CARNET

Korištenje alata Volatility za forenzičku analizu radne memorije računala

NCERT-PUBDOC-2018-4-358

CERT.hr

Sadržaj

1 Uvod

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.

Jedna posebno zanimljiva primjena forenzike radne memorije je analiza napada na računalne sustave zlonamjernim softverom (eng. *malware*) jer su u tom slučaju tragovi često namjerno prikrivani. Primjerice, napredni zlonamjerni softver često ne zapisuje nikakve podatke na disk te šifrira sve podatke koje šalje mrežom zbog čega su uobičajene forenzičke metode neefikasne.

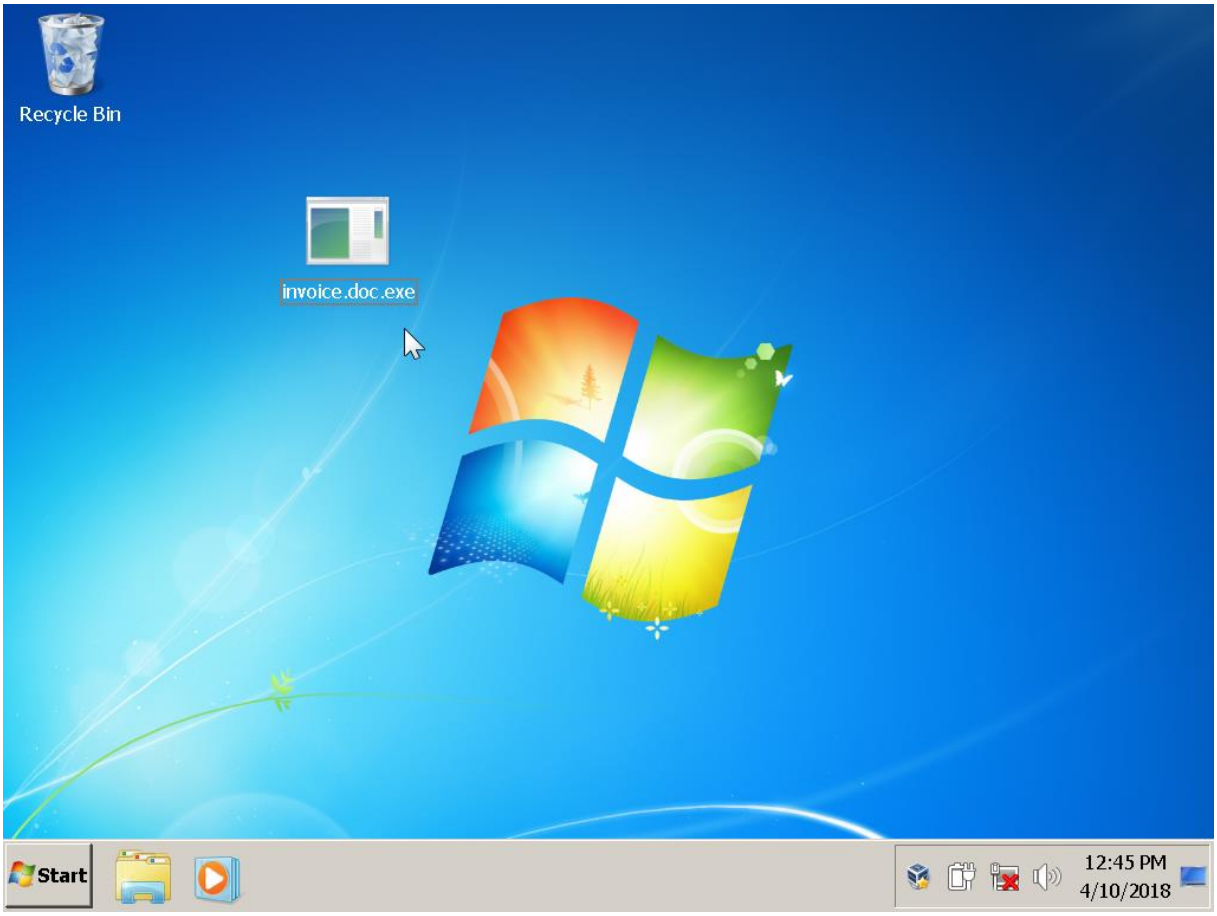
Forenzikom radne memorije neke od tih tehnika mogu se lakše zaobići te zbog toga ona predstavlja važan doprinos ostalim mehanizmima koje se koriste u analizi zlonamjernog softvera. Iz tog je razloga forenzika memorije grana računalne forenzike koja se zadnjih godina ubrzano razvija te se kontinuirano stvaraju nove tehnike korištene u analizi radne memorije.

