SVEUČILIŠTE/UNIVERZITET „VITEZ“

FAKULTET INFORMACIJSKIH TEHNOLOGIJA

ZULKA MUSIĆ

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

SEMINARSKI RAD

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)

SEMINARSKI RAD

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. UVOD

1.1. PROBLEM, PREDMET I OBJEKT ISTRAŽIVANJA

U savremenom digitalnom okruženju podaci predstavljaju jednu od najvrijednijih imovina za pojedince i organizacije. Ipak, mnogi korisnici imaju pogrešnu predstavu o tome šta se dešava s podacima nakon njihovog brisanja pomoću osnovnih funkcija operativnog sistema, poput opcija Delete ili Shift + Delete. Iako se smatra da su podaci tada trajno uklonjeni, oni u stvarnosti često ostaju fizički prisutni na mediju za pohranu.

Do ovog problema dolazi zbog načina na koji fajl sistemi, poput NTFS-a na Windows operativnom sistemu, upravljaju podacima. Prilikom klasičnog brisanja uklanja se samo informacija o lokaciji fajla, dok stvarni sadržaj ostaje na disku i može se povratiti pomoću forenzičkih ili recovery alata. To predstavlja ozbiljan sigurnosni rizik, naročito kada su u pitanju povjerljive poslovne ili lične informacije. Dodatni izazov javlja se kod namjernog prikrivanja digitalnih tragova, gdje se koriste softverski alati za potpuno brisanje podataka, poznati kao wipe alati. Ovi alati primjenjuju metode prepisivanja podataka s ciljem njihovog trajnog uništavanja, čime se otežava ili onemogućava forenzička analiza. Zbog toga je razumijevanje razlike između klasičnog i sigurnog brisanja podataka ključno za ovo istraživanje.

Predmet istraživanja u ovom radu su softverski alati za potpuno brisanje podataka sa računara (wipe alati) i njihova uloga u sigurnom uklanjanju digitalnih informacija.

Objekt istraživanja obuhvata metode i tehnike sigurnog brisanja podataka, s posebnim naglaskom na način rada wipe alata, primijenjene standarde (posebno DoD 5220.22-M) i njihove forenzičke implikacije, uključujući moguće tragove koje ovi alati ostavljaju na sistemu.

1.2. SVRHA I CILJEVI ISTRAŽIVANJA

Svrha istraživanja jeste detaljno objasniti razliku između klasičnog brisanja podataka i sigurnog brisanja pomoću wipe alata, te prikazati značaj ovih alata u kontekstu računarske forenzike i zaštite podataka. Rad ima za cilj da poveže teorijska znanja sa praktičnom primjenom kroz realističan scenario i demonstraciju rada wipe alata.

Ciljevi istraživanja su:

- objasniti osnovne principe brisanja podataka na Windows operativnom sistemu,
- analizirati razliku između „Delete“ i „Wipe“ metoda brisanja,
- detaljno opisati DoD 5220.22-M standard sigurnog prepisivanja podataka,
- predstaviti i uporediti najčešće korištene wipe alate.

1.3. RADNA I POMOĆNE HIPOTEZE

Radna hipoteza ovog istraživanja glasi:

Primjenom wipe alata koji koriste višestruke metode prepisivanja podataka moguće je trajno uništiti podatke tako da oni ne mogu biti povraćeni standardnim forenzičkim alatima.

Na osnovu radne hipoteze postavljene su sljedeće pomoćne hipoteze:

- Klasično brisanje podataka (Delete) ne uklanja fizički sadržaj fajla sa diska. Podaci obrisani klasičnom metodom mogu se uspješno povratiti forenzičkim alatima.
- DoD 5220.22-M standard višestrukog prepisivanja značajno smanjuje mogućnost povrata podataka.

- Wipe alati ostavljaju sekundarne digitalne tragove koji mogu biti forenzički analizirani. Efikasnost wipe metoda zavisi od vrste medija za pohranu (HDD ili SSD).

1.4. NAUČNE METODE

U radu su korištene sljedeće naučne i istraživačke metode:

- Analitička metoda, kojom se analizira postojeća stručna literatura, standardi i tehnička dokumentacija.
- Eksperimentalna metoda, kroz praktično testiranje wipe alata na kontrolisanom primjeru.
- Forenzička metoda, primijenjena pri analizi digitalnih tragova prije i poslije brisanja podataka.
- Komparativna metoda, korištena za poređenje klasičnog brisanja i sigurnog brisanja podataka.
- Deduktivna metoda, kojom se na osnovu teorijskih i praktičnih nalaza izvode zaključci.

1.5. STRUKTURA RADA

Rad je strukturiran u jedanaest tematski povezanih poglavlja koja omogućavaju sistematičan i postepen pristup analizi problema brisanja, povrata i trajnog uništavanja podataka u kontekstu računarske forenzike.

U prvom poglavlju dat je uvod u temu rada, gdje su definisani problem, predmet i objekt istraživanja, svrha i ciljevi rada, postavljene radna i pomoćne hipoteze, kao i naučne metode korištene tokom istraživanja. Na kraju poglavlja prikazana je struktura rada.

Drugo poglavlje obuhvata osnovne pojmove računarske forenzike. U ovom dijelu objašnjeni su pojam i značaj računarske forenzike, koncept digitalnog dokaza, integritet digitalnih dokaza, uloga hash funkcija u forenzičkoj validnosti, kao i značaj forenzičke kopije (image) digitalnog medija. Poseban akcenat stavljen je na važnost ovih pojmova za analizu wipe alata.

U trećem poglavlju analiziran je proces brisanja podataka na računaru, s fokusom na razliku između klasičnog brisanja (Delete) i sigurnog brisanja podataka (Wipe). Objašnjen je način rada ovih metoda i njihov forenzički značaj.

