Forenzika radne memorije

Krapljan, Bruno

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Bruno Krapljan

Forenzika radne memorije

ZAVRŠNI RAD

Sisak, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Bruno Krapljan

Matični broj: 0016132471

Studij: Primjena informacijske tehnologije u poslovanju

Forenzika radne memorije

ZAVRŠNI RAD

Mentor:

Doc. dr. sc. Igor Tomičić

Sisak, svibanj 2021.

Bruno Krapljan

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Izabranom temom završnog rada pod imenom forenzika radne memorije uvodno će u radu biti objašnjeno što je radna memorija, kako je snimiti kod korisnika na računalu, zašto je ključna u digitalnoj forenzici, znanost o procesima i registrima, te promatranje pokrenutih procesa na računalu. Nakon objašnjene opće metodologije, radne memorije, procesa i forenzičke analize iste, slijedi simulacija zaraze računala ransomware virusom pod imenom „Jigsaw“ putem USB stick-a na virtualnom stroju koji pokreće Jigsaw program nakon određenog vremena gdje slijedi kriptiranje datoteka žrtvinog računala. Radi se o simulaciji profesor – studenti gdje četiri studenta priključuje USB stick u profesorovo računalo kako bi izlagali svoje prezetacije, te jedan student ima namjeru zaraziti profesorovo računalo zlonamjernim programom. Slijedi prepoznavanje malicionzog koda kroz snimljenu sliku radne memorije zaraženog računala, te vrijeme kada se priključio USB stick koji je izvor malicioznog programa i ujedno forenzičkom analizom utvrditi vlasnika USB stick-a. Kao zadnji korak slijedi oporavak računala gdje se poduzimaju sve potrebite metode izolacije i ubijanja zlonamjernog programa, te zaključno razmatranje kako najbolje zaštiti sebe i računalo od sličnih napada.

Ključne riječi: RAM; procesi; ransomware; forenzika; USB; oporavak; virusi;

Sadržaj

1. Uvod

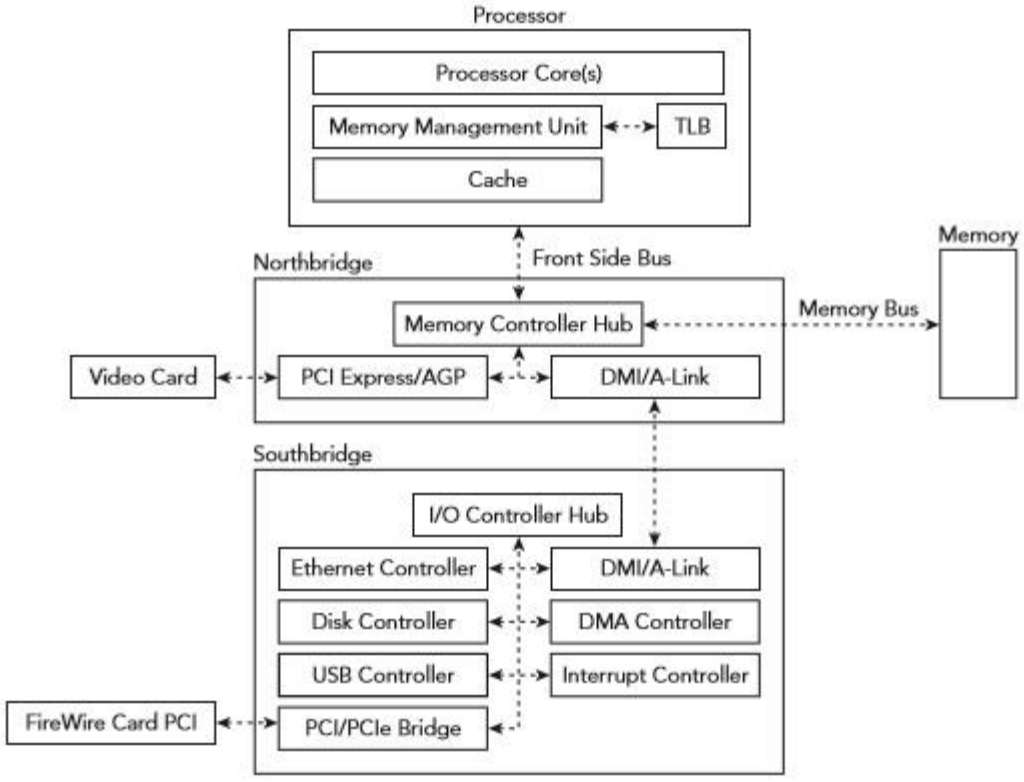
Razvojem interneta kao i kod razvoja bilo čega, javlja se potreba za širokim spektrom znanja manipuliranja određenih aspekata i držanja stvari pod kontrolom jer ljudi po prirodi ako znaju nešto jako dobro, to će iskoristiti, bilo u dobru ili lošu svrhu. Računala se razvijaju, mrežne infrastrukture, programski jezici, uvode se nova zanimanja, podučavaju se ljudi, kako u školama, tako i samostalno. Kada osoba nauči nešto samostalno, to je vrlo pohvalno, lijepo, zapanjujuće, te dokazuje inteligenciju i sposobnost čovjeka, no da li svaki čovjek posjeduje moral kada u pitanju dolazi znanje i moć, što kada osoba nauči nešto što pogađa privatnost pojedinca, krađu identiteta, štetu imovine ili kompletni zastoj funkcioniranja ogromne korporacije, bolnice ili državne institucije, što ako je naš sustav već pogođen. Tada na red dolazi digitalna forenzika koja se bavi prikupljanjem artefakata, digitalnih dokaza kojim se dolazi do glavnog krivca promatranog slučaja. Digitalna forenzika, koja je vrlo širok pojam biti će spomenuta samo ovdje, u uvodu, a ja ću se kao glavnom temom ovoga rada baviti forenzikom radne memorije u Volatility alatu, koja isključivo prikuplja dokaze iz radne memorije. Trenutna slika radne memorije se može snimiti kod bilo kojeg računala, te uzeti kao uzorak za forenzičku analizu, u ovom slučaju u Volatility alatu iz koje se može saznati puno bitnih artefakata za daljnju istragu u cijelom sklopu digitalne forenzike.

2. Arhitektura PC-a

U ovom poglavlju posebni fokus će biti stavljen na opću hardversku arhitekturu osobnog računala (PC). Važno je napomenuti da se terminologija s vremenom mijenja, a detalji implementacije neprestano se mijenjaju kako bi poboljšali cijene i performanse. Iako se specifične tehnologije mogu promijeniti, primarne funkcije koje ove komponente obavljaju ostaju iste. [1, p. 4.]

2.1. Organizacija arhitekture

Računalo je sastavljeno od štampanih pločica koje međusobno povezuju različite komponente i osiguravaju priključke za periferne uređaje. Glavna ploča unutar ove vrste sustava, matična ploča, pruža veze koje omogućuju komunikaciju komponenti sustava. Ti se komunikacijski kanali obično nazivaju sabirnice (eng. *bus*). Slika 1 prikazuje kako su obično organizirane različite komponente. [1, p. 4.]



Slika 1. Arhitektura računala [1, p. 4.]

2.2. CPU

Dvije najvažnije komponente na matičnoj ploči su procesor koji izvršava programe i glavna memorija koja privremeno pohranjuje izvršene programe i pridružene podatke. Procesor se obično naziva centralna procesna jedinica (CPU). CPU pristupa glavnoj memoriji radi dobivanja svojih uputa, a zatim izvršava te upute za obradu podataka.

Čitanje iz glavne memorije često je dramatično sporije od čitanja iz vlastite memorije CPU-a. Kao rezultat toga, moderni sustavi koriste više slojeva brze memorije, zvane predmemorije, kako bi se nadoknadio taj nesrazmjer. Svaka razina predmemorije (L1, L2, itd.) Relativno je sporija i veća od prethodne. U većini sustava predmemorija se ugrađuju u procesor i svaku njegovu jezgru. Ako se podaci ne nalaze u određenoj predmemoriji, podaci se moraju preuzeti iz sljedeće predmemorije ili glavne memorije. CPU se oslanja na svoju jedinicu za upravljanje memorijom (MMU) radi lakšeg pronalaženja mjesta pohrane podataka. MMU je hardverska jedinica koja prevodi adresu traženu od strane procesora u glavnu memoriju. Budući da dani

prijevod može zahtijevati više operacija čitanja memorije, procesor koristi posebnu predmemoriju, poznatu kao međuspremnik prijevoda (TLB), za tablicu prijevoda MMU. Prije svakog pristupa memoriji, savjetuje se s međuspremnikom prijevoda prije nego što zatraži jedinicu za upravljanje memorijom da izvrši skup operacija prevođenja adrese. [1, pp. 4-5]

2.3. Northbridge i southbridge

CPU se oslanja na memorijski kontroler kako bi upravljao komunikacijom s glavnom memorijom. Memorijski kontroler odgovoran je za posredovanje potencijalno istodobnih zahtjeva za sistemsku memoriju od procesora i uređaja. Memorijski kontroler može se implementirati na zasebnom čipu ili integrirati u sam procesor. Na starijim računalima CPU se povezao sa northbridge-om pomoću sabirnice s prednje strane. Uređaji (na primjer, mrežne kartice i diskovni kontroleri) bili su povezani preko drugog čipa, nazvanog southbridge-om / izlaz, koji je imao jedinstvenu zajedničku vezu s northbridge-om za pristup memoriji i CPU-u. Da bi poboljšali performanse i smanjili troškove novijih sustava, većina mogućnosti povezanih s memory controller hub-om sada je integrirana u procesor. Preostala funkcionalnost chipset-a, prethodno implementirana na southbridge-u, koncentrirana je na čipu poznatom kao čvorište kontrolera platforme. [1, p. 6.]

2.4. RAM

Glavna memorija računala je implementirana u memoriju sa slučajnim pristupom (RAM), koja pohranjuje kod i podatke kojima procesor aktivno pristupa te ih pohranjuje. U kontrastu sa memorijom uzastopnog pristupa koja je obično povezana s diskovima, slučajni pristup odnosi se na karakteristiku stalnog vremena pristupa bez obzira na to gdje su podaci pohranjeni na mediju. Glavna memorija na većini računala je dinamička RAM-a (DRAM). Dinamična je jer koristi razliku između napunjenog i pražnjenog stanja kondenzatora za pohranjivanje bit-a podataka. Da bi kondenzator mogao održavati ovo stanje, mora ga se povremeno osvježavati - zadatak koji memorijski kontroler obično izvršava. RAM se smatra nestalnom memorijom jer joj je potrebna uključenost u struju kako bi podaci ostali dostupni. Stoga, osim u slučaju napada hladnog pokretanja, nakon isključivanja računala nestaje memorija. To je glavni razlog zašto se ne

preporučuje taktika reakcije na incident "pull the plug" na hrvatskom iskopčaj kabal ako namjeravate sačuvati dokaze o trenutnom stanju sustava. [1, pp. 6-7]

3. Napadi na računalo i sustav

Nesumnjivo se povećava broj cyber napada koji ciljaju vladin, vojni, javni i privatni sektor. Ti se cyber napadi fokusiraju na ciljanje pojedinaca ili organizacija s nastojanjem da se izvuku vrijedne informacije. Ponekad su ti cyber napadi navodno povezani s kibernetičkim kriminalom ili grupama koje sponzoriraju država, ali mogu ih provoditi i pojedine skupine kako bi postigle svoje ciljeve. Većina tih cyber napada koristi zlonamjerni softver (eng. *malware*) da bi zarazili žrtve napada. Znanje, vještine i alati potrebni za analizu zlonamjernog softvera ključni su za otkrivanje, istraživanje i obranu od takvih napada. [2, p. 6]

3.1. Računalni zlonamjerni softveri

Zlonamjerni softver (eng. *malware*) je kod koji vrši zlonamjerne radnje, a može imati oblik izvršne datoteke (`.exe`), skripte, koda ili bilo kojeg drugog softvera. Napadači koriste zlonamjerni softver kako bi ukrali osjetljive informacije, špijunirali zaraženi sustav ili preuzeli kontrolu nad sustavom. Obično ulazi u sustav bez pristanka i znanja, te ga se može isporučiti putem različitih komunikacijskih kanala poput e-pošte, weba ili USB-a. Zlonamjerni softver naziv je širokog spektra koji se odnosi na različite vrste zloćudnih programa poput trojana, virusa, crva i rootkita. Tijekom izvođenja analize zlonamjernog softvera često ćete naići na razne vrste zlonamjernih programa, a neki od tih zlonamjernih programa kategorizirani su na temelju njihove funkcionalnosti i vektora napada kako je ovdje spomenuto:

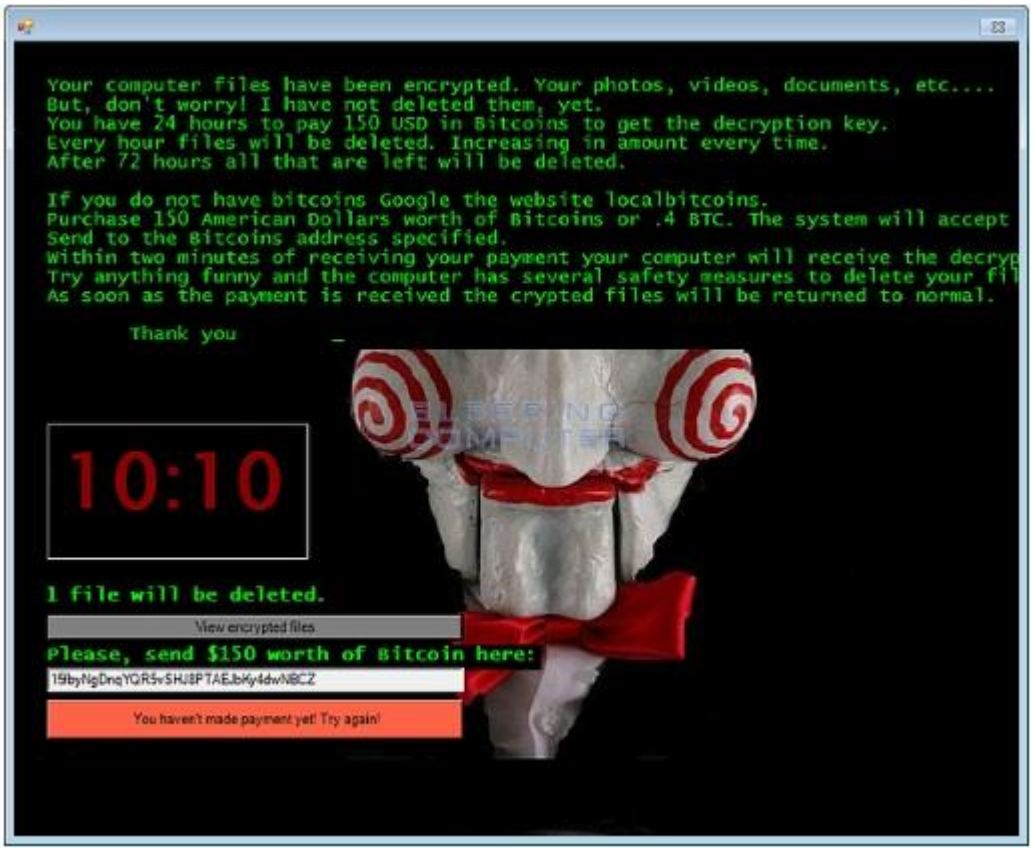
- Virus ili crv: zlonamjerni softver koji se može kopirati i širiti na druga računala. Virusu je potrebna intervencija korisnika, dok se crv može proširiti bez intervencije korisnika.
- Trojanski softver: zlonamjerni softver koji se prerušava u redoviti program kako bi izigrao korisnike da ga instaliraju na svoje sustave. Jednom instaliran može izvoditi zlonamjerne radnje poput krađe osjetljivih podataka, učitavanja datoteka na napadačev poslužitelj ili nadgledanja web-kamera.

- Trojanski pozadinski / udaljeni pristup (RAT): Ovo je vrsta trojanskog programa koji omogućuje napadaču pristup i izvršavanje naredbi na kompromitiranom sustavu.
- Adware: zlonamjerni softver koji korisniku predstavlja neželjene reklame (oglase). Obično ih se isporučuje putem besplatnih preuzimanja i prisilno instaliraju softver na vaš sustav.
- Botnet: Ovo je skupina računala zaraženih istim zlonamjernim softverom (zvani botovi) koji čekaju da dobiju upute od poslužitelja za naredbe i kontrole kojim upravlja napadač. Napadač može tim naredbama izdati naredbu koja može obavljati zlonamjerne aktivnosti poput DDOS napada ili slanje neželjene e-pošte.
- Information stealer: zlonamjerni softver dizajniran za krađu osjetljivih podataka poput bankarskih vjerodajnica ili upisanih pritiska tipke iz zaraženog sustava. Neki primjeri ovih zlonamjernih programa uključuju ključne zapise, špijunski softver, sniffer-e i grabilice obrasca.
- Ransomware: zlonamjerni softver koji drži zaraženi sustav kriptiranim radi otkupnine, čini računalo neupotrebljivim, te iz tog razloga prisiljava žrtvu na isplatu otkupnine radi očuvanja žrtvinih podataka. [2, p. 7.] Ransomware je prvi put zapazio FBI u 2011. godini. IC3 (Internet crime complaint center) je na svojoj web stranici objavio upozorenje o aplikaciji u svibnju 2012. godine, a s vremenom je virus postao sve raširenij u SAD-u i ostalim dijelovima svijeta. Neke inačice mogu čak uključiti računalne web kamere i prikazati sliku žrtve na smrznutom zaslonu. [3]
- Rootkit: zlonamjerni softver koji napadaču pruža povlašteni pristup zaraženom sustavu i prikriva njegovu prisutnost ili prisutnost drugog softvera.
- Preuzimanje ili kapaljka: zlonamjerni softver dizajniran za preuzimanje ili instaliranje dodatnih komponenti zlonamjernog softvera. [2, pp. 7-8]

3.1.1. Jigsaw ransomware

Maliciozni softver koji će biti izvor zaraze na žrtvinom računalu u ovom radu pod imenom “Jigsaw” spada u kategoriju ransomware-a. Zlonamjerni softver radi samo na windows OS, izvorno nazvan BitcoinBlackmailer.exe ili JIGSAW, slijedi uobičajenu praksu šifriranja datoteka žrtve i dodavanja .FUN ekstenzije. Pojavni ekran, koji nosi lice iz kultnog filma "Slagalica strave" lutke pod imenom Billy tada počinje postavljati zahtjeve. Na ekranu se prikazuje vrijeme odbrojavanja, a od žrtve se traži 20 dolara u Bitcoin-u kao zamjena za dešifriranje datoteka. No,

kako sati prolaze, zlonamjerni softver će početi brisati datoteke, prvo samo nekoliko, ali broj će porasti, kao i otkupnina potrebna za dešifriranje istih. Nakon 72 sata, sve datoteke na ciljnom računalu bit će izbrisane, a otkupnina se popela na 150 dolara vrijednih Bitcoina. Korisnik uvijek može isključiti računalo, ali kad ga ponovo uključi, 1.000 datoteka bit će izbrisano kao kazna. Što se tiče IT stručnjaka, Jigsaw je lako probiti reverznim inženjeringom jer je napisan u .NET-u koji u izvornom kodu sadrži ključ za dešifriranje. [4]



Slika 2. Jigsaw Ransomware [4]

3.2. Analiza zloćudnog softvera

Analiza zlonamjernog softvera proučava ponašanje zlonamjernog softvera. Cilj analize zlonamjernog softvera je razumjeti funkcioniranje istog, te kako ga otkriti i ukloniti. To uključuje analizu sumnjivog binarnog materijala u sigurnom okruženju kako bi se utvrdile njegove

karakteristike i funkcionalnosti tako da se može zaštititi mreža. Evo nekoliko razloga zbog kojih će se izvršiti analiza zlonamjernog softvera:

- Da bi se odredila priroda i svrha zlonamjernog softvera. Na primjer, može pomoći pri otkrivanju informacije da li je zlonamjerni softver ukraditelj informacija, HTTP bot, neželjeni bot, rootkit, keylogger ili RAT, steći razumijevanje kako je sustav ugrožen.
- Za prepoznavanje mrežnih pokazatelja povezanih sa zlonamjernim softverom koji se zatim mogu koristiti za otkrivanje sličnih infekcija pomoću mrežnog nadzora. Na primjer, tijekom analize, ako se utvrdi da zlonamjerni softver kontaktira određenu domenu, tada se može koristiti ta domena za stvaranje potpisa i nadziranje mrežnog prometa da bi se identificirali svi domaćini koji kontaktiraju tu domenu / IP adresu.
- Da bi se izvukli pokazatelji koji se temelje na hostu, poput naziva datoteka, i ključeva registra, koji se zauzvrat mogu koristiti za određivanje slične infekcije pomoću praćenja na temelju hosta. Na primjer, ako se sazna da zlonamjerni softver stvara registarski ključ, može se upotrijebiti ovaj registarski ključ kao pokazatelj za stvaranje potpisa ili skeniranje mreže kako bi se identificirali hostovi koji imaju isti registarski ključ.
- Kako bi se utvrdila namjera i motiv napadača. Na primjer, tijekom analize ako se ustanovi da zlonamjerni softver krade bankarske vjerodajnice, može se zaključiti da je motiv napadača novčana dobit. [2, pp. 8-9]

3.2.1. Vrste analiza zlonamjernog softvera

Da bi se razumio rad i karakteristike zlonamjernog softvera i procijena njegovog utjecaja na sustav, često će se koristiti različite tehnike analize. Slijedi klasifikacija ovih tehnika analize:

- Statička analiza: Ovo je postupak analize binarne datoteke bez izvršenja. To je najlakše za izvedbu i omogućuje izdvajanje metapodataka povezanih sa sumnjivim binarnim datotekama. Statička analiza možda neće otkriti sve potrebne informacije, ali ponekad može pružiti zanimljive informacije koje pomažu u određivanju gdje usmjeriti buduće napore u analizi.
- Dinamička analiza (analiza ponašanja): Ovo je postupak izvršavanja sumnjive binarne datoteke u izoliranom okruženju i praćenja njegovog ponašanja. Ova

tehnika analize je jednostavna za izvođenje i daje vrijedan uvid u aktivnost binarne datoteke tijekom izvođenja. Ova tehnika analize je korisna, ali ne otkriva sve funkcionalnosti neprijateljskog programa.

