Forenzična analiza Windows log datoteka

Maras, Stipe

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University Department for Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:821369

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

FORENZIČNA ANALIZA WINDOWS LOG DATOTEKA

STIPE MARAS

Split, srpanj 2020

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI
FORENZIKA I NACIONALNE SIGURNOSTI

FORENZIČNA ANALIZA WINDOWS LOG DATOTEKA

MENTOR: IZV. PROF. DR. SC. TONI PERKOVIĆ
KOMENTOR: DOC. DR. SC. NINA MIŠIĆ RADANOVIĆ

STIPE MARAS

Matični broj: 467/2018

Split, srpanj 2020.

Rad je izrađen na Sveučilišnom odjelu za forenzične znanosti u Splitu pod mentorstvom izv. prof. dr. sc. Toni Perković i doc. dr. sc. Nina Mišić Radanović,

Datum predaje diplomskog rada: 15. srpanj 2020
Datum prihvaćanja diplomskog rada: 21. srpanj 2020
Datum usmenog polaganja: 22. srpanj 2020

Ispitno povjerenstvo:

1. Prof. dr. sc. Josip Kasum
2. Doc. dr. sc. Marko Perkušić
3. Izv. prof. dr. sc. Toni Perković

Sadržaj

1. Uvod

Forenzična znanost se u principu definira kao multidisciplinarna znanost koja se koristi u svrhu primjene zakona odnosno koristi svoja znanja i pruža nepristrane znanstvene dokaze prilikom procesuiranja kaznenih djela. Riječ forenzika potječe od latinske riječi *„forensis"* što znači „pred ili prije forum" odnosno u javnosti, budući da su se u rimskim vremenima prva ispitivanja i suđenja izvodila na glavnim gradskim trgovima (forumima). Naravno da se Forenzika kao znanstvena disciplina mijenja sukladno razvoju i promijeni društvenih vrijednosti i tehnologija.

Danas je opće prihvaćeno da se tehnologija neprekidno razvija (uključujući računala, internet, e-trgovine, e-usluge i slično) te je tako uključena u većinu aspekata našeg života. Tako možemo reći da je život u 21. stoljeću nezamisliv bez primjene moderne tehnologije. To se dobro može očitovati na najsvježijem primjeru oko pandemije koronavirusa COVID-19 (eng. Coronavirus disease 2019) kada je cijeli svijet ostao paraliziran, većina svjetskih i europskih država je proglasilo „karantenu". U takvim uvjetima gdje je ograničena ljudska sloboda kretanja gotovo je nemoguće zamisliti funkcioniranje svakodnevnog života. Općepoznato je da su većina ljudskih djelatnosti na neki način informatizirane, a upravo ova kriza s kojom smo se susreli je ubrzala proces informatizacije i digitalizacije zdravstva, gospodarstva, obrazovanja, javne uprave, e-trgovine te svakodnevnog života općenito. U Hrvatskoj svjedočimo uspostavi e-propusnica, digitalnih tržnica, nastave na daljinu na svim razinama školstva, te takozvanog rada na daljinu. Tako se putem računala i mreže sprema i pristupa informacijama koji su ključni faktor modernog poslovanja te ih je iz tih razloga potrebno zaštiti. No bez obzira na politike, pravila, uredbe i postupke kojima se upravlja radi zaštite povjerljivosti i integriteta digitalnih podataka učestalo smo svjedoci kršenja zakonskih odredbi te zlouporabe informacija i podataka. Veliki broj organizacija suočava se s raznim vrstama računalnih zločina, a kriminalci koji počine takva djela imaju niz različitih motiva. Od pokušaja da naštete nečijem ugledu ili stjecanju novčane dobiti pa sve do terorizma.

Otkako su se zločini sve više počeli pojavljivati u računalnom okruženju, pojavila se potreba za razvijanjem novog polja u forenzičnim istragama koji se naziva Računalna forenzika koja se danas sve češće naziva digitalnom forenzikom. Postoji nekoliko definicija računalne forenzike:

- „Računalne tehnike ispitivanja i analize koje uključuju identifikaciju, očuvanje, ekstrakciju, dokumentiranje i tumačenje računalnih podataka radi utvrđivanja potencijalnih pravnih dokaza [1].“
- „Računalna forenzika obično se odnosi na forenzičko ispitivanje komponenata računala i njihovog sadržaja kao što su tvrdi diskovi, kompaktni diskovi i pisači [2].“
- „Računalna forenzika je prikupljanje, čuvanje, analiza i prezentacija vezana uz računalne dokaze [3].“

Iz definicija je vidljivo kako je osnovni cilj računalne forenzike pronaći digitalni dokaz koji može biti prihvaćen na sudu. Iz tog razloga programski alati koji se koriste za istragu moraju biti testirani i licencirani od strane nadležnih tijela. Kako se takvi alati naplaćuju i nisu dostupni širokom krugu ljudi, za potrebe ovog rada biti će korišteni isključivo besplatni programski alati dostupni javnosti. Takvi alati ne mogu se koristiti kao dokazna sredstva u sudskom postupku, ali svakako mogu biti korisni u istraživačkom smislu.

Novi izazovi u računalnoj forenzici pojavljuju se uvođenjem novijih i modernijih operacijskih sustava. Najzastupljeniji operacijski sustav na svijetu je svakako Microsoftov Windows. Prema podacima sa Microsoftove službene stranice preko milijardu uređaja koristi najnoviju inačicu Windows-a (Windows 10) [4]. Kada govorimo o računalnoj forenzici Windows-a, forenzika Windows Log datoteka ima bitnu ulogu zbog velike količine podataka koju sadrže i važnosti pohranjenih podataka koji mogu biti ključni za rješavanje istrage. Nažalost iskusnim kriminalcima je jedno od prvih pravila prilikom upada u sustav obrisati ili modificirati datoteku ovakvih zapisa tako da prikriju svoju aktivnost na sustavu.

Cilj ovog rada je prikazati sadržaj Windows log datoteka i neke od osnovnih metoda njihove analize. Dnevnici događaja i Registar svakako su jedni od vitalnih dijelova Windows operacijskog sustava, oni sadrže kritične informacije potrebne sustavu i aplikacijama za normalno funkcioniranje. Gotovo svaka radnja korisnika na računalu zapisana je unutar ovih datoteka, upravo iz tog razloga ovo može biti jako bogat izvor dokaza na sudu.

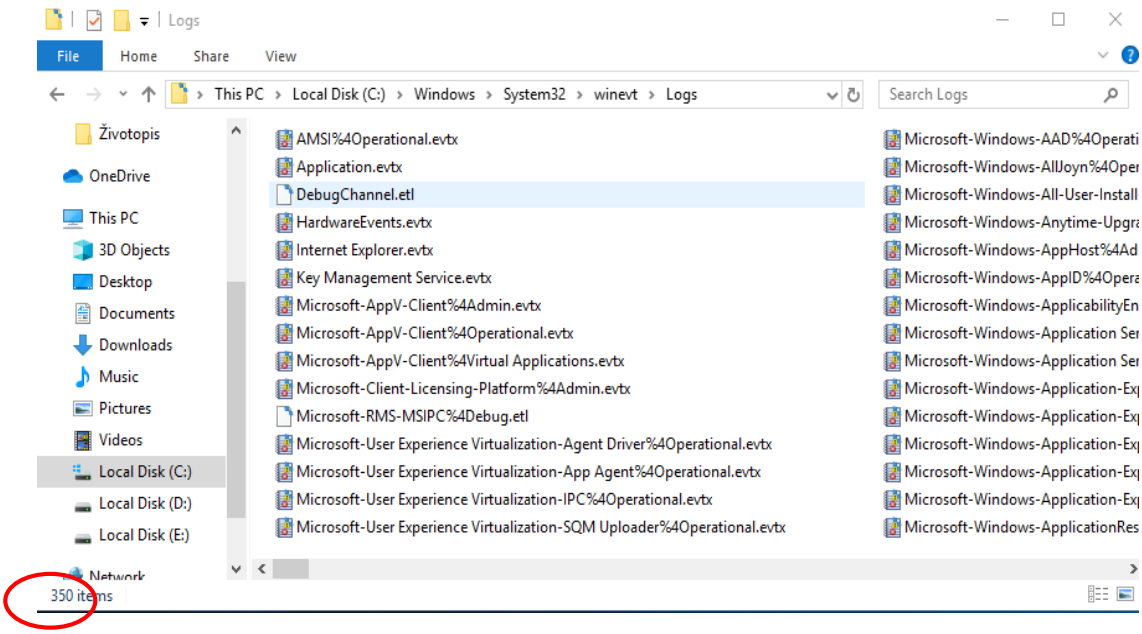
U prvom dijelu rada objasnit ćemo pojam, strukturu i organizaciju Dnevnika događaja i Registra. Kako ove datoteke sadrže mnoštvo podataka i informacija, navest ćemo neke bitnije zapise na koje bi forenzični istražitelj prilikom istrage svakako trebao obratiti

pozornost i analizirati ih. Za bolje razumijevanje teme napravit ćemo par praktičnih primjera analiza uz pomoć nekomercijalnih forenzičnih programskih alata. Takvi alati se ne mogu koristiti kao dokazna sredstva u sudskom postupku, zbog toga što nisu licencirani ali nam i dalje pružaju učinkovito analiziranje ovakvih datoteka. U završnom dijelu ovoga rada kratko su opisani pravni aspekti Republike Hrvatske u borbi protiv prevencije i suzbijanja računalnog kriminaliteta te povećanja informacijske sigurnosti općenito. Na samom kraju rada napravit ćemo kratak zaključak na temelju ranije opisanih saznanja i činjenica.

2. Dnevnik događaja (Event Log)

Dnevnici događaja detaljno bilježe različite svakodnevne događaje koji se događaju na Windows operacijskom sustavu te se mogu postaviti kako bi zabilježili niz dodatnih događaja [5]. Aplikacije i operacijski sustav koriste ove zapise događaja za snimanje važnih hardverskih i softverskih radnji koje mogu pomoći korisniku uočiti točan izvor određenog događaja. Windows operacijski sustav prati određene događaje u svojim datotekama dnevnika, poput instalacija aplikacija, upravljanja sigurnošću, operacija postavljanja sustava pri početnom pokretanju i problema ili pogreške [6].

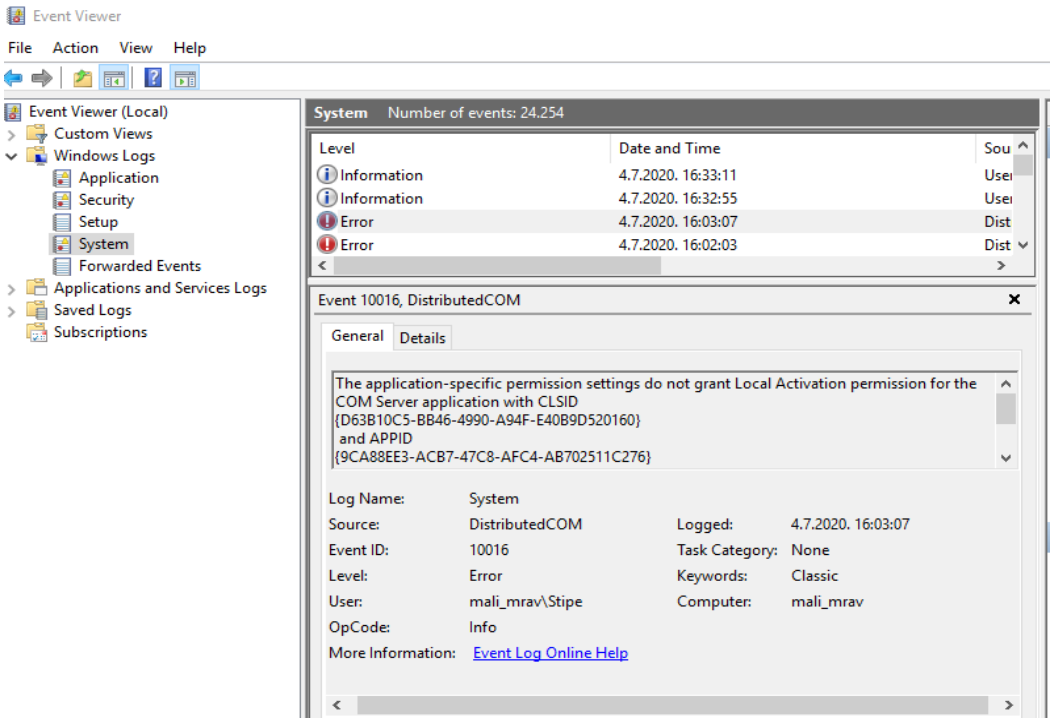
Dnevnik događaja uveden je u operacijski sustav Windows NT 3.1 iz 1993. godine te se od tada nalazi u svakoj verziji Windows operacijskog sustava. Ovakve starije verzije sustava uključujući Windows XP imaju tri binarne datoteke dnevnika događaja: Aplikacije (eng. Application), Sustav (eng. System), Sigurnost (eng. Security) koje su u EVT formatu i nalaze se na C: \Windows\ system32\config. Moderni Windows sustavi (Vista i noviji) pohranjuju dnevnike u direktoriju C:\Windows\System32\winevt\Logs u binarnom formatu Windows XML event log (EVTX) [7]. Ove novije verzije imaju uz tri standardna dnevnika (Application, System, Security) i mnoštvo novih dnevnika, tako Windows 10 broji preko 300 različitih dnevnika događaja. Ovaj rad biti će usmjeren na noviji format logova.



Slika 1. Direktorij Windows Dnevnika događaja

Postoji pet različitih vrsta događaja koji se bilježe unutar Windows dnevnika događaja[8]:

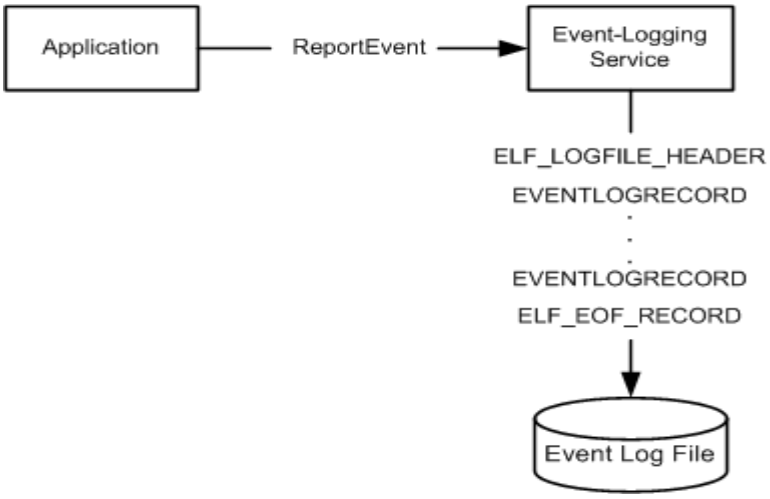
- **Pogreška (eng. Error) -** događaj koji ukazuje da je došlo do značajnog problema, poput gubitka podataka ili funkcionalnosti. Na primjer, ako se usluga ne pokrene prilikom njenog pokretanja zabilježit će se događaj pogreške.
- **Upozorenje (eng. Warning) –** ovo je događaj koji trenutno nije nužno značajan ali ukazuje kako bi u budućnosti mogao nastati problem. Na primjer, kada je tvrdom disku preostalo malo slobodnog prostora zabilježit će se ovaj događaj upozorenja.
- **Informacija (eng. Information) -** označava uspješan rad aplikacije, upravljačkog programa ili neke usluge. Na primjer, ako se aplikacija uspješno pokrene, sustav može zabilježiti takav informacijski događaj.
- **Revizija uspjeha (eng. Success Audit) –** ukazuje da je određeni sigurnosni događaj bio uspješan. Na primjer uspješna prijava korisnika bilježi se kao događaj revizije uspjeha.
- **Revizija neuspjeha (eng. Failure Audit) –** suprotno od revizije uspjeha, to je događaj koji bilježi pokušaj neuspješne prijave korisnika.



