koristiti više različitih alata kako bi se došlo do željenog cilja. Uz navedeni problem, većina alata ima i neki od sljedećih nedostataka:

- ne mogu rekonstruirati datoteke ako su one fragmentirane;
- ako alati i mogu izvršiti oporavak fragmentiranih datoteka, najčešće podržavaju samo ograničeni broj različitih formata datoteka;
- samo jedan alat (*Defraser*) omogućava povrat parcijalnih datoteka (datoteka čiji su dijelovi izgubljeni), ali on podržava samo pet formata datoteka (MPEG-1, MPEG-2, AVI, MPEG-4 i 3GP);
- većina alata koriste baze potpisa datoteka koje su ograničene i ne ažuriraju se dovoljno često.

Iako je postignut napredak u tehnikama *file carvinga*, još uvijek postoji značajan potencijal za daljnji razvoj, stoga je ovo jedno od važnijih područja istraživanja i razvoja unutar računalne forenzike.

5 Literatura

1. **Kessler, Gary C.** File Signatures. [Mrežno] 15. siječnja 2019. [Citirano: 6. veljače 2019.] https://www.garykessler.net/library/file_sigs.html.
2. **Pontello, Marco.** Marco Pontello's Home - Software - TrID. [Mrežno] 5. veljače 2019. [Citirano: 6. veljače 2019.] http://mark0.net/soft-trid-e.html.
3. **NIST.** Forensic Images for File Carving. [Mrežno] [Citirano: 5. veljače 2019.] https://www.cfreds.nist.gov/FileCarving/index.html.
4. **Forensic Focus.** Test Images and Forensic Challenges | ForensicFocus.com. [Mrežno] [Citirano: 6. veljače 2019.] https://www.forensicfocus.com/images-and-challenges.
5. **CGSecurity.** PhotoRec - Digital Picture and File Recovery. [Mrežno] 4. lipnja 2016. [Citirano: 6. veljače 2019.] https://www.cgsecurity.org/wiki/PhotoRec.
6. **X-Ways Software Technology AG.** WinHex: Hex Editor & Disk Editor, Computer Forensics & Data Recovery Software. [Mrežno] [Citirano: 6. veljače 2019.] https://www.x-ways.net/winhex/.
7. **Foremost.** Foremost. [Mrežno] [Citirano: 6. veljače 2019.] http://foremost.sourceforge.net/.