Najpopularniji slobodni (eng. *free and open source*) alat za forenziku radne memorije je Volatility. Upute za instalaciju i osnovno korištenje alata Volatility opisane su u prethodnom dokumentu Nacionalnog CERT-a: „Volatility“. Ovaj dokument proširit će ta znanja te objasniti kako ih primijeniti na stvarnom primjeru forenzičke analize radne memorije računala zahvaćenog zlonamjernim softverom.

2 Scenarij napada

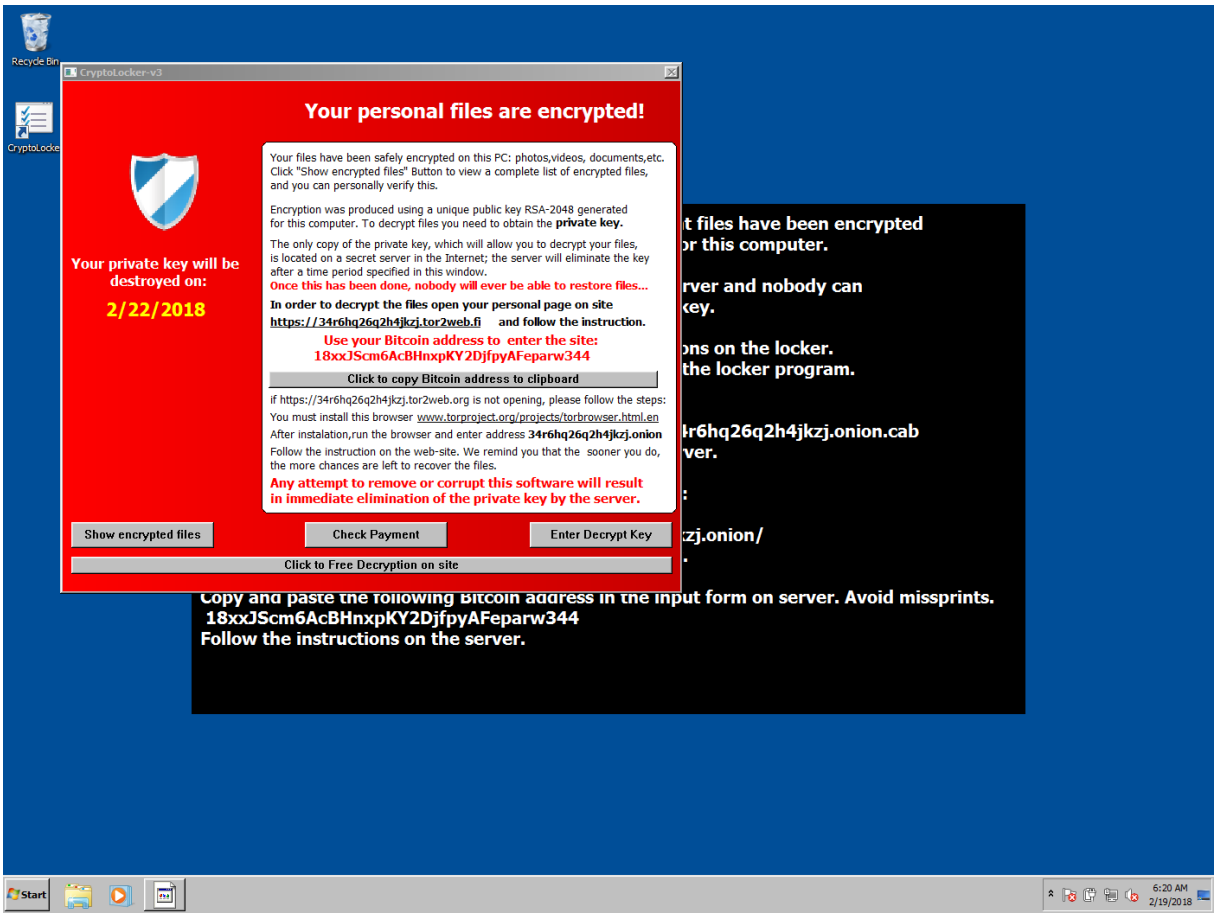
U ovom dokumentu, forenzička analiza radne memorije računala bit će objašnjena kroz primjer. Bit će analizirana slika radne memorije računala zahvaćenog zlonamjernim softverom.