Slika 2. Windows Event Viewer

2.1. Svojstva Windows Event Log datoteka

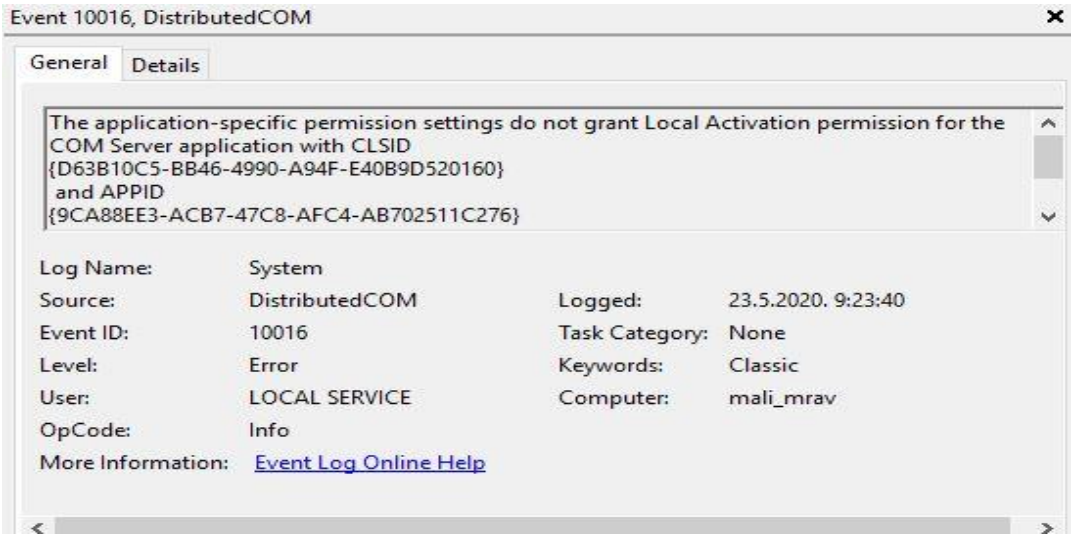
Kada određena aplikacija ili neki proces Windows operacijskog sustava želi stvoriti vlastiti zapis, šalje se zahtjev s podacima Event-Log servisu koji zatim dobivene podatke zapisuje u log datoteku. Svaki dnevnik događaja sadrži zaglavlje (predstavljeno strukturom ELF_LOGFILE_HEADER) koje ima fiksnu veličinu, zatim varijabilni broj zapisa događaja (predstavljen strukturama EVENTLOGRECORD) i zapis na kraju datoteke (predstavljen strukturom ELF_EOF_RECORD). Struktura ELF_LOGFILE_HEADER i struktura ELF_EOF_RECORD pišu se u dnevnik događaja kada se kreira dnevnik događaja i ažuriraju svaki put kad se događaj zapiše u dnevnik [8].



Slika 3. Protokol stvaranja aplikacijskog zapisa u logove [8].

Glavni elementi svakog događaja u zapisu se sljedeći (Slika 4.):

- Izvor – objekt koji je zatražio zapis događaj
- ID događaja – broj koji generira Windows te identificira tip događaja
- Razina – Informacije / Upozorenje / Pogreška
- Korisnik – korisničko ime za račun koji je prijavljen u trenutku kada se dogodio događaj.
- Datum i vrijeme – datum i vrijeme zapisa događaja
- Računalo – naziv računala na kojem se događaj dogodio.
- Opis – opis onoga što se dogodilo za pokretanje događaja



Slika 4. Glavni elementi log datoteke

Za detaljnije informacije o događaju možemo otvoriti Log u obliku XML datoteke kao što je vidljivo na slici 5.

Slika 5. Event Log u obliku XML datoteke

Tablica 1. Značenje polja u XML sistemskom zapisu Windows OS-a [9]

POLJE	OPIS
Provider	Izvor tj. proces koji je zatražio zapis događaja
Event ID	Broj koji identificira tip događaja
Version	Može sadržavati podatke o verziji događaja.
Level	Numerička oznaka razine važnosti događaja
Task	Ovo polje ostavlja se na korištenje procesu koji poziva zapisivanje događaja, a može sadržavati podatke o pozivu
Opcode	Numerička vrijednosti koja označava aktivnost koja se izvršavala u vrijeme kada je kreiran zahtjev za stvaranjem zapisa o događaju.
Keywords	Ključne riječi koje mogu pomoći pri pretraživanju srodnih zapisa.
TimeCreated	Sistemsko vrijeme kreiranja zapisa.
EventRecordID	Specifična oznaka tog zapisa, odnosno događaja
Execution	Sadrži oznaku procesa i dretve koji su generirali događaj.
Channel	Log u koji se zapisuje događaj.
Computer	Ime računala na kojem se dogodio događaj.
Security	Sigurnosni podaci o aktivnom korisniku / računalu.
EventData	EventData predstavlja „tijelo“ zapisa unutar kojeg se nalaze podaci o samom događaju, a može sadržavati atribute kao što su ime.
Data	Podaci o samom događaju.

2.2. Tipovi Windows Event Log datoteka

Dnevnici događaja stvaraju zapise o realiziranim aktivnostima (događajima) unutar operacijskog sustava i zapise o aktivnostima aplikacija koje se koriste na sustavu. Odabir vrste dnevnika događaja koji će se analizirati ponajviše ovisi o vrsti forenzičke istrage koja se provodi. Tijekom istrage koriste se osnovni elementi dnevnika događaja kao što su ključ dnevnika događaja, identifikacijski broj događaja, zapisi dnevnika događaja i podaci o događajima [10]. Iz dnevnika događaja možemo čitati, na primjer, informacije o uspješnom izvršavanju zadatka ili možemo vidjeti događaje upozorenja koji prepoznaju potencijalne probleme, također su važni i sigurnosni događaji te upozorenja o neuspjelim aktivnostima. Microsoft Windows pruža jednostavan preglednik dnevnika događaja „Event Viewer“ koji je integriran u sustav i možete pronaći na sljedećem linku: Control Panel\All Control Panel Items\Administrative Tools\Computer Management\Event Viewer. On nudi jednostavno sučelje za pretraživanje i istraživanje događaja. Microsoft također preporuča korisniku koje događaje pratiti zbog toga što ti događaji mogu biti pokazatelji kompromitiranog sustava.

Na službenim Microsoftovim stranicama možete pronaći detaljan opis svih događaja uz pomoć njegovog identifikacijskog broja (ID) bilo da se radi o starijim Windows operacijskim sustavima (Windows XP i ranije) ili Windows sustavima novije generacije (od Windows Viste do Windowsa 10). Pojedinačni ID-ovi događaja ukazuju na određene vrste događaja, a nedavne verzije sustava Windows imaju odvojene datoteke dnevnika događaja za razne aplikacije i usluge. Vidjeli smo u prethodnom tekstu kako je takvih dnevnika događaja unutar sustava Windows 10 preko 300. Unatoč mogućnostima filtriranja, digitalni forenzičari mogu imati poteškoća pri pronalasku događaja koji su bitni za njihove istrage iz velikog broja pohranjenih logova [11]. U daljnjem tekstu nalazi se popis ključnih događaja koji mogu biti korisni za dobivanje bitnih dokaznih podataka iz Windows evidencije događaja.

- **Aplikacija –** ovaj zapisnik događaja sadrži događaje koji su zabilježeni u aplikacijama ili programima. Dnevnik događaja aplikacija ovisi o samoj aplikaciji, neke aplikacije koriste Windows sustav zapisa dok druge imaju svoj vlastiti sustav zapisa. Obično se bilježe: informacije o instalaciji, zahtjevi i odgovori arhitekture klijent - poslužitelj, informacije o korisničkim računima, informacije o korištenju, akcije koje program ima u registru operacijskog sustava i sl. [12]. Također bilježe se događaji vezani za aplikacije koje su blokirane od strane sustava. Bilo koji blokirani programi mogu biti zlonamjerni softveri ili korisnici koji pokušavaju pokrenuti nedozvoljene softvere. Također i prestanak rada aplikacije može sugerirati da se radi o pojedinim nedozvoljenim radnjama i softverima. Kategorije prestanka rada aplikacije podrazumijevaju plavi ekran (eng. Blue Screen of Death – BSOD), Izvještavanje o pogreškama Windows sustava (eng. Windows error reporting – WER), pad aplikacije (eng. Application Crash) i aplikacija prestaje odgovarati (eng. Application Hang – stop responding).
    - 1000 – App Error
    - 1002 – App Hang
    - 1001 – BSOD, WER
- **Sigurnost** - Sigurnosni dnevnik sadrži događaje poput valjanih i nevaljanih pokušaja prijave, kao i događaje povezane s korištenjem resursa, poput stvaranja, otvaranja ili brisanja datoteka ili drugih objekata.

- **Sustav** - pohranjuje događaje operacijskog sustava ili njegovih komponenti, na primjer, kvarove pri pokretanju usluga ili inicijalizaciju upravljačkih programa, poruke na cijelom sustavu i ostale poruke povezane sa sustavom u cjelini. Ako se ovakve pogreške učestalo ponavljaju na pojedinom računalu to može biti znak da je računalo meta napada. Zapisnik događaja Sustava navodi događaje iz različitih izvora (komponenti sustava), tako da se pri analiziranju zapisnika sustava treba osloniti i na ID događaja zajedno s izvorom događaja.
- **Windows vatrozid** – također postoji mogućnost prikupljanja događaja za praćenje stanja vatrozida (eng. Firewall). Na primjer kada se isključi aktivnost vatrozida taj podatak se bilježi, „normalni“ korisnici računala uglavnom ne mijenjaju postavke vatrozida. Tako da je to podatak koji svakako može biti koristan za istragu.
    - 2004 - Firewall Rule Add
    - 2005 - Firewall Rule Change
    - 2006, 2033 - Firewall Rule Deleted
    - 2009 - Firewall Failed to load Group Policy
- **Upotreba računa** – informacije o korisničkom računu kao što su prijava na korisnički račun, dodavanje korisnika u povlaštenu grupu i zaključavanje računa mogu pomoći u otkrivanju neovlaštenog korištenja računala.
    - 4740 - Account Lockouts
    - 4728, 4732, 4756 - User Added to Privileged Group
    - 4735- Security-Enabled group Modification
    - 4624 - Successful User Account Login
    - 4625 - Failed User Account Login
    - 4648 - Account Login with Explicit Credentials
- **Aktivnosti Windows Defender-a** - Microsoft je razvio Windows Defender Antivirus koji pruža zaštitu u stvarnom vremenu od softverskih prijetnji poput virusa, zlonamjernog softvera i špijunskog softvera putem e-pošte, aplikacija, oblaka i weba. Sve obavijesti o otkrivanju, uklanjanju i sprečavanju tih zlonamjernih programe treba istražiti.

- 1005 - Scan Failed
- 1006 - Detected Malware
- 1008 - Action on Malware Failed
- 1010 - Failed to remove item from quarantine
- 2001 - Failed to update signatures
- 2003 - Failed to update engine
- 2004 - Reverting to last known good set of signatures
- 3002 - Real – Time Protection failed
- 5008 - Unexpected Error

- **Instalacija** - događaji koji se dogode tijekom instalacije i konfiguracije operacijskog sustava i njegovih komponenata bilježe se u ovaj zapisnik.
    - 7022, 7023, 7024, 7026, 7031, 7032, 7034 - Windows service Fails or Crashes
    - 20, 24, 25, 31, 34, 35 - Windows Update Failed
- **Proslijeđeni događaji** - to je zadana lokacija za bilježenje događaja primljenih iz drugih sustava. Ako je konfigurirano prosljeđivanje događaja, događaji poslani s drugih poslužitelja bit će spremani u ovaj zapisnik.
- **Aktivnost bežičnih uređaja –** Bežični uređaji su sveprisutni i praćenje njihovih aktivnosti svakako može biti korisno. Bežični uređaj može postati kompromitiran tijekom komunikacije između različitih mreža, bez obzira na protokol koji se koristi za komunikaciju.
    - 10000, 10001 - Network Connection and Disconnection status
    - 8000, 8011 - Starting a Wireless connection
    - 8001 - Successfully connected to Wireless connection
    - 8003 - Disconnect from Wireless connection
    - 11000, 11001, 11002 - Wireless Association Status
    - 11004, 11005, 11010, 11006 - Wireless Security

- 8002 - Wireless Connection Failed
- 12011, 12012, 12013 - Wireless Authentication Started and Failed

- **Detekcija vanjskih (eksternih) uređaja** - Otkrivanje upotrebe određenih eksternih uređaja u stvarnom vremenu može biti od presudnog značaja za istragu. Zapis se bilježi svaki put kada je upravljački program instaliran ili ažuriran. Identifikacijski broj događaja koji bilježi instalaciju i ažuriranje uređaja je 20001, a 20003 bilježi ažuriranje i instalaciju usluge. Informacije o događaju 20001 uključuju podatke o ID-a proizvoda i proizvođača te serijski broj uređaja.
- **Revizijska politika –** mijenjanjem revizijske politike korisnika utječe se direktno na dokazne postupke istražitelja bilo da je promjena napravljena od strane administratora računala ili pak od strane napadača. Tako Windows bilježi ove događaje promjena kada se one pojave.
    - 4719 - System audit policy was changed
- **Task Scheduler** - pokreće pozadinske zadatke i aplikacije prema rasporedu. Pregledavanjem događaja 4624 možemo saznati vrijeme i datum upotrebe Task Scheduler-a, naziv odredišnog računala, informacije o mreži, ID sigurnosne prijave (SID) i ostalo.
- **Udaljena radna površina –** koristi se za povezivanje s drugim uređajem putem mreže kako bi korisniku omogućili upravljanje tim računalom na daljinu. Napadači ponekad koriste udaljenu radnu površinu (eng. Remote Desktop Protocol - RDP) za prijavu na udaljena računala dok su korisnici daleko od računala, ili za prodor na računalne servere.
    - 4624 - An account was successfully logged on
    - 4648 - A logon was attempted using explicit credentials
    - 4778 - A session was reconnected to a Window Station
    - 4779 - A session was disconnected from a Window Station.
- **Brisanje zapisa događaja** – Ako prilikom pretraživanja dnevnika događaja utvrdimo da nedostaju podaci mala je vjerojatnost da bi se podaci dnevnika događaja izbrisali tijekom normalne korisničke upotrebe. Takva radnja je sumnjiva i svakako upućuje na to da napadač pokušava prekriti zapise brisanjem dnevnika

događaja. Središnje prikupljanje događaja dodatno otežava napadaču da prekrije svoju aktivnost. Prosljeđivanje događaja omogućuje izvorima da naprave više kopija prikupljenih podataka o događajima.