- Analiza koda: To je napredna tehnika koja se fokusira na analiziranje koda da bi se razumjelo unutarnje funkcioniranje binarne datoteke. Ova tehnika otkriva informacije koje nije moguće utvrditi samo statičkom i dinamičkom analizom. Analiza koda dalje je podijeljena na statičku analizu koda i dinamičku analizu koda. Statička analiza koda uključuje rastavljanje sumnjivog binarnog materijala i gledanje koda da bi se razumjelo ponašanje programa, dok dinamička analiza koda uključuje uklanjanje pogrešaka sumnjivog binarnog materijala na kontrolirani način kako bi se razumjela njegova funkcionalnost. Analiza koda zahtijeva razumijevanje programskog jezika i koncepata operativnog sustava.
- Analiza radne memorije: Ovo je tehnika analize RAM-a računala za forenzičke artefakte. To je obično forenzička tehnika, ali integriranje u analizu zlonamjernog softvera pomoći će u razumijevanju ponašanja zlonamjernog softvera nakon infekcije. Analiza radne memorije posebno je korisna za utvrđivanje nepomičnih i izbjegavajućih mogućnosti zlonamjernog softvera. [2, pp. 9-10]

4. Forenzika radne memorije

Forenzika radne memorije područje je računalne forenzike koje se bavi prikupljanjem i analizom tragova iz radne memorije računala. Radna memorija računala značajna je za forenziku jer sadržava neke tragove koje nije moguće pronaći drugim forenzičkim metodama, primjerice forenzikom diska ili forenzikom mreže. [5, p. 3.]

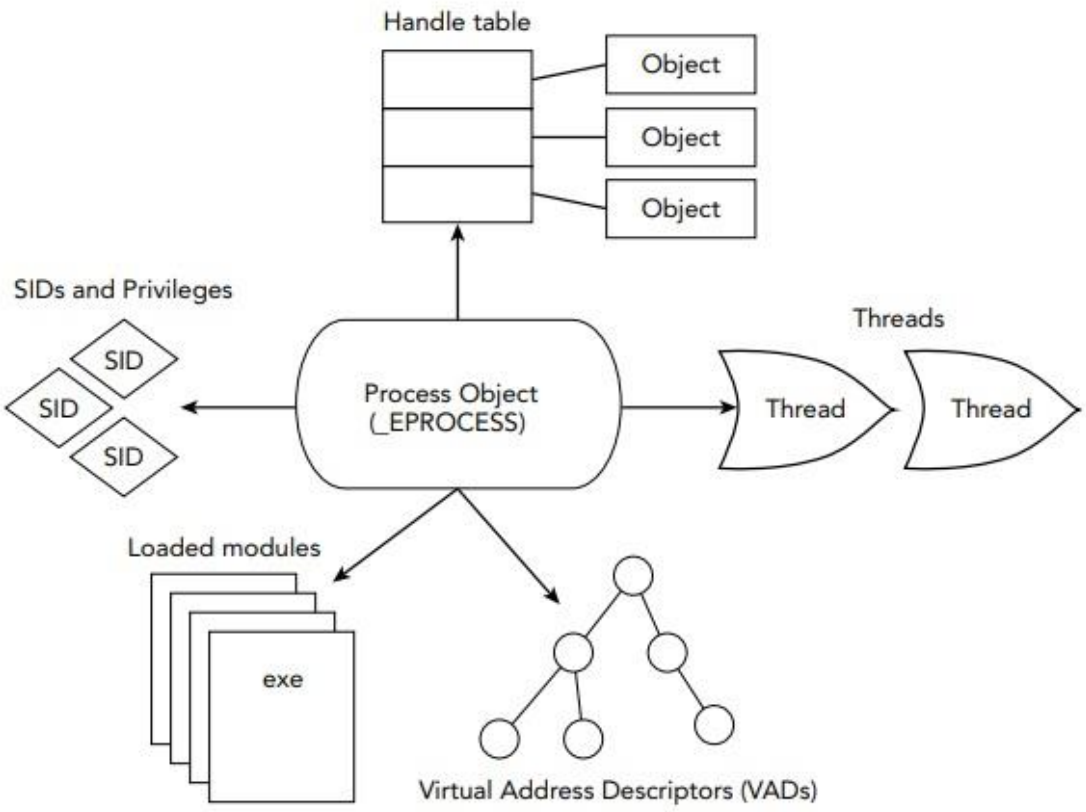
4.1. Izvršni objekti

Veliki dio forenzike radne memorije uključuje pronalaženje i analizu izvršnih datoteka (`.exe`). Windows je napisan u C programskom jeziku i intenzivno koristi C strukture za organiziranje povezanih podataka i atributa. Neke od tih struktura nazivaju se izvršni objekti zato što njima upravlja, stvara, štiti, briše i slično. Windows Object Manager je komponenta jezgre koju implementira NT modul. Konstrukcija tehnički postaje izvršni objekt kada operativni sustav

pretvara u nju zaglavlja kako bi upravljao uslugama poput imenovanja, kontrole pristupa i referentnih brojeva. Prema ovoj definiciji, svi izvršni objekti su strukture, ali nisu sve strukture izvršni objekti. [1, p. 118.]

4.2. Procesi

Proces se odnosi na skup instrukcija koje trenutno obrađuje CPU. Na primjer, u sustavu Windows može se vidjeti svaki proces koji se odvija otvaranjem kartice "proces" u upravitelju zadataka. Windows procesi su Windows servisi i pozadinski programi koji se obično ne vide. Proces može biti program printera koji se pokreće u pozadini i nadzire razine tinte i ostale postavke printera dok računalo radi. [6]. Slika 3 prikazuje nekoliko osnovnih resursa koji pripadaju određenom procesu. U središtu je `_EPROCESS`, što je naziv strukture koju koristi Windows kao postupak. Iako se nazivi struktura sigurno razlikuju između Windows-a, Linux-a i Mac-a, svi operacijski sustavi imaju iste koncepte koji su opisani u slici 3. Na primjer, svi imaju jednu ili više niti (eng. *thread*) koje izvršavaju kod i svi imaju tablicu ručki (eng. *handles* ili *file descriptors*) prema jezgrinim objektima kao što su datoteke, mrežne utičnice i mutexi. Svaki postupak ima svoj privatni prostor virtualne memorije koji je izoliran od drugih procesa. [1, p. 149.]



Slika 3. Resursi procesa [1, p. 149.]

Kao što prikazuje i slika, svaki `_EPROCESS` upućuje na popis sigurnosnih identifikatora (SID-ova) i podataka s privilegijama. Ovo je jedan od glavnih načina na koji jezgra provodi sigurnost i kontrolu pristupa. Kombinacijom svih ovih koncepata u istražni postupak može se prikupiti značajna količina dokaza kako bi se utvrdilo koji su procesi uključeni zlonamjerne aktivnosti, koji su artefakti povezani s incidentom i koji korisnički računi bi mogli biti ugroženi. [1, pp. 149-150]

4.2.1. Struktura podataka

U ovom potpoglavlju biti će prikazana struktura podataka oko koje se bazira uvid u procese, kako ih jedinstveno prepoznati, kada su započeti, da li još uvijek traju i slično.

- PCB: Kontrolni blok jezgre procesa (`_KPROCESS`). Ova struktura sadrži nekoliko kritičnih polja, uključujući DirectoryTableBase za translaciju adrese i količinu vremena koje je proces proveo u jezgrinom načinu rada i načinu rada korisnika.

- CreateTime: Vremenska oznaka UTC koja pokazuje kada se proces prvi put pokrenuo.
- ExitTime: Oznaka vremena UTC koja pokazuje vrijeme izlaska procesa. Ova vrijednost je nula za još uvijek pokrenute procese.
- UniqueProcessID: Broj koji jedinstveno identificira proces (također poznat kao PID).
- ActiveProcessLinks: dvostruko povezan popis koji povezuje aktivne procese. Većina API-ja na pokrenutom sustavu oslanja se na prolasku po tom popisu.
- SessionProcessLinks: Još jedan dvostruko povezan popis koji povezuje procese u istoj sesiji.
- InheritedFromUniqueProcessId: Broj koji specificira identifikator roditeljskog procesa. Nakon pokretanja procesa, on se ne mijenja, čak i ako njegov roditelj prestaje.
- Session: Pohranjuju podatke o sesiji za prijavu korisnika i grafičko korisničko sučelje (GUI) objekata. [1, pp. 151-152]

4.2.2. Kritični procesi sustava

Pored istih struktura podataka slijedi popis postupaka koji su nužni za rad sustava, a dobro će ih znati samo ljudi s iskustvom u radu s njima koji mogu brzo zaključiti koji procesi pobuđuju sumnju.

- Idle i System: Ovo nisu stvarni procesi (u smislu da nemaju odgovarajuće izvršne datoteke na disku). Idle je samo spremnik koji jezgra koristi za punjenje CPU-a. Slično tome, System služi kao zadana baza za niti koje se izvode u jezgrinom načinu rada. Sistemski proces uvijek ima PID 4 poslužitelja igra ulogu u stvaranju i brisanju procesa i niti.
- csrss.exe: kreira i briše procese i niti, te održava privatni popis objekata koji se mogu koristiti za unakrsnu referencu s drugim izvorima podataka.
- services.exe: Upravlja Windows servisima i održava popis servisa u svom privatnom memorijskom prostoru.
- svchost.exe: čisti sustav ima više zajedničkih procesa koji se istovremeno pokreću, a svaki nudi spremnik za DLL-ove koji implementiraju usluge. Njegov roditelj trebao bi biti services.exe, a put do izvršne datoteke treba upućivati na direktorij system32.
- lsass.exe: Provjera lozinki i stvaranje pristupnih tokena. Kao takav, to je često cilj ubrizgavanja koda, jer se u njemu mogu pronaći hashevi otvorenog teksta. Trebao bi postojati samo jedan primjerak lsass.exe, a njegov roditelj je winlogon.exe.

- winlogon.exe: Ovaj postupak predstavlja interakciju za prijavu, pokreće čuvar zaslona kada je to potrebno, pomaže u učitavanju korisničkih profila i odgovara na rad tipkovnice kao naprimjer (`CTRL + ALT + DEL`).
- explorer.exe: vidljiv je po jedan Windows Explorer postupak za svakog prijavljenog korisnika. Odgovoran je za rukovanje raznim interakcijama korisnika, poput mape koja se temelji na GUI-ovoj navigaciji, predstavljanje početne navigacije (eng. *menu*) i tako dalje. Također ima pristup osjetljivim materijalima poput dokumenata koje otvarate i vjerodajnice koje koristite za prijavu na FTP web mjestu putem Windows Explorera.
- smss.exe: Upravitelj sesija je prvi pravi način rada korisnika koji započinje tijekom redoslijeda pokretanja. Odgovoran je za kreiranje sesija koje izoliraju OS od različitih korisnika. [1, p. 154.]

4.3. Registri

Registar je skup koji sadrži različite postavke i konfiguracije za operacijski sustav, aplikacija i korisnika na računalu. Kao osnovna komponenta sustava, njemu se pristupa neprestano tijekom rada. Logikom ima smisla da sustav sprema sve ili dio datoteka registra u memoriju. Nadalje, registar sadrži mnoštvo informacija korisnih u forenzičke svrhe. Na primjer, koristi se radi utvrđivanja koji su se programi nedavno pokrenuli, oznake zaporki za određene potrebe, ili istraživanje ključeva i vrijednosti koji su zlonamjerni kod unosili u sustav. [1, p. 281.]

4.3.1. Ključni pojmovi registra

Kao i kod procesa, biti će spomenuti ključni parametri što se tiče registra.

Hive je logička skupina ključeva, potključeva i vrijednosti u registru koja sadrži skup podržanih datoteka učitanih u memoriji kada je operativni sustav pokren ili korisnik prijavi. [7]

- HiveList: Dvostruko povezan popis s ostalim `_CMHIVE` strukturama.
- FileFullPath: Jezgrin put uređaja (naprimjer `\Device\HarddiskVolume1\WINDOWS\system32\config\software`) u hive registra.

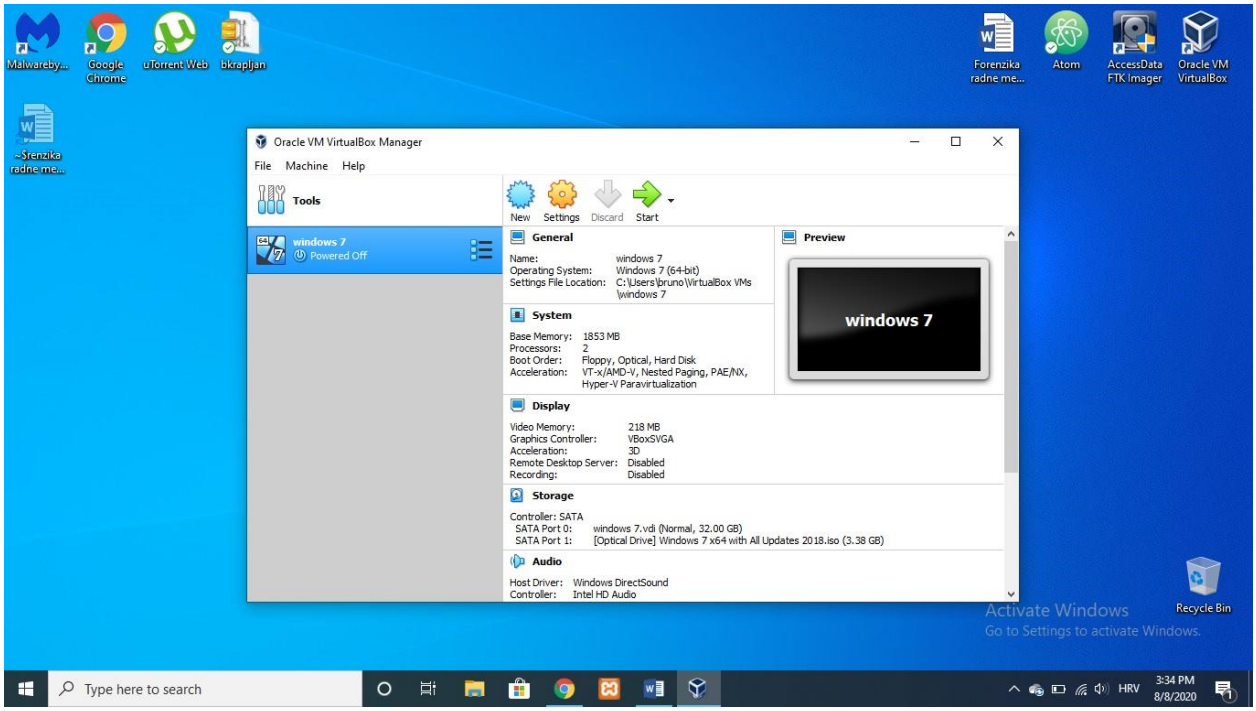
- HiveRootPath: Predstavljen u sustavu Windows Vista, ovaj član sadrži put registra (naprimjer `\REGISTRY\MACHINE\SOFTWARE`).
- Signature: potpis datoteke registra. Važeće datoteke registra imaju potpis od `0xbee0bee0`.
- BaseBlock: koristi se za pronalaženje korijenskog ključa (prvog ključa) registra.
- Pohrana: Mapiranje virtualnih adresnih prostora za ključeve registra. [1, p. 283.]

5. Nužni alati za sigurnu istragu

Forenzika radne memorije je samo jedno polje digitalne forenzike, a svako polje zahtjeva određeni set znanja i alata. Nakon usvajanja osnovnog znanja koja su potrebna za forenzičku istragu radne memorije, slijedi uvod i prikaz alata koji su nužni za rad, a to su VirtualBox, FTK Imager i Volatility. Svrha svakog alata biti će opisana u idućim poglavljima.

5.1. VirtualBox

VirtualBox je virtualizator opće namjene za x86 hardware, usmjeren na poslužitelj, radnu površinu i ugrađenu upotrebu. [8]. VirtualBox za primjer ima namjenu pokretanja više operacijskih sustava istovremeno, a u ovome radu će poslužiti za ispitivanje i oporavak od katastrofe. Virtualni stroj i njegov virtualni tvrdi disk može se smatrati spremnikom koji se može proizvoljno zaustaviti, pokrenuti, kopirati, napraviti sigurnosnu kopiju i transportirati između računala. Također ima opciju snimke koju je moguće spremiti u određeno stanje virtualnog stroja i vratiti se u to stanje, ako je potrebno. Na taj se način slobodno može eksperimentirati s računalnim okruženjem. Ako nešto pođe po zlu, poput problema nakon instaliranja programa ili zaraze virtualnog stroja virusom, lako se može prebaciti na prethodni snimak i izbjeći određeni problem. [9]

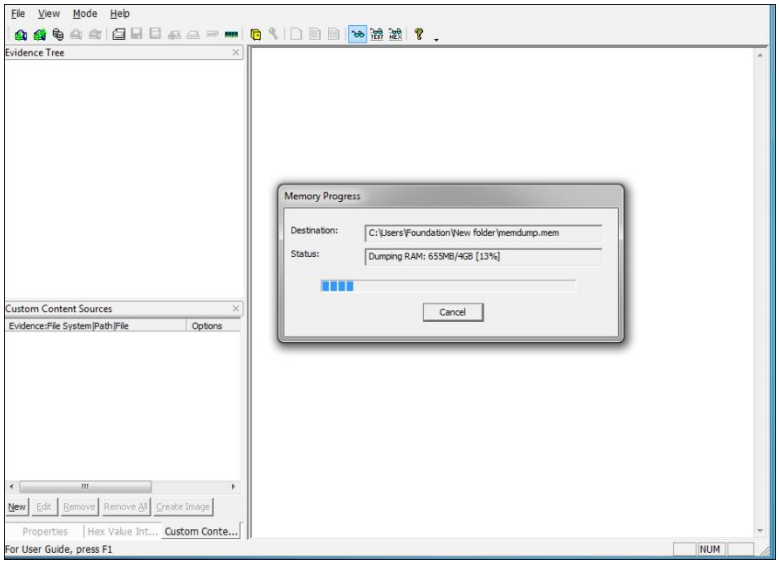


Slika 4. Virtualni stroj unutar VirtualBox-a [autorski rad]

Slika 4 prikzuje postavljeni virtualni stroj sa svojim postavkama i virtualni hard disk na kojem je instaliran Windows 7 i spreman za upotrebu.

