SVEUČILIŠTE/UNIVERZITET „VITEZ“

FAKULTET INFORMACIJSKIH TEHNOLOGIJA

ZULKA MUSIĆ

ANALIZA I OPIS SOFTVERSKIH ALATA ZA POTPUNO BRISANJE PODATAKA SA PC-A (WIPE ALATI)

SCENARIO ISTRAŽIVANJA

Predmet: Računarska forenzika

Mentor: prof.dr.sc. Jasmin Azemović

Asistent: Admir Sivro

Travnik, 2025. godina

SVEUČILIŠTE/UNIVERZITET „VITEZ“

FAKULTET INFORMACIONIH TEHNOLOGIJA

ANALIZA I OPIS SOFTVERSKIH ALATA ZA POTPUNO BRISANJE PODATAKA SA PC-A (WIPE ALATI)

SCENARIO ISTRAŽIVANJA

IZJAVA: Ja **Zulka Musić**, studentica Sveučilišta/Univerziteta „VITEZ“, Indeks broj: **390-24/RIIT** odgovorno i uz moralnu i akademsku odgovornost izjavljujem da sam ovaj rad izradila potpuno samostalno uz korištenje citirane literature i pomoć predmetnog profesora.

Student: Zulka Musić

Predmet: Računarska forenzika

Mentor: prof.dr.sc. Jasmin Azemović

Asistent: Admir Sivro

SADRŽAJ

1. OPIS SLUČAJA (CASE SCENARIO)

Slučaj: „Trajno brisanje osjetljivih dokumenata na Windows računaru“

Opis incidenta:

U kompaniji X utvrđeno je da je računar koji je korišten za obradu povjerljivih dokumenata pripremljen za dalje korištenje ili prodaju. Prije ponovne upotrebe sistema, postojala je potreba da se provjeri da li je klasično brisanje podataka dovoljno za uklanjanje osjetljivih informacija ili je neophodno koristiti specijalizovane wipe alate za trajno uništavanje podataka.

Menadžment sumnja da su dokumenti prethodno obrisani korištenjem standardne Delete opcije, ali želi forenzičku potvrdu da li se takvi podaci mogu povratiti i da li je primjena wipe alata efikasna metoda zaštite podataka.[1]

2. CILJ I ZADACI ISTRAGE

Cilj istrage:

Cilj ove forenzičke analize jeste demonstrirati razliku između klasičnog brisanja podataka (Delete) i sigurnog brisanja pomoću wipe alata (Eraser), te dokazati efikasnost wipe metoda kroz pokušaj povrata podataka korištenjem alata Recuva.

Zadaci istrage:

1. Demonstrirati klasično brisanje fajla pomoću Delete metode.
2. Pokušati povrat obrisanog fajla korištenjem alata Recuva.
3. Izvršiti sigurno brisanje istog fajla pomoću wipe alata Eraser.

[1] Zbog sigurnosti sistema, demonstracija je izvedena na testnom USB uređaju, a ne na produkcionom disku računara.

4. Pokušati ponovni povrat fajla nakon primjene wipe metode.
5. Uporediti rezultate i donijeti forenzički zaključak.

3. METODOLOGIJA I KORIŠTENI ALATI

U ovoj istrazi poštovani su osnovni principi računarske forenzike. Analiza je vršena u kontrolisanom okruženju, bez ugrožavanja stvarnih korisničkih podataka.

Korišteni alati:

- Windows Delete - za klasično brisanje fajlova.
- Recuva - alat za povrat obrisanih podataka.
- Eraser - wipe alat za trajno brisanje podataka putem prepisivanja.
- OBS Studio - za snimanje ekrana i glasovnu demonstraciju postupaka.

4. TOK ISTRAGE I ANALIZA (STEP-BY-STEP)

4.1. KORAK 1: KLASIČNO BRISANJE FAJLA (DELETE)

Na testnom dokumentu izvršeno je klasično brisanje korištenjem opcije Delete. Fajl je uklonjen iz vidljivog dijela fajl sistema, ali nije fizički obrisan sa diska.

Forenzička napomena:

Kod NTFS fajl sistema, prilikom Delete operacije briše se samo zapis o fajlu u MFT tabeli, dok stvarni podaci ostaju u nealociranom prostoru.

4.2. KORAK 2: POKUŠAJ POVRATA FAJLA POMOĆU RECUVA ALATA

Nakon klasičnog brisanja, pokrenut je alat Recuva kako bi se izvršila analiza diska i pokušao povrat obrisanog fajla.

Rezultat:

Recuva je uspješno pronašla obrisani fajl i omogućila njegov povrat, čime je dokazano da klasično brisanje ne predstavlja sigurnu metodu uklanjanja podataka.

4.3. KORAK 3: SIGURNO BRISANJE FAJLA POMOĆU ERASER ALATA

Nakon povrata fajla, izvršeno je njegovo trajno brisanje korištenjem wipe alata Eraser, uz primjenu metode višestrukog prepisivanja podataka.

Forenzička napomena:

Eraser primjenjuje algoritme prepisivanja koji zamjenjuju originalni sadržaj fajla nasumičnim podacima, čime se onemogućava kasniji povrat.

4.4. KORAK 4: POKUŠAJ POVRATA FAJLA NAKON WIPE METODE

Nakon primjene Eraser alata, ponovo je pokrenut alat Recuva s ciljem da se provjeri da li je moguće povratiti prethodno obrisani fajl.

Rezultat:

Recuva nije bila u mogućnosti da pronađe niti povrati fajl, što potvrđuje da je primijenjena wipe metoda bila uspješna i da su podaci trajno uništeni.

5. VREMENSKA LINIJA (TIMELINE)

Vrijeme	Događaj
10:05	Kreiranje testnog dokumenta
10:07	Brisanje fajla pomoću Delete metode
10:10	Povrat fajla pomoću Recuva alata
10:15	Sigurno brisanje fajla pomoću Eraser alata
10:18	Neuspješan pokušaj povrata pomoću Recuva

6. ZAKLJUČAK

Na osnovu sprovedene forenzičke analize, utvrđeno je da klasično brisanje fajlova pomoću Delete metode ne predstavlja sigurnu metodu uklanjanja podataka, jer se obrisani fajlovi mogu uspješno povratiti korištenjem alata za oporavak podataka.

Suprotno tome, primjena wipe alata Eraser, koji koristi metode višestrukog prepisivanja, rezultirala je trajnim uništenjem podataka, čime je povrat fajla postao nemoguć čak i uz korištenje forenzičkih alata.

Ovim scenarijem praktično je demonstrirana važnost pravilne sanitizacije podataka i razlika između klasičnog i sigurnog brisanja u kontekstu računarske forenzike.