- 104 - Event Log was Cleared
- 1102 - Audit Log was Cleared

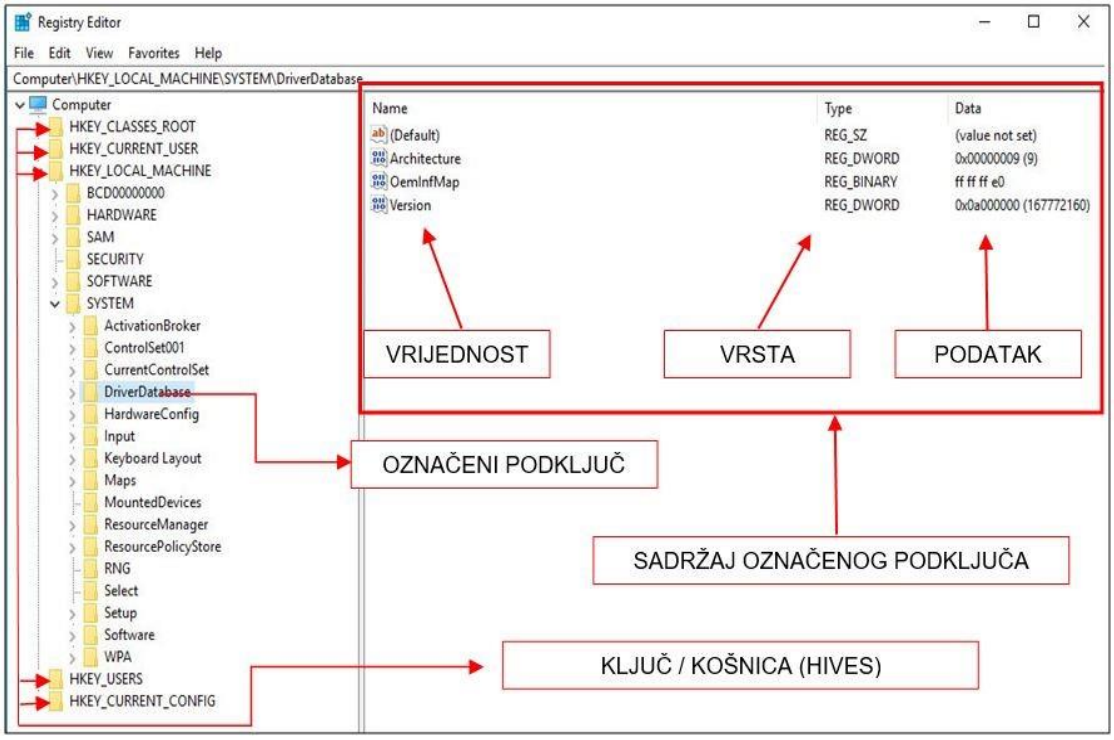
3. Windows Registar (Windows Registry)

Windows registar je hijerarhijska baza podataka koja sadrži podatke koji su kritični za rad operacijskog sustava, aplikacija i svih ostalih usluga koje se koriste na Windows sustavu [13]. Također je jedna od osnovnih komponenti svakog operacijskog sustava Windows još od verzije Windows NT (3.1). Pohranjuje veliki dio informacija i postavki za softverske programe, korisničke postavke i informacije o hardverskim uređajima. Također pohranjiva povijest aktivnosti za svakog pojedinog korisnika kako bi svakom od korisnika pružio što personaliziraniji rad i korištenje samog operacijskog sustava. Tako analizom Windows registra možemo pronaći popis nedavno posjećenih web stranica, otvaranih dokumenata, popis povezivanih USB uređaja, koji su programski alati zadnji upotrebljavani i slično [14]. S obzirom da sadrži mnogo informacija koje mogu biti potencijalni izvor dokaznim radnjama možemo uvidjeti njegovu važnost u računalnoj forenzici. Podaci u registru su strukturirani u obliku stabla gdje se svaki od čvorova na stablu naziva ključem. Svaki ključ može sadržavati i potključeve i unose podataka koji se nazivaju vrijednostima. Fizički podaci Windows registra nisu pohranjeni u jednu datoteku na tvrdom disku nego se pohranjuju u odvojene binarne datoteke koje se nazivaju košnice (eng. Hives) [13].

3.1. Struktura Windows Registra

U Windows operacijskom sustavu Windows Registar logički je organiziran u više korijenskih ključeva i alati kao što je, uređivač registra sustava Windows, mogu se koristiti za prikaz logičke strukture sustava registra. U registru sustava Windows nalazi se pet logičkih korijenskih ključeva [15]:

1. HKEY_CLASSES_ROOT
2. HKEY_CURRENT_USER
3. HKEY_LOCAL_MACHINE
4. HKEY_USERS
5. HKEY_CURRENT_CONFIG

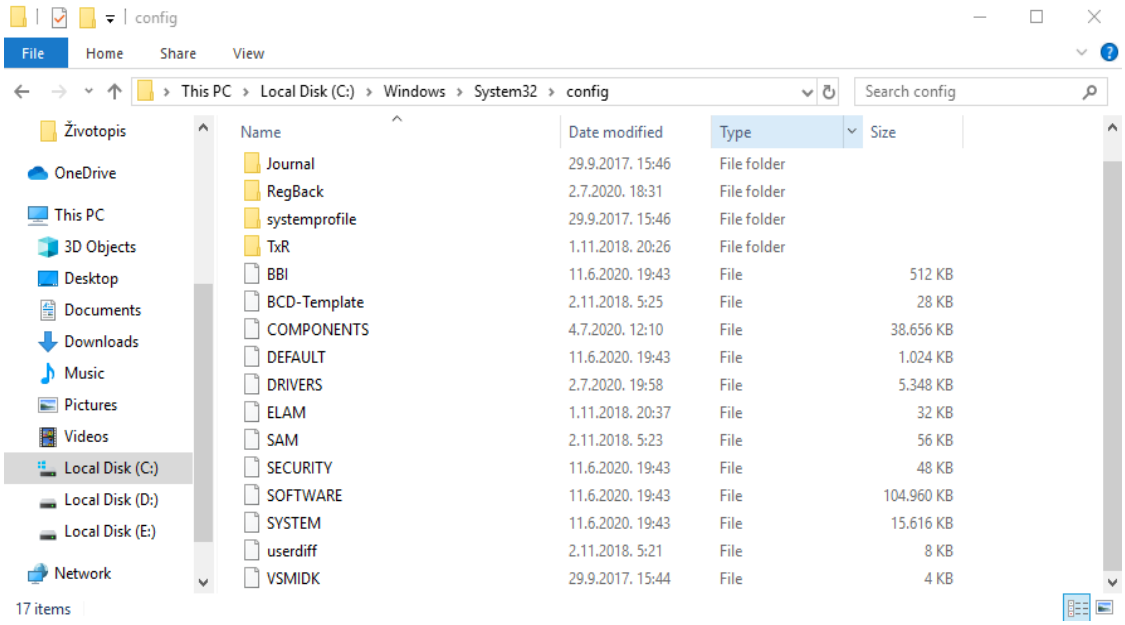


Slika 6. Registry Editor

Na slici 6. prikazan je logički prikaz uređivača registra odnosno Registry Editora. Direktoriji koji se nalaze na lijevoj strani Registry Editora predstavljaju registarski ključ ili njegov podključ. Svaki registarski ključ ima jednu ili više vrijednosti, a svaka vrijednost ima tri atributa: ime, vrstu i same podatke [13]. Vrsta vrijednosti ovisi o tipu podataka koju ta vrijednost sadrži. Uobičajene vrste vrijednosti u registru su: REG_SZ koja sadrži niz podataka fiksne duljine, REG_DWORD sadrži podatke s dvije riječi odnosno 32-bita i REG_BINARY koja sadrži binarne vrijednosti, Kada aplikacija pročita podatke vrijednosti u formatu REG_BINARY iz registra, ona odlučuje kako dekodirati vrijednost. Aplikacija može pohraniti podatke u binarne datoteke da pri tome koristi svoju vlastitu podatkovnu strukturu jer na taj način samo aplikacija zna kako interpretira takve datoteke. Na primjer, rezultat interpretiranja REG_BINARY podataka kao 8-bitne ASCII vrijednosti ili 16-bitne Unicode može dati dvije različite vrijednosti. Ova tehnika se može koristiti za sakrivanje podataka ili za zbunjivanje forenzičkog ispitivača. Također, neke aplikacije REG_SZ i REG_DWORD vrstu podataka pohranjuju kao REG_BINARY, kako bi također prikrili podatke i otežali samo pronalaženje istih. Bez obzira na vrstu vrijednosti, registar zapravo čuva sve vrijednosti u binarnom formatu u stvarnom zapisu. Budući da su sve vrijednosti pohranjene zajedno sa svojom odgovarajućom vrstom Registry Editor na taj način ispravno interpretira podatke [16].

3.2. Organizacija Windows Registra

Iako se Windows Registar pojavljuje kao jedinstvena hijerarhija u alatima kao što je Registry Editor, on se zapravo sastoji od više različitih binarnih datoteka koje se nazivaju košnice (eng. Hives). Fizički podaci registra nisu pohranjeni u jednu datoteku na tvrdom disku nego se pohranjuju u odvojene binarne datoteke koje se nalaze u direktoriju C:\Windows\System32\config [17].



Slika 7. Fizički podaci Windows registra

HKEY_LOCAL_MACHINE i HKEY_USERS su jedini ključevi koje Windows fizički sprema u datoteke. HKEY_CURRENT_USER je samo simbolička veza na pod-ključeve koji su zapravo smješteni u HKEY_USERS, HKEY_CLASSES_ROOT i HKEY_CURRENT_CONFIG su simboličke veze prema pod-ključevima spremljenim u HKEY_LOCAL_MACHINE [16].

1. HKEY_LOCAL_MACHINE

HKLM sadrži informacije o lokalnom računalnom sustavu uključujući značajke i podatke o hardveru i operacijskom sustavu, kao što su vrsta sabirnice, sistemska memorija, upravljački programi uređaja te kontrola aplikacija koje se automatski pokreću prilikom pokretanja u sustavu Windows [18]. Sadrži postavke koje se primjenjuju na sve korisnike koji se prijavljuju na to računalo. Unutar ključa HKLM nalaze se sljedeći pod-ključevi [19]:

- **HARDWARE** – sadrži podatke o hardveru koje Windows učitava svaki put prilikom pokretanja računala, uključuje podatke i o upravljačkim programima (eng. device drivers). Pod-ključevi se dinamički stvaraju tijekom pokretanja sustava.
- **SOFTWARE** – sadrži postavke programa specifične za svakog pojedinog korisnika računala.
- **SAM** – upravitelj sigurnosnih računa (eng. Security Accounts Manager) je baza podataka koja sadrži informacije o lokalnim korisnicima i grupama, uključujući njihova korisnička imena i lozinke. Iz tog razloga ovaj pod-ključ je zanimljiv hakerima. „Access Control Lists“ (ACL) sprječava administratora da pregleda ovaj pod-ključ.
- **SYSTEM** – sadrži kontrolni skup koji sadrži upravljačke programe (drivere) i servisne konfiguracije.
- **SECURITY** – sadrži Windows sigurnosnu bazu podataka na kojoj je korisnik prijavljen, ili sa košnicom registra na lokalnom računalu ako se korisnik prijavo u domenu lokalnog sustava. „Access Control Lists“ (ACL) također sprječava administratora da pregleda ovaj pod-ključ.

2. HKEY_USER

HKU sadrži informacije o svakom korisničkom profilu unutar sustava Windows, a većinom su vezane za vizualne postavke te postavke programskih alata. HKU sadrži najmanje ova 3 pod-ključa [19]:

- .DEFAULT (hrv. Zadano)
- SID
- SID_CLASSES

3. HKEY_CURRENT_USER

HKCU sadrži konfiguracijske postavke za korisnika koji je trenutno prijavljen na računalo, uključujući postavke radne površine, aplikacija, mrežne veze i korisnikove direktorije [20]. Ovaj ključ ne sadrži nikakve podatke nego je samo simbolička vezu prema HKU ključu, u kojem su zapravo fizički spremljene sve navedene postavke.

4. **HKEY_CURRENT_CONFIG**

HKCC sprema informacije o trenutnoj konfiguraciji sustava [21]. Zapravo simbolička veza prema pod-ključu HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Currenut, kojem je fizički pohranjena trenutna konfiguracija sustava.

5. **HKEY_CLASSES_ROOT**

HKCR sadrži postavke koje osiguravaju da se zadani programski alat otvori pri izvršavanju određenih naredbi. HKCR zauzima većinu registarskog prostora, iako Windows spaja dva ključa - HKLM\SOFTWARE\Classes (sadrži zadane, pretpostavljene postavke) i HKCU\Software\Classes (sadrži korisničke postavke) kako bi održavao HKCR i imao lakši pristup svim postavkama [22].

4. Forenzična analiza Windows Registra

U Windows registru nalazi se na tisuće različitih ključeva, odabir ključeva koji će se analizirati ovisi o vrsti forenzične istrage koja se provodi. Mnogi ključevi koji su važni za istragu se mogu grupirati u nekoliko kategorija na temelju potencijalnih dokaznih podataka koje možemo pronaći: Opće forenzične informacije, uređaji priključeni na računalo, sigurnosni identifikatori i aktivnosti povezane sa upadom u sustav [23]. Analiza podataka unutar Windows Registra može se napraviti pomoću dviju metoda. Analizom uživo (eng. Live analysis) možemo pristupiti registru kao i na bilo kojem računalu pomoću ugrađenog uređivača registra kao što je Registry Editor, ili ako se registar nalazi u okviru forenzičke slike. Na taj će se način računalni forenzički program koristiti za istraživanje datoteka registra slično kao i prilikom pregledavanja datoteka pomoću programskog alata Registry Editor [14]. Ako ispitujemo Windows registar uz pomoć forenzičke slike, potrebno je poznavati gdje se nalaze košnice (eng. Hives) Windows Registra (C:\Windows\ System32\config – kao što je opisano u prethodnom poglavlju) . Nakon što smo pronašli datoteke potrebno je izraditi forenzičnu sliku datoteka kako bih mogli naknadno izvršiti analizu uz pomoć računalnih forenzičnih paketa.

Forenzičnu sliku košnica možemo jednostavno izraditi uz pomoć besplatnog programskog alata „AccessData FTK Imager“. Nakon uspješne izrade slike podataka iste možemo pohraniti na eksternu memoriju kako bi ih naknadno mogli analizirati putem različitih forenzičnih alata. Većina forenzičnih programskih alata može ispitati registar sustava Windows iz ovako izrađene forenzične slike podataka. Postoji mnogo programskih alata specijaliziranih za analizu Registry hives vrijednosti. Alat koji je dostupan na svakom Windows operacijskom sustavu je prethodno spomenuti Registry Editor kojeg se može pokrenuti s administratorskim ovlastima. „AccessData Registry Explorer“ je također besplatni primjerak programskog alata kojega je moguće iskoristiti za navigaciju kroz ključeve i analizu istih. Osim njega postoje još mnogi drugi alati koji pomažu pri analizi točno određenih ključeva i pod-ključeva ili vrijednost.