5.2. FTK Imager

FTK Imager je alat za pregled i obradu podataka pomoću kojeg je moguće brzo dobiti elektroničke dokaze, poput preslike radne memorije. [10]. Preslika radne memorije je vrlo jednostavna, otvara se program FTK Imager, te klikom na „File“ u navigacijskoj traci izabere se „Capture memory“, zatim direktorij u koji se želi spremiti snimljena slika memorije i pod kojim nazivom, a zatim klikom na gumb „Capture memory“, te se izvršava sama radnja preslike radne memorije i čeka na izvršavanje akcije ovisno o veličini RAM-a. [11]



Slika 5. FTK Imager [11]

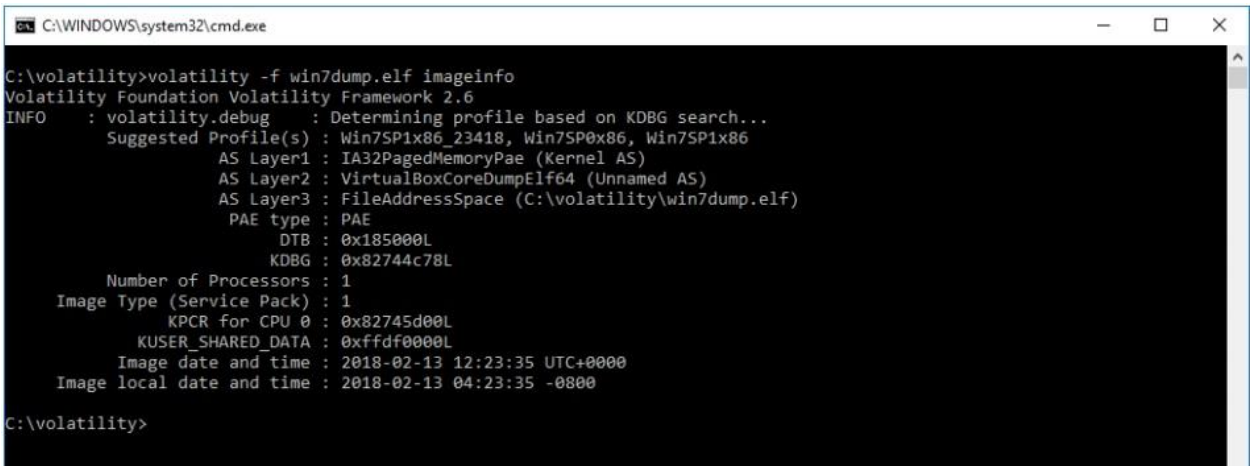
5.3. Volatility

Alat Volatility namijenjen je za analizu slike radne memorije. [12, p. 3.]Za operacijski sustav Windows, Volatility dolazi kao jedna izvršna datoteka te koristi se izravnim pozivanjem iz naredbenog retka. [12, p. 4.]

5.3.1. Uvod u rad u Volatility alatu

Kako bi alat Volatility znao koju sliku memorije treba analizirati, u pozivu alata iz naredbenog retka koristi se parametar `-f` iza kojeg slijedi putanja do slike memorije. Koristi se slika imena `win7dump.elf` koja se nalazi u istom direktoriju kao i alat Volatility, pa će zato parametar `-f win7dump.elf` biti korišten prilikom svakog poziva alata. U nekim slučajevima, nije poznato koji operacijski sustav se nalazio na računalu s kojega je snimljena slike memorije, a ta informacija potrebna je alatu Volatility kako bi ispravno radio analizu. Alat Volatility ima naredbu `imageinfo` koji služi za prepoznavanje profila tj. inačice operacijskog sustava s kojeg je snimljena slika memorije. U pozivima alata Volatility koristiti se parametar `–profile= <ime profila>` kako bi Volatility znao pronaći i interpretirati strukture u memoriji specifične za tu

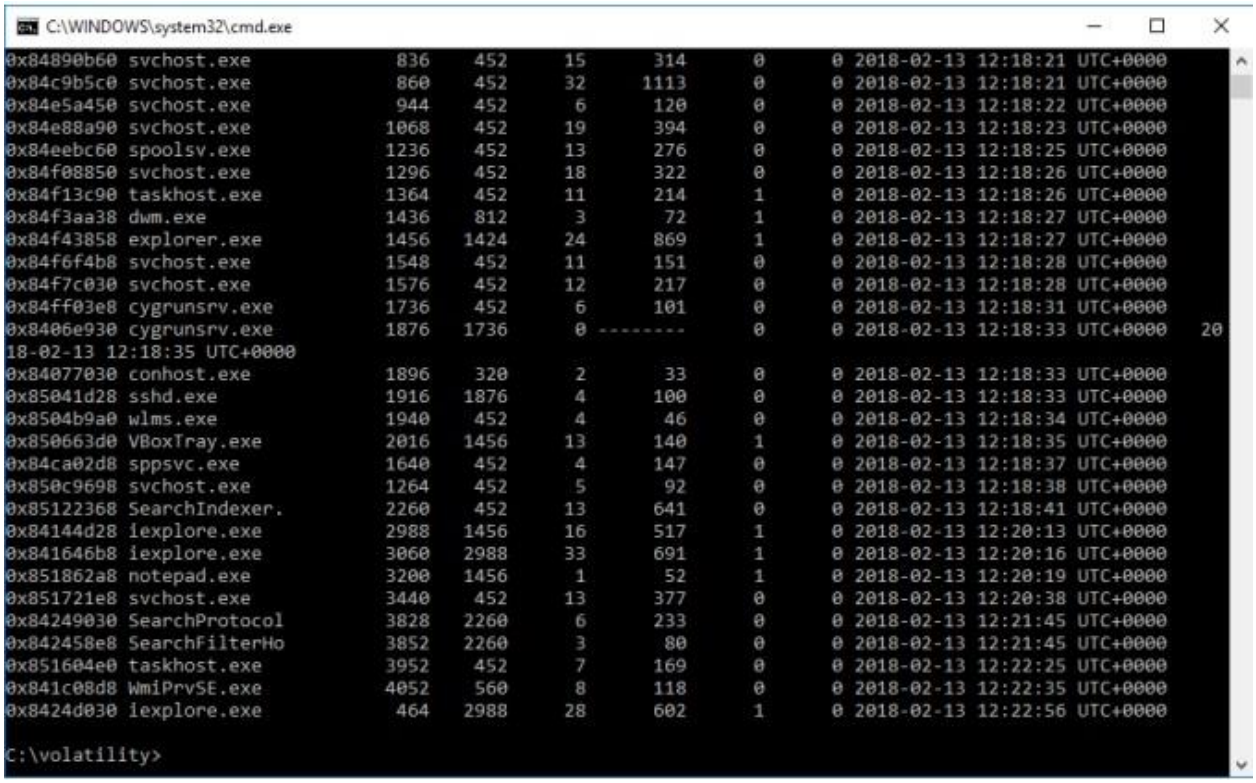
inačicu operacijskog sustava. Naredba za otkrivanje informacija o slici memorije je: volatility `-f win7dump.elf imageinfo`. U ovom primjeru, Volatility je prepoznao tri potencijalna profila operacijskih sustava, od kojih su sva tri inačice operacijskog sustava Windows 7. Kako je unaprijed poznato da je ovo slika memorije operacijskog sustava Windows 7 SP1, u nastavku će se koristiti profil Win7SP1x86_23418, te će sve naredbe počinjati s: `volatility -f win7dump.elf --profile=Win7SP1x86_23418` [12, p. 8.]



Slika 6. Volatility [12, p. 8.]

5.3.2. Popis procesa u Volatility alatu

Jedna od korisnih informacija u radnoj memoriji računala je popis procesa koji su bili pokrenuti u trenutku snimanja slike memorije. Za ispis popisa procesa iz slike radne memorije operacijskog sustava Windows koristi se naredba pslist. Ispis naredbe istovjetan je popisu procesa u upravitelju zadataka (eng. task manager) sustava Windows. Cijela naredba korištena u ovom primjeru je: `volatility -f win7dump.elf --profile=Win7SP1x86_23418 pslist` [12, pp. 8-9]



Slika 7. Volatility lista procesa [12, p. 9.]

Naredba `pstree` na jednak način pronalazi procese koji su bili pokrenuti na sustavu, no za razliku od naredbe `pslist`, u ispisu i vizualno prikazuje hijerarhiju procesa. Kada jedan proces stvori drugi proces, proces koji je pokrenut naziva se „proces dijete“ (eng. *child process*) dok se proces koji ga je pokrenuo naziva „proces roditelj“ (eng. *parent process*). U ispisu naredbe `pstree` jasno se može vidjeti koji proces je roditelj, a koji dijete, tj. može se primijetiti koje sve procese je pokrenuo neki proces. Ovakva informacija o vezama između procesa može biti izrazito korisna u analizi. [5, p. 6.]

5.3.3. Ručke

Ručke (eng. *handles*) su apstrakcija operacijskog sustava Windows – to su identifikatori pomoću kojih proces pristupa objektima operacijskog sustava. Primjeri takvih objekata su datoteke, ključevi registra i sinkronizacijski mehanizmi. Tablice ručki procesa su zapisane u memoriji računala te ih se može pročitati Volatility naredbom `handles`. Proučavanjem objekata operacijskog sustava koje proces koristi obično se može dobiti šira slika njegova rada. Kako proces tipično koristi velik broj ručki, ovakav ispis naredbe je velik, te je korisnije ciljano gledati objekte po vrsti. To je moguće ostvariti kroz prosljeđivanje ispisa alata Volatility alatu za filtriranje

teksta. Na Unix sustavima i sustavima izvedenim iz Unixa, u tu svrhu se najčešće koristi alat `grep`, dok se u ovom dokumentu koristi alat `findstr`, koji je dostupan iz naredbenog retka sustava Windows. [5, p. 9.]

5.3.4. Registarski ključevi

Zlonamjerni softver često koristi Windows registar u sklopu svojih mehanizama trajnosti (eng. *persistence mechanisms*). U Windows registar moguće je zapisati određene ključeve na temelju kojih će se program pokretati prilikom pokretanja računala. Te ključeve koriste i zlonamjerni programi kako ih se ne bi moglo riješiti jednostavnim ponovnim pokretanjem računala. Jedan izvor za popis takvih registarskih ključeva nalazi se na https://resources.infosecinstitute.com/common-malware-persistence-mechanisms/. Kao primjer, sadržaj jednog od tih ključeva Windows registra moguće je provjeriti pokretanjem sljedeće naredbe: `volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 printkey --key="Software\Microsoft\Windows\CurrentVersion\Run"` [5, p. 17.]

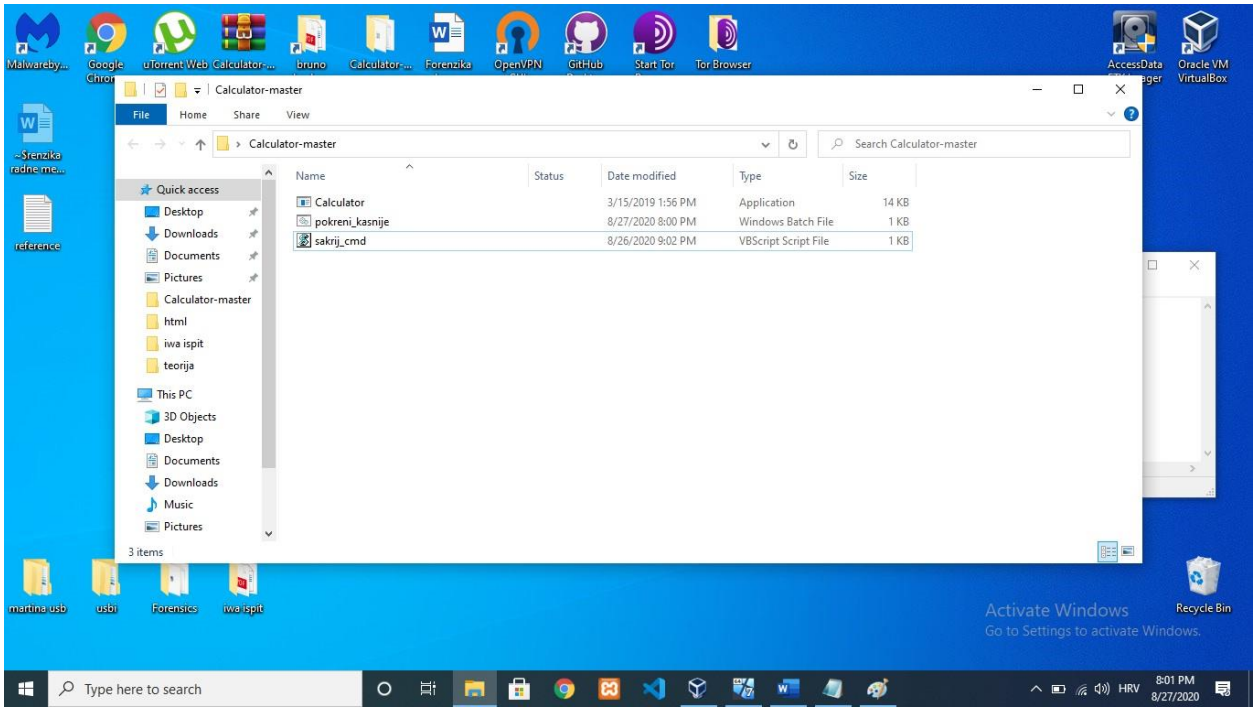
Da ne dođe do zabune, .elf je drukčiji od prošlog potpoglavlja jer se radi o primjeru iz druge literature.

6. Simulacija napada ransomware-om

Nakon objašnjene teorije slijedi simulacija napada koju karakterizira scenarij od četiri učenika gdje svatko ima svoj USB stick, a cilj je izlaganje prezentacije na profesorovom računalu, gdje svaki učenik na svom USB stick-u ima svoju prezentaciju, te jedan od četiri učenika na svom USB stick-u sadrži maliciozni kod koji će pokrenuti Jigsaw ransomware program s ciljem da kriptira podatke na profesorovom računalu, te ih sve uništi u slučaju da profesor ne plati traženu otkupninu. Učenici su Antonio, Bruno, Cecilio i Dario, a profesor je Profesor.

6.1. Perspektiva napadača

Pravo pitanje je kako će dotični učenik pokrenuti ransomware, izložiti prezentaciju, vratiti se na mjesto i bez ikakve sumnje od strane ikoga, a kamoli profesora proći ne zapaženo. Odgovor je otprilike jednostavan, a leži u tome da je potrebno napisati batch i vbs skriptu.



Slika 8. Skripte za tihi rad [autorski rad]

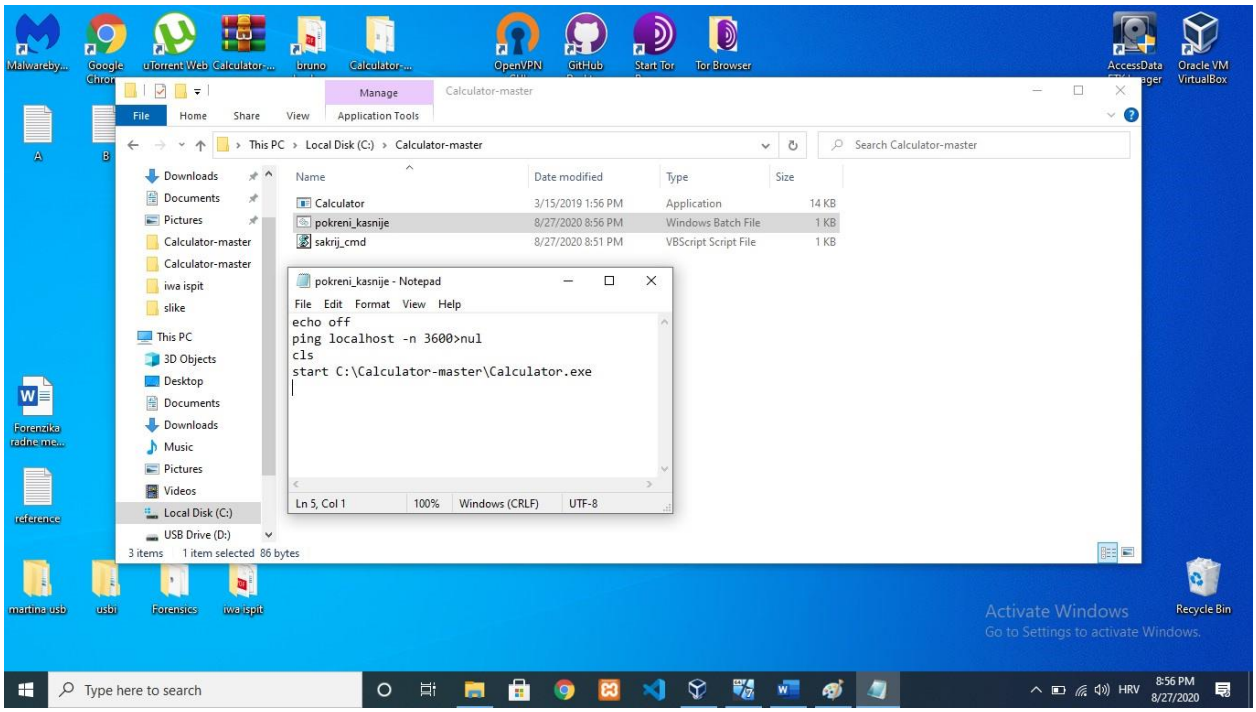
Na slici 8 se vidi o čemu se točno radi, calculator.exe je radi primjera običan kalkulator, te unutar njega nije sadržan ikakav oblik malicioznog koda. Prilikom pokretanja batch skripte „pokreni_kasnije“ otvara se cmd.exe koji radi latenciju tj. kašnjenje programa zadanim parametrom `ping localhost -n 3600>nul` gdje 3600 označava broj sekundi, a 3600s = 1h, latencija djeluje na program koji je zadan parametrom „start“, a potrebno je uključiti cijelu putanju do datoteke. Cijeli kod „pokreni_kasnije.bat“ je:

```
echo off
ping localhost -n 3600>nul cls
start C:\Calculator-master\Calculator.exe
```

[13]

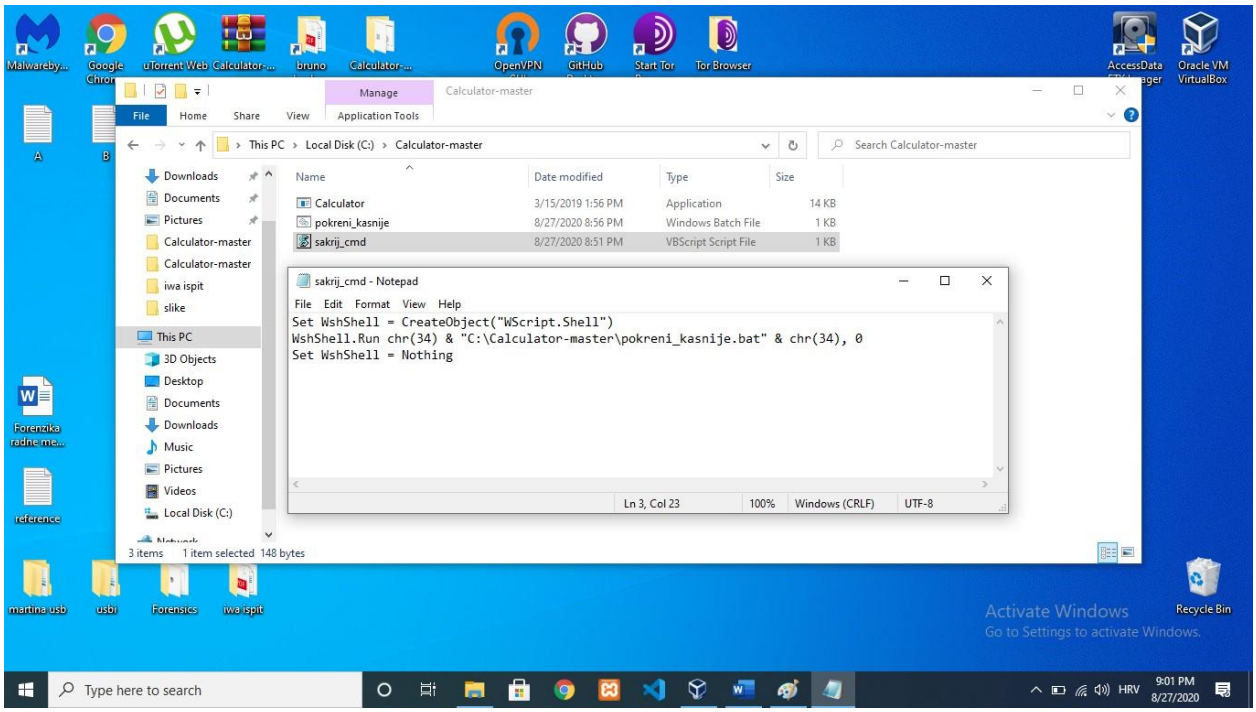
Naredba "echo off" isključuje prikaz svih komandi prilikom pokretanja skripte, a "ping" se koristi za provjeru može li terminal koji pokreće naredbu kontaktirati drugi terminal, čija adresa slijedi nakon ključne riječi ping, koja je u ovom slučaju localhost, a localhost je inače trenutno računalo koje se koristi. Localhost se obično odnosi na sam terminal, a IP adresa povezana s njim je "127.0.0.1". Opcija "- n" koristi se za određivanje vremena latencije terminala, te se zatim odredi broj u sekundama. Nadalje, koristi se operator preusmjeravanja naredbe ">" za prijenos

izlaza naredbe u datoteku čiji naziv slijedi nakon operatora preusmjeravanja (>). Za ime datoteke koristi se "nul" koji djeluje kao nulta datoteka, gdje izlaz nigdje nije registriran, a "cls" čisti sliku terminala. Zadnji ostaje "start" koji vrši naredbu pokretanja zadanog programa proslijeđujući mu parametre u kojima se opisuje destinacija programa na računalu. Uz „ping“ latenciju još od nekih metoda su „timeout“ koja radi na operacijskom sustavu Windows 7 i dalje, te „sleep“ metoda koja radi na Windows XP. U radu je korišten „ping“ jer radi na svim Windows operacijskim sustavima, a sintaksa mu nije kompliciranа. [14] Za efektivan način zaraze na žrtvino računalo putem ove metode, potrebno je premjestiti cijeli direktorij na C:\ putanju, jer je najjednostavije i s najmanjim rizikom jer žrtva neće lako primjetiti novi direktorij koji napadač sprema na žrtvino računalo. [autorski rad]



Slika 9. Skripta "pokreni-kasnije" [autorski rad]

Idući problem koji dolazi jest da prilikom pokretanja batch skripte, cmd.exe je otvoren, te je vidljiv na programskoj traci i na radnoj površini, što znači da je cmd.exe koji radi latenciju od jedan sat na program, potrebno učiniti nevidljivim žrtvi, tako da je vidljiv samo na task manageru. Kao rješenje dolazi vbs skripta koja će to omogućiti.