Četvrto poglavlje posvećeno je softverskim aplikacijama za povrat obrisanih podataka. U ovom poglavlju objašnjen je pojam i značaj softvera za povrat podataka, način njihovog rada, analizirani su najčešće korišteni alati (Recuva, PhotoRec i Autopsy), njihova ograničenja, kao i njihov forenzički značaj.

U petom poglavlju obrađeni su standardi za sigurno brisanje podataka. Posebna pažnja posvećena je DoD 5220.22-M standardu, njegovim fazama, prednostima i ograničenjima, kao i drugim relevantnim standardima poput NIST SP 800-88 i Gutmann metode.

Šesto poglavlje sadrži analizu i opis softverskih alata za potpuno brisanje podataka (wipe alata). U ovom dijelu definisan je pojam i klasifikacija wipe alata, detaljno su analizirani alati Eraser, SDelete, CCleaner i DBAN, te su predstavljene njihove prednosti, nedostaci i forenzički tragovi koji mogu ostati nakon njihove upotrebe.

U sedmom poglavlju razmatra se odnos između wipe metoda i različitih medija za pohranu podataka, s posebnim osvrtom na razlike između HDD i SSD diskova, kao i ulogu TRIM komande kod SSD uređaja.

Osmo poglavlje bavi se forenzičkom detekcijom wipe aktivnosti. Analizirani su tragovi koje wipe alati mogu ostaviti na sistemu, log fajlovi wipe alata i analiza nealociranog prostora diska.

U devetom poglavlju obrađena je uloga wipe alata u anti-forenzici. Definisan je pojam anti-forenzike i objašnjeno kako se wipe alati koriste kao anti-forenzičko sredstvo za prikrivanje digitalnih tragova.

U desetom poglavlju dat je zaključak rada, u kojem su sumirani rezultati istraživanja, potvrđene postavljene hipoteze i istaknut značaj pravilnog razumijevanja brisanja i trajnog uništavanja podataka u računarskoj forenzici.

Jedanaesto poglavlje sadrži popis korištene literature koja je poslužila kao teorijska i praktična osnova za izradu ovog rada.

2. OSNOVNI POJMOVI RAČUNARSKE FORENZIKE

2.1. RAČUNARSKA FORENZIKA - POJAM I ZNAČAJ

Računarska forenzika predstavlja granu digitalne forenzike koja se bavi identifikacijom, prikupljanjem, analizom i prezentacijom digitalnih dokaza pronađenih na računarskim sistemima i digitalnim medijima. Cilj računarske forenzike jeste rekonstrukcija događaja i utvrđivanje činjenica na način koji je tehnički tačan i pravno prihvatljiv.

U kontekstu modernih informacionih sistema, računarska forenzika ima ključnu ulogu u istragama vezanim za krađu podataka, neovlašteni pristup sistemima, industrijsku špijunažu, ali i u slučajevima namjernog prikrivanja tragova, poznatih kao anti-forenzičke aktivnosti. Upravo upotreba wipe alata predstavlja jednu od najčešćih anti-forenzičkih tehnika, zbog čega je njihovo razumijevanje važno za svakog forenzičkog istražitelja (Casey, 1999).

Računarska forenzika se ne bavi samo pronalaskom podataka, već i analizom načina na koji su podaci izmijenjeni, obrisani ili pokušani da budu trajno uništeni. Zbog toga je neophodno razumjeti kako operativni sistemi upravljaju podacima i koje tragove ostavljaju različite korisničke aktivnosti (Kent, Chevalier, Grance, & Dang, 2006).

2.2. DIGITALNI DOKAZ

Digitalni dokaz predstavlja svaku informaciju pohranjenu ili prenesenu u digitalnom obliku koja može imati dokaznu vrijednost u forenzičkoj istrazi. To mogu biti fajlovi, log zapisi, e-mail poruke, internet historija, sistemski zapisi, kao i ostaci obrisanih podataka u nealociranom prostoru diska.

Za razliku od fizičkih dokaza, digitalni dokazi su izuzetno osjetljivi jer se mogu lako izmijeniti ili uništiti, čak i nenamjerno. Iz tog razloga, postupanje sa digitalnim dokazima mora biti strogo kontrolisano i dokumentovano, uz poštivanje forenzičkih principa.

U kontekstu wipe alata, digitalni dokaz može biti:

- zapis o instalaciji wipe alata,
- log fajl koji potvrđuje izvršeno brisanje,
- promjene u fajl sistemu,
- nepostojanje podataka koji bi inače bili povratljivi (Nelson, Phillips, & Steuart , 2019).

2.3. INTEGRITET DIGITALNIH DOKAZA

Integritet digitalnih dokaza označava očuvanje originalnog stanja dokaza od trenutka prikupljanja do njegove analize i prezentacije. Svaka neovlaštena izmjena digitalnog dokaza može dovesti u pitanje njegovu vjerodostojnost i prihvatljivost u pravnom postupku (Kent, Chevalier, Grance, & Dang, 2006).

Kako bi se osigurao integritet dokaza, u računarskoj forenzici se primjenjuju sljedeći principi:

- analiza se ne vrši na originalnom mediju,
- koristi se forenzička kopija (image),
- sve radnje se dokumentuju,
- primjenjuju se kriptografske hash funkcije.

Posebno je važno napomenuti da analiza wipe alata i njihovih tragova mora biti izvršena na forenzičkoj kopiji diska, kako bi se spriječila dodatna izmjena podataka (Casey, 1999).

2.4. HASH FUNKCIJE I FORENZIČKA VALIDNOST

Hash funkcije predstavljaju matematičke algoritme koji generišu jedinstveni digitalni otisak (hash vrijednost) za određeni skup podataka. U računarskoj forenzici hash funkcije se koriste za provjeru integriteta digitalnih dokaza (Carrier, 2005).