4.1. Analiza operacijskog sustava

Windows registar sadrži mnogo informacija o operacijskom sustavu, poput postavki i konfiguracije sustava. Postoji niz vrijednosti koje bi mogle zanimati forenzičkog istražitelja:

- **(HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion)** – ovdje možemo pronaći informacije o verziji Windows sustava, serijski ključ Windows-a, registriranog vlasnika, vrsti instalacije, o korijenskom direktoriju sustava i o drugim podacima.
- **(HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName)** – ovdje možemo iščitati naziv računala.
- **(HKLM\SYSTEM\CurrentControlSet\Control\Windows) –** u ovom ključu se nalazi vrijednost iz koje možemo iščitati kada se računalo zadnji put isključilo. Vrijednost se pohranjuje koristeći binarnu vrijednost, kako bi smo jednostavno dekodirali vrijednost možemo koristiti besplatni programski alat „DCode".
- **(HKLM\HARDWARE\ DESCRIPTION\System\BIOS)** – ovaj ključ sadržava informacije o sustavu BIOS (engl. basic input/output system, osnovni ulazno/izlazni sustav). BIOS je prvi program koji se pokreće prilikom paljenja računala. Pokreće operacijski sustav i upravlja protokom podataka između operacijskog sustava i priključenih uređaja poput tvrdog diska, video adaptera, tipkovnice, miša i sl. [24].
- **(HKCU\Software\Microsoft\Protected Storage System Provider)** – ovaj ključ sadrži „Windows Protected Storage" (hrv. Zaštićena pohrana) koji Microsoftovi proizvodi koriste za pohranu privatnih datoteka. Na primjer ovdje pohranjene lozinke mogu obuhvaćati one za Internet Explorer lozinke kreirane i održavane kad je odabrana opcija „Upamti lozinku". Budući da su ove vrijednosti šifrirane, drugi alat (npr. Cain & Able, PassView, IE PassView, PStoreView itd.) trebali bi se upotrijebiti za dešifriranje i pregled lozinki.
- **(HKLM\SYSTEM\ControlSet001\Control\TimeZoneInformation ili HKLM\ Software\Microsoft\WindowsNT\CurrentVersion\TimeZones) - v**rijednost „ActiveTimeBias" u prvom ključu predstavlja trenutnu vremensku razliku od GMT/UTC u minutama, a vrijednost „Bias" predstavlja razliku u minutama između GMT/UTC i lokalnog vremena. Vrijednosti drugog ključa pohranjuju informacije koje se odnose na sve vremenske zone.
- **(HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall)** – svaki pod-ključ predstavlja neki od instaliranih programa na računalu. Svaki ovaj pod-ključ odgovara programima koji su navedeni u Upravljačkoj Ploči > Programi i Značajke > Dodaj/Ukloni programe. Međutim, postoje i programi koji se ne nalaze

unutar navedene liste kao što su upravljački programi, Windows zakrpe i slično. Svaki pod-ključ uobičajeno sadrži naziv programa, podatke o datumu instaliranja, izvoru instalacije i verziji aplikacije.

- **(HKLM\SOFTWARE\Microsoft\CommandProcessor) -** Ovaj ključ sadrži vrijednost registra koja se naziva „Autorun“ koja sadrži naredbu koja se automatski izvršava svaki put kada se cmd.exe (naredbeni redak) pokrene. Zlonamjerni softveri poput „Trojanca“ mogu iskoristiti značajku cmd.exe kako bi se učitao i pokrenuo bez znanja korisnika. Također i sam korisnik može prikriveno pokrenuti sumnjivi softver tako što će „Autorun“ softvera postaviti i izvršni direktorij značajke cmd.exe. [25].
- **(HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon)** - ovaj ključ sadrži vrijednost „Shell“ sa zadanim podacima explorer.exe. Zlonamjerni softver poput „Kwbota“ mijenja zadane podatke explorer.exe u Shell > explorer.exe%system%System32.exe tako da održi postojanost prilikom ponovnog pokretanja i prijave u sustav [25].
- **(HKLM\SYSTEM\CurrentControlSet\Services)** – ovaj ključ sadrži popis Windows usluga. Svaki pod-ključ predstavlja uslugu i sadrži podatke poput konfiguracije pokretanja. Neki će se zlođudni softveri poput „BackOrifice2K“ instalirati u sustav poput nekih od usluga [25]. Te će raditi štetu sustavu, stoga u ovom ključu možemo naći trag za postojanje nekih od zlođudnih softvera.
- **(HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options) -** Ovaj ključ omogućava administratoru da preslika ime izvršne datoteke u drugi izvor ispravljača pogrešaka, na taj način korisnik može uklanjati pogreške unutar određenog programa uz pomoć drugog programa. Što znači da korisnik može pokrenuti određeni program pod krinkom sasvim različitog programa. Na primjer osumnjičeni stvori pod-ključ pod nazivom notepad.exe tako da izgleda dobroćudno. Zatim ispod tog pod-ključa stvara vrijednost (REG_SZ) koju naziva „Debugger“ (hrv. ispravljač pogreški) i usmjerava je u tajni program (npr. C: \ Windows \ system32 \ telnet.exe). Kada korisnik pokrene notepad.exe, telnet klijent se pokreće umjesto Notepad-a. Ako primjerice osumnjičeni pokreće notepad.exe putem Windows run-a (hrv. Windows pokreni) na njegovom će se popisu povijesti prikazivati samo notepad.exe. Na taj način osumnjičeni prikriva

trag prilikom forenzičkog ispitivanja. Zlonamjerni softver koristi ovu značajku da bi se učitao bez korisničkih znanja [25].

- **(HKCR\exefile\shell\open\command)** – ovaj ključ sadrži upute za izvršavanje bilo koje datoteke s ekstenzijom .exe. U ključu se nalazi zadana vrijednost s podacima "% 1"% *. Međutim, ako se podaci vrijednosti promjene u neki sličan filename.exe "% 1"% *, postoji mogućnost da se neki drugi skriveni program automatski pokreće kada se izvrši stvarna .exe datoteka. Zloćudni softver mijenja ovu vrijednost kako bi se tajno učitao, također se ova tehnika na druge slične ključeve (HKEY_CLASSES_ROOT\ batfile\shell\open\command i HKEY_CLASSES_ROOT\comfile\shell\ open\command) [25].
- **Lista najčešće korištenih datoteka (eng. Most recently used - MRU)** – Ova usluga ažurira popis nedavno otvorenih ili spremljenih datoteka putem tipičnih dijaloški okvira u stilu Windows Explorera (tj. Otvori dijaloški okvir i spremi dijaloški okvir) [26]. Mnoge aplikacije koje se pokreću u Windows-u koriste MRU listu kao što su nedavno otvorene datoteke unutar Windows Media Playera ili nedavno posjećene web stranice [26].

  - ***HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU ili HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU*** - ova dva ključa sadrže imena svih nedavno korištenih izvršnih datoteka i prečace do njihovih mapa.
  - ***HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU ili HKU\[SID]\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU*** - ovi ključevi održavaju popise svih nedavno otvorenih ili spremljenih datoteka (.pdf, .txt, .jpg, .doc, .docx, ppt, pptx, itd.)
  - ***HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU*** – sadrži povijest pokretanja putem usluge „RUN“ (hrv. Pokreni)
  - ***HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs*** – unutar ovog ključa nalazi se popis posljednjih deset datoteka kojima je trenutno prijavljeni korisnik pristupio ili se izvršio putem Windows Explorera.

- **Nedavno pretraživani termini –** kada koristimo Windows pretraživač za pronalaženje određenih datoteka ili mapa povijest takvog pretraživanja spremiti će se u ovaj ključ (HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ WordWheelQuery). Dok u ključu (HKCU\Software\ Microsoft\WindowsSearch\ ProcessedSearchRoots\0003\Default) možemo vidjeti u kojem se direktoriju pohranjuju pretraživanja.
- **Registry „Lastwrite Time“** - Svi ključevi unutar registra imaju pridružene vrijednosti koje se zovu „Last Write Time“ (hrv. vrijeme posljednjeg zapisa), koja je slična vremenu posljednje izmjene datoteke MAC – Modified, Accesed, Created (hrv. Modificirano, Pristupljeno, Stvoreno). Oni se ažuriraju kada se pristupi, izmjeni ili stvori ključ. Možemo dobiti samo vrijeme posljednjeg zapisa ključa, ali ne i vrijeme zapisa za pojedinu vrijednost ključa. Programski alat poput „Keytime.exe“ pruža ispitivaču mogućnost da preuzme vrijeme posljednjeg zapisa određenog ključa [27]. Poznavanje vremena posljednjeg zapisa datoteke može nam pomoći prilikom određivanja približnog vremena za pojedini događaj ili aktivnost. Iako je teško točno odrediti koja se vrijednost unutar ključa promijenila, vrijednost promijene ključa možemo usporediti s nekim drugim parametrima. Tako na primjer usporedbom vremena posljednjeg zapisa ključa i s MAC vremenom datoteke na koju ukazuje vrijednost registra možemo znati vrijeme kreiranja vrijednosti registra ako se vrijeme posljednjeg zapisa ključa podudara s MAC vremenom datoteke [25].

4.2. Analiza mreže i internetskih preglednika

Kada god korisnik Windows operacijskog sustava poveže svoje računalo na mrežu registar će tu radnju zapisati u neki od određenih ključeva. Nekada ti podaci mogu biti od vitalnog značaja za forenzičkog istraživača.

- **(HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ Interfaces)** - unutar ovog ključa možemo pronaći nedavne postavke mrežnog adaptera, kao što je IP adresa sustava i zadani mrežni pristupnik (eng. Network gateway) za odgovarajuće mrežne adaptere.
- **(HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkCards) –** ovaj ključ sadrži popis svih mrežnih kartica bez obzira da li je kartica integrirana ili je eksterna. Na prijenosnim računalima većinom postoje dvije mrežne kartice i to Ethernet i Wi – Fi mrežna kartica.

- **(HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Nla\Cache\Intranet) –** lista svih intranetskih mreža na koje se računalo ikada spajalo može se naći unutar ovoga ključa.
- **(HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Nla\ Wireless) –** Sadrži identifikator svih bežičnih mreža na koje je sustav bio spojen, ne sadrži detaljne informacije o bežičnoj mreži.
- **(HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Signatures) -** Sadrži detaljne informacije o svakoj bežičnoj vezi na računalu kao što je MAC adresa pristupnika, SSID i slično. Kako bi smo dobili sveobuhvatne informacije o mreži potrebno je povezati identifikatore bežične mreže koje smo iščitali iz prethodno navedenog ključa.
- **(HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles) -** sadrži "Datum kreiranja" i "Datum posljednjeg spajanja" odabrane bežične veze.
- **Internet Explorer – (**HKU\S-1-5-21-1116317277-3122546273-4014252621 -1000 \Software\Microsoft\ Internet Explorer\Main) – ovdje se pohranjuju korisničke postavke, početna stranica, informacije o trakama za pretraživanje i slično), dok se u povijest pretraživanih URL adresa nalazi u sljedećem ključu (HKU\S-1-5-21-1116317277-3122546273-4014252621-1000\ Software \Microsoft\ Internet Explorer\TypedURLs)

4.3. Analiza vanjskih (eksternih) uređaja

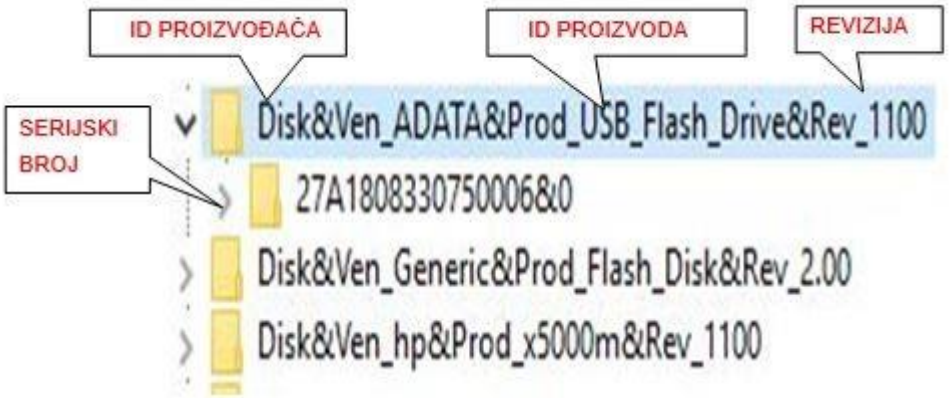
Budući da su danas gotovo svi uređaji vrste "plug and play", što znači da sadrže datoteke upravljačkih programa napisane na firmware-u samog uređaja, sustav ih može izravno instalirati, isključujući potrebu za zasebnim instalacijskim diskom. Kad god je takav Plug-and-Play USB uređaj povezan na sustav, Plug-and-Play (PnP) upravitelj prima ovaj događaj i pita opis uređaja u njegovom firmware-u, poput proizvođača, serijskog broja itd. Po primitku informacijama, PnP upravitelj locira upravljačke programe uređaja i stvara se niz ključeva registra [28].

(HKLM \SYSTEM\MountedDevices) – unutar ovog ključa možemo iščitati popis eksternih uređaja, s pripadajućim jedinstvenim identifikatorom za svaki uređaj. Ovaj ključ

sadrži svaki uređaj koji je priključen na računalo i dodijeljeno mu je pripadajuće slovo jedinice (npr. C:). Unutar ključa registra one vrijednosti čije ime započinje s „\DosDevices\“ i završava sa pripadajućim slovom jedinice, sadrže podatke o određenom uređaju pod tim slovom. Ako binarni podaci unutar navedene vrijednosti sadrže „\??Storage #RemoveableMedia“ na početku vrijednosti, to znači da je USB uređaj spojen na USB port od računala.

- **USB UREĐAJI**

  - **HKLM\SYSTEM\ControlSet001\Enum\USBSTOR –** ovaj ključ pohranjuje podatke o ID-a proizvoda i proizvođača te serijski broj uređaja. Ako je drugi znak serijskog broja „&“ to znači da uređaj nema serijski broj te mu je sustav Windows-a automatski dodijelio serijski broj. Ovdje se nalaze svi USB uređaji koji su priključeni u operaciski sustav od njegove instalacije.



Slika 8. Ključ USB uređaja

- **HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoint2 -** Ova tipka bilježi koji je korisnik bio prijavljen u Windows kada je spojen određeni USB uređaj. Ključ uključuje i podatak o vremenu zadnjeg spajanja na sustav ("Last Write Time") za svaki uređaj.

- **Prvo spajanje USB uređaja** - informaciju kada je istraživani uređaj prvi put spojen na sustav možemo pronaći unutar sljedećeg direktorija tako da potražimo serijski broj određenog USB uređaja [29]:

  - **C:\Windows\INF \setupapi.upgrade.log – Windows 10**
  - **C:\Windows\INF \setupapi.dev.log – Windows 8, 7 i Vista**
  - **C:\Windows\INF \setupapi. Log – Windows XP**

4.4. Problemi prilikom analize Windows Registra

Analiza Windows Registra predstavlja veliki izazov za svakog forenzičnog istražitelja. Nekoliko je glavnih problema s kojima se istražitelji moraju suočiti prilikom analize datoteka registra [30]:

- **Cjelovitost podataka** – koja je količina podataka potrebna prilikom istrage ovisi ponajviše o vrsti same istrage. Zbog toga je iznimno važno da istražitelj osigura da svi podaci koji su dostupni budu prisutni i potpuni.
- **Prikupljanje podataka** – prilikom izuzimanja košnica registra sa određenog računala istražitelj mora izraditi sliku registra. Nedostatak ove metode izuzimanja podataka je ta što istražitelji nakon što izrade sliku košnica ne mogu prikupljati daljnje informacije i podatke. Osim Registry Editora ne postoji mogućnost analize u stvarnom vremenu.
- **Nedostatak znanja o ključevima –** kao što smo prethodno objasnili Windows Registar pohranjuju podatke u jedinstvene ključeve. Nepoznavanje sadržaja određenih ključeva može rezultirati nedostatkom nekih ključnih informacija za samu istragu.
- **Format datoteke registra –**košnice Windows Registra pohranjuju se u direktorij „*C:drive/windows/system32/config*“ i moraju se ukloniti i pretvoriti u čitljiv format prije upotrebe u istrazi. Pri otvaranju datoteka registra postoji ozbiljan rizik ako ne znate odakle datoteke potječu, zbog toga što se tada mogu izbrisati važni podaci.