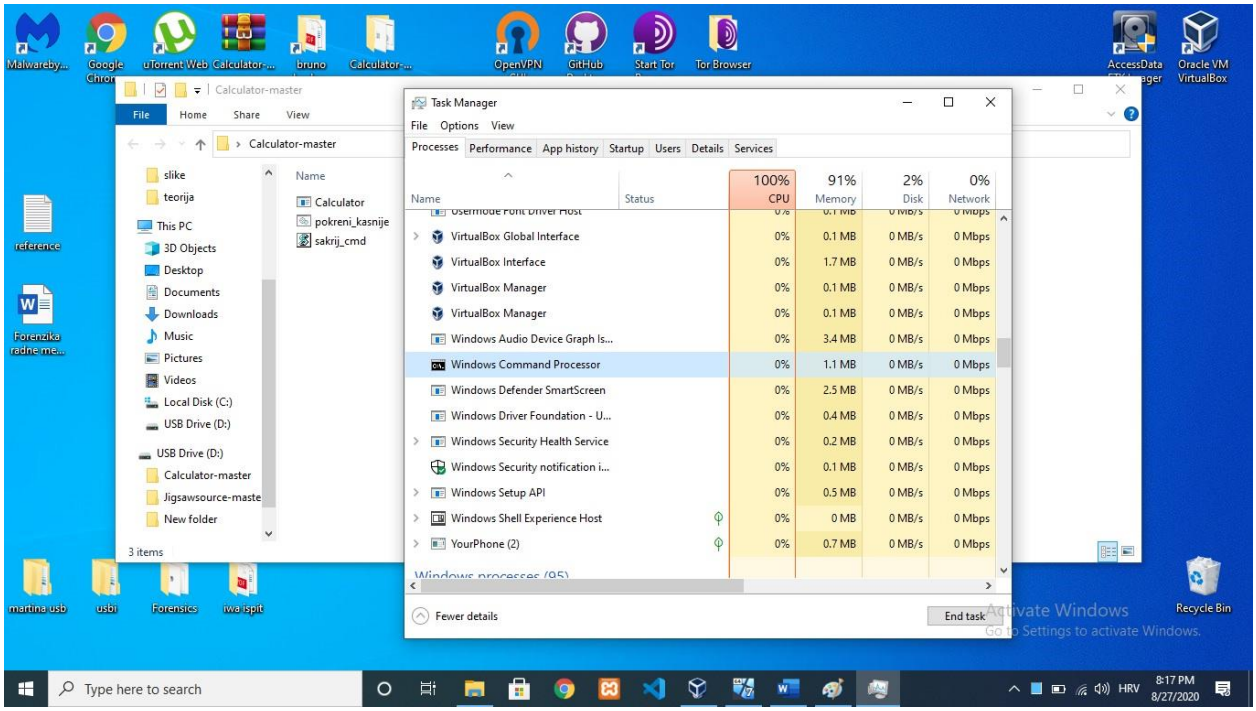
Slika 10. Skripta "sakrij-cmd" [autorski rad]

Potrebno je također dodijeliti istu putanju kao i kod batch datoteke, samo što ovaj put umjesto programa u batch skripti, dodjeljujemo samu batch skriptu kao što je vidljivo na slici 10. Cijeli kod skripte „sakrij_cmd.vbs“ glasi:

```
Set WshShell = CreateObject("WScript.Shell")

WshShell.Run chr(34)&

"C:\Users\bruno\OneDrive\Desktop\Calculator-master\pokreni_kasnije.bat"      &
chr(34), 0

Set WshShell = Nothing
```

[15]

Na slici 11 se vidi prikaz dotičnog cmd.exe stvoren od batch skripte koju je zapravo pokrenula vbs skripta činujući ga nevidljivim.

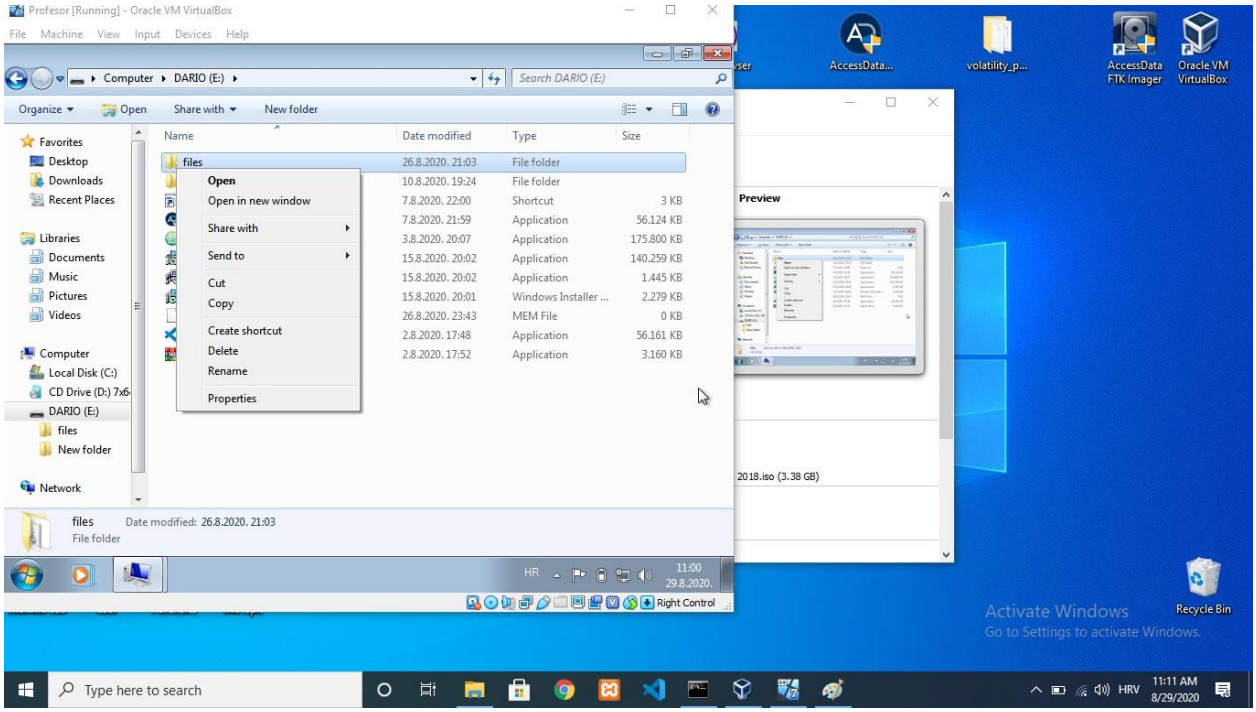


Slika 11. Prikaz skrivenog procesa cmd.exe [autorski rad]

Dakle, napadač će ovaj primjer primjeniti na JigsawRansomware.exe kojeg će sadržavati na svom USB stick-u gdje će prilikom priključivanja na profesorovo računalo kopirati folder pod imenom „files“ na C:\ disk, te prilikom završetka kopiranja koje traje relativno brzo (pod relativno brzo znači 1-2 sekunde jer se radi o datoteci koja sadrži manje od 1 mb), pokrenuti će tihi način rada tako što će pokrenuti skriptu „sakrij_cmd.vbs“, koja otvara i čini „pokreni_kasnije.bat“ vidljivom samo u procesu, a „pokreni_kasnije.bat“ otvara `JigsawRansomware.exe` nakon 3600 sekundi što je ekvivalentno jednom satu. [JigsawRansomware preuzet s: https://github.com/LeechxSys/Jigsawsource]

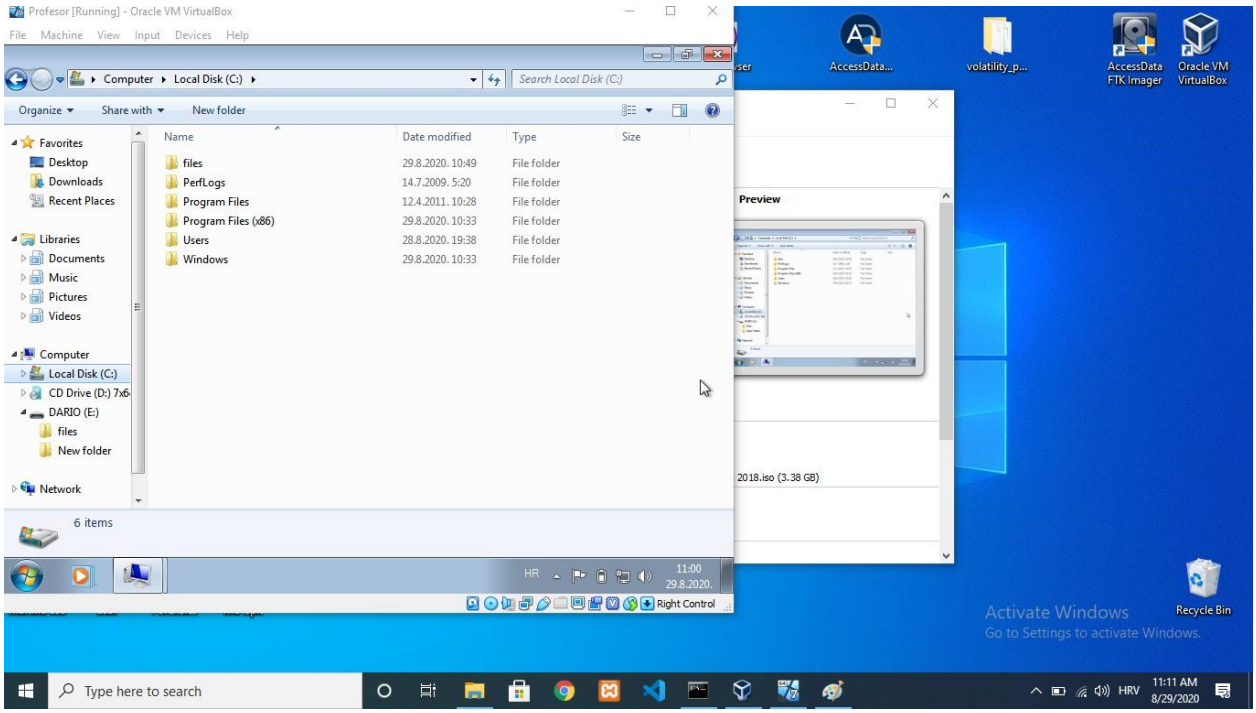
6.1.1. Napad na profesorovo računalo

Redoslijed prezentiranja učenika je sljedeći: Antonio, Dario, Bruno, Cecilio. Znači tim redoslijedom će učenici priključiti svoje USB stick-ove s prezentacijom. Napadač je učenik Dario, a upravo perspektiva Daria će biti prikazana na idućim slikama:



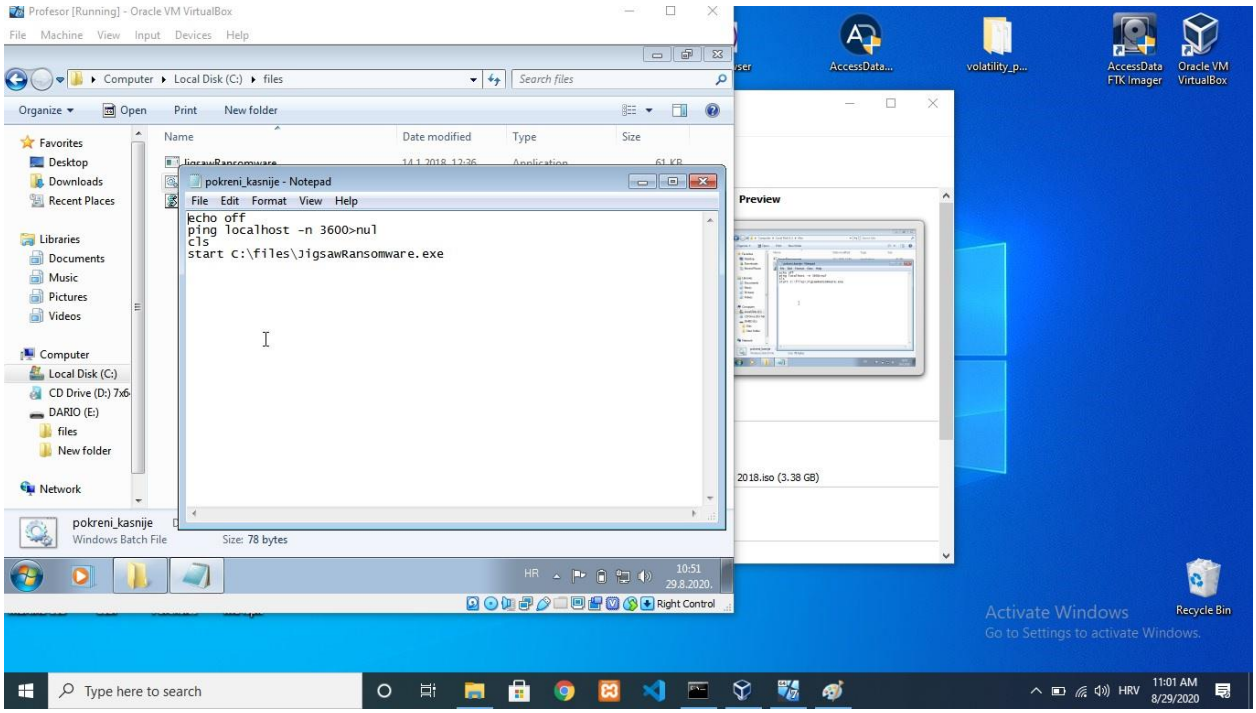
Slika 12. Kopiranje datoteke [autorski rad]

Dario priključuje USB i kopira spreman folder pod imenom „files“ koji sadrži ransomware.



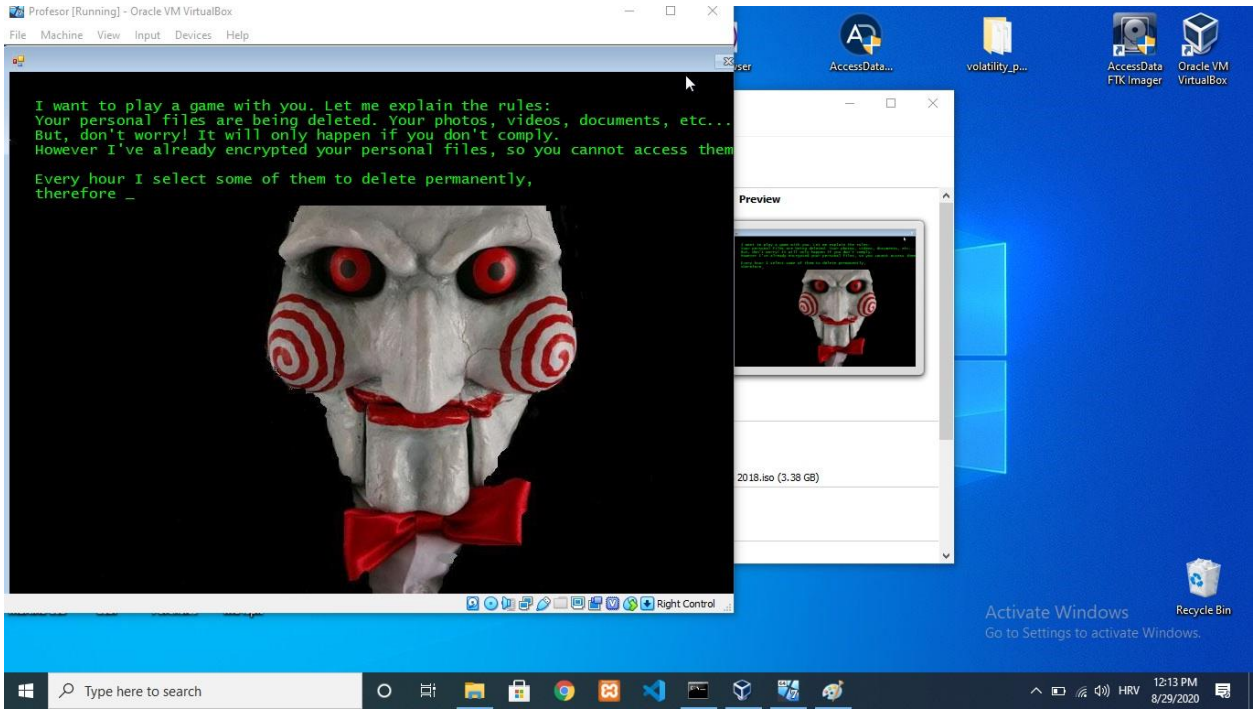
Slika 13. Lijepljenje datoteke [autorski rad]

Dario lijepi folder „files“ na C:\ disk profesorovog računala i otvara skriptu „sakrij_cmd.vbs, a na slici 14 je kratki osvrt na izgled batch skripte s naredbom: `echo off ping localhost -n 3600>nul start C:\files\JigsawRansomware.exe`.