Najčešće korištene hash funkcije su:

- MD5
- SHA-1
- SHA-256

Ako se hash vrijednost fajla ili diska prije i poslije analize poklapa, smatra se da dokaz nije izmijenjen. U suprotnom, integritet dokaza je narušen (NIST , 2024).

U kontekstu wipe alata, hash funkcije se koriste da bi se potvrdilo da je sadržaj prije brisanja bio drugačiji od sadržaja nakon primjene wipe metode, čime se dokazuje uspješnost trajnog brisanja.

2.5. FORENZIČKA KOPIJA (IMAGE) DIGITALNOG MEDIJA

Forenzička kopija, ili image, predstavlja bit-po-bit kopiju digitalnog medija koja uključuje sve podatke, uključujući i obrisane fajlove, nealocirani prostor i slack space. Za razliku od običnog kopiranja fajlova, forenzička kopija zadržava cjelokupnu strukturu diska.

Alati poput FTK Imager ili Guymager koriste se za kreiranje forenzičkih kopija uz automatsko generisanje hash vrijednosti. Na taj način se osigurava da originalni medij ostane netaknut, a analiza se vrši na kopiji (exterro, bez datuma).

U slučaju analize wipe alata, forenzička kopija omogućava istražiteljima da ispituju:

- tragove instalacije alata,

- log zapise,
- strukturu fajl sistema nakon brisanja,
- nealocirani prostor diska.

2.6. ZNAČAJ OSNOVNIH FORENZIČKIH POJMOVA ZA ANALIZU WIPE ALATA

Razumijevanje osnovnih pojmova računarske forenzike predstavlja temelj za analizu wipe alata. Bez poznavanja načina na koji se digitalni dokazi prikupljaju, čuvaju i analiziraju, nemoguće je pravilno interpretirati rezultate sigurnog brisanja podataka.

Wipe alati ne brišu samo podatke, već mijenjaju i strukturu diska, ostavljajući indirektne tragove koji mogu biti ključni u forenzičkoj istrazi. Upravo zbog toga, osnovni forenzički koncepti predstavljaju polaznu tačku za dalju analizu procesa brisanja podataka, koja će biti obrađena u narednom poglavlju (Chandramouli & Hibbard, 2025).

3. BRISANJE PODATAKA NA RAČUNARU - RAZLIKA IZMEĐU "DELETE" I "WIPE" METODA

3.1. KLASIČNO BRISANJE PODATAKA (DELETE)

Klasično brisanje podataka na Windows operativnom sistemu podrazumijeva korištenje osnovnih funkcija kao što su opcije Delete, Shift + Delete ili pražnjenje Recycle Bin-a. Ove metode predstavljaju logičko brisanje podataka, pri čemu operativni sistem ne uklanja fizički sadržaj fajla sa medija za pohranu (Carrier, 2005).

Kod NTFS fajl sistema, prilikom brisanja fajla, sistem uklanja zapis o lokaciji fajla u Master File Table (MFT) i označava zauzeti prostor kao slobodan. Međutim, stvarni podaci ostaju netaknuti na disku sve dok taj prostor ne bude prepisan novim podacima. Iz tog razloga, obrisani fajlovi mogu biti povraćeni pomoću specijalizovanih alata za oporavak podataka ili forenzičkih alata (Microsoft Learn, bez datuma).

Ovakav način brisanja predstavlja ozbiljan sigurnosni problem, naročito u slučajevima kada se radi o osjetljivim dokumentima, poslovnim tajnama ili ličnim podacima. U kontekstu računarske forenzike, klasično brisanje podataka ne smatra se pouzdanom metodom uklanjanja digitalnih tragova.

3.2. SIGURNO BRISANJE PODATAKA (WIPE)

Za razliku od klasičnog brisanja, *wipe* metoda podrazumijeva trajno uništavanje podataka putem prepisivanja memorijskog prostora na kojem su se podaci nalazili. Wipe alati koriste različite algoritme prepisivanja, pri čemu se originalni sadržaj fajla zamjenjuje nasumičnim ili unaprijed definisanim vrijednostima (Casey, 1999).

Cilj wipe metoda jeste onemogućavanje povrata podataka, čak i korištenjem naprednih forenzičkih tehnika. Ove metode su posebno važne u okruženjima gdje se zahtijeva visok

nivo sigurnosti podataka, kao što su državne institucije, vojska, finansijski sektor i zdravstveni sistemi.

U računarskoj forenzici, wipe alati se često posmatraju kao dio anti-forenzičkih tehnika, jer se koriste sa ciljem prikrivanja digitalnih tragova i otežavanja istrage (Nelson, Phillips, & Steuart , 2019).

3.3. RAZLIKA IZMEĐU DELETE I WIPE METODA

Osnovna razlika između Delete i Wipe metoda ogleda se u načinu tretiranja fizičkog sadržaja fajla. Dok Delete uklanja samo referencu na fajl, Wipe aktivno mijenja sadržaj memorijskog prostora.

Tabela 1. Prikaz karakteristika za Delete i Wipe

Karakteristika	**Delete**	**Wipe**
Brisanje MFT zapisa	Da	Da
Prepisivanje podataka	Ne	Da
Mogućnost povrata	Visoka	Izuzetno mala
Forenzička otpornost	Niska	Visoka
Namjena	Uobičajeno brisanje	Sigurno uništavanje

Iz forenzičkog ugla, wipe metoda predstavlja znatno ozbiljniji izazov za istražitelje, jer pravilno primijenjeni algoritmi prepisivanja značajno smanjuju šanse za rekonstrukciju originalnog sadržaja (Nelson, Phillips, & Steuart , 2019).