5. Forenzični alati za analizu Windows Log datoteka

Digitalni dokazi su osjetljivi, lako se brišu i mijenjaju, iz tog razloga je prilikom forenzične analize nekog digitalnog dokaza potrebno koristiti specijalizirane forenzične alate. Neki alati za digitalnu forenziku dizajnirani su samo za jednu svrhu, dok drugi nude veliki spektar funkcionalnosti. Specifičnost svake istrage odredit će koji će se forenzični alat koristiti za predmetnu istragu [31]. Trenutno postoji mnogo alata s kojima je moguće provesti analizu Windows Log datoteka. Uz prethodno spomenute programske alate „Event Viewer“ i „Registry Editor“ koji su besplatni i integrirani unutar svakog Windows operacijskog sustava te ih je moguće pokrenuti s administratorskim ovlastima, postoje još mnogo drugih programskih alata. U ovom istraživanju obradit ćemo samo neke od programskih alata koji su besplatni i lako dostupni svim korisnicima. Prilikom upotrebe ovih alata sa svakim od njih smo napravili jedan praktični primjer analize, kako bi što jasnije i zornije prikazali mogućnosti alata.

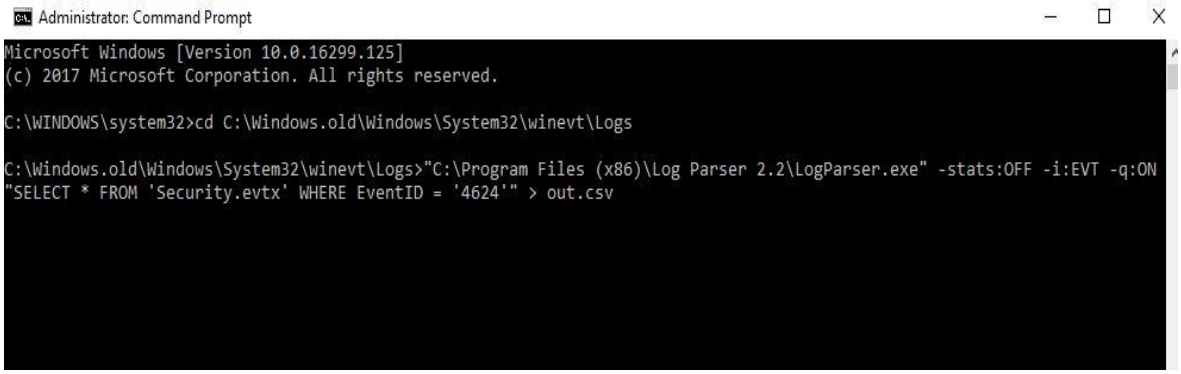
- **Log Parser**

Log Parser je Microsoftov programski alat koji pruža upit za pristup tekstualnim podacima te ključnim izvorima podataka u Windows operacijskim sustavima kao što je *Event Log* i *Registry*. Log Parser sastoji se od tri komponente koje su: 1) ulazni servis, 2) SQL servis upita, 3) izlaznog servisa. SQL (eng. Structured Query Language) je programski jezik koji se koristi za upravljanje podatcima unutar relacijskih baza podataka. Program funkcionira tako da ga usmjerite na izvor o informacijama koje su vam potrebne te u kojem formatu se nalaze(Event logs, Windows registry, IIS log files, itd.), definirate upit i odaberete lokaciju na koju će se spremiti izlazni produkt. Rezultati upita tako mogu biti u tekstualnom obliku (CSV, XML, TSV, itd.), SQL bazi podataka ili u obliku grafikona [32].

Na praktičnom primjeru ćemo prikazati kako na temelju ulazne informacije možemo dobiti popis svih uspješnih korisničkih prijava na Windows operacijski sustav. Kao ulaznu informaciju odnosno upit koristit ćemo poznati ID događaja uspješne prijave na korisnički račun sustava (4624 - Successful User Account Login). Kako bismo započeli s radom potrebno je otvoriti Komandu Liniju (eng. Command Prompt) cmd.exe u korijenu mape gdje se nalaze dnevnici događaja.(C:\Windows\System32\ winevt\Logs). Svaki SQL upit mora minimalno sadržavati dvije naredbe i to „SELECT“ kojom govorimo programu što odabrati i „FROM“ kojom definiramo koji je izvor iz kojeg

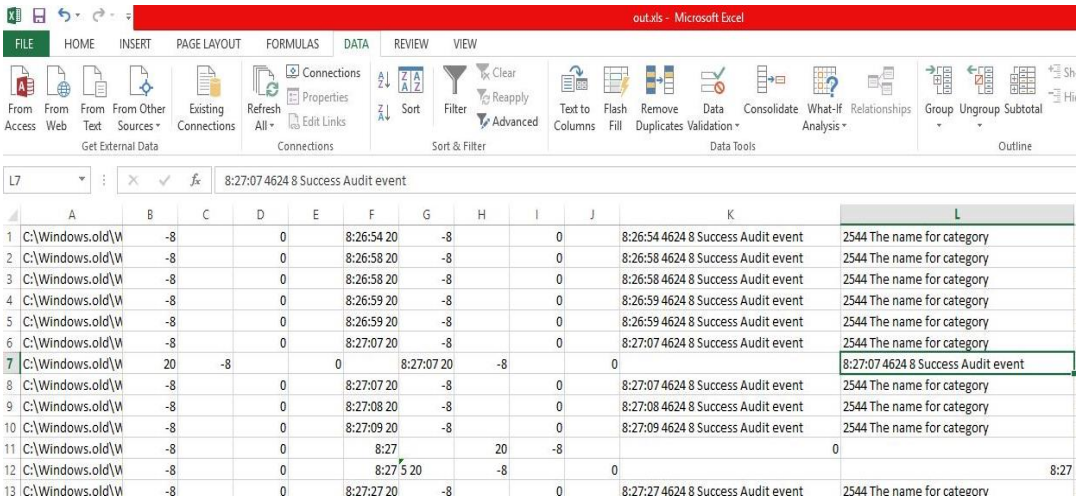
dobivamo informaciju. Nakon toga možemo dodavati našem upitu ostale parametre uz pomoć kojih ćemo definirati što nas točno zanima. Za naš upit o ID događaju 4624 u sučelju naredbenog retka upisujemo sljedeće:

*"C:\Program Files (x86)\Log Parser 2.2\LogParser.exe" -stats:OFF -i:EVT –q:ON "SELECT * FROM 'Security.evtx' WHERE EventID = '4624'" > out.csv*



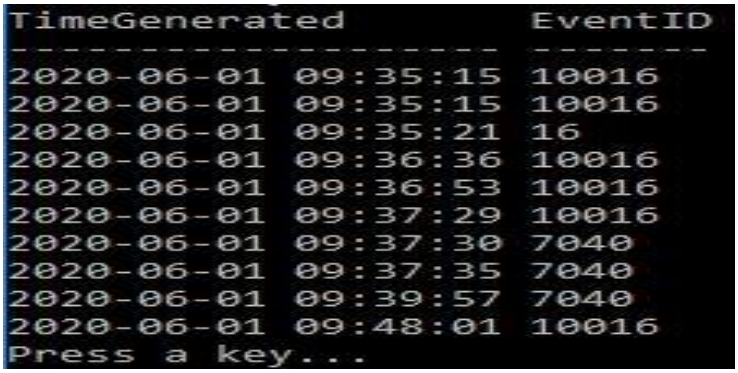
Slika 9. Command Prompt (Log Parser 2.2)

U prvom dijelu naredbe, definirali smo direktorij u kojem se nalazi aplikacija LogParser.exe, zatim smo dodali naredbu stats:OFF kojom ćemo ukloniti nepotrebne statističke podatke kako bi dobili čitljiviji tekst, i:EVT govori kako format datoteke evt, te uz dva obvezna parametra SELECT I FROM dodali smo ID traženog događaj te tekstualni format izlaznog produkta (.csv). Nakon pritiska tipke „Enter“ naš produkt će se automatski spremiti u datoteci dnevnika događaja. Zatim datoteku možemo pokrenuti u programskom alatu „Excel“ gdje ćemo imati uvid u sve uspješne prijave iz koji ćemo moći iščitati: naziv računala, domenu, vrijeme prijave, ime korisnika koji se prijavljuje i ostale slične informacije.



Slika 10. Pregled događaja u Excel-u

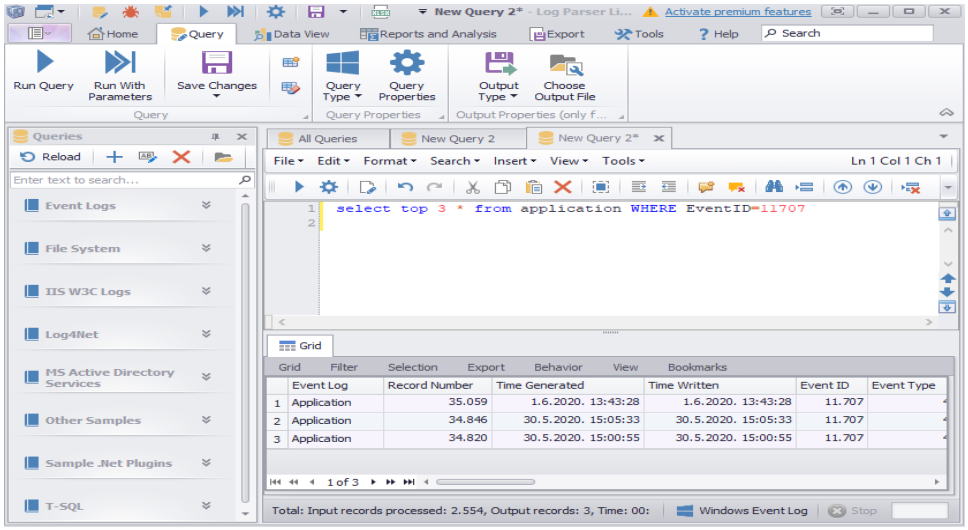
Uz naredbu "C:\Program Files (x86)\Log Parser 2.2\LogParser.exe" -i:EVT - "SELECT TimeGenerated, EventID FROM System" program će prikazati sve događaje prema vremenskom slijedu. Tako na primjer možemo iščitati kojih se 10 zadnjih dnevnika događaja zabilježilo na sustavu. U ovom slučaju to su događaji koje prikazuje slika 11. Iz priložene slike je vidljivo vrijeme i datum zapisa dnevnika te njegov ID.



Slika 11. Zadnjih 10 zapisa dnevnika događaja

- **Log Parser Lizard GUI**

  Log Parser Lizard GUI je programski alat koji je nadogradnja na prethodno spomenuti program *Log Parser*. Pruža korisniku jednostavno i pregledno grafičko sučelje što uvelike pojednostavljuje pregled log datoteka. Program putem SQL servisa za upite učinkovito analizira log datoteke te omogućuje korisniku da kreira Excel ili PDF izvješća [33]. Prednost ovoga programa je što ne morate imati prevelika znanja o programskim jezicima, ali bi bilo poželjno posjedovati osnovna znanja o SQL-u i njegovoj sintaksi kako bi jednostavnije pronašli željeni izvor podataka. Ovaj program bilježi povijest upita i omogućava njihovo spremanje i organiziranje zbirke upita, na taj način nam pojednostavljuje buduća testiranja i analize. Uz pomoć ovog programa vidjeti ćemo koje su posljednje 3 aplikacije instalirane na sustav koristeći „Microsoft Installer“ uslugu. U sučelju naredbenog retka upisat ćemo sljedeće: *select top 3 * from application WHERE EventID=11707*



Slika 12. Log Parser Lizard GUI

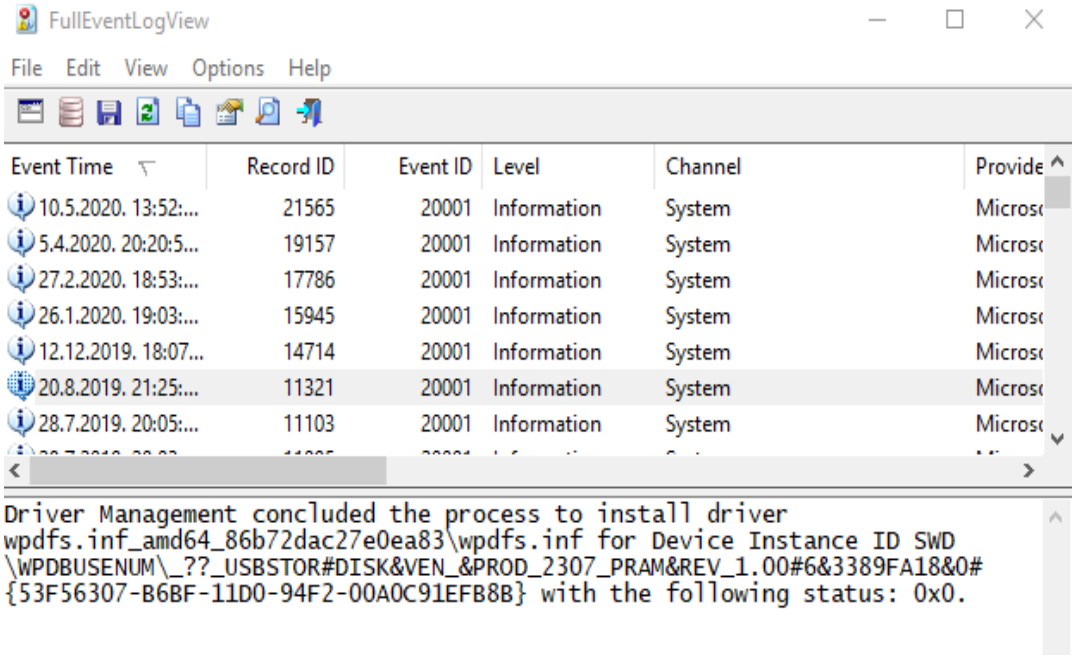
MsiInstaller	Product: Log Parser 2.2 -- Installation completed successfully.|(NULL)|(NULL)|(NULL)|
MsiInstaller	Product: Google Earth Pro -- Installation completed successfully.|(NULL)|(NULL)|(NULL
MsiInstaller	Product: AccessData Registry Viewer -- Installation operation completed successfully.

Slika 13. Popis posljednje 3 instalirane aplikacije

- **FullEventLogView**

FullEventLogView je programski alat koji u tablici prikazuje informacije o svim događajima unutar Windows dnevnika događaja, uključujući njihov detaljan opis [34]. Ovaj program ne zahtijeva instalaciju što nam omogućava da ga nosimo na USB memoriji. Omogućuje pregled lokalnog računala, udaljenog računala koji je spojen putem mreže i svih datoteka u formatu .evtx. Nakon pokretanja programa on automatski učitava sve događaje u posljednjih 7 dana na računalu. Pomoću naprednih postavki možemo mijenjati zadani filtar vremena ili postaviti dodatne filtere uz pomoć kojih ćemo lakše pronaći željene zapise događaja. Tablica događaja prikazuje vrijeme događaja, izvor, ID događaja, razinu informacije, naziv korisnika, naziv računala, opis događaja i slično. Klikom na zaglavlje bilo kojeg od tih redaka razvrstava tablicu prema tom polju što može biti korisno kada želimo organizirati tablicu prema vremenskom slijedu događaja ili za grupiranje događaja prema njihovoj važnosti i slično. Također sve događaje možemo izvesti u txt, csv, xml formatu ili kao HTML izvješće. Uz pomoć ovog programa ćemo napraviti listu svih eksternih uređaja koji su korišteni na računalu. Zapis za ovu vrstu događaja se bilježi svaki put kada je upravljački program eksternog uređaja instaliran ili ažuriran. Ako znamo da je identifikacijski broj događaja koji bilježi instalaciju i ažuriranje uređaja 20001 onda

ćemo uz pomoć naprednih postavki programa postaviti filter za prikazivanjem samo specifičnih ID događaja te ćemo filter vremenskih postavki promijeniti da nam prikazuje događaje od početka korištenja sustava.