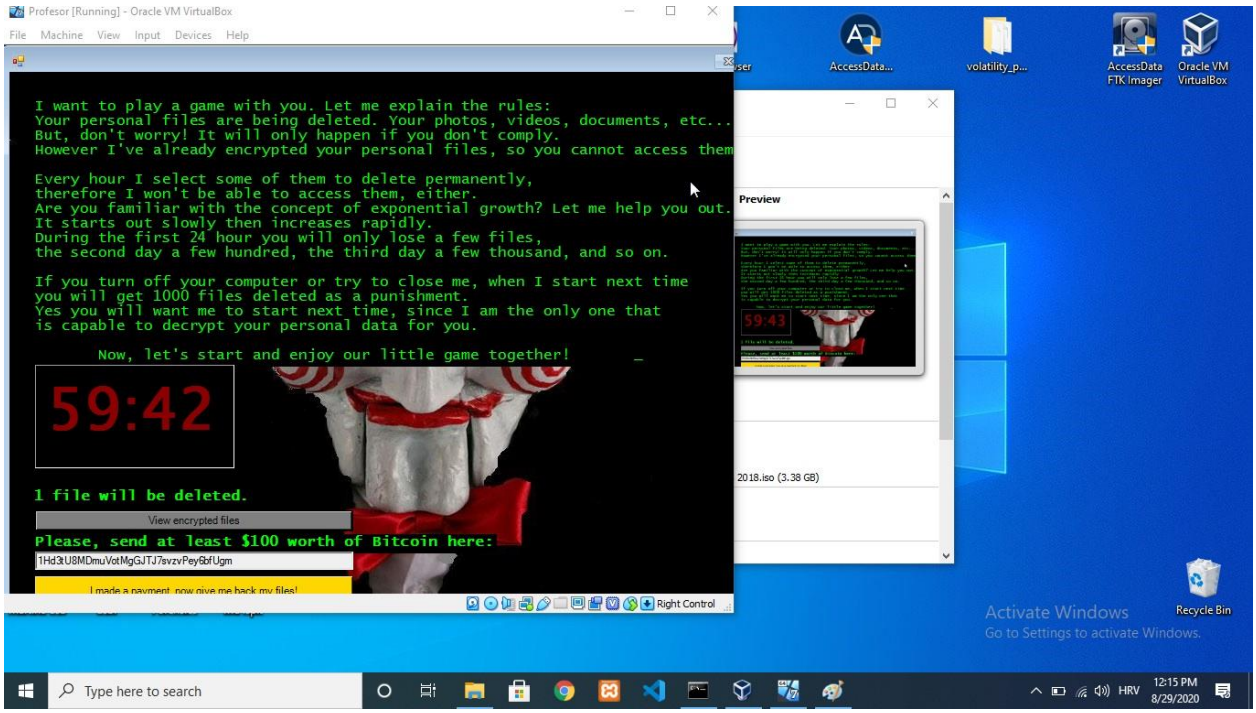


Slika 14. Zlonamjerna batch skripta [autorski rad]

Nakon sat vremena kada je već prošao određeni period vremena i svi su ujedno završili s prezentacijama, otvara se `JigsawRansomware.exe` i dobiva se iduća poruka sa slikom u dotičnom programu što je prikazano na slici 15 i 16.



Slika 15. Pojava zlonamjernog programa prvi dio [autorski rad]



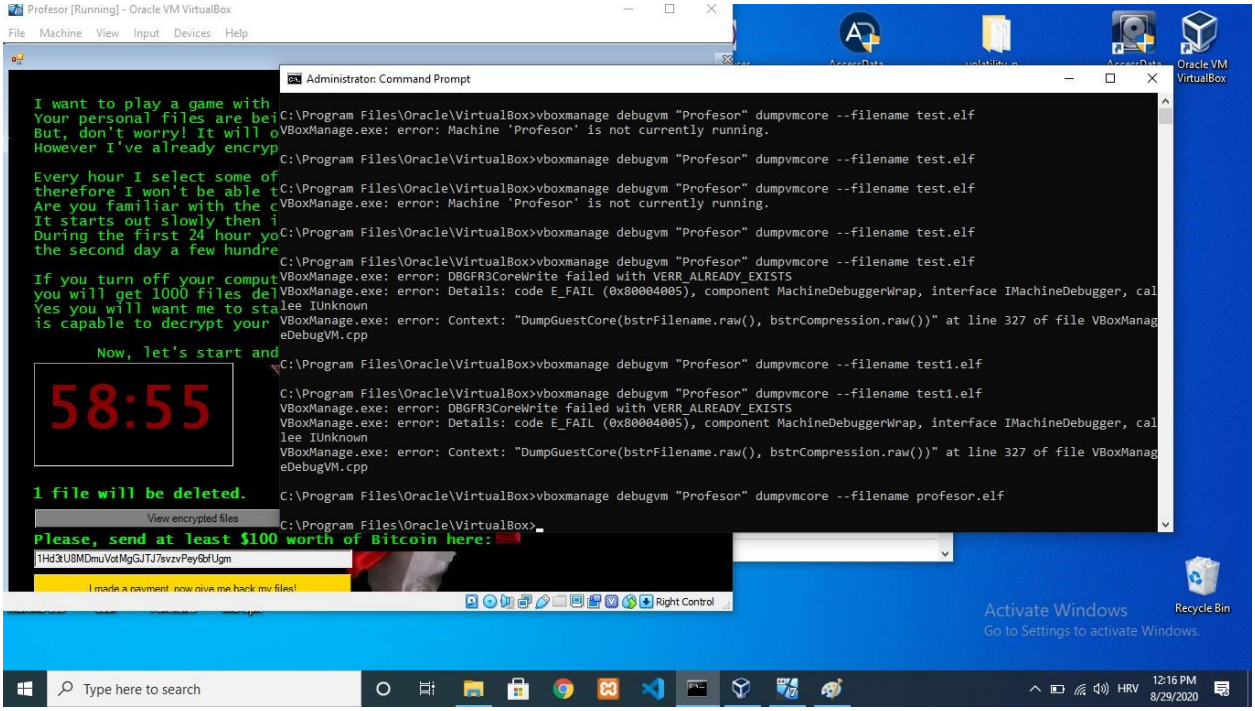
Slika 16. Pojava zlonamjernog programa drugi dio [autorski rad]

Napad je također mogao biti izvršen na automatski način tako da se skripta „sakrij_cmd.vbs“ pokrene odmah prilikom priključivanja USB stick-a na profesorovo računalo, ali kako je odavno poznato da je automatsko pokretanje (eng. *autorun*) veliki sigurnosni propust koji je popravljen u ranijim verzijama od strane Microsoft-a, u ovome radu koristit će se manualni „copy & paste“, koji neće biti primjetan, prvenstveno zbog male memorije zlonamjernog paketa. Također profesor je mogao potpuno isključiti automatsko pokretanje putem upravljačke ploče što zapravo može svatko, a pogotovo tko stalno radi s određenom frekvencijom ljudi putem vlastitog računala na način da se često uštekavaju eksterna sklopovlja kao što je USB na računalo te osobe. U takvoj neugodnoj situaciji po napadača, napad bi propao. [16] Nadalje u radu, napad je izvršen, a profesor u očaju se obraća stručnoj pomoći, gdje na red dolazi forenzičar koji uzima sliku radne memorije, te na temelju nje vrši analizu.

6.2. Perspektiva forenzičara

U realnoj situaciji, slika radne memorije bi se preuzela putem alata kao što je FTK Imager, no pošto u ovome primjeru se radi s virtualnim strojem, ta radnja je ne moguća jer je potrebno isključiti virtualizaciju na računalu, a virtualizacija pokreće virtualni stroj, ukoliko probamo napraviti takav primjer, virtualni stroj će se srušiti, točnije prikazati će se plavi ekran smrti (eng .*blue screen of death*) ili upozorenje prilikom preuzimanja slike radne memorije na kojem kaže „Unable to start driver“. [17] Zbog rada na virtualnom stroju, slika radne memorije će biti preuzeta putem „vboxmanage“ komandnog sučelja, ugrađeno u VirtualBox. [18]

Preuzimanje slike radne memorije putem vboxmanage sučelja je prikazano na slici 17, gdje je potrebno ući u direktorij gdje se nalazi VirtualBox komandom `cd`, te zatim izvršiti preuzimanje slike radne memorije komandom: `vboxmanage debugvm "Profesor" dumpvmcore --filename profesor.elf` [19]



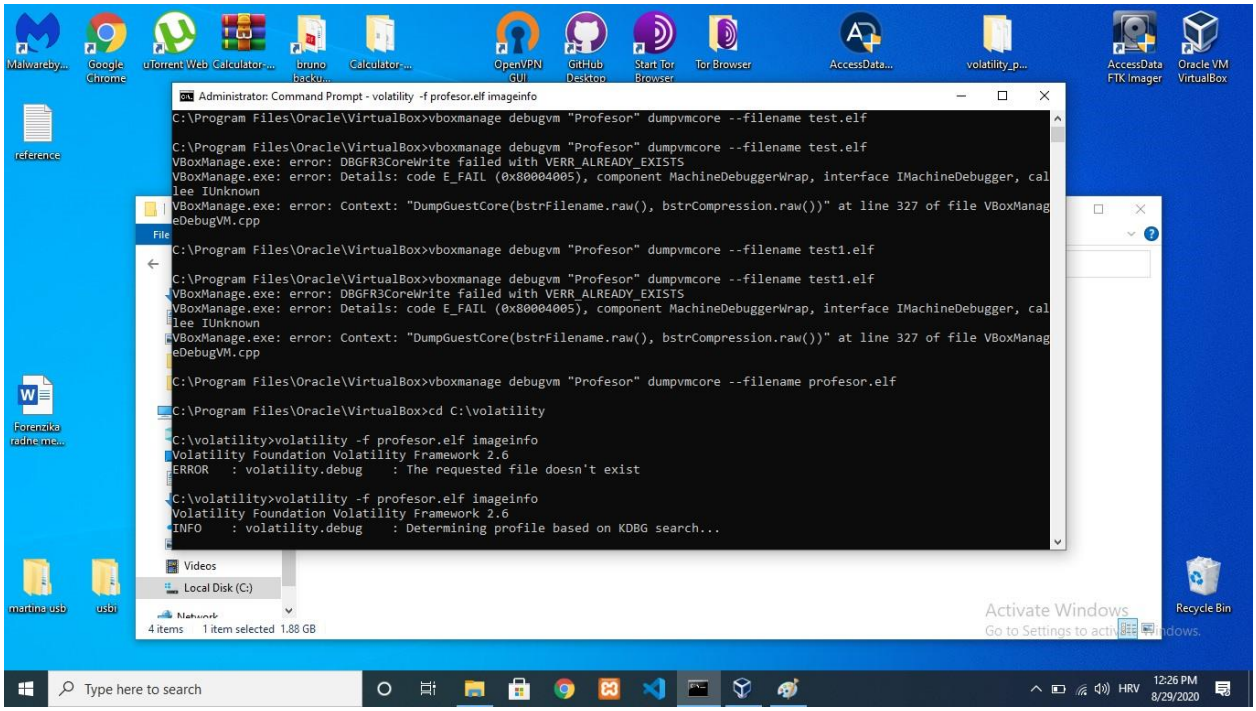
Slika 17. Preuzimanje slike radne memorije putem vboxmanage-a [autorski rad]

6.2.1. Analiza slike radne memorije

Nakon uspješnog preuzimanja slike radne memorije, potrebno je sliku pod nazivom „profesor.elf“ postaviti u direktorij gdje se nalazi Volatility, komandno sučelje u kojem vršimo analizu slike radne memorije. [12, p. 8.]

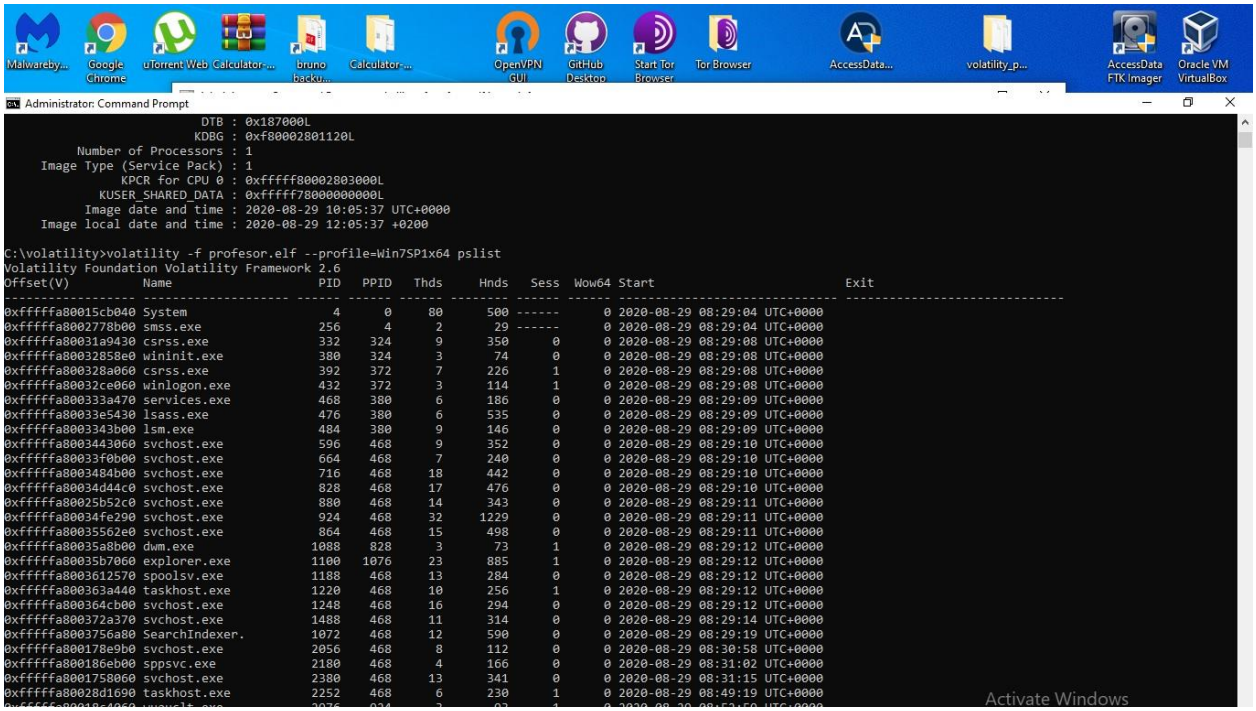
Zatim se ulazi u cmd.exe gdje je potrebno promjeniti radni direktorij naredbenog retka u direktorij u kojem se nalazi Volatility, a to je `C:\volatility`, pozicioniranje se vrši naredbom `cd`, a puni kod glasi: `cd c:\volatility`. [12, p. 6.] Nakon pozicioniranja u direktorij, kako bi alat Volatility znao koju sliku memorije treba analizirati, u pozivu alata iz naredbenog retka koristi se parametar `-f` iza kojeg slijedi putanja do slike memorije, zatim potrebno je odrediti koji operacijski sustav se nalazio na računalu s kojeg je snimljena slika memorije, a ta informacija potrebna je alatu Volatility kako bi ispravno radio analizu. Alat Volatility ima naredbu `imageinfo` koji služi za prepoznavanje profila tj. inačice operacijskog sustava s kojeg je snimljena slika memorije. U pozivima alata Volatility koristiti se parametar `--profile=` kako bi Volatility znao pronaći i interpretirati strukture u memoriji specifične za tu inačicu operacijskog sustava. Cijeli kod za

promjenu direktorija: `cd c:\volatility`, a za pronalazak profila: `volatility -f profesor.elf imageinfo` [12, p. 8.]



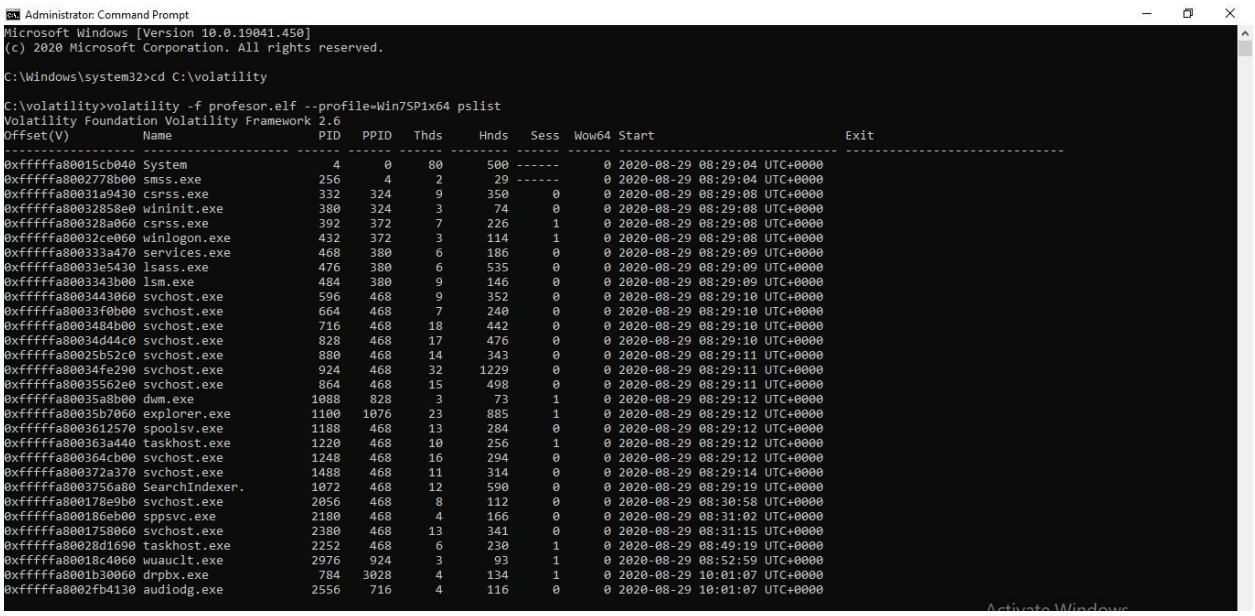
Slika 18. Traženje profila u Volatility alatu [autorski rad]

Profil koji će biti analiziran je „Win7SP1x64“, a odmah nakon saznatog profila vrši se ispis popisa procesa koji su bili pokrenuti u trenutku preuzimanja slike radne memorije operacijskog sustava Windows, a koristi se naredba `pslist`. Ispis naredbe istovjetan je popisu procesa u upravitelju zadataka (eng. *task manager*) sustava Windows.



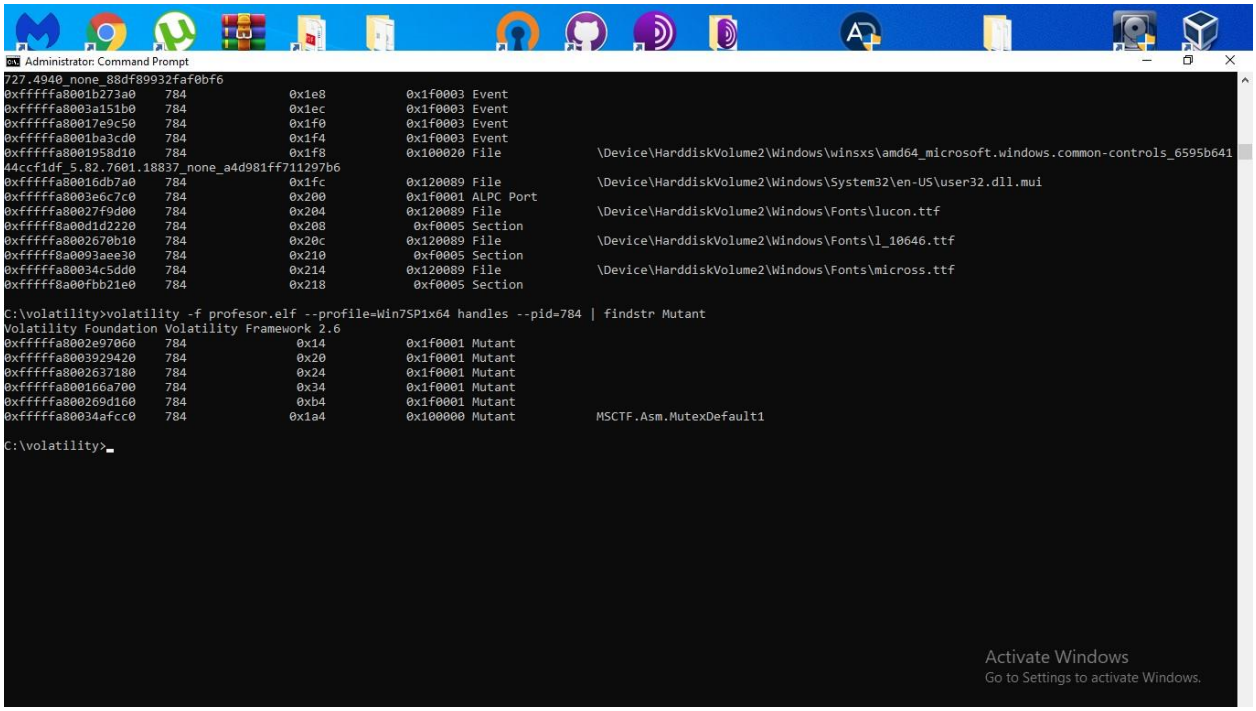
Slika 19. Popis pokrenutih procesa uz naredbu pslist [autorski rad]

U ispisu naredbe na slici 19 koja glasi `volatility -f profesor.elf –profile=Win7SP1x64 pslist` moguće je vidjeti uz ostala obilježja procesa, imena procesa koji su bili pokrenuti. Važno je napomenuti kako ovo ne mora biti potpuna lista procesa pokrenutih u operacijskom sustavu. Moguće je da je zlćudni program sakrio svoj proces iz liste procesa te ga je zato potrebno potražiti drugim metodama, primjerice naredbom psscan. [12, p. 9.]Također potrebno je primjetiti razliku između vremena na virtualnom stroju i host-u, razlika je točno dva sata. [autorski rad]