3.4. FORENZIČKI ZNAČAJ WIPE METODA

Sa forenzičkog aspekta, wipe metode predstavljaju dvostruki izazov. S jedne strane, one služe legitimnoj svrsi zaštite podataka, dok s druge strane mogu biti korištene za namjerno uništavanje dokaza.

Iako pravilno izvršen wipe može onemogućiti povrat podataka, tragovi poput instalacije wipe alata, sistemskih logova, promjena u fajl sistemu i vremenskih zapisa i dalje mogu biti predmet forenzičke analize. Zbog toga wipe alati ne garantuju potpunu anonimnost korisnika, već samo otežavaju direktan pristup obrisanim podacima (Kent, Chevalier, Grance, & Dang, 2006).

4. SOFTVERSKE APLIKACIJE ZA POVRAT OBRISANIH PODATAKA

4.1. POJAM I ZNAČAJ SOFTVERA ZA POVRAT PODATAKA

Softverske aplikacije za povrat podataka predstavljaju alate koji omogućavaju rekonstrukciju i vraćanje digitalnih fajlova koji su obrisani korištenjem klasičnih metoda brisanja (Delete, Shift+Delete, formatiranje bez prepisivanja).

Ovi alati koriste činjenicu da operativni sistem prilikom standardnog brisanja ne uklanja stvarni sadržaj fajla sa diska, već samo briše reference na njega unutar fajl sistema. Sve dok memorijski prostor nije prepisan novim podacima, postoji realna mogućnost povrata.

U računarskoj forenzici, alati za povrat podataka imaju ključnu ulogu jer omogućavaju:

- vraćanje obrisanih dokaza,
- dokazivanje neuspješnog pokušaja prikrivanja tragova,
- razlikovanje između delete i wipe metoda brisanja (Carrier, 2005).

4.2. NAČIN RADA ZA POVRAT OBRISANIH FAJLOVA

Aplikacije za povrat podataka funkcionišu analizom struktura fajl sistema i nealociranog prostora diska. Njihov rad se zasniva na nekoliko osnovnih principa:

- skeniranje MFT zapisa (NTFS fajl sistem),
- prepoznavanje obrisanih, ali neprepisanih klastera,
- rekonstrukcija fajlova na osnovu metapodataka,

- file carving tehnike (prepoznavanje tipa fajla po zaglavljima).

Efikasnost povrata zavisi od vremena koje je proteklo od brisanja i stepena prepisivanja memorijskog prostora (Casey, 1999).

4.3. NAJČEŠĆE KORIŠTENI ALATI ZA POVRAT OBRISANIH PODATAKA

4.3.1. RECUVA

Recuva je jedan od najpoznatijih alata za povrat obrisanih fajlova, prvenstveno namijenjen krajnjim korisnicima. Podržava povrat podataka sa hard diskova, USB uređaja i memorijskih kartica.

Osnovne karakteristike:

- grafički interfejs prilagođen korisnicima,
- mogućnost brzog i dubinskog skeniranja,
- prikaz stanja fajla (odlična, djelimična ili nemoguća obnovljivost).

Recuva se često koristi za demonstraciju razlike između klasičnog brisanja i sigurnog brisanja podataka (CCleaner, bez datuma).

4.3.2. PHOTOREC

PhotoRec je open-source alat koji se fokusira na povrat fajlova putem file carving tehnika. Ne oslanja se na fajl sistem, što ga čini izuzetno efikasnim u slučajevima oštećenih ili formatiranih diskova.

Ključne karakteristike:

- podrška za veliki broj formata fajlova,

- rad iz komandne linije,
- mogućnost povrata podataka sa različitih fajl sistema.

U forenzičkom kontekstu, PhotoRec se koristi kada metapodaci više nisu dostupni (PhotoRec, bez datuma).

4.3.3. AUTOPSY

Autopsy je forenzički alat koji, pored kompletne analize sistema, omogućava povrat obrisanih fajlova i pregled nealociranog prostora.

Njegove prednosti uključuju:

- integraciju sa Sleuth Kit alatima,
- detaljnu analizu fajl sistema,
- vizuelni prikaz forenzičkih artefakata.

Autopsy je široko prihvaćen u akademskim i profesionalnim forenzičkim istragama (Autopsy User's Guide, bez datuma).

4.4. OGRANIČENJA SOFTVERA ZA POVRAT PODATAKA

Iako su alati za povrat podataka moćni, oni imaju značajna ograničenja:

- ne mogu vratiti podatke nakon pravilno izvršenog wipe-a,
- uspješnost opada kod SSD diskova zbog TRIM komande,
- djelimično oštećeni fajlovi mogu biti neupotrebljivi,
- pogrešna upotreba može dodatno prepisati podatke.

Ova ograničenja dodatno potvrđuju važnost pravilne primjene sigurnih metoda brisanja podataka (Carrier, 2005).

4.5. FORENZIČKI ZNAČAJ ALATA ZA POVRAT OBRISANIH PODATAKA

U digitalnim istragama, softver za povrat podataka omogućava dokazivanje:

- pokušaja prikrivanja aktivnosti,
- neadekvatnog brisanja osjetljivih podataka,
- postojanja digitalnih dokaza koji su namjerno uklonjeni.

Rezultati dobijeni ovim alatima često se koriste kao ključni dokazi u sudskim postupcima, pod uslovom da je analiza izvršena na forenzičkoj kopiji medija (Casey, 1999).