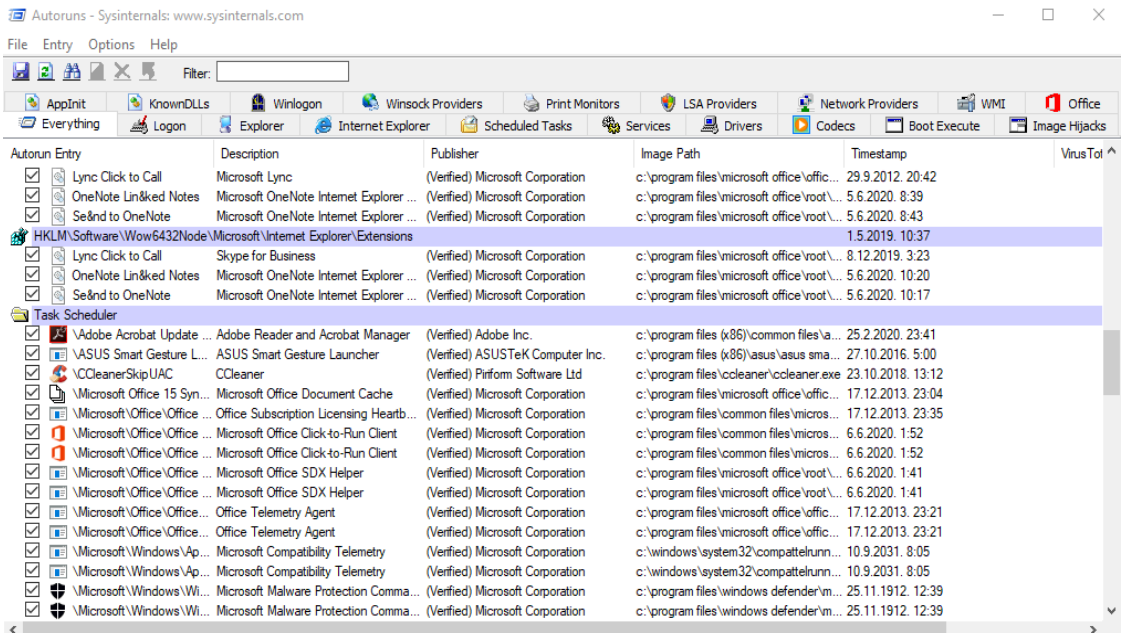


Slika 14. FullEventLogView - Popis eksternih uređaja

Iz priložene slike vidljivo je da imamo ukupno 68 različitih eksternih uređaja čiji opis uključuje podatke o ID-u proizvoda i proizvođača te serijski broj uređaja. Na ovaj način možemo otkriti kada je traženi eksterni uređaj prvi put bio priključen na računalo, te koliko je različitih eksternih uređaja bilo priključivano na računalo.

- **Autoruns**

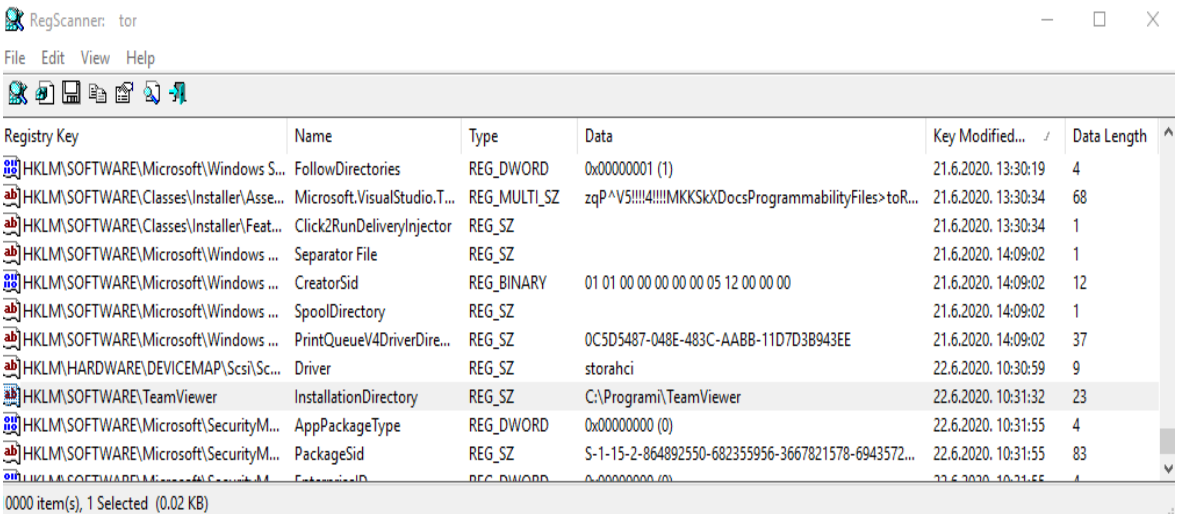
Autoruns je Microsoftov programski alat pomoću kojega možemo pretražiti koje su to usluge i programi postavljeni da se automatski pokreću prilikom pokretanja operacijskog sustava ili prilikom pokretanja pojedinih aplikacija kao što su Internet Explorer, Windows Media Player, Office i slično [35]. Također pomoću ovoga programa možemo otkriti i neki zlonamjerni softver koji se može pokretati bez znanja korisnika. Na taj način mogu se vršiti nedozvoljene radnje bez da sam vlasnik računala zna da se to događa.



Slika 15. Autoruns

- **RegScanner**

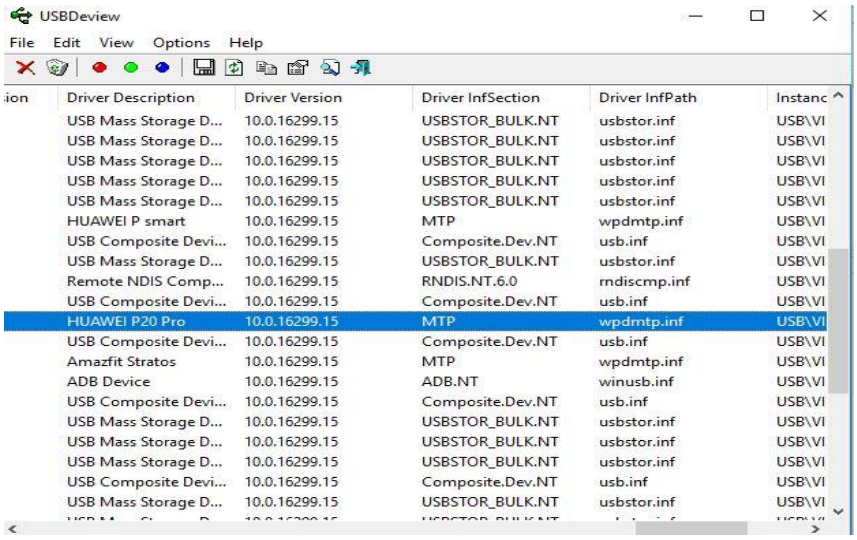
RegScanner je programski alat koji omogućuje pretraživanje Windows Registra prema specifičnim kriterijima koje postavi korisnik. Rezultati pretrage se prikazuju na popisu, a pronađene vrijednosti mogu se izvesti u .reg datoteku. Također se svaka od stavki s popisa može posebno otvoriti unutar Registry Editora [36]. Prikazat ćemo kako pomoću ovoga programa vrlo jednostavno možete stvoriti popis svih programa koji su instalirani na računalu ili su nekad bili instalirani. To nam je jako bitno ako tražimo neki specifični program koji nas može upućivati da je korisnik vršio radnje koje nisu dozvoljene. Moramo uzeti u obzir kako ovakvom pretragom nećemo pronaći programe koji imaju mogućnost pokretanja bez da su instalirani na sustav, nego se mogu direktno pokrenuti sa USB uređaja ili slično. Na priloženoj slici možemo vidjeti popis instaliranih programa, s opisom registarskih ključeva programa, nazivom vrijednosti, tipom vrijednosti, datumom zadnje izmjene i slično.



Slika 16. RegScanner

- **USBDeview**

USBDeview je programski alat koji će izraditi listu svih USB uređaja koji su trenutno spojeni na računalo ili su nekada bili spojeni [37].



Slika 17. USBDeview

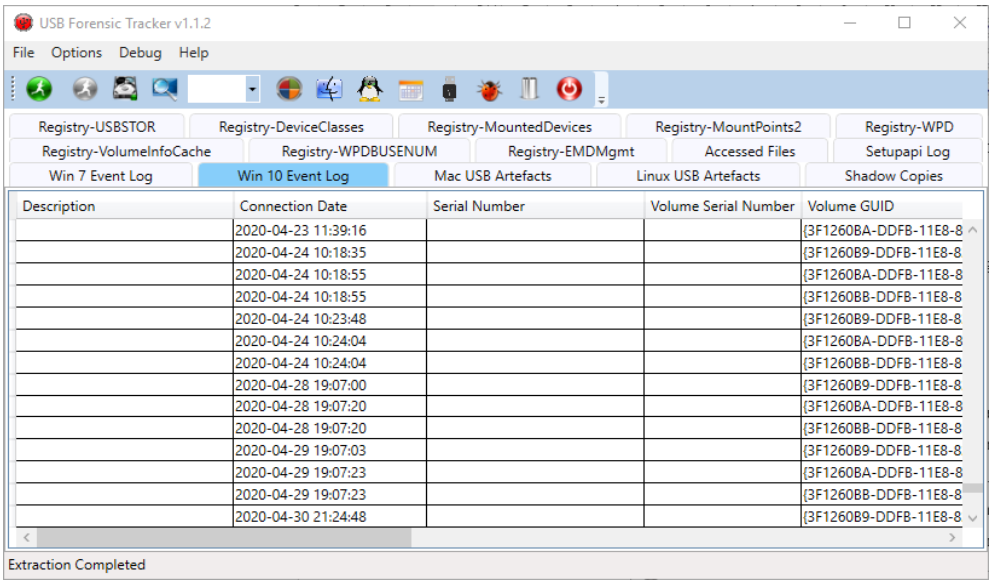
Za svaki USB uređaj prikazuju se proširene informacije: Naziv, opis uređaja, vrsta uređaja, serijski broj datum i vrijeme dodavanja uređaja, VendorID, ProductID i još mnogo toga.

Na slici 18. možemo vidjeti primjer detaljnih informacija na kojem se radi o USB uređaju android mobilnog telefona.

Slika 18. USB Deview – Android mobilni uređaj

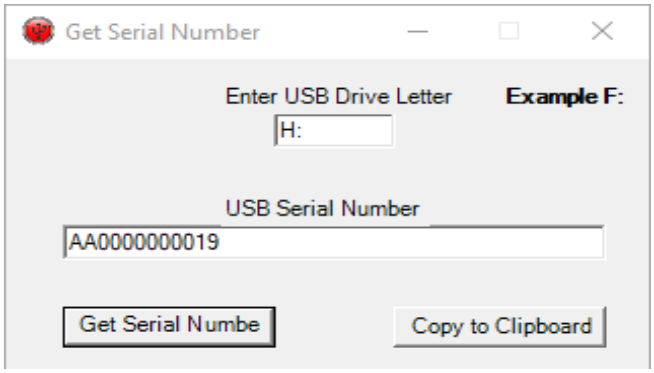
- **USB Forensic Tracker**

USB Forensic Tracker je višenamjenski programski alat uz pomoć kojega možemo dobiti informacije o USB uređajima iz operacijskog sustava uživo, iz forenzičnih slika ili sistemskih datoteka Windowsa [38]. Podatke o uređajima program svrstava unutar tablice ili se mogu izvesti u Excel datoteku gdje se spremaju ovisno o vrsti izvora podataka u zasebne radne listove što čini podatke jako preglednim.



Slika 19. USB Forensic Tracker

Kao izvor informacija ovaj alat koristi više različitih ključeva registra i dnevnika događaja Windows operacijskog sustava. Upravo ta činjenica omogućuje korisniku da uz pomoć jednostavne alatne trake detaljno analizira informacije za svaki pojedini USB uređaj. Na slici 20. je prikazano kako se uz pomoć ovoga alata vrlo jednostavno može utvrditi serijski ključ USB uređaja koji je trenutno u sustavu.



Slika 20. Serijski broj USB uređaja

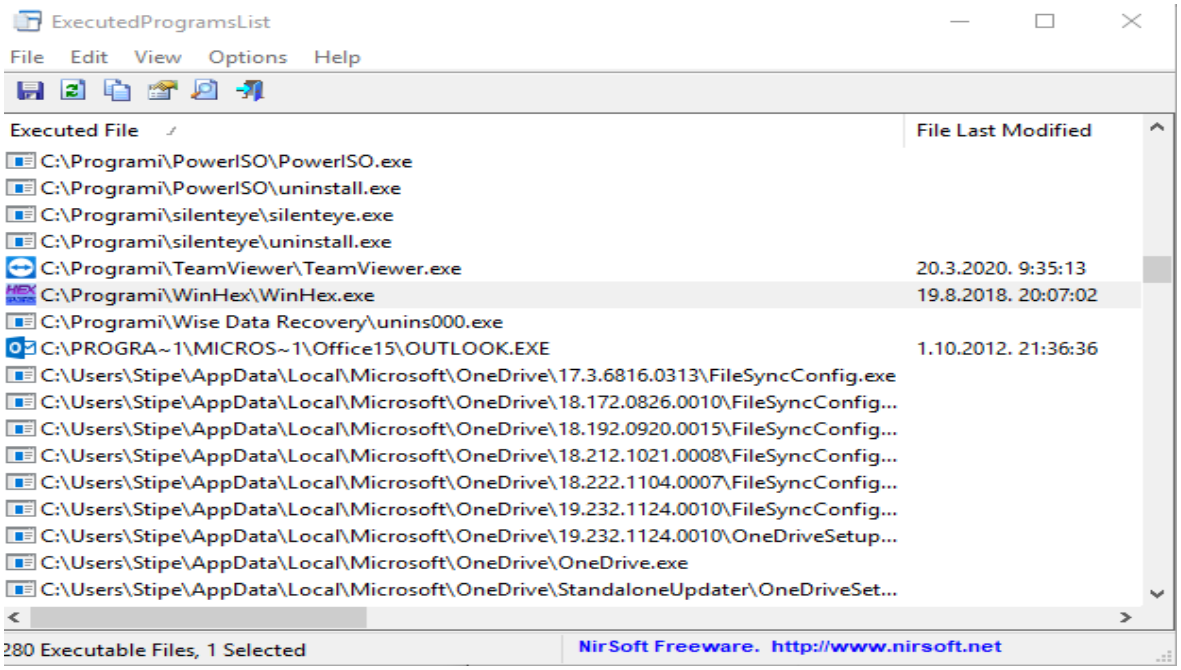
Daljnjom analizom USB uređaja sa serijskim ključem (AA0000000019) možemo utvrditi naziv uređaja, serijski broj i naziv proizvođača, datum i vrijeme prvog ili posljednjeg spajanja uređaja na računalno, koji je korisnik u to vrijeme bio prijavljen na Windows sustavu, možemo pregledavati dnevnike događaja koji su se zapisivali u vrijeme kada je uređaj bio priključen na računalo i slično.