Slika 20. Svi pokrenuti procesi [autorski rad]

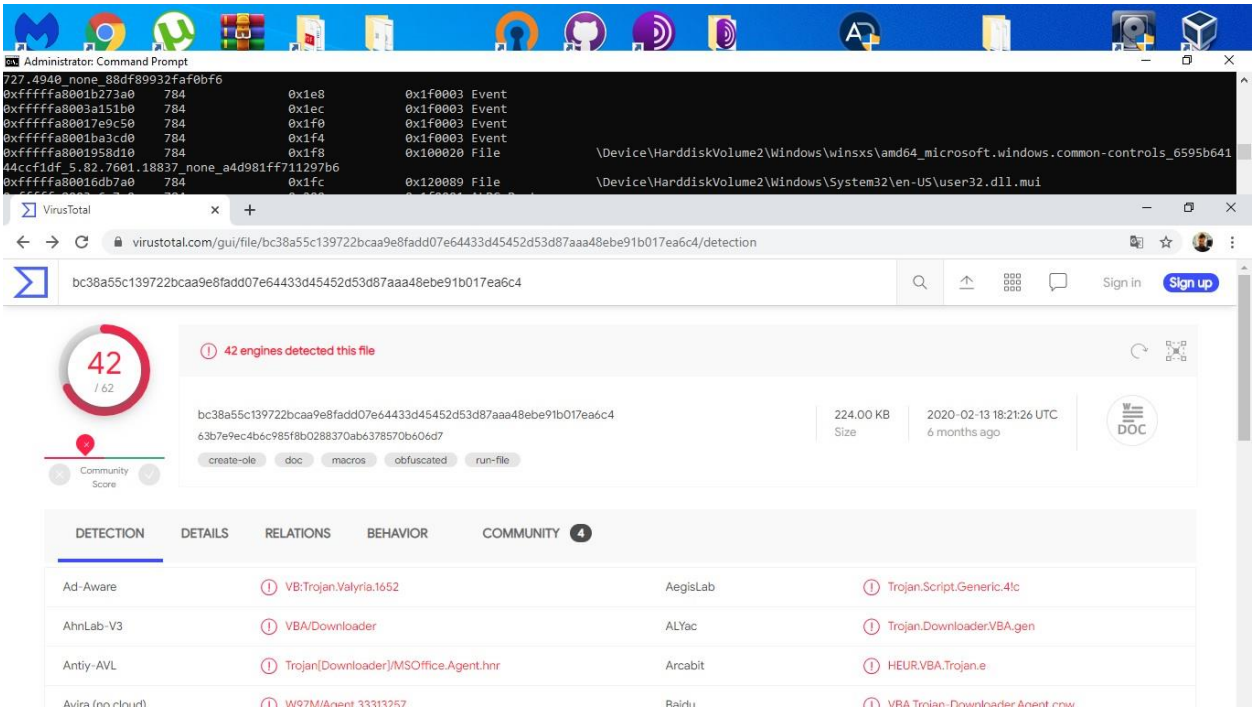
Lista svih procesa prikazana je na slici 20, gdje svi procesi dijele isto vrijeme pokretanja osim `drpbx.exe` i `audiodg.exe`. `Drpbx.exe` će odmah biti analiziran jer je neizgled izgeneriranog karaktera. Zlonamjerni program često stvara mutex kako se ne bi više instanca zlonamjernog programa pokrenulo i međusobno si smetalo, npr. više puta šifriralo istu datoteku. Unutar jezgre operacijskog sustava Windows, mutex objekti se ne zovu Mutex, već Mutant. Zato kako bi se iz ispisa filtrirale ručke mutex objekata potrebno je pokrenuti sljedeću naredbu kao što je prikazano na slici 21 koja glasi: `volatility -f profesor.elf --profile=Win7SP1x64 handles --pid=784 | findstr Mutant`.



Slika 21. Filtriranje ručki na temelju mutex objekta [autorski rad]

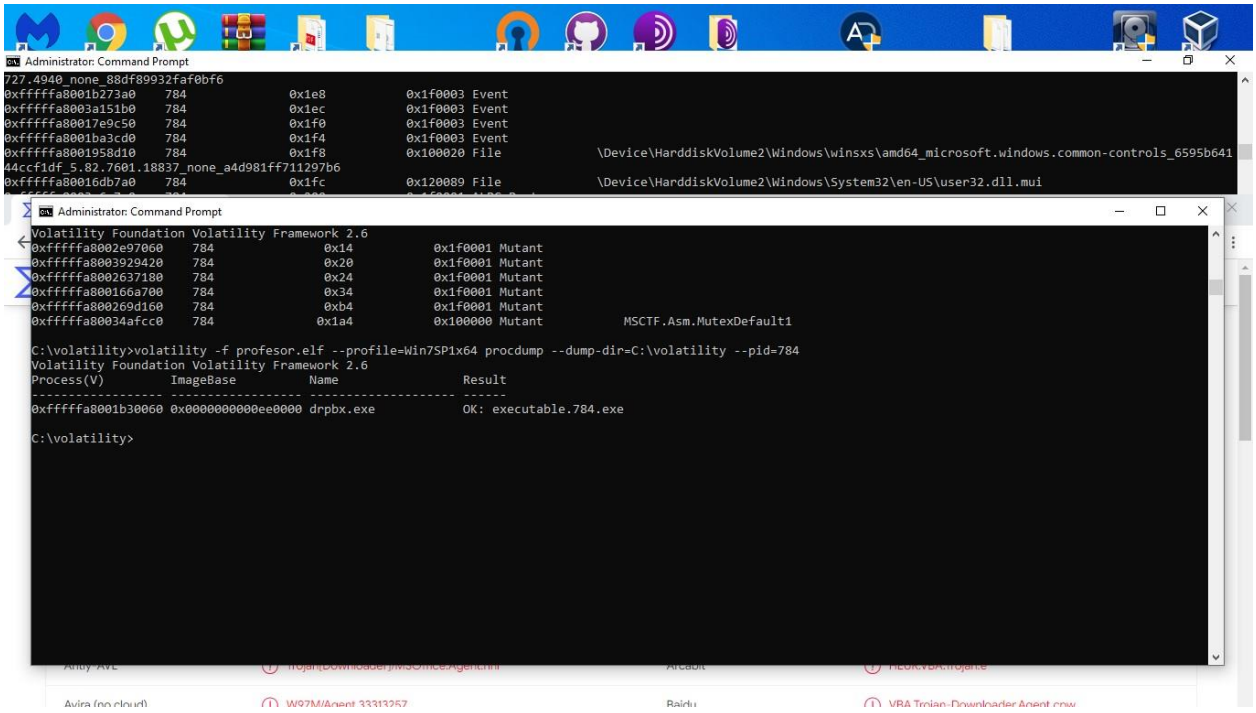
6.2.2. Prepoznavanje zlonamjernog koda

Mutex objekti koji nemaju ime koriste se lokalno, unutar jednog procesa, dok se za sinkronizaciju više procesa koriste mutex objekti s imenom. Upravo ti mutex objekti s imenom su zanimljivi u ovom kontekstu – u ovom slučaju to je: „MSCTF.Asm.MutexDefault1“. Iako na prvi pogled imena možda i ne izgleda sumnjivo, korisno je internetskim tražilicama pretražiti da li se to ime pojavljivalo kod drugih zlonamjernih softvera, pretraga će biti izvršena na VirusTotal.com[https://www.virustotal.com/gui/file/bc38a55c139722bcaa9e8fadd07e64433d45452d53d87aaa48ebe91b017ea6c4/behavior/Tencent%20HABO] [5, p. 11.]



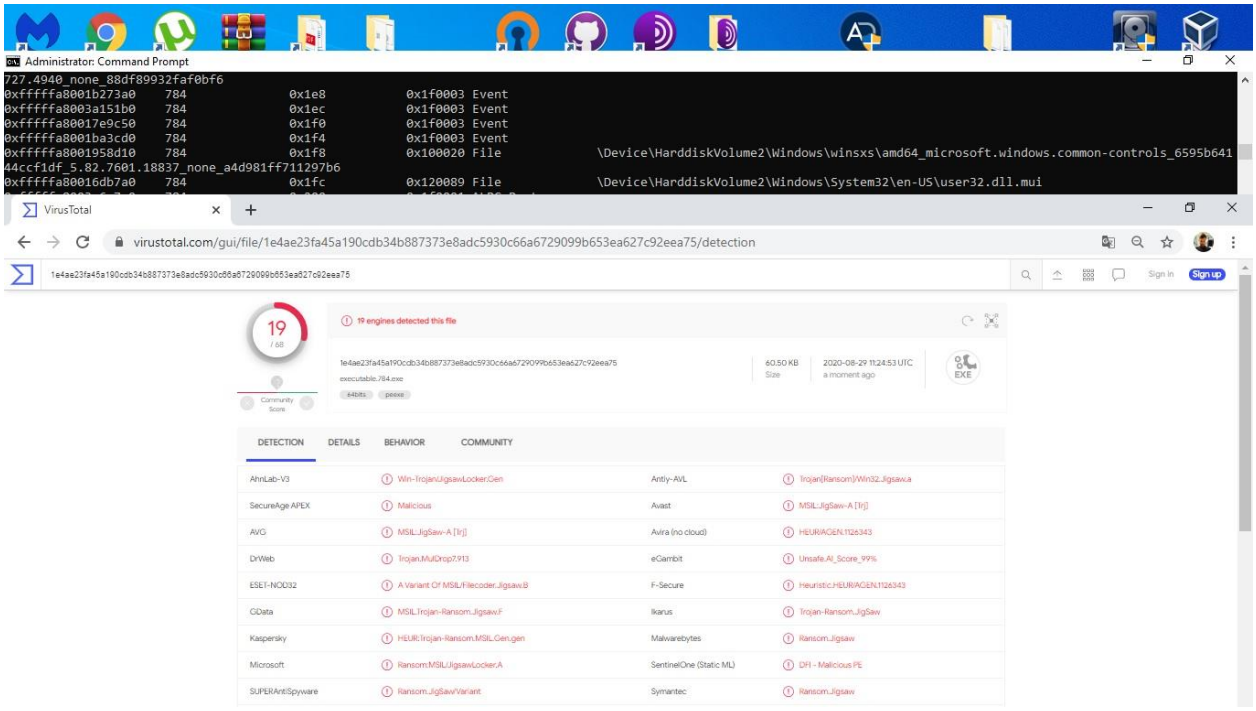
Slika 22. Drpbx.exe proces na VirusTotal.com [autorski rad]

Kao što se vidi na slici 22, mutex objekt pod imenom „MSCTF.Asm.MutexDefault1“ se pojavljivao do sad na trojancima, što daje dovoljan razlog za detaljniju analizu procesa „drpbx.exe“. Kako bi utvrdili da je uistinu dotični proces izvor ransomware-a naredbom `procdump`, Volatility može iz procesa pokušati rekonstruirati izvršnu (`.exe`) datoteku. Naredbi `procdump` je, uz identifikator procesa za rekonstrukciju, potrebno zadati i naredbu `-dump-dir=` gdje je vrijednost jednaka putanji do direktorija u koji će biti spremljena datoteka. [5, p. 11.]Putanja do direktorija će jednostavno biti C:\volatility, što znači da puna naredba glasi: `volatility -f profesor.elf --profile=Win7SP1x64 procdump --dump-dir=C:\volatility --pid=784` [autorski rad]



Slika 23. Preuzimanje zlonamjernog procesa [autorski rad]

Rekonstruirana izvršna datoteka će također biti učitana na ranije spomenuti VirusTotal – Web stranicu koja učitane datoteke predaje na analizu većem broju antivirusnih alata te korisniku prikazuje rezultat analize. Na taj način moguće je lako saznati što razni antivirusni alati misle o toj datoteci – smatraju li da ta datoteka sadržava zlonamjerni softver, i ako da, što misle koji konkretno zlonamjerni softver sadržava. [5, p. 12.]

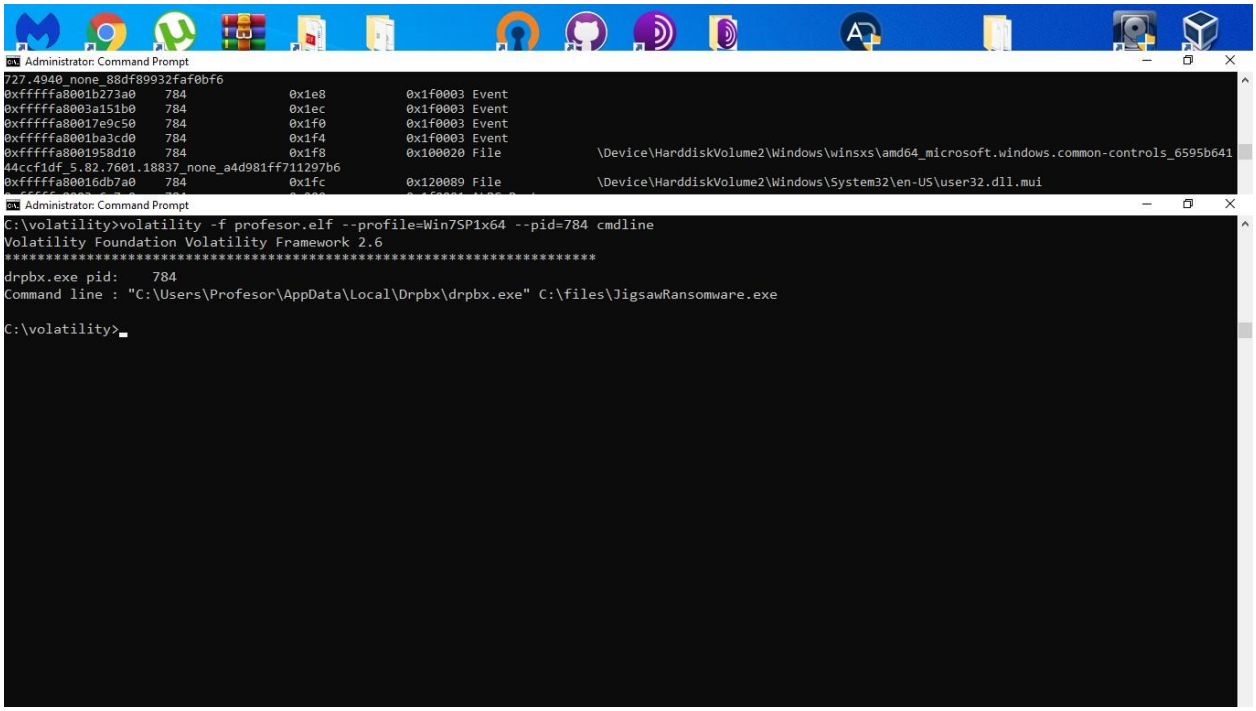


Slika 24. Prikaz rekonstruirane izvršne datoteke na VirusTotal.com [autorski rad]

Na slici 24 je vidljivo da VirusTotal tvrdi da je rekonstruirana izvršna datoteka jednaka JigsawRansomware-u.

6.2.3. Analiza pokretanja zlonamjernog koda

Pošto je ne jasno kako se proces „drpbx.exe“ pokrenuo sam od sebe u 10:01 h, jedan od slučaja koji može biti jest pokretanje procesa preko komandne linije, a potrebno je saznati s kojim argumentima naredbene linije je program pozvan, a upravo to je moguće saznati naredbom `cmdline`. Argumentom `--pid=784` moguće je ograničiti njen rad samo na prethodno navedeni proces koji želimo detaljnije istražiti, kako bi se smanjila količina ispisanih podataka. [5, p. 8.]



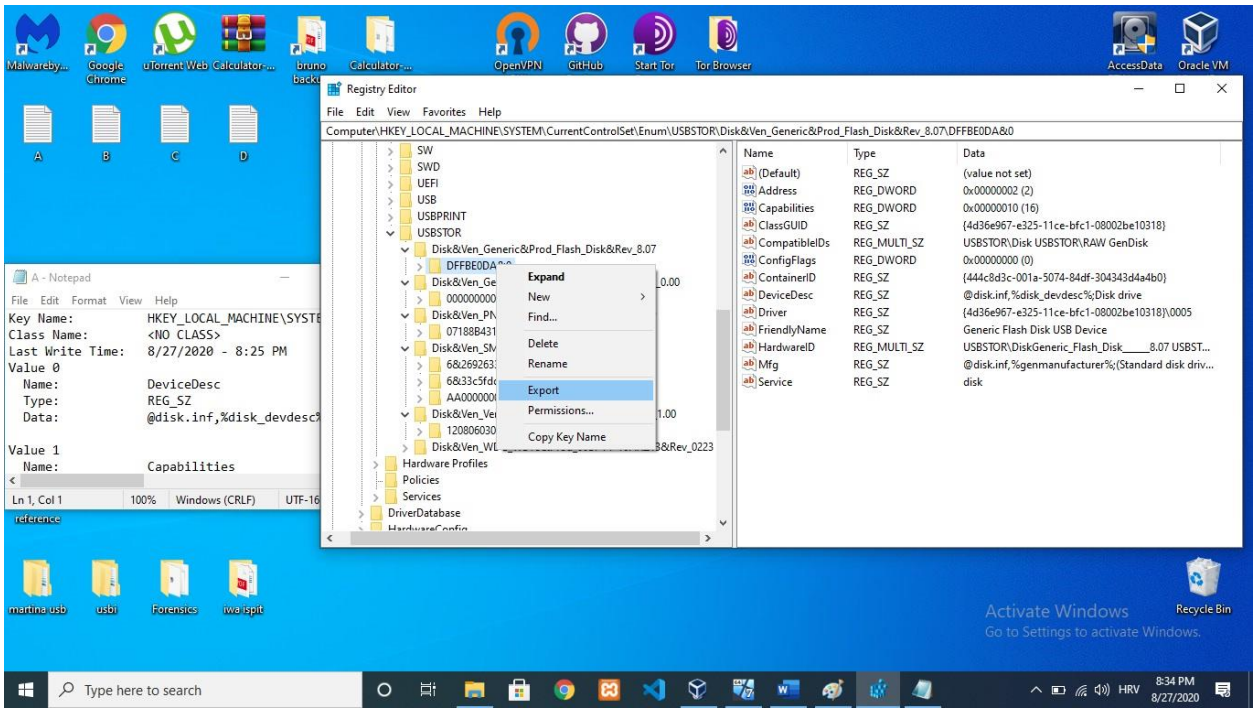
Slika 25. Analiza komandne linije [autorski rad]

Na slici 25 je vidljivo da u naredbi koja glasi: `volatility -f profesor.elf –profile=Win7SP1x64 --pid=784 cmd` jest upisana putanja do datoteke koja će izvršiti datoteku `C:\files\JigsawRansomware.exe`, gdje forenzičar dolazi do pretpostavke da se radi o kasnom pokretanju zlonamjernog koda pomoću određene skripte, te također ima uvid gdje se nalazi zlonamjerna datoteka. Forenzičar potražuje datoteku, te prilikom pronalaženja sve mu postaje jasno, radi se o tihom načinu rada programa, gdje se `JigsawRansomware.exe` pokreće nakon 3600 sekundi od pokretanja batch skripte. Proces `drpbx.exe` se pokreće u 10:01 h, oduzimajući 3600 sekundi, što je 1 h, zaključak govori da je postupak napada pokrenut u 9:01 h. [autorski rad]

6.2.4. Analiza priključenih USB stick-ova učenika

Nakon utvrđenog vremena pokretanja napada potrebno je saznati napadača. Kad god se priključi USB u računalo, stvara se ključ registra s imenom "USBSTOR". Ovaj ključ registra pohranjuje sve informacije koje operacijski sustav treba o tom USB uređaju. Podaci kao što su serijski broj, manualno dodano ime ukoliko postoji, vremenska oznaka pristupanja USB stick-a računalu. Određene informacije nije moguće jasno vidjeti u samom registru, te je potrebno eksportirati ključ iz registra kao tekstualnu datoteku, kao jednu od metoda u uvid korisnim

informacijama. [20] Vremenska oznaka USB stick-a može služiti kao izravan dokaz, a te iste vremenske oznake nalaze se u registru ključeva u putanji `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\` koja detaljno prikazuje putanju do identifikatora USB stick-a, te preuzimanjem ključa određenog USB stick-a na radnu površinu kao tekstualni dokument i priložene podatke o određenom USB stick-u kao što je „Last write time“ što je potrebno u ovoj istrazi. [21, pp. 1-2]