5. STANDARDI ZA SIGURNO BRISANJE PODATAKA

Sigurno brisanje podataka predstavlja ključni segment zaštite informacija u savremenim informacionim sistemima. Za razliku od proizvoljnog ili nestrukturiranog prepisivanja podataka, standardi za sigurno brisanje definišu precizne procedure, broj prolaza i način validacije procesa brisanja, kako bi se osiguralo trajno uništenje podataka. U računarskoj forenzici, poznavanje ovih standarda je od posebnog značaja jer omogućava procjenu da li su podaci mogli biti povratljivi, kao i identifikaciju potencijalne namjere prikrivanja digitalnih tragova.

5.1. DoD 5220.22-M STANDARD

DoD 5220.22-M je jedan od najpoznatijih i najčešće citiranih standarda za sigurno brisanje podataka. Standard potiče iz sigurnosnog priručnika Ministarstva odbrane Sjedinjenih Američkih Država (Department of Defense – DoD) i prvobitno je bio namijenjen za zaštitu povjerljivih vojnih informacija pohranjenih na magnetnim medijima.

Osnovna ideja ovog standarda jeste višestruko prepisivanje memorijskog prostora na kojem su se nalazili podaci, s ciljem onemogućavanja njihove rekonstrukcije, čak i primjenom naprednih forenzičkih tehnika. Zbog svoje jasno definisane strukture, DoD 5220.22-M je široko prihvaćen i implementiran u brojnim wipe alatima, posebno na Windows platformi.

Iako standard više nije zvanično preporučen od strane DoD-a za moderne sisteme, njegova primjena i dalje ima značajnu edukativnu i forenzičku vrijednost, te se često koristi kao referenca u akademskim i profesionalnim radovima (Department of Defense, 2020).

5.1.1. TRI FAZE DoD 5220.22-M METODE

Klasična verzija DoD 5220.22-M metode sastoji se od tri uzastopna prolaza prepisivanja podataka:

1. Prvi prolaz - prepisivanje nulama (0) - U ovom prolazu, svi bitovi u ciljanom memorijskom prostoru prepisuju se nulama. Time se briše originalni binarni sadržaj fajla.
2. Drugi prolaz - prepisivanje jedinicama (1) - Nakon prvog prolaza, isti prostor se ponovo prepisuje, ali ovoga puta jedinicama. Cilj ovog koraka je dodatno narušavanje magnetnih tragova prethodnog zapisa.
3. Treći prolaz - prepisivanje nasumičnim vrijednostima uz verifikaciju - U završnoj fazi, podaci se prepisuju nasumičnim vrijednostima, a zatim se vrši verifikacija kako bi se potvrdilo da je prepisivanje uspješno izvršeno.

Ovakav višeslojni pristup ima za cilj da minimizira mogućnost povrata podataka čak i korištenjem specijalizovanih forenzičkih tehnika koje analiziraju magnetne ostatke na disku (Carrier, 2005).

5.1.2. PREDNOSTI I GRANIČENJA DoD STANDARDA

Prednosti DoD 5220.22-M standarda:

- jasno definisana i standardizovana procedura brisanja,
- široka podrška u komercijalnim i open-source wipe alatima,
- visok nivo sigurnosti na HDD medijima,
- jednostavna implementacija u forenzičkim i edukativnim okruženjima.

Ograničenja DoD standarda:

- smanjena efikasnost na SSD diskovima zbog TRIM i wear leveling mehanizama,
- produženo vrijeme brisanja kod velikih diskova,
- savremeni standardi smatraju da višestruki prolazi nisu uvijek neophodni,
- standard je formalno zastario u odnosu na nove NIST preporuke.

Iz tog razloga, iako DoD 5220.22-M i dalje ima značajnu ulogu u teoriji i praksi, savremene forenzičke smjernice preporučuju prilagođavanje metode vrsti medija za pohranu (NIST , 2024).

5.2. OSTALI STANDARDI BRISANJA PODATAKA

Pored DoD 5220.22-M standarda, razvijeni su i drugi standardi za sigurno brisanje podataka koji uzimaju u obzir savremene tehnologije pohrane i nove sigurnosne zahtjeve. Među njima se posebno izdvajaju NIST SP 800-88 i Gutmann metoda.

5.2.1. NIST SP 800-88

NIST SP 800-88 predstavlja savremeni standard za sanitizaciju medija koji je razvio Nacionalni institut za standarde i tehnologiju (National Institute of Standards and Technology – NIST). Ovaj standard pruža smjernice za sigurno uklanjanje podataka sa različitih vrsta medija, uključujući HDD, SSD, mobilne uređaje i cloud okruženja.

NIST definiše tri nivoa sanitizacije:

- Clear – logičko uklanjanje podataka (npr. prepisivanje),
- Purge – napredne metode (kriptografsko brisanje, Secure Erase),
- Destroy – fizičko uništavanje medija.

Za razliku od DoD standarda, NIST SP 800-88 naglašava da višestruko prepisivanje nije uvijek neophodno, naročito na modernim diskovima, te preporučuje metode prilagođene tehnologiji pohrane (Chandramouli & Hibbard, 2025).

5.2.2. GUTMANN METODA

Gutmann metoda je jedna od najagresivnijih metoda sigurnog brisanja podataka i podrazumijeva čak 35 prolaza prepisivanja različitim obrascima. Ovu metodu je razvio Peter Gutmann s ciljem eliminacije magnetnih ostataka podataka na starijim vrstama diskova.

Iako se Gutmann metoda često navodi kao izuzetno sigurna, savremena istraživanja ukazuju da je ona u velikoj mjeri zastarjela i neefikasna za moderne diskove. Njena primjena danas se rijetko preporučuje zbog dugog trajanja procesa i minimalne dodatne sigurnosti u odnosu na jednostavnije metode (Gutmann, 1996).