Description	First Connection Date	Serial Number
USB Device	2019-06-26 21:03:27	17100908002490
2307 PRAM USB Device	2019-05-18 18:14:34	6&2fcd1090
hp x5000m USB Device	2019-05-18 18:09:23	AA0000000019

Slika 21. Naziv i datum prvog spajanja USB uređaja

- **ExecutedProgramsList**

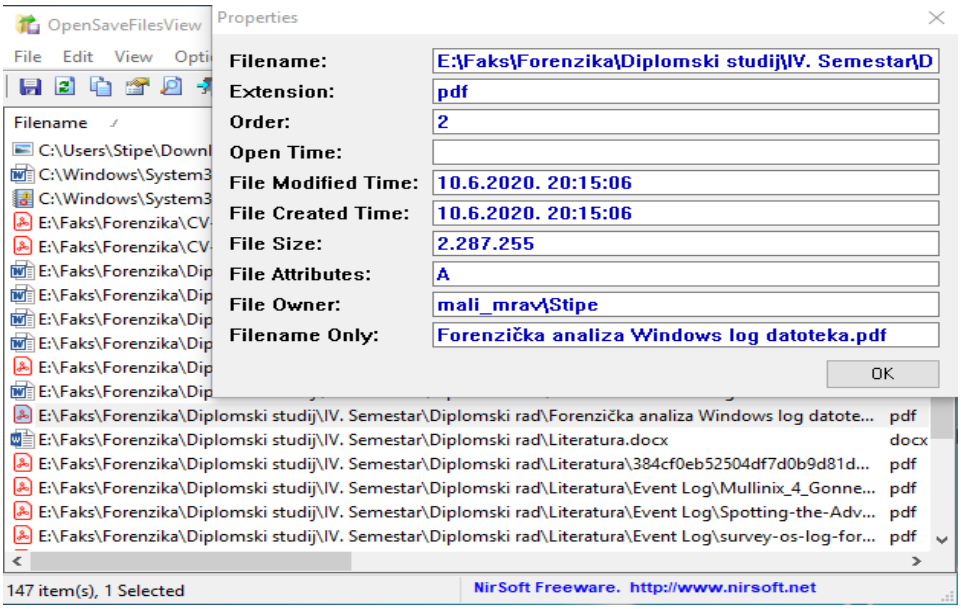
ExecutedProgramsList je programski alat pomoću kojega je moguće kreirati popis programa koji su prethodno otvarani na računalu [39]. Za svaku stavku s popisa prikazuje se .exe datoteka, kreirano i modificirano vrijeme datoteke, naziv i inačica proizvoda i slično. Program omogućava izvoz liste u txt, csv, xml formatu ili kao HTML izvješće.



Slika 22. ExecutedProgramsList

- **OpenSaveFilesView**

Ovaj nam programski alat omogućava izradu liste datoteka koje su prethodno otvarane na računalu uz pomoć standardnog otvori / spremi Windows dijaloškog okvira [40]. Program također omogućava izvoz liste u txt, csv, xml formatu ili kao HTML izvješće. Za svaku datoteku s popisa možemo vidjeti: njen naziv, ekstenziju, red (redoslijed otvaranja datoteka za svako proširenje datoteke), vrijeme otvaranja i slično.



Slika 23. OpenSaveFilesView

6. Pravni aspekti računalne forenzike

Kako smo u samom uvodu ovog rada konstatirali da se računala i ostali elektronički uređaji sve više koriste u svakodnevnom životu i poslovanju, tako nažalost danas svjedočimo sve većem broju računalnih kriminalnih radnji. Upravo iz tog razloga možemo reći kako digitalni trag na elektroničkim medijima može biti važan dio istrage i sudskog postupka. Računala mogu biti uključena u najrazličitije zločine uključujući čak zločine poput ubojstva, terorizma, špijunaže, krivotvorenja, trgovine drogama i slično. Računalo može imati jednu od triju uloga u računalnom zločinu: može biti meta zločina, može biti instrument zločina ili može poslužiti kao spremište dokaza u kojem se pohranjuju vrijedne informacije o zločinu [3]. Računalni kriminal nema svoju definiciju upravo zbog toga što je to jako širok pojam te ga znanstvenici tumače na različite načine. Općenito možemo reći za računalni kriminal da su to sva protupravna, nemoralna i nedopuštena ponašanja koja se poduzimaju uz pomoć računala ili kojima je računalo ili računalni sustav cilj djelovanja [41].

6.1. Zakonski okvir u Republici Hrvatskoj

Hrvatsko zakonodavstvo 1997. godine prvi put uvodi kazneno djelo računalnog kriminaliteta pod nazivom „Oštećenje i uporaba tuđih podataka“ [42]. Sve brže integriranje telekomunikacijske i informatičke tehnologije i njihova međusobna ovisnost dovode i do njihove zlouporabe, pa pojam računalni kriminalitet postaje preuzak i zamjenjuje ga širi pojam kibernetički kriminalitet. Tako Vijeće Europe 2001. godine donosi međunarodni ugovor pod nazivom Konvencija o kibernetičkom kriminalu [43]. Konvencija donosi zakonske i druge mjere kojima bi se omogućio kazneni progon počinitelja kaznenih djela protiv tajnosti, integriteta i dostupnosti računalnih sustava i podataka, kaznenih djela u svezi s računalom, kaznenih djela u svezi sa sadržajem, kao i kaznenih djela u vezi s povredama autorskih i drugih srodnih prava te kažnjavanje pokušaja, poticanja i pomaganja tih djela [44]. Rezultat ove konvencije čija potpisnica je bila i Republika Hrvatska je novi Zakon o izmjenama i dopunama Kaznenog zakona koji stupa na snagu 2004. godine. Ovim izmjenama uveden je niz novih članaka pod naslovom „Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava [45]“. Nove velike izmjene dogodile su se 2011. godine kada je donesen novi Kazneni zakon koji 2013. godine stupa na snagu. Tim zakonom kaznena djela protiv računalnih sustava, programa i podatka definirana su unutar Glave XXV. „Kaznena djela protiv računalnih sustava, programa i podataka“. Ova sasvim nova glava kaznenog zakona sastoji se od osam članaka: članak 266. „Neovlašteni

pristup“, članak 267. „Ometanje rada računalnog sustava“, članak 268. „Oštećenje računalnih podataka“, članak 269. „Neovlašteno presretanje računalnih podataka“, članak 270. „Računalno krivotvorenje“, članak 271. „Računalna prijevara“, članak 272. „Zlouporaba naprava“, članak 273 „Teška kaznena djela protiv računalnih sustava, programa i podataka“ [46]. Posljednja izmjena Kaznenog zakona stupila je na snagu 01.01.2020. godine, međutim tim zakonom nije se dogodila nikakva značajna izmjena što se tiče računalnog kriminaliteta.

Osim Kaznenog zakona koji predstavlja glavni instrument u borbi protiv računalnog kriminaliteta, Republika Hrvatska je donijela još niz drugih zakona u cilju prevencije i suzbijanja računalnog kriminaliteta te zaštitu privatnosti građana i računalnih sustava općenito. Neki od važnijih zakona su:

- **Zakon o informacijskoj sigurnosti** – „Ovim se Zakonom utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti [47]“.
- **Zakon o tajnosti podataka –** „Ovim se Zakonom utvrđuju pojam klasificiranih i neklasificiranih podataka, stupnjevi tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima, njihova zaštita i nadzor nad provedbom ovoga Zakona [48]“.
- **Zakon o provedbi Opće uredbe o zaštiti podataka –** „Ovim Zakonom osigurava se provedba Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka [49]“.
- **Zakon o elektroničkim komunikacijama –** Ovim Zakonom se uređuje područje elektroničkih komunikacija, gospodarenje komunikacijskom infrastrukturom te određuje tijelo nadležno za nadzor i kontrolu komunikacija i davatelja usluga [50].

Uza sve zakonske okvire veoma je bitno spomenuti Nacionalnu strategiju kibernetičke sigurnosti [51] i Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti [52] koji su doneseni 2015. godine. Strategijom kibernetičke sigurnosti propisuje se 8 ciljeva koje treba postići, koji su usmjereni na borbu protiv kibernetičkih prijetnji te sigurnost kibernetičkog prostora. Dok se Akcijskim planom

nastoji definirati mjere koje je potrebno poduzeti za ostvarenje tih ciljeva. Rezultat ovih dvaju dokumenata je osnivanje Nacionalnog vijeća za kibernetičku sigurnost i Operativno – tehnička koordinacija za kibernetičku sigurnost. Razlog povećanja svijesti i suradnje u borbi protiv kibernetičkog kriminala je svakako činjenica da se broj kaznenih dijela povezanih sa takvom vrstom kriminalnih radnji konstantno povećava.

6.2. Kaznena djela protiv računalnog sustava programa i podataka

Već smo ranije spomenuli kako se Kaznenim zakonom Republike Hrvatske definiraju pojmovi vezani za računalni kriminalitet i propisuju kaznena djela unutar glave dvadesetpete.

- **Članak 266. „Neovlašteni pristup“ –** Ovaj članak propisuje kaznu za počinitelja koji pristupa računalnim podacima i sustavu koji su zakonom zabranjeni ili nema odobrenje vlasnika ili osobe koja je ovlaštena dati odobrenje za pristup podacima. *„Tko neovlašteno pristupi računalnom sustavu ili računalnim podacima kaznit će se kaznom zatvora do jedne godine. Tko kazneno djelo iz ovoga članka počini u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, tijela jedinica lokalne ili područne (regionalne) samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa, kaznit će se kaznom zatvora do tri godine*[53]“.

- **članak 267. „Ometanje rada računalnog sustava“ –** „*Tko onemogući ili oteža rad ili korištenje računalnog sustava, računalnih podataka ili programa ili računalnu komunikaciju, kaznit će se kaznom zatvora do tri godine* [53]“.

- **članak 268. „Oštećenje računalnih *podataka*“ –** „*Tko neovlašteno u cijelosti ili djelomično ošteti, izmijeni, izbriše, uništi, učini neuporabljivim ili nedostupnim ili prikaže nedostupnim tuđe računalne podatke ili programe, kaznit će se kaznom zatvora do tri godine* [53]“.

- **članak 269. „Neovlašteno presretanje računalnih podataka“ –** „*Tko neovlašteno presretne ili snimi nejavni prijenos računalnih podataka, uključujući i elektromagnetsku emisiju računalnog sustava, ili drugome učini dostupnim tako pribavljene podatke, kaznit će se kaznom zatvora do tri godine* [53]“.

- **članak 270. „Računalno krivotvorenje“ –** „*Tko neovlašteno izradi, unese, izmijeni, izbriše ili učini neuporabljivim ili nedostupnim računalne podatke koji imaju vrijednost za pravne odnose, u namjeri da se oni uporabe kao vjerodostojni, ili tko*

takve podatke uporabi ili nabavi radi uporabe, kaznit će se kaznom zatvora do tri godine [53]“.

- **članak 271. „Računalna prijevara“ –** „*Tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad računalnog sustava i na taj način prouzroči štetu drugome, kaznit će se kaznom zatvora od šest mjeseci do pet godina. Ako je kaznenim djelom iz ovoga članka pribavljena znatna imovinska korist ili prouzročena znatna šteta, počinitelj će se kazniti kaznom zatvora od jedne do osam godina* [53]“.
- **članak 272. „Zlouporaba naprava“ –** „*Tko izradi, nabavi, proda, posjeduje ili čini drugome dostupne uređaje ili računalne programe ili računalne podatke stvorene ili prilagođene za počinjenje kaznenih djela iz članka 266., članka 267., članka 268., članka 269., članka 270. i članka 271. ovoga Zakona s ciljem da ih se uporabi za počinjenje nekog od tih djela, kaznit će se kaznom zatvora do tri godine. Tko izradi, nabavi, proda, posjeduje ili čini drugome dostupne računalne lozinke, pristupne šifre ili druge podatke kojima se može pristupiti računalnom sustavu s ciljem da ih se uporabi za počinjenje kaznenih djela iz članka 266., članka 267., članka 268., članka 269., članka 270. i članka 271. ovoga Zakona, kaznit će se kaznom zatvora do jedne godine* [53]“.
- **članak 273 „Teška kaznena djela protiv računalnih sustava, programa i podataka“ –** „*Tko kazneno djelo iz članka 267. do članka 270. ovoga Zakona počini u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, tijela jedinica lokalne ili područne (regionalne) samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa, kaznit će se kaznom zatvora od šest mjeseci do pet godina. Tko kazneno djelo iz članka 267. do članka 269. ovoga Zakona počini sredstvom namijenjenim za izvršenje napada na veći broj računalnih sustava ili kojim je prouzročena znatna šteta, kaznit će se kaznom zatvora od jedne do osam godina* [53]“.

U Republici Hrvatskoj prema službenim statističkim podacima Ministarstva unutarnjih poslova za 2018. godinu ukupan broj kaznenih djela kibernetičkog kriminaliteta iznosi 1564 dok je taj broj za 2017. godinu 1410, što predstavlja porast za oko 11% [54].

Tablica 2**.** Kaznena djela kibernetičkog kriminaliteta u RH (2017. – 2018.) [54]

Kaznena djela	Prijavljena			Razriješena			Naknadno otkrivena		
	Broj djela		%	Broj djela		%	Broj djela		%
	2017.	2018.		2017.	2018.		2017.	2018.	
Neovlašteni pristup	7	16	129	5	13	160	3	12	300
Ometanje rada računalnog sustava	11	1	-90,9	10	1	-90	9	/	/
Oštećenje računalnih podataka	7	/	/	7	/	/	1	/	/
Neovlašteno presretanje računalnih podataka	1	/	/	0	/	/	/	/	/
Računalno krivotvorenje	37	32	-13,5	35	39	11,4	35	37	5,7
Računalna prijevara	1114	1310	17,6	915	1162	27	901	1144	27
Zlouporaba naprava	9	17	88,9	7	17	143	5	16	220
Ukupno	1186	1376	16	979	1232	25,8	954	1209	26,7

Uzevši u obzir podatke Ministarstva unutarnjih poslova RH za 2017. i 2018. godinu daleko najveći broj kaznenih djela računalnog kriminaliteta odnosi se na računalnu prijevaru. Nakon računalne prijevare po učestalosti, slijede računalno krivotvorenje i zlouporaba naprava. Uzevši u obzir ove brojke koje su u stalnom porastu dolazimo do zaključka koliko je borba protiv suzbijanja i prevencije kibernetičkog kriminaliteta bitna za društvo ali i očuvanje osnovnog ljudskog prava na privatnost kako izvan tako i unutar računalnog i kibernetičkog prostora.

7. Zaključak

Kao što smo već u samom početku ovog rada zaključili kako svjedočimo ubrzanoj tehnološkoj globalizaciji koja sve više ima utjecaja na svaki aspekt ljudskog života. Uz bezbroj pozitivnih stvari koje sa sobom nosi tehnologija je donijela i jednu negativnu stranu, a to je računalni kriminal. Zbog širokog spektra mogućnosti koje tehnologija pruža i činjenice da kriminalci učestalo razvijaju nove načine njene zloupotrebe, jako je teško donijeti učinkovit mehanizam u prevenciji i suzbijanju takve vrste kriminala. S obzirom na popularnost Windows operacijskog sustava na računalnom tržištu, s aspekta digitalnog forenzičara važno je razumjeti važnost log datoteka. Njihovo filtriranje i analiza mogu biti veoma značajni i učinkoviti za prikupljanje informacija o događajima koji su se dogodili na računalu ili mreži.