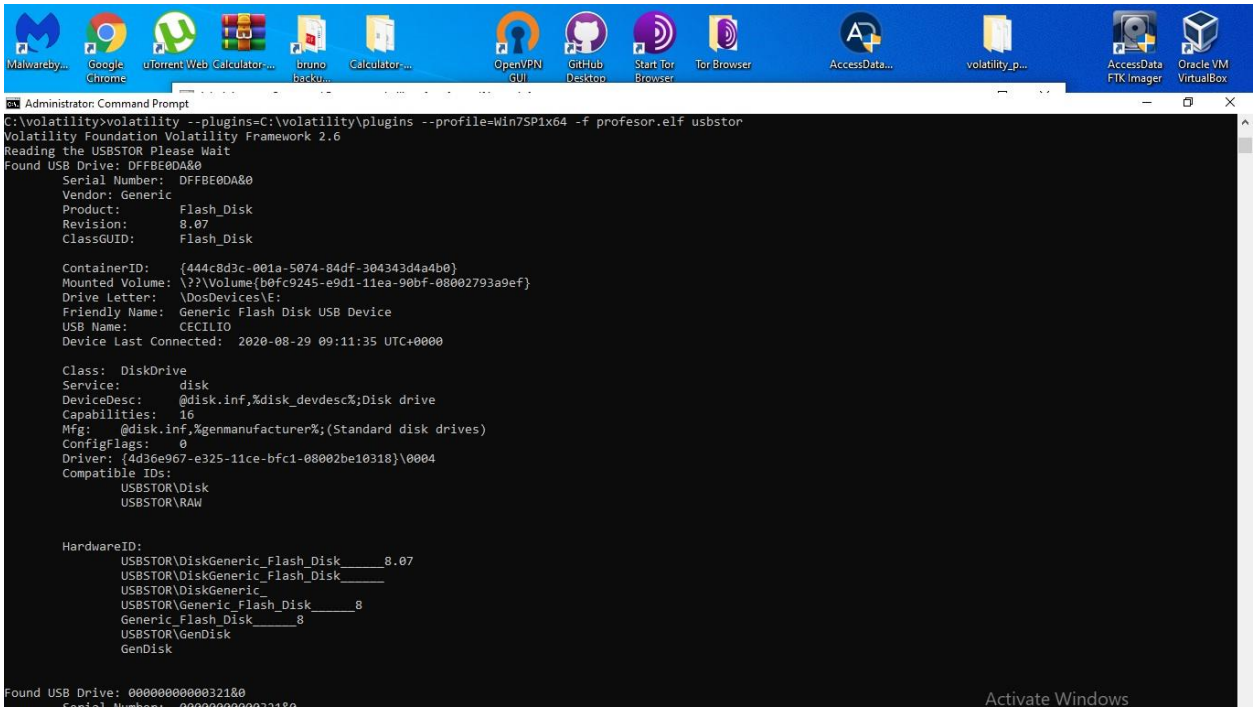


Slika 26. Putanja u registru do ključeva USB stick-ova [autorski rad]

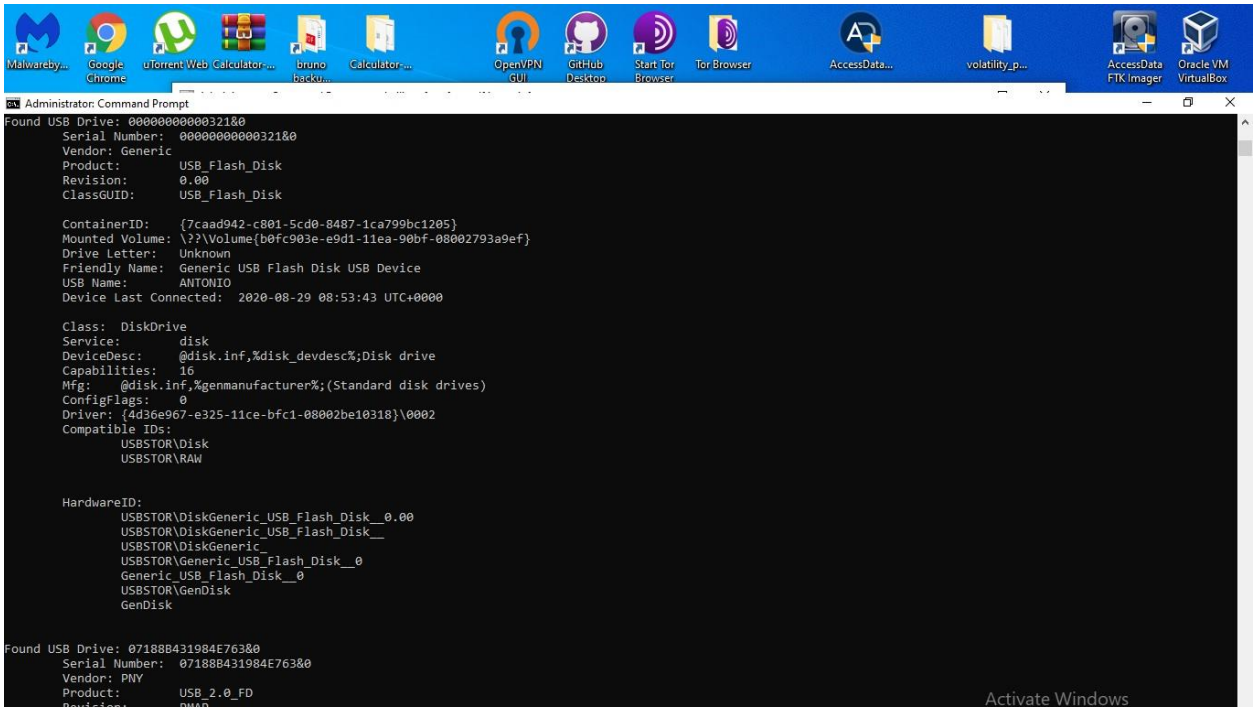
Naravno, podatke kao što je vremenska oznaka treba dohvatiti iz registra snimljene radne memorije, taj proces može biti ubrzan pomoću dodatka na Volatility alatu koji ne dolazi u originalnom paketu alata, a dodatak nakon instalacije, koja zahtjeva samo kopiranje u direktorij gdje je instaliran Volatility alat, izravnim upisom u komandnu liniju prikazuje podatke o USB stick-ovima.

Poziva se na `volatility --plugins=plugindir --profile=Win7SP1x64 -f win7mem.img usbstor`, a kod u ovome slučaju glasi: `volatility --plugins=C:\volatility\plugins --profile=Win7SP1x64 -f profesor.elf usbstor`

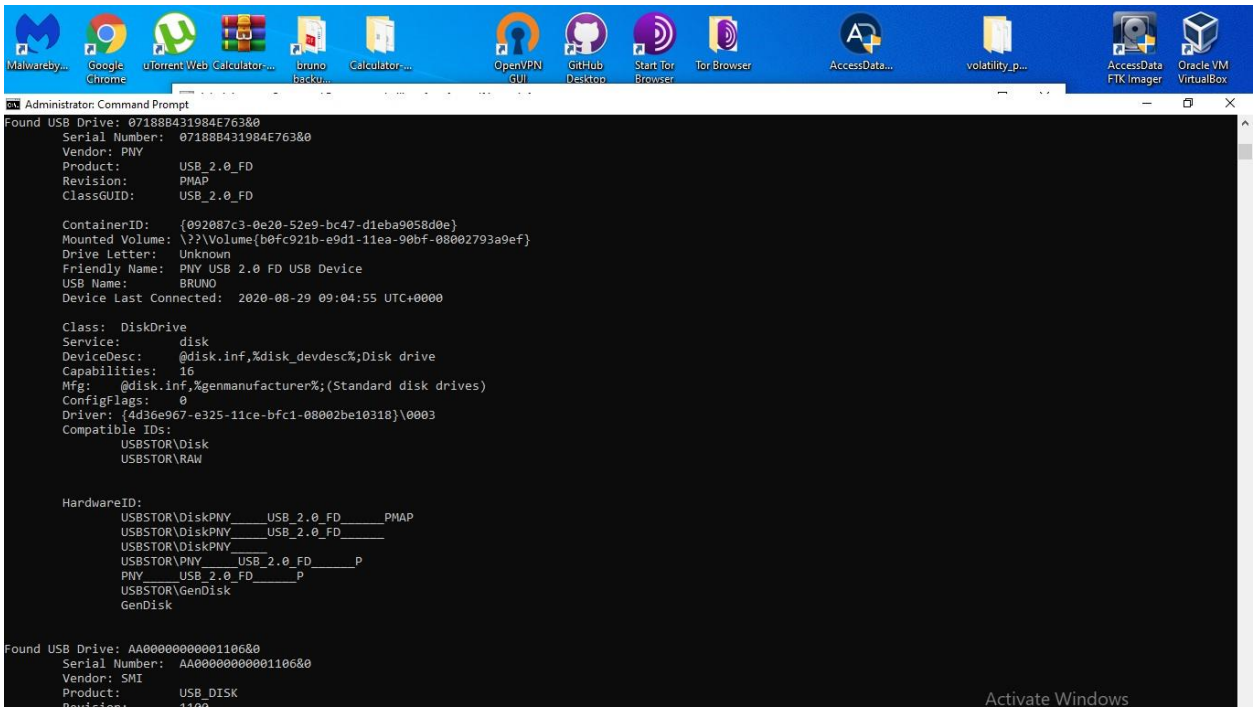
[Preuzeto s: https://github.com/kevthehermit/volatility_plugins] Sljedeće slike prikazuju popis USB stick-ova učenika koji su sudjelovali u prezentaciji prilikom napada.



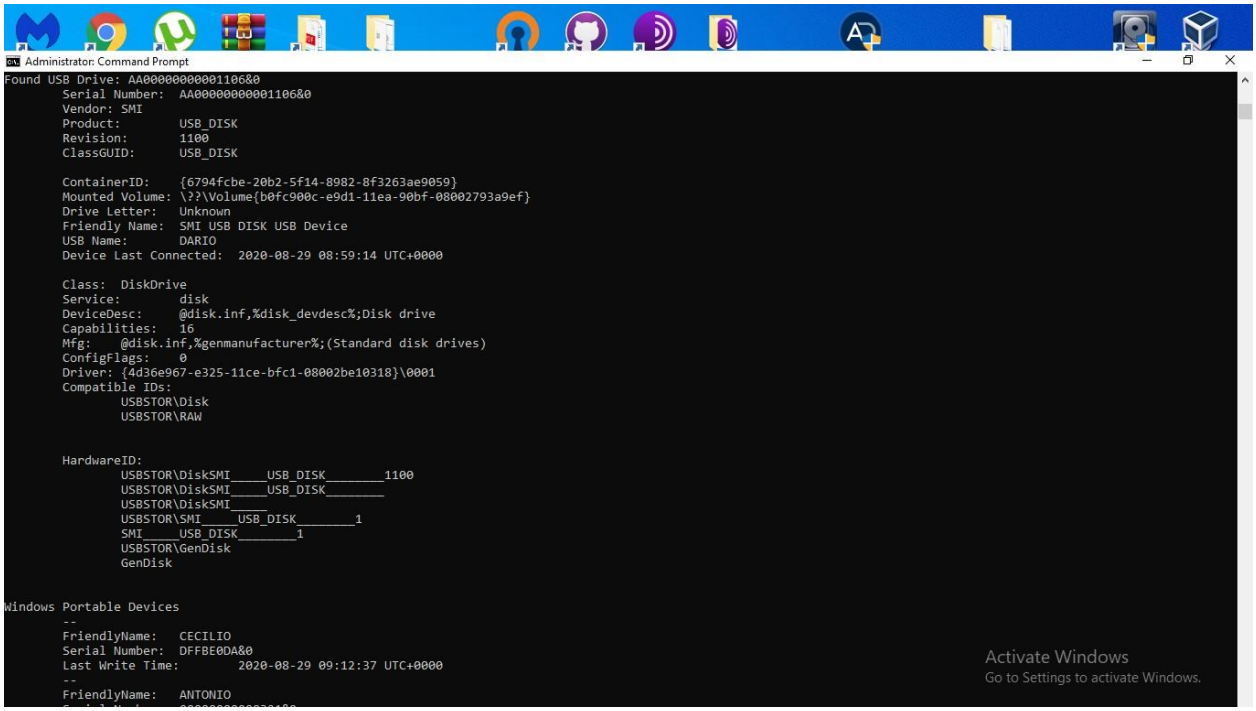
Slika 27. Informacije o USB stick-u učenika Cecilio [autorski rad]



Slika 28. Informacije o USB stick-u učenika Antonio [autorski rad]



Slika 29. Informacije o USB stick-u učenika Bruno [autorski rad]



Slika 30. Informacije o USB stick-u učenika Dario [autorski rad]

USBSTOR dodatkom, forenzičar ima jasan i korisničko prijateljski (eng. *user friendly*) uvid u sve informacije o USB stick-ovima kao što je serijski broj, produkt, ime uređaja, vremenska oznaka zadnje konekcije USB uređaja s računalom. Na slikama 27, 28, 29 i 30 vidljivi su svi opisani podaci učenika koji su prezentirali svoje prezentacije putem USB stick-a. Fokus će biti stavljen na vrijeme zadnje konekcije uređaja (eng. *device last connected*), a redom izbačeni rezultati su Cecilio: 2020-08-29 09:11:35, Antonio: 2020-08-29 08:53:43, Bruno: 2020-08-29 09:04:55 i Dario: 2020-08-29 08:59:14. Ovim putem se jasno može vidjeti da je napadač učenik pod imenom Dario, koji je priključio svoj USB stick u točno 08:59 h što znači da prilikom priključenja svog USB stick-a Dario kopira datoteku „files“, ljepi ju na C:\ disk, otvara zaljepljenu datoteku „files“ i pokreće napad otvarajući skriptu pod nazivom `sakrij_cmd.vbs`. Proces `drpbx.exe` koji je pokrenut u 10:01, pokrenut je batch skriptom pod nazivom `pokreni_kasnije.bat` koja radi latenciju od jedan sat na isti proces, a batch skripta je pokrenuta vbs skriptom pod nazivom `sakrij_cmd.vbs` koja čini batch skriptu ne vidljivom, što je već zapravo i utvrđeno, ali ponovljeno, a kašnjenje kreiranja procesa `drpbx.exe` točnije otvaranja izvršne datoteke `JigsawRansomware.exe` od otprilike jednu minutu ovisi o performansama računala, pošto je u ovom slučaju proces pokrenut na virtualnom stroju koji ima karakteristike kao što su

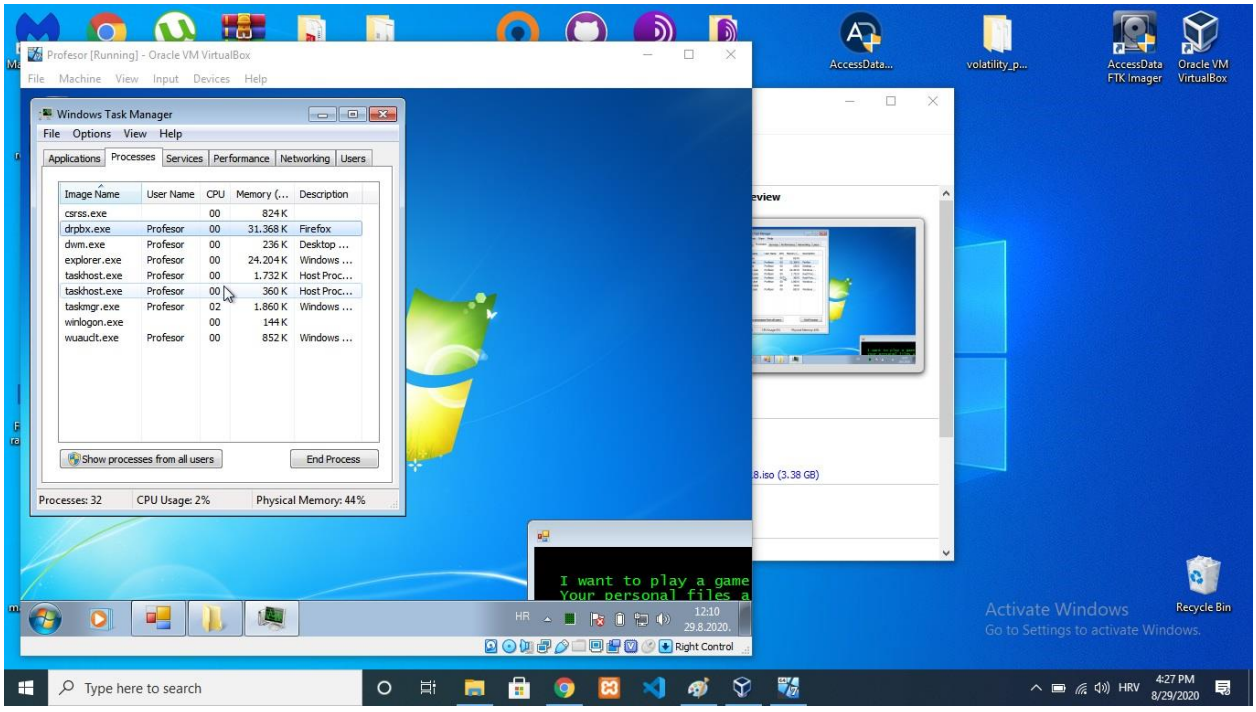
prikazane na slici 4, kašnjenje od otprilike jednu minutu je sasvim očekivano. Zaključak je donesen i pokriven dokazima da je učenik pod imenom Dario napadač. [autorski rad]

6.3. Oporavak od napada

Nakon riješene forenzičke istrage, slijedi proces oporavka žrtvinog računala u što spada ubijanje i sprječavanje ponovnog pokretanja zlonamjernog procesa, dekriptiranje podataka i micanja svih stavki zlonamjernog programa u antivirusnom programu.

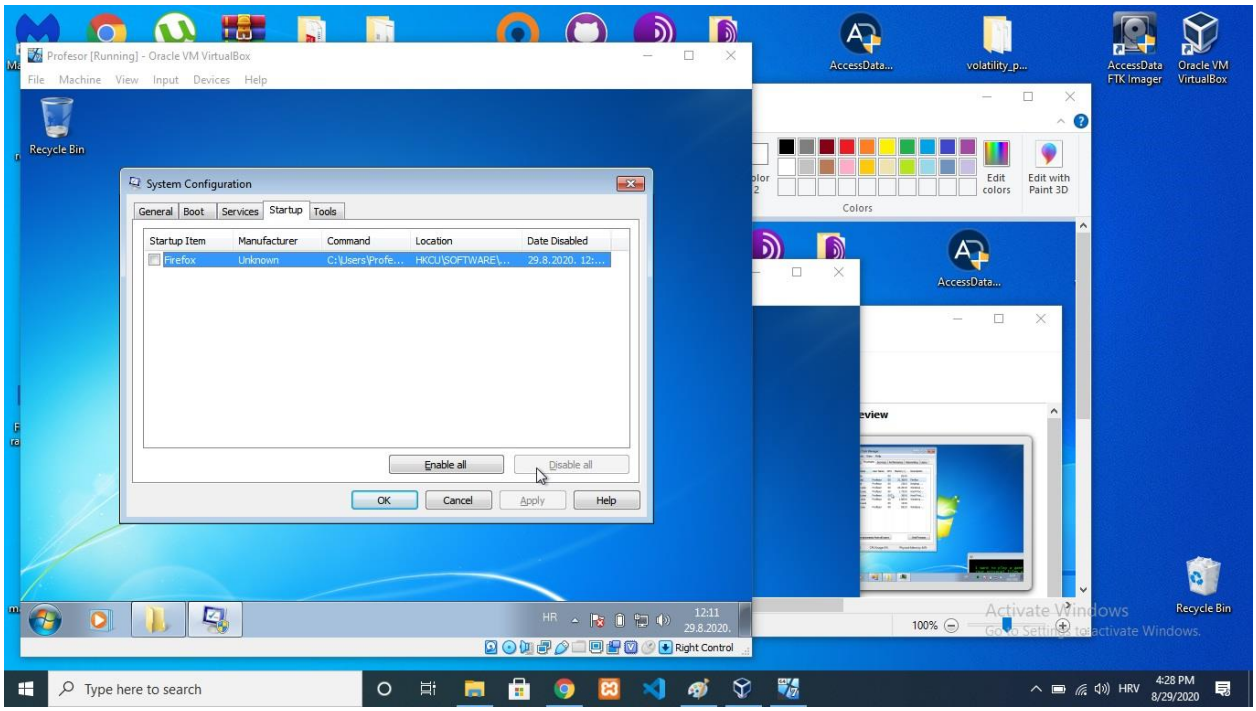
6.3.1. Ubijanje procesa zlonamjernog programa

Prvo što je potrebno jest ubiti zlonamjerni proces `drpbx.exe`, točnije kompletno stablo procesa, aktivni proces moguće je vidjeti u „Task manager“ programu (otvara se pritiskom `CTRL+ALT+DEL`) kao što je prikazano na slici 31 gdje desnim klikom na proces odabiremo „end process tree“.