6. ANALIZA I OPIS SOFTVERSKIH ALATA ZA POTPUNO BRISANJE PODATAKA (WIPE ALATI)

6.1. POJAM I KLASIFIKACIJA WIPE ALATA

Wipe alati predstavljaju specijalizovani softver čija je osnovna funkcija trajno uklanjanje podataka sa digitalnih medija putem prepisivanja memorijskog prostora. Za razliku od standardnih sistemskih funkcija za brisanje, wipe alati koriste unaprijed definisane algoritme i standarde koji onemogućavaju kasniji povrat podataka (Casey, 1999).

Wipe alati se mogu klasifikovati prema:

- obimu djelovanja (brisanje pojedinačnih fajlova, foldera, slobodnog prostora ili cijelog diska),
- metodi prepisivanja (jedan prolaz, višestruki prolazi, kriptografsko brisanje),
- platformi (Windows, Linux, cross-platform),
- namjeni (lična upotreba, poslovna okruženja, vojni i državni sektor).

U kontekstu računarske forenzike, wipe alati se posmatraju kao alati sa dvostrukom namjenom - mogu se koristiti za legitimnu zaštitu podataka, ali i za anti-forenzičke aktivnosti (Chandramouli & Hibbard, 2025).

6.2. ERASER - DETALJNA ANALIZA ALATA

Eraser je jedan od najpoznatijih i najčešće korištenih open-source wipe alata za Windows operativne sisteme. Ovaj alat omogućava sigurno brisanje fajlova, foldera, slobodnog prostora na disku, kao i podataka pohranjenih na eksternim medijima.

Glavne karakteristike Erasera:

- podrška za više standarda brisanja (DoD 5220.22-M, Gutmann, Random Data),
- integracija u Windows kontekstni meni (desni klik),
- detaljni log zapisi izvršenih operacija,
- mogućnost zakazivanja zadataka (scheduler).

Eraser je posebno pogodan za edukativne i forenzičke svrhe jer omogućava preciznu kontrolu nad procesom brisanja i jasno prikazuje korištenu metodu prepisivanja (Eraser, bez datuma).

6.3. SDELETE (MICROSOFT SYSINTERNALS)

SDelete je alat komandne linije koji je razvio Microsoft Sysinternals tim. Njegova osnovna funkcija jeste sigurno brisanje fajlova i slobodnog prostora na NTFS fajl sistemima.

Za razliku od grafičkih alata, SDelete zahtijeva osnovno poznavanje komandne linije, ali nudi visok nivo pouzdanosti i integracije sa Windows okruženjem.

Ključne karakteristike:

- korištenje DoD 5220.22-M metode prepisivanja,
- mogućnost čišćenja slobodnog prostora,
- minimalni tragovi u sistemu (nema GUI-a),
- često korišten u profesionalnim i forenzičkim okruženjima.

SDelete se često navodi kao referentni alat u akademskoj literaturi zbog činjenice da dolazi direktno od proizvođača operativnog sistema (Russinovich, 2023).

6.4. CCLEANER I OGRANIČENJA WIPE FUNKCIJA

CCleaner je popularan alat za održavanje sistema koji, pored osnovnih funkcija čišćenja, nudi i mogućnost sigurnog brisanja slobodnog prostora diska.

Međutim, CCleaner nije primarno forenzički wipe alat. Njegove wipe funkcije su ograničene i ne pružaju detaljne log zapise niti napredne opcije kontrole prepisivanja kao što to čine specijalizovani alati poput Erasera ili SDelete-a.

U forenzičkom kontekstu, CCleaner se češće posmatra kao alat za uklanjanje tragova korištenja sistema, nego kao pouzdan alat za potpuno uništavanje podataka (Chandramouli & Hibbard, 2025).

6.5. DBAN (DARIK'S BOOT AND NUKE)

DBAN (Darik’s Boot And Nuke) je specijalizovani softverski alat namijenjen za potpuno i trajno brisanje podataka sa tvrdih diskova. Za razliku od alata koji se pokreću unutar operativnog sistema, DBAN funkcioniše kao bootabilno okruženje i pokreće se nezavisno od instaliranog operativnog sistema.

Zbog ovakvog načina rada, DBAN ima direktan pristup diskovima i omogućava brisanje kompletnog sadržaja diska, uključujući operativni sistem, korisničke podatke i nealocirani prostor.

Ključne karakteristike:

- pokretanje sa eksternog medija (USB ili CD/DVD),
- potpuno brisanje cijelog diska,
- podrška za više metoda prepisivanja (uključujući DoD 5220.22-M i Gutmann metodu),
- namijenjen za pripremu računara za prodaju, donaciju ili trajno povlačenje iz upotrebe.

DBAN se često koristi u profesionalnim i visokosigurnosnim okruženjima, ali se njegova primjena preporučuje prvenstveno za HDD diskove, dok za SSD uređaje postoje ograničenja zbog TRIM mehanizama (NIST , 2024).

6.6. PREDNOSTI I NEDOSTACI WIPE ALATA

Prednosti:

- trajno uklanjanje osjetljivih podataka,
- smanjenje rizika od curenja informacija,
- usklađenost sa sigurnosnim standardima,
- jednostavna primjena kod određenih alata.

Nedostaci:

- moguća zloupotreba u anti-forenzičke svrhe,
- neadekvatna primjena može ostaviti tragove,
- ograničena efikasnost na SSD uređajima,
- rizik od nenamjernog brisanja podataka.

Zbog navedenih nedostataka, upotreba wipe alata mora biti pažljivo planirana i dokumentovana (Nelson, Phillips, & Steuart , 2019).

6.7. FORENZIČKI TRAGOVI NAKON KORIŠTENJA WIPE ALATA

Iako wipe alati imaju za cilj potpuno uništavanje podataka, njihova upotreba često ostavlja indirektne forenzičke tragove. Ti tragovi mogu uključivati:

- zapise o instalaciji softvera,

- log fajlove wipe alata,
- promjene u MFT tabeli,
- sistemske event logove,
- vremenske zapise (timestamps).