Razumijevanje osnova Dnevnika događaja i Registra te njihovog načina funkcioniranja s forenzičkog stajališta koji su prethodno opisani u ovom radu temelji su koji će pomoći istražitelju da se jednostavnije i učinkovitije snalazi u mnoštvu informacija koje sadrže ove datoteke. Zbog brojnosti i kompleksnosti log datoteka unutar Windows operacijskog sustava nije moguće obuhvatiti sve detalje na koje bi forenzičar trebao obratiti pozornost. Iz tog razloga u ovom radu su prikazane neke tehnike pronalaska podataka koji su „skriveni“ unutar registra i dnevnika događaja. Ne postoji unaprijed propisane metode prilikom analize ovih datoteka nego se sva saznanja o ovom sustavu temelje na prethodnim istraživanjima i otkrivanjem forenzičarima bitnih datoteka. Zbog toga je važno proučavati i otkrivati nove informacije unutar log datoteka kako bi postupak forenzičke istrage Windows-a trajao manje vremena i bio što učinkovitiji.

Svakako ne smijemo zanemariti činjenicu da kriminalci sve više koriste sofisticiranije i složenije tehnike kako bi izbjegli forenzičke metode i alate. Te činjenicu da Microsoft tretira registar i dnevnik događaja kao internu uslugu koja sadrži postavke sustava i da kao takvi često ne pružaju sveobuhvatne i cjelovite informacije. Ove dvije činjenice svakako otežavaju pretragu ovakve vrste zapisa, međutim ako korisnik nije ručno onemogućio ili izbrisao uslugu evidentiranja događaja, forenzički postupak opisan u ovom radu može se primijeniti na većinu forenzičkih istraga koje uključuju Windows operacijski sustav.

8. Literatura

[1] Solomon, M., Barrett, D., & Broom, N., Computer Forensics JumpStart, Indianapolis, Indiana, SAD, Sybex, 2005.

[2] Casey E., Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computer and Internet, Baltimore, Maryland, SAD, Academic Press, 2011.

[3] Vacca, J. R., Computer Forensic, Computer crime scene investigation, Second Edition, Boston, Massachusetts, SAD, Charles River Media,2010.

[4] Microsoft by the Numbers, Microsoft, https://news.microsoft.com/bythenumbers/en/windowsdevices, dostupno na 22.03.2020.

[5] Carvey H., Windows Forensic Analysis DVD Toolkit 2E, Burlington, SAD, Syngress , 2009.

[6] Event Logging, Microsoft https://docs.microsoft.com/hr-hr/windows/win32/eventlog dostupno na 22.03.2020

[7] Windows Event Log Analysis, Forward Defense, Steve Anson https://www.forwarddefense.com/pdfs/Event_Log_Analyst_Reference.pdf, dostupno na 24.03.2020.

[8] Event logging, Microsoft, https://docs.microsoft.com/hr-hr/windows/win32/eventlog/event-logging , dostupno na 24.03.2020.

[9] Nacionalni CERT, Osnove analize logova pri računalnim incidentima, dokument NCERT-PUBDOC-2014-02-341, https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2014-04-341.pdf, dostupno na 06.04.2020.

[10] Process mining of events log from Windows, Radim Dolak, Milena Janakova, Josef Botlik, http://ceur-ws.org/Vol-2270/short5.pdf , dostupno na 06.04.2020.

[11] Windows Event Forensic Process, Quang Do, Ben Martini, Jonathan Looi, Yu Wang, Kim-Kwang Choo https://hal.inria.fr/hal-01393763/document , dostupno na 06.04.2020.

[12] Centar Informacijske sigurnosti, Sigurno rukovanje dnevničkim podacima, dokument CIS-DOC-2012-08-058, https://www.cis.hr/files/dokumenti/CIS-DOC-2012-08-058.pdf, dostupno na 06.04.2020.

[13] Structure of the Registry, Microsoft https://docs.microsoft.com/hr-hr/windows/win32/sysinfo/structure-of-the-registry , dostupno na 16.04.2020

[14] Windows Registry Forensics: Investigating the Registry for Evidence, Joseph Moronwi, https://netseedblog.com/security/windows-registry-forensics-investigating-the-registry-for-evidence/ , dostupno na 16.04.2020

[15] Russinovich, M., Inside the Regisry, https://docs.microsoft.com/en-us/previous-versions//cc750583(v=technet.10)?redirectedfrom=MSDN, dostupno na 16.04.2020.

[16] Honeycutt, J., Microsoft Windows XP Registry Guide, Redmond, Washington, SAD Microsoft Press, 2003.

[17] Registry Hives, Microsoft, https://docs.microsoft.com/hr-hr/windows/win32/sysinfo/registry-hives, dostupno na 17.04.2020.

[18] HKEY_LOCAL_MACHINE, Microsoft, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc784983(v=ws.10)?redirectedfrom=MSDN, dostupno na 17.04.2020.

[19] Honeycutt, J., Microsoft Windows Registry Guide, Second Edition, Paperback Bargain Price, Redmond, Washington, SAD, Microsoft Press, 2005.

[20] HKEY_CURRENT_USER, Microsoft, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc779816(v=ws.10) , dostupno na 17.04.2020.

[21] HKEY_CURRENT_CONFIG, Microsoft, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc776168(v=ws.10), dostupno na 17.04.2020.

[22] HKEY_CLASSES_ROOT, Microsoft, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc739822(v=ws.10), dostupno na 17.04.2020.

[23] Barbara, J., J., Windows 7 Registry Forensics, https://www.itdaan.com/tw/e1190165ae2025501d9c802ad0bc53ab, dostupno na 22.04.2020.

[24] Rouse, M., BIOS, https://whatis.techtarget.com/definition/BIOS-basic-input-output-system, dostupno na 22.04.2020.

[25] Forensic Analysis of the Windows Registry, Forensic Focus, https://articles.forensicfocus.com/2011/07/10/forensic-analysis-of-the-windows-registry/ dostupno na 09.05.2020.

[26] MRU Source List, Microsoft, https://docs.microsoft.com/en-us/windows/win32/setupapi/mru-source-list, dostupno na 09.05.2020.

[27] The Windows Registry as a forensic resource, Carvey, H., Digital Investigation, https://www.dfir.training/windows/mru/179-the-windows-registry-as-a-forensic-resource/file, dostupno na 09.05.2020.

[28] Tanushree, R., Aruna, J., Windows Registry Forensics: An Imperative Stepin Tracking Data Theft via USB Devices, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.4521&rep=rep1&type=pdf, dostupno na 18.05.2020.

[29] Moronwi, J., USB Anti-forensics https://netseedblog.com/security/usb-anti-forensics/?fbclid=IwAR0nftKRKj6fYp5452cjPrKgwH1g3xz67t7ylWNI085JmmiCC9ILNu6f_3I, dostupno na 18.05.2020.

[30] Windows Registry Analysis 101, Forensic Focus https://articles.forensicfocus.com/2019/04/05/windows-registry-analysis-101/, dostupno na 18.05.2020.

[31] Casey, E., Computer Crime Investigation Forensic Tools and Technology, London UK, Elsevier Academic Press, 2004.

[32] Giuseppini, G., Burnett, M., Microsoft Log Parser toolkit, Rockland, Maine, SAD, Syngress, 2004.

[33] Log Parser Lizard, http://www.lizard-labs.com/log_parser_lizard.aspx, dostupno na 29.05.2020.

[34] FullEventLogView, http://www.nirsoft.net/utils/full_event_log_view.html, dostupno na 29.05.2020.

[35] Autoruns for Windows, https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns, dostupno na 30.05.2020.

[36] RegScanner, https://www.nirsoft.net/utils/regscanner.html, dostupno na 30.05.2020.

[37] USBDeview, https://www.nirsoft.net/utils/usb_devices_view.html, dostupno na 30.05.2020.

[38] USB Forensic Tracker, http://www.orionforensics.com/forensics-tools/usb-forensic-tracker/, dostupno na 30.05.2020.

[39] ExecutedProgramsList, https://www.nirsoft.net/utils/executed_programs_list.html, dostupno na 30.05.2020.

[40] OpenSaveFilesView, http://www.nirsoft.net/utils/open_save_files_view.html dostupno na 30.05.2020.

[41] V. Babić, Kompjuterski kriminal: metodologija kriminalističkih istraživanja, razjašnjavanja i suzbijanja kompjuterskog kriminala, Sarajevo, BiH: RABIC Sarajevo, 2009.

[42] Kazneni zakon, Narodne novine (110/1997-1668), https://narodne-novine.nn.hr/clanci/sluzbeni/1997_10_110_1668.html dostupno na 03.06.2020.

[43] Zakon o potvrđivanju konvencije o kibernetičkom kriminalu, Narodne novine (9/2002) http://cnzd.org/uploads/document/attachment/15/KONVENCIJA_O_KIBERNETI_KOM_KRIMINALU.pdf, dostupno na 03.06.2020.

[44] Kokot, I., Kaznenopravna zaštita računalnih sustava, programa i podataka, Zagrebačka pravna revija, 3 (3), 303-330., 2014.

[45] Zakon o izmjenama i dopunama Kaznenog zakona, Narodne novine (105/2004-202) https://narodne-novine.nn.hr/clanci/sluzbeni/2004_07_105_2026.html, dostupno na 03.06.2020.

[46] Kazneni zakon, Narodne novine (125/2011-2498), https://narodne-novine.nn.hr/clanci/sluzbeni/2011_11_125_2498.html, dostupno na 03.06.2020.

[47] Zakon o informacijskoj sigurnosti, Narodne novine (79/07), https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, dostupno na 03.06.2020.

[48] Zakon o tajnosti podataka, Narodne novine (77/07, 86/12), https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka, dostupno na 03.06.2020.

[49] Zakon o provedbi Opće uredbe o zaštiti podataka, Narodne novine(42/18), https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html, dostupno na 03.06.2020.

[50] Zakon o elektroničkim komunikacijama, Narodne novine (73/08, 90/11, 133/12, 80/13, 71/14, 72/17), https://www.zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama, dostupno na 03.06.2020.

[51] Nacionalna strategija kibernetičke sigurnosti, Narodne novine (NN108/2015), https://www.uvns.hr/UserDocsImages/dokumenti/Akcijski%20plan%20za%20provedbu%20Nacionalne%20strategije%20kiberneticke%20sigurnosti%20(2015.).pdf, dostupno na 03.06.2020.

[52] Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti, Narodne novine (NN108/2015), https://www.uvns.hr/UserDocsImages/dokumenti/Akcijski%20plan%20za%20provedbu%20Nacionalne%20strategije%20kiberneticke%20sigurnosti%20(2015.).pdf, dostupno na 03.06.2020.

[53] Kazneni zakon, Narodne novine (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19), https://www.zakon.hr/z/98/Kazneni-zakon, dostupno na 03.06.2020.

[54] Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018. godini, MUP, dokument KLASA: 953-01/19-01/1, URBROJ: 511-01-142-19-1 https://mup.gov.hr/UserDocsImages/statistika/2019/Pregled%20sigurnosnih%20pokazatelja%20u%202018%20godini/Statisticki%20pregled%202018_web.pdf#page=81&zoom=100,92,96, dostupno na 04.06.2020.

Sažetak

Forenzična analiza Windows log datoteka

Windows log datoteke sadrže mnoštvo informacija koje mogu poslužiti kao potencijalni dokaz ili kao pomoć forenzičarima u nekim drugim aspektima istrage. Cilj ovog rada je prikazati sadržaj Windows log datoteka te načine kako učinkovito prikupiti i filtrirati informacije o događajima koji su se dogodili unutar računala ili mreže. Kako ove datoteke sadrže mnoštvo informacija, navedeni su neki bitniji zapisi koje bi forenzični istražitelj prilikom istrage trebao analizirati. Analiza datoteka dnevnika događaja i registra Windows operacijskog sustava napravljena je uz pomoć nekomercijalnih forenzičnih programskih alata. U radu su prikazani pravni aspekti Republike Hrvatske koji reguliraju računalni kriminalitet i sigurnost informacija općenito. Razumijevanje i poznavanje pravnih normi računalnog kriminaliteta te osnova funkcioniranja dnevnika događaja i registra koji su opisani u ovom radu temelji su koji će pomoći forenzičnom istražitelju da jednostavnije i učinkovitije analizira i obradi ključne informacije koje sadrže Windows log datoteke.

Ključne riječi: Windows, dnevnik događaja, registar, analiza, pravni aspekti

Summary

Forensic analysis of Windows log files

Windows log files contain plenty of information that can be used as potential evidence or assist forensics in some other aspects of an investigation. The main aim of this paper is to show the contents of Windows log files and ways to effectively collect information about events that have occurred within a computer or network. As these files contain plenty of information, some important records are listed that the forensic investigator should analyze during the investigation. Analysis of Windows Registry and event log files was performed using non-commercial forensic software tools. The paper presents the main legal norms of the Republic of Croatia that regulate computer crimes and information security. Understanding the legal norms of computer crime and knowing the basics of Windows Registry and event log files described in this paper will help the forensic investigator to more easily and efficiently analyze key information contained in Windows log files.

Keywords: Windows, Event log, Registry, analysis, legal norms

Životopis

OSOBNE INFORMACIJE

Maras Stipe

Podosoje 36, 21236 Vrlika (Hrvatska)

095 876 3781

smaras100@gmail.com

OBRAZOVANJE I OSPOSOBLJAVANJE

2013–2016 **Prvostupnik Inženjer građevinarstva**

Fakultet Građevinarstva Arhitekture i Geodezije, Split (Hrvatska)

OSOBNE VJEŠTINE

Materinski jezik Hrvatski

Strani jezici

	RAZUMIJEVANJE		GOVOR		PISANJE
	Slušanje	Čitanje	Govorna interakcija	Govorna produkcija	
Engleski	B2	B2	B2	B2	B2
Njemački	A2	A2	A2	A2	A2

Stupnjevi: A1 i A2: Početnik - B1 i B2: Samostalni korisnik - C1 i C2: Iskusni korisnik

Komunikacijske vještine dobre komunikacijske vještine stečene dosadašnjim iskustvom

Organizacijske / rukoviteljske vještine Iskustvo rukovođenja i zapovijedanja

Poslovne vještine samo- motivacija

sposobnost prilagođavanja promjenama
sposobnost rada u timu

izvršavanje zadaća unutar rokova i ograničenja

Digitalne vještine

SAMOPROCJENA			
Obrada informacija	Komunikacija	Stvaranje sadržaja	Sigurnost
Samostalni korisnik	Samostalni korisnik	Samostalni korisnik	Samostalni korisnik

Vozačka dozvola A, B

Popis slika

Popis tablica

SVEUČILIŠTE U SPLITU

Sveučilišni odjel za forenzične znanosti

Izjava o akademskoj čestitosti

Ja, Stipe Maras, izjavljujem da je moj diplomski rad (zaokružite odgovarajuće) pod naslovom "Forenzična analiza Windows log datoteka" rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ičija autorska prava. Izjavljujem da nijedan dio ovoga rada nije iskorišten u ijednom drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi. Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Split, 10. srpnja 2020. godine

Potpis studenta/studentice: _____