Slika 31. Prikaz drpbx.exe procesa [autorski rad]

Zatim slijedi sprječavanje ponovnog pokretanja programa tako da kroz „run“ ulazimo u konfiguraciju sistema tako da u „run“ upisujemo „msconfig“ gdje pod sekcijom „startup“ isključujemo „Firefox“ jer je upravo „Firefox“ jednak opisu procesa `drpbx.exe` što je vidljivo na prethodnoj slici 32. [22]

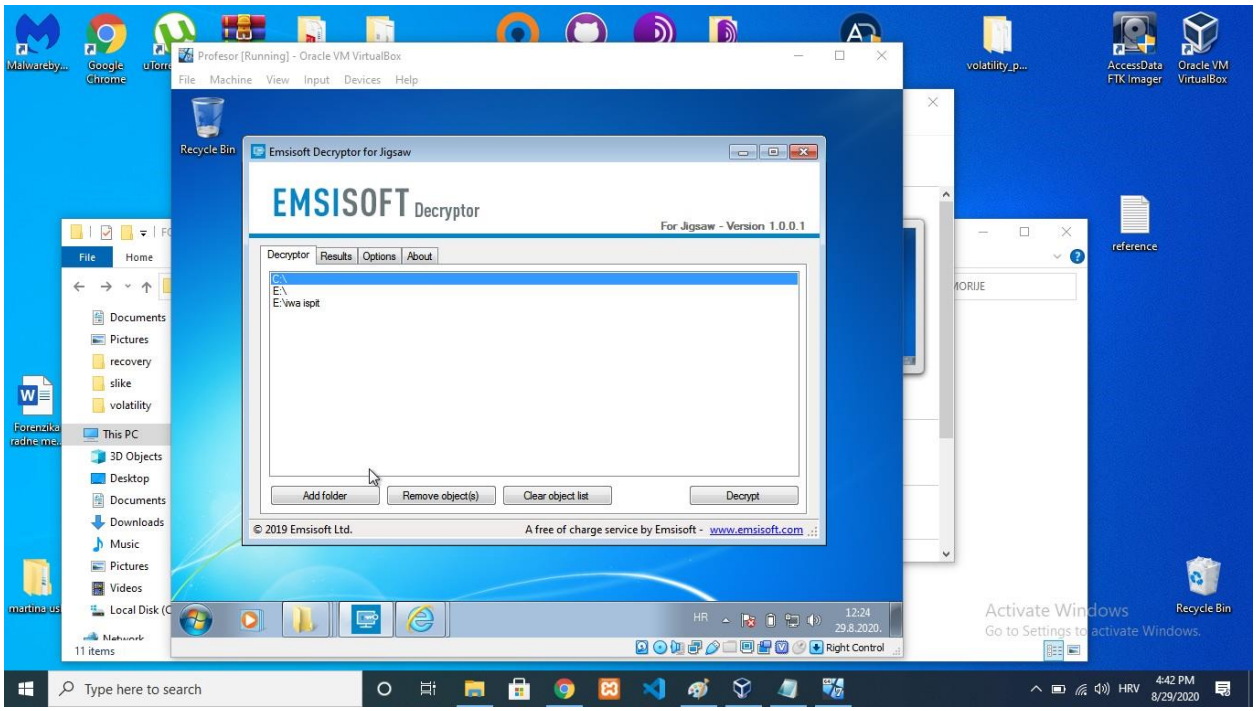


Slika 32. Prikaz konfiguracije sistema [autorski rad]

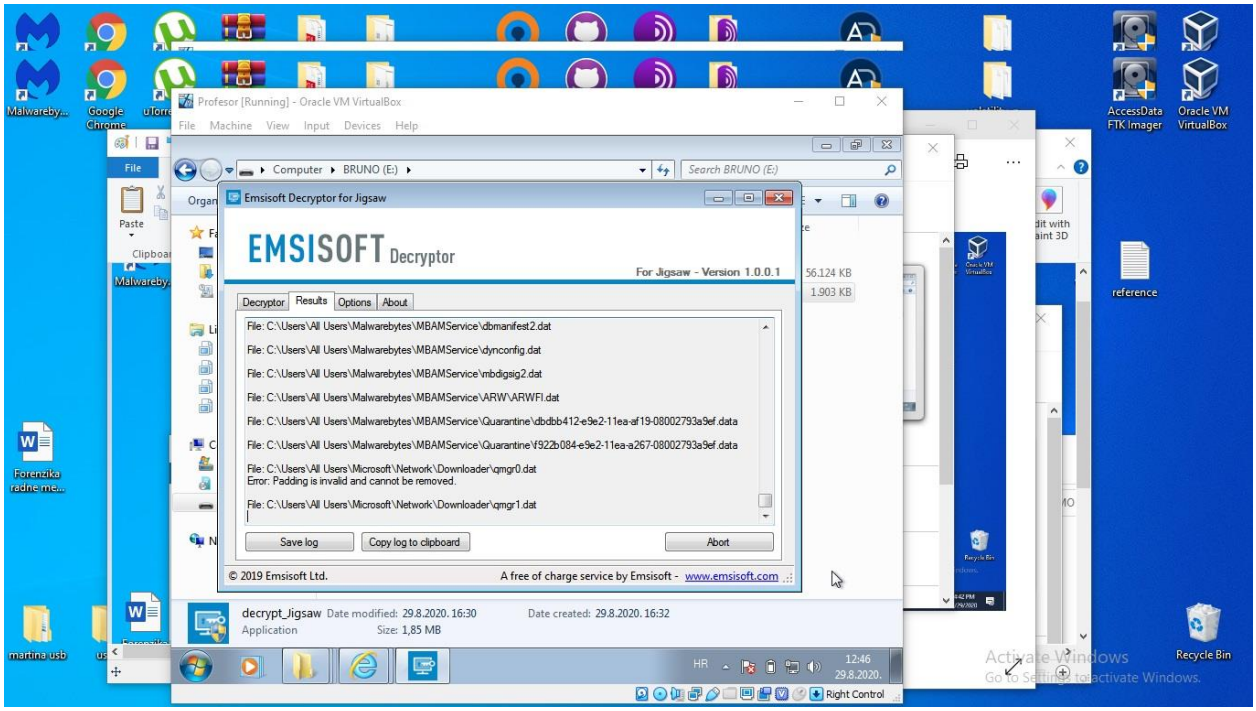
6.3.2. Dekriptiranje podataka

Proces dekriptiranja podataka je vrlo složen proces koji uključuje pronalaženje ključa za dekriptiranje, te izradu programa za dekriptiranje. Srećom, kako je JigsawRansomware već poznat ransomware, postoje već izrađeni programi za dekripciju kao što je „Jigsaw Decrypter“[Preuzeto s: https://www.bleepingcomputer.com/download/jigsaw-decrypter/] kod kojeg je potrebno otvoriti program, izabrati datoteku ili cijeli disk, što je u ovom slučaju napada da se dekriptiraju apsolutno svi podaci koji su kriptirani, tj. dodana im ekstenzija .fun, .kkk, .btc, .gws, .porno, .pornoransom, .payransom, .paybtcs, .AFD, .payms, .pays, .paym, .paymrss, .payrms,

.paymts, .paymds, .paymrts, .epic, te pritiskom na gumb „Decrypt“ dekriptira sve datoteke na izabranom disku, što je u ovom slučaju disk C. Proces je prikazan na slici 33 i 34. [22]



Slika 33. Dekriptiranje podataka prvi dio [autorski rad]

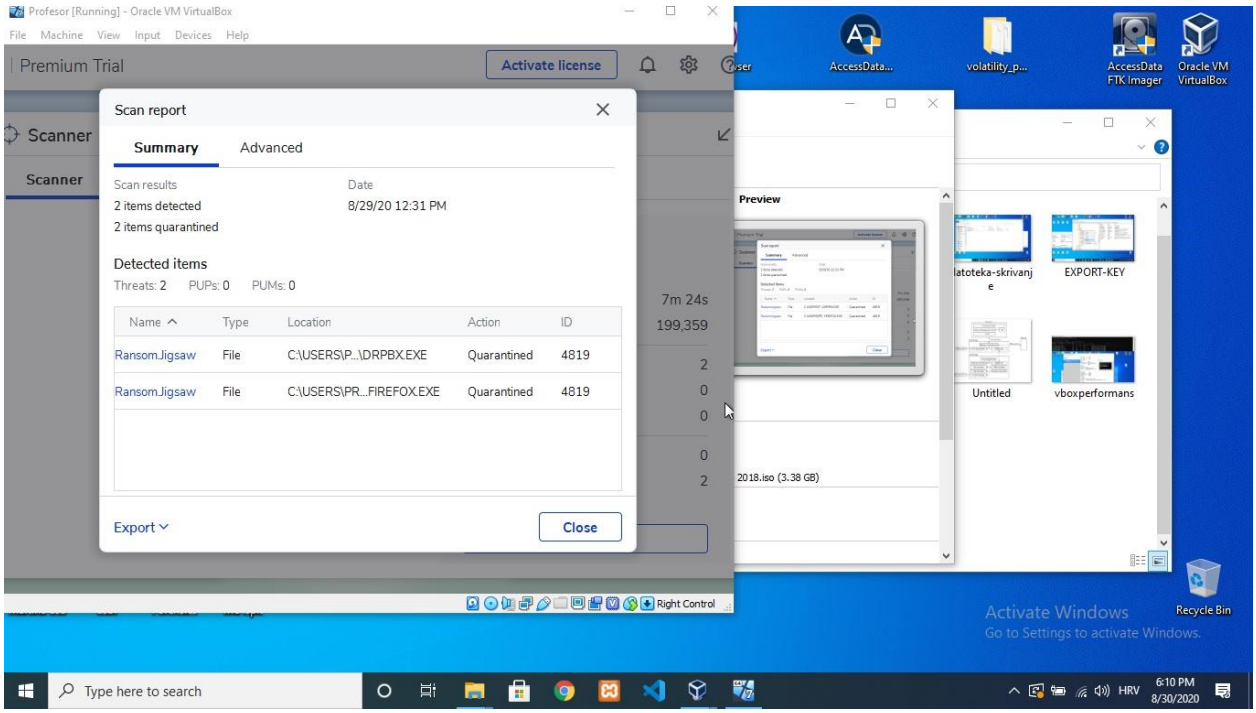


Slika 34. Dekriptiranje podataka drugi dio [autorski rad]

Prilikom dekriptiranja svih podataka, jedino što ostaje jest micanje svih stavki zlonamjernog programa u antivirusnom programu.

6.3.3. Micanje svih stavki zlonamjernog programa

Zadnji korak oporavka jest micanje svih stavki zlonamjernog programa koji će se izvršiti u MalwareBytes antivirusnom programu [Preuzeto s: https://www.malwarebytes.com/] gdje se skenira kompletno računalo i pronalaskom neželjenih programa, automatski se svrstavaju u karantenu i izbrišu što je prikazano na slici N prilikom završetka skeniranja.



Slika 35. Rezultat skeniranja u MalwareBytes programu [autorski rad]

6.3.4. Metode i tehnike prevencije napada

Postoji mnoštvo virusa i načina kako napraviti virus, generacija je sve više online te upravo zbog toga svakim danom platforme, web stranice, aplikacije, računi, osobni podaci spremljeni u bazi podataka određene tvrtke su pod velikom prijetnjom. Pod velikom prijetnjom misli se na to da svaki pojedinac koji je informatički pismen može bez problema napraviti ili skinuti, te modificrati virus ako ima volje. Online izvora, tutoriala, načina ima bezbroj, te je lako dostupno svima. Zato krenuvši od pojedinca, najbitnije se zaštititi. Pojedinac se može zaštititi:

- Instalacijom bilo kojeg antivirusnog programa, preporuka je ranije spomenuti Malwarebytes jer je vrlo ažuran što se tiče najnovijih virusa i često izlaze nove verzije za nadogradnju, a pogotovo PRO verzija koja nudi pravo-vremensku zaštitu (eng. *real-time protection*). Da je antivirusni program kao što je Malwarebytes PRO bio instaliran na računalu profesora, cijeli napad bi propao jer bi antivirusni program automatski primjetio ransomware i izolirao ga od računala.
- Dodatne opcije su naravno, kao i ranije spomenuto, isključivanje automatskog pokretanja eksternih programa. Stvar je u tome što recimo žrtva može posjetiti određenu web stranicu, te u pozadini gumba kao što je „prihvati kolačiće“ može se nalaziti objekt zlonamjerne skripte koja sadrži metode nevidljivog skidanja i pokretanja istog tog objekta. Pritiskom na gumb žrtva misli da je prihvatila kolačiće, ali je zapravo prihvatila nešto drugo.
- Također je vrlo bitno povremeno izrađivati sigurnosne kopije (eng. *backup),* jer ako dođe do sličnog napada, žrtva ima spremljene podatke na sigurnom, te se stres tokom napada, što je u ovom slučaju kriptiranje i uništenje podataka, reducira za značajan postotak. Sigurnosne kopije se mogu izraditi i na vrlo jednostavan način kao što je prebacivanje bitnih podataka na vlastiti USB stick.

7. Zaključak

Cilj ovog rada je bio prikazati nepravilnosti u radu koje se još uvijek događaju u školama, fakultetima i drugim ustanovama, točnije rad u Windows 7 operacijskom sustavu koji više ne dobiva sigurnosne zakrpe i nema podršku Microsofta. Virus koji je prikazan u ovome radu, odavno je poznat, ali ga i dalje bitdefender Windows 7 nije prikazao kao prijetnju i izolirao od operacijskog sustava. Također, popriličan broj ljudi tvrdi da antivirusni programi usporavaju rad na računalu, te ne posežu za takvim programima, čak ni u besplatnim verzijama kao MalwareBytes koji je i u besplatnoj verziji odličan program. USB stick-ovi također su velika prijetnja, ako žrtva ne posjeduje određeni stupanj zaštite, a ovaj primjer izrade zlonamjernog programa je vrlo jednostavan jer je potrebno s GitHub-a preuzeti virus, napraviti dvije skripte s „par“ linija koda koje ga čine neprimjetnim ovisno o situaciji. U slučaju situacije kao što je prikazana u ovome radu, najbitnije je ostati smiren, kontaktirati stručno osoblje, a ne plaćati otkupninu jer samim time nesvjesno žrtva podržava i financira računalni kriminal, što daje dojam napadaču da je nepobjediv i tako nastavlja dalje s napadima. Problemi se daju riješiti, ali čemu izgubiti vrijeme zbog nepažnje koje je samo po sebi trošak, podatke koji mogu biti trajno obrisani što rezultira velikim gubicima i propašću, kako materijalnom tako i duševnom.

Popis literature

[1] M. H. Ligh, A. Case, J. Levy i A. Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, Indianapolis: John Wiley & Sons, 2014.

[2] M. K. A, Learning Malware Analysis, Birmingham: Packt Publishing Ltd., 2018.

[3] FBI, »New internet scam - FBI,« 9 8 2012. [Mrežno]. Available: https://www.fbi.gov/news/stories/new-internet-scam/new-internet-scam. [Pokušaj pristupa 5 8 2020].

[4] I. Thomson, »The register,« 20 8 2016. [Mrežno]. Available: https://www.theregister.com/2016/04/20/jigsaw_ransomware/. [Pokušaj pristupa 5 8 2020].

[5] Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, »CERT.hr | Korištenje alata Volatility za forenzičku analizu radne memorije računala,« 19. travanj 2018.. [Mrežno]. Available: https://www.cert.hr/koristenje-alata-volatility-za-forenzicku-analizu-radne-memorije-racunala/. [Pokušaj pristupa 5. kolovoz 2020.].

[6] Computer Hope, »Computer hope,« 30. lipanj 2019.. [Mrežno]. Available: https://www.computerhope.com/jargon/p/process.htm. [Pokušaj pristupa 5. kolovoz 2020.].

[7] Microsoft, »Registry hives,« 31. svibanj 2018. [Mrežno]. Available: https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives. [Pokušaj pristupa 7. kolovoz 2020.].

[8] Oracle, »About virtual Box,« Oracle, [Mrežno]. Available: https://www.virtualbox.org/wiki/VirtualBox. [Pokušaj pristupa 6. kolovoz 2020.].

[9] Oracle, »Why is virtualization useful,« Virtual box, [Mrežno]. Available: https://www.virtualbox.org/manual/ch01.html#virt-why-useful. [Pokušaj pristupa 7. kolovoz 2020.].

[10] Access Data, »FTK® IMAGER Evidence aquistion tool,« [Mrežno]. Available: https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager. [Pokušaj pristupa 9. kolovoz 2020.].

[11] Packtpub.com, »Acquiring memory using FTK Imager,« [Mrežno]. Available: https://subscription.packtpub.com/book/networking_and_servers/9781782174905/2/ch02lvl1sec23/acquiring-memory-using-ftk-imager. [Pokušaj pristupa 9. kolovoz 2020.].

[12] Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, »CERT.hr | Volatility,« 12. ožujak 2018.. [Mrežno]. Available: https://www.cert.hr/volatility/. [Pokušaj pristupa 10. kolovoz 2020.].

[13] Code stop, »Youtube,« 29. listopad 2011.. [Mrežno]. Available: https://www.youtube.com/watch?v=6tYeF_MTB6k. [Pokušaj pristupa 27. kolovoz 2020.].

[14] S. Wadhwa, »Quora.com,« 22. travanj 2014.. [Mrežno]. Available: https://www.quora.com/What-is-the-use-of-ping-localhost-n-001-nul-command-in-batch-script. [Pokušaj pristupa 10. rujan 2020.].

[15] Max Koon, »Youtube - comment,« 2016.. [Mrežno]. Available: https://www.youtube.com/watch?v=xrP43DiUBTU . [Pokušaj pristupa 27. kolovoz 2020.].

[16] C. Hoffman, »How AutoRun Malware Became a Problem on Windows, and How It Was (Mostly) Fixed,« 28 studeni 2014.. [Mrežno]. Available: https://www.howtogeek.com/203522/how-autorun-malware-became-a-problem-on-windows-and-how-it-was-mostly-fixed/. [Pokušaj pristupa 10. rujan 2020.].

[17] B. Harmon, »Access Data - FTK Imager Memory Dump Collection Crashes Or Causes Blue Screen,« Access Data, 26. travanj 2017.. [Mrežno]. Available: https://support.accessdata.com/hc/en-us/articles/115006360008-FTK-Imager-Memory-Dump-collection-crashes-or-causes-blue-screen. [Pokušaj pristupa 29. kolovoz 2020.].

[18] Oracle, »Virtual Box - Introduction,« [Mrežno]. Available: https://www.virtualbox.org/manual/ch08.html#vboxmanage-intro. [Pokušaj pristupa 29. kolvooz 2020.].

[19] A. Fortuna, »How to extract a RAM dump from a running VirtualBox machine,« 23. lipanj 2018.. [Mrežno]. Available: https://www.andreafortuna.org/2017/06/23/how-to-extract-a-ram-dump-from-a-running-virtualbox-machine/. [Pokušaj pristupa 29. kolovoz 2020.].

[20] S. Izhar, »USB Forensics: Find the History of Every Connected USB Device on Your Computer,« 22. svibanj 2018.. [Mrežno]. Available: https://www.cybrary.it/blog/0p3n/usb-forensics-find-the-history-of-every-connected-usb-device-on-your-computer/. [Pokušaj pristupa 10. kolovoz 2020.].

[21] 13cubed.com, »SANS DFIR Cheat Sheet,« [Mrežno]. Available: https://www.13cubed.com/downloads/dfir_cheat_sheet.pdf. [Pokušaj pristupa 30. kolovoz 2020.].

[22] T. Meskauskas, »Jigsaw ransomware removal instructions,« 14. kolovoz 2020.. [Mrežno]. Available: https://www.pcrisk.com/removal-guides/9942-fun-ransomware. [Pokušaj pristupa 30. kolovoz 2020.].

Popis slika