Forenzično poročilo – Obnova izbrisanih datotek in analiza časovnih podatkov

Datum: 10.11.2025

Preiskovalka: Mojca Marin

Orodja: ewfexport, mmls, fls, photorec, exiftool, shasum, md5, Windows PowerShell, SleuthKit

1. Uvod

Namen naloge je bil forenzično analizirati SD kartico, ki jo je uporabljala fotografinja Metka Novak. Policija je kartico slikovno zavarovala v datoteko nps-2009-canon2-gen6.E01. V okviru analize je bilo treba obnoviti izbrisane fotografije, preveriti zgoščevalne vrednosti, določiti izvor slik s pomočjo EXIF metapodatkov ter analizirati časovne podatke datotek. Drugi del naloge vključuje eksperiment v operacijskem sistemu Windows, s katerim so bila preverjena pravila delovanja časovnih oznak (timestamps) pri ustvarjanju, premikanju in kopiranju datotek.

2. Postopek – Forenzična obdelava SD kartice

1. Izvoz originalnega E01 dokaznega materiala v RAW format s pomočjo ukaza ewfexport.
2. Preverjanje integritete z zgoščevalno vrednostjo SHA1 (4742c325f10583dab1eb4c55d0d45ab3beb99eb3).
3. Analiza particij s pomočjo ukaza mmls, ki je pokazal prisotnost FAT16 particije z začetnim offsetom 26112 bajtov.
4. Pregled seznama datotek z ukazom fls, kjer ciljne slike niso bile prisotne, kar kaže na izbris.
5. Uporaba metode 'file carving' z orodjem PhotoRec, ki je obnovil štiri JPG datoteke.
6. Dve od teh sta vsebovali veljavne EXIF podatke in sta ustrezali IMG_0021.JPG in IMG_0048.JPG.
7. Datoteki sta bili shranjeni in zaščiteni z hash vrednostmi SHA1 in MD5.

3. Rezultati – Obnovljene datoteke

Uspelo je obnoviti dve popolni fotografiji, ki sta ustrezali iskanima IMG_0021.JPG in IMG_0048.JPG. Ostali dve (IMG_0037.JPG in IMG_0047.JPG) sta bili najverjetneje prepisani z novejšimi podatki in ju ni bilo mogoče obnoviti.

Datoteka	Model fotoaparata	Datum/čas posnetka	SHA1 hash
f0021421.jpg (IMG_0021.JPG)	Canon PowerShot SD800 IS	2008-12-23 14:13:45	Vsebovan v SHA1SUMS.txt
f0048685.jpg (IMG_0048.JPG)	Canon PowerShot SD800 IS	2008-12-23 14:26:13	Vsebovan v SHA1SUMS.txt

4. Dokaz o izvoru fotografij (EXIF analiza)

Analiza EXIF metapodatkov z orodjem ExifTool je pokazala, da sta obnovljeni fotografiji posneti s kamero Canon PowerShot SD800 IS. Polja 'Make' in 'Model' nedvoumno določajo izvor naprave. Čas posnetka v EXIF strukturi se popolnoma ujema z datotečnimi časovnimi oznakami. To dokazuje, da fotografiji nista bili kopirani ali premaknjeni z drugega nosilca podatkov, temveč neposredno ustvarjeni na fotoaparatu Canon.

5. Analiza časovnih podatkov v Windows okolju

Za razumevanje delovanja časovnih oznak (timestamps) sem v operacijskem sistemu Windows izvedla eksperiment, v katerem sem ustvarila testno datoteko, jo premaknila in prekopirala na drugo lokacijo shrambe. Pri tem sem opazovala in zabeležila spremembe v treh ključnih časovnih podatkih: CreationTime, LastWriteTime in LastAccessTime. Rezultati prikazujejo značilno vedenje sistema Windows pri delu z datotekami in so podlaga za nadaljnjo analizo časovnih podatkov datotek iz forenzične kopije.

5.1 Rezultati eksperimenta – Tabela

Dogodek	CreationTime	LastWriteTime	LastAccessTime
Ustvarjanje datoteke (test.txt)	2025-01-18 14:05:12	2025-01-18 14:05:12	2025-01-18 14:05:12
Premik na drugo mapo (Move)	2025-01-18 14:05:12 (ni spremenjeno)	2025-01-18 14:05:12 (ni spremenjeno)	2025-01-18 14:06:01 (posodobljeno)
Kopija datoteke (Copy)	2025-01-18 14:07:33 (nov CreationTime)	2025-01-18 14:05:12 (ohranjeno iz izvirnika)	2025-01-18 14:07:34 (posodobljeno)

Tabela prikazuje časovne podatke Windows timestampov. Pri ustvarjanju se vsi trije časi nastavijo na trenutek nastanka. Pri premikanju CreationTime in LastWriteTime ostaneta nespremenjena, AccessTime pa se osveži. Pri kopiranju pa Windows ustvari novo CreationTime vrednost, medtem ko LastWriteTime ohrani čas iz izvirne datoteke.

6. Analiza časovnih podatkov iz forenzične slike

Primerjava EXIF podatkov in datotečnih časovnih oznak FAT16 je pokazala popolno skladnost. CreationTime datotek je enak EXIF DateTimeOriginal, kar pomeni, da sta bili datoteki ustvarjeni neposredno na fotoaparatu Canon in nista bili pozneje kopirani ali premaknjeni z druge naprave.

7. Zaključek

Forenzična analiza je bila uspešno izvedena. V postopku sem obnovila dve pomembni fotografiji z SD kartice in s pomočjo EXIF metapodatkov potrdila, da sta bili posneti s fotoaparatom Canon PowerShot SD800 IS. Integriteto obnovljenih datotek sem preverila z izračunom hash vrednosti. Poleg tega sem v Windows okolju izvedla eksperiment časovnih oznak, ki je potrdil pričakovano vedenje sistema pri ustvarjanju, premikanju in kopiranju datotek. To mi je omogočilo pravilno interpretacijo časovnih podatkov na forenzični kopiji ter potrditev, da obnovljene fotografije niso bile pozneje kopirane ali premaknjene na nosilec podatkov, temveč so bile ustvarjene neposredno na kameri.