Forenzička analiza ovih tragova može pomoći istražiteljima da dokažu postojanje namjere prikrivanja dokaza, čak i kada sami podaci nisu povratljivi (Kent, Chevalier, Grance, & Dang, 2006).

7. WIPE I RAZLIČITI MEDIJI ZA POHRANU PODATAKA

7.1. HDD DISKOVI

Tradicionalni tvrdi diskovi (HDD – Hard Disk Drive) koriste magnetno zapisivanje podataka na rotirajuće ploče. Podaci se zapisuju u sektore i klastere, a njihova fizička lokacija na disku je relativno stabilna i predvidiva. Upravo zbog ovakvog načina rada, wipe metode koje se zasnivaju na prepisivanju podataka pokazale su se kao veoma efikasne na HDD uređajima.

Kod HDD diskova, proces wipe-a podrazumijeva direktno prepisivanje istih fizičkih sektora na kojima su se nalazili originalni podaci. Višestruki prolazi prepisivanja (npr. DoD 5220.22-M metoda) značajno smanjuju mogućnost povrata podataka, čak i korištenjem naprednih forenzičkih tehnika.

Iz forenzičke perspektive, pravilno izveden wipe na HDD disku rezultira:

- potpunim uništenjem originalnog sadržaja,
- nepostojanjem prepoznatljivih fajl struktura,
- nemogućnošću file carving tehnika.

Zbog navedenog, HDD diskovi se smatraju medijima na kojima wipe alati postižu najviši stepen efikasnosti (Chandramouli & Hibbard, 2025).

7.2. SSD DISKOVI I TRIM KOMANDA

Za razliku od HDD diskova, SSD (Solid State Drive) uređaji koriste flash memoriju i potpuno drugačiji način upravljanja podacima. SSD diskovi primjenjuju mehanizme poput wear leveling-a i garbage collection-a, koji automatski raspoređuju zapise podataka kako bi se produžio vijek trajanja memorijskih ćelija.

Jedan od ključnih mehanizama kod SSD diskova je TRIM komanda, koja operativnom sistemu omogućava da obavijesti SSD kontroler koji blokovi podataka više nisu u upotrebi. Nakon TRIM operacije, SSD može interno obrisati te blokove bez eksplicitnog prepisivanja od strane operativnog sistema.

Zbog ovih karakteristika, klasične wipe metode zasnovane na višestrukom prepisivanju nisu uvijek pouzdane na SSD diskovima. Operativni sistem nema direktnu kontrolu nad fizičkom lokacijom podataka, što znači da prepisivanje logičkih adresa ne mora garantovati prepisivanje stvarnih memorijskih ćelija.

Savremeni standardi preporučuju alternativne metode sanitizacije SSD diskova, kao što su:

- kriptografsko brisanje (crypto erase),
- korištenje proizvođačkih Secure Erase funkcija,
- fizičko uništavanje medija u visokosigurnosnim okruženjima (Samsung Electronics Co., 2013).

8. FORENZIČKA DETEKCIJA WIPE AKTIVNOSTI

8.1. TRAGOVI WIPE ALATA NA SISTEMU

Iako wipe alati imaju za cilj potpuno uklanjanje podataka, njihova upotreba često ostavlja indirektne tragove na operativnom sistemu. Ovi tragovi mogu poslužiti kao važan forenzički dokaz da je izvršena namjerna radnja brisanja podataka.

Najčešći tragovi wipe alata na sistemu uključuju:

- instalacione foldere i konfiguracione fajlove alata,
- zapise u Windows Registry bazi,
- Prefetch fajlove koji ukazuju na pokretanje wipe alata,
- promjene u NTFS metapodacima (MFT, $LogFile, $UsnJrnl).

Prisustvo ovih artefakata omogućava forenzičarima da identifikuju korištenje wipe alata čak i kada su originalni podaci trajno uništeni (Kent, Chevalier, Grance, & Dang, 2006).

8.2. LOG FAJLOVI WIPE ALATA

Mnogi wipe alati generišu log fajlove koji sadrže informacije o izvršenim operacijama brisanja. Ovi zapisi mogu imati značajnu dokaznu vrijednost u forenzičkoj istrazi.

Log fajlovi najčešće sadrže:

- datum i vrijeme izvršenja wipe operacije,
- naziv ili putanju obrisanih fajlova,
- korištenu metodu prepisivanja,

- status uspješnosti brisanja.

Analiza log fajlova omogućava rekonstrukciju događaja i dokazivanje namjere korisnika da trajno ukloni podatke (Carrier, 2005).

8.3. ANALIZA NEALOCIRANOG PROSTORA

Nealocirani prostor diska predstavlja ključnu oblast u forenzičkoj analizi. Kod klasičnog brisanja, u ovom prostoru se često mogu pronaći ostaci obrisanih fajlova. Međutim, nakon primjene wipe alata, nealocirani prostor je najčešće prepisan uniformnim obrascima podataka.

Forenzička analiza može ukazati na:

- prisustvo ponavljajućih uzoraka (npr. nule ili nasumični podaci),
- nepostojanje struktura fajlova,
- nemogućnost primjene file carving tehnika.

Ovakvi nalazi upućuju na primjenu sigurnih metoda brisanja podataka (Nelson, Phillips, & Steuart , 2019).

9. ULOGA WIPE ALATA U ANTI-FORENZICI

9.1. ANTI-FORENZIKA - POJAM

Anti-forenzika predstavlja skup tehnika i postupaka kojima se namjerno otežava ili onemogućava digitalna forenzička analiza. Cilj anti-forenzičkih aktivnosti jeste prikrivanje tragova, uništavanje digitalnih dokaza ili dovođenje istražitelja u zabludu.

Najčešće anti-forenzičke tehnike uključuju:

- trajno brisanje podataka,
- enkripciju,
- manipulaciju vremenskim zapisima,
- skrivanje ili izmjenu sistemskih artefakata.

U tom kontekstu, wipe alati zauzimaju značajno mjesto jer direktno utiču na dostupnost digitalnih dokaza (Casey, 1999).

9.2. WIPE ALATI KAO ANTI-FORENZIČKO SREDSTVO

Wipe alati se mogu koristiti u legitimne svrhe zaštite podataka, ali i kao sredstvo anti-forenzike kada se primjenjuju sa namjerom uništavanja dokaza. Njihova upotreba prije ili tokom istrage može značajno otežati forenzičku analizu.

Forenzička interpretacija korištenja wipe alata zasniva se na:

- vremenskoj povezanosti brisanja sa incidentom,
- vrsti podataka koji su obrisani,
- prisustvu dodatnih tragova prikrivanja aktivnosti.

Iako wipe alati mogu spriječiti povrat podataka, oni ne garantuju potpunu anonimnost korisnika, jer njihova upotreba često ostavlja indirektne forenzičke tragove (Chandramouli & Hibbard, 2025).

10. ZAKLJUČAK

U savremenom digitalnom okruženju, gdje se ogromne količine podataka svakodnevno stvaraju, obrađuju i brišu, pitanje sigurnog uklanjanja informacija predstavlja značajan izazov kako za pojedince, tako i za organizacije. Ovim radom analiziran je proces brisanja podataka sa računara, s posebnim fokusom na razliku između klasičnog brisanja i sigurnog brisanja pomoću wipe alata.

Istraživanje je pokazalo da klasične metode brisanja podataka, poput opcija Delete ili pražnjenja Recycle Bin-a, ne uklanjaju fizički sadržaj fajlova sa medija za pohranu, već samo brišu reference u fajl sistemu. Zbog toga se podaci obrisani na ovaj način mogu uspješno povratiti korištenjem softverskih alata za oporavak podataka i forenzičkih tehnika.

Analiza softverskih aplikacija za povrat obrisanih podataka potvrdila je da je povrat podataka u velikom broju slučajeva moguć sve dok memorijski prostor nije prepisan novim sadržajem. Time je dodatno potvrđena potreba za korištenjem pouzdanih metoda trajnog brisanja u situacijama kada je neophodna zaštita osjetljivih informacija.

Rezultati rada potvrđuju radnu hipotezu da primjena wipe alata koji koriste višestruke metode prepisivanja može trajno uništiti podatke i onemogućiti njihov povrat standardnim forenzičkim alatima. Ipak, istraživanje je takođe pokazalo da wipe alati ne garantuju potpunu anonimnost korisnika, jer njihova upotreba često ostavlja indirektne forenzičke tragove, kao što su log zapisi, promjene u fajl sistemu i sistemski događaji.

Posebna pažnja posvećena je uticaju vrste medija za pohranu na efikasnost wipe metoda. Dok se višestruko prepisivanje pokazalo kao efikasno rješenje kod HDD diskova, kod SSD uređaja su potrebne alternativne metode sanitizacije podataka zbog specifičnih mehanizama upravljanja memorijom.

Na osnovu provedenog istraživanja može se zaključiti da pravilno razumijevanje razlike između brisanja, povrata i trajnog uništavanja podataka ima ključnu ulogu u računarskoj forenzici, ali i u svakodnevnoj praksi zaštite informacija. Ovaj rad doprinosi boljem razumijevanju wipe alata, recovery softvera i njihove uloge u forenzičkim i anti-

forenzičkim procesima, te predstavlja dobru osnovu za dalja praktična istraživanja kroz forenzičke scenarije.

11. LITERATURA

Preuzeto od CCleaner: https://www.ccleaner.com/recuva

Autopsy User's Guide. (bez datuma). Preuzeto od Autopsy User Documentation: https://sleuthkit.org/autopsy/docs/user-docs/4.22.0/

Carrier, B. (2005). *File System Forensic Analysis.* Addison Wesley Professional.

Casey, E. (1999). *Digital Evidence and Computer Crime - Third Edition.* cmdLabs, Baltimore, Maryland, USA: Elsevier.

Chandramouli, R., & Hibbard, E. (2025). *Guidelines for Media Sanitization.* NIST.

Department of Defense. (2020). *National Industrial Security Program (NISP).* Department of Defense.

Eraser. (bez datuma). *Documentation*. Preuzeto od Eraser: https://eraser.heidi.ie/help/

exterro. (bez datuma). *The Basics of Digital Forensics*. Preuzeto od exterro: https://www.exterro.com/basics-of-digital-forensics/chapter-2-the-forensic-investigation-process

Gutmann, P. (1996). *Secure Deletion of Data from Magnetic and Solid-State Memory.* San Jose: University of Auckland.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response.* NIST - National Institute of Standards and Technology.

Microsoft Learn. (bez datuma). *NTFS overview*. Preuzeto od Microsoft Learn: https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview

Nelson, B., Phillips, A., & Steuart , C. (2019). *GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS - Sixth Edition.* Boston: Cengage Learning, Inc.

NIST . (09. September 2024). *Hash Functions*. Preuzeto od NIST - National Institute of Standards and Technology: https://csrc.nist.gov/projects/hash-functions

PhotoRec. (bez datuma). Preuzeto od CGSecurity: https://www.cgsecurity.org/wiki/PhotoRec

Russinovich, M. (23. September 2023). *SDelete v2.05*. Preuzeto od Microsoft Learn: https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete

Samsung Electronics Co. (2013). *Samsung Solid State Drive - White Paper.* Samsung.