U primjeru je žrtva (korisnik računala) primila poruku elektroničke pošte s datotekom *invoice.doc.exe* u privitku. To je izvršna datoteka koja sadržava zlonamjerni program, a nastavkom *.doc.exe* pokušava zavarati žrtvu i uvjeriti ju da datoteka zapravo sadržava običan dokument. Žrtva je datoteku preuzela na radnu površinu, kao što je prikazano na slici 1.



Slika 1 – Slika radne površine računala prije pokretanja zlonamjernog programa

Zatim, žrtva je, uvjerena da otvara bezopasan dokument, dvostrukim klikom na preuzetu datoteku pokrenula zlonamjerni program. Nakon nekoliko trenutaka, pojavila se poruka koja tvrdi da su datoteke na računalu šifrirane. U poruci se nalazi i zahtjev za otkupninom (eng. *ransom note*), iz čega se može zaključiti kako je računalo zaraženo zlonamjernim programom vrste *ransomware. Ransomware* je vrsta zlonamjernih programa koji šifriraju datoteke ili na neki drugi način onemogućuju rad na računalu te zatim od korisnika traže otkupninu kako bi vratili računalo u upotrebljivo stanje. Slika 2 prikazuje sliku radne površine nakon pokretanja zlonamjernog programa.



Slika 2 – Slika radne površine računala nakon pokretanja zlonamjernog programa

Konkretno u ovom slučaju, zlonamjerni program pokrenut je unutar virtualnog stroja kako bi se ograničila potencijalna šteta. Kada se pojavila poruka sa zahtjevom za otkupninu, forenzičar je zaustavio izvršavanje virtualnog stroja i njegova memorija je snimljena u datoteku pod nazivom *infected_teslacrypt.elf*. Na taj način pribavljena je slika memorije računala te analiza može započeti.

3 Analiza slike radne memorije

Tehnike analize memorije u ovom dokumentu oslanjaju se na osnovna predznanja korištenja alata Volatility opisana u prethodnom dokumentu Nacionalnog CERT-a (instalacija, pozivanje naredbi, razumijevanje argumenata *-f* odnosno *--file* i *--profile*). Također, kako su izlazni podaci alata Volatility u pravilu u tekstualnom obliku, za analizu rezultata očekuju se osnovne vještine baratanja tekstom u naredbenoj liniji, primjerice filtriranje linija teksta po ključnoj riječi. Jedan od poznatijih takvih alata je *grep*, koji se koristi na Unix operacijskim sustavima, a u ovom dokumentu se koristi *findstr*, koji je dostupan na operacijskim sustavima Windows.

Primjeri korištenja alata Volatility u ovom dokumentu napravljeni su na operacijskom sustavu Windows, iz njegovog naredbenog retka (eng. *Command Line*), no u načelu je korištenje alata Volatility jednako i na drugim operacijskim sustavima. Neke naredbe zauzimaju dva reda u ovom dokumentu zbog svoje duljine, no sve naredbe potrebno je napisati u **jednom retku** u naredbenom retku operacijskog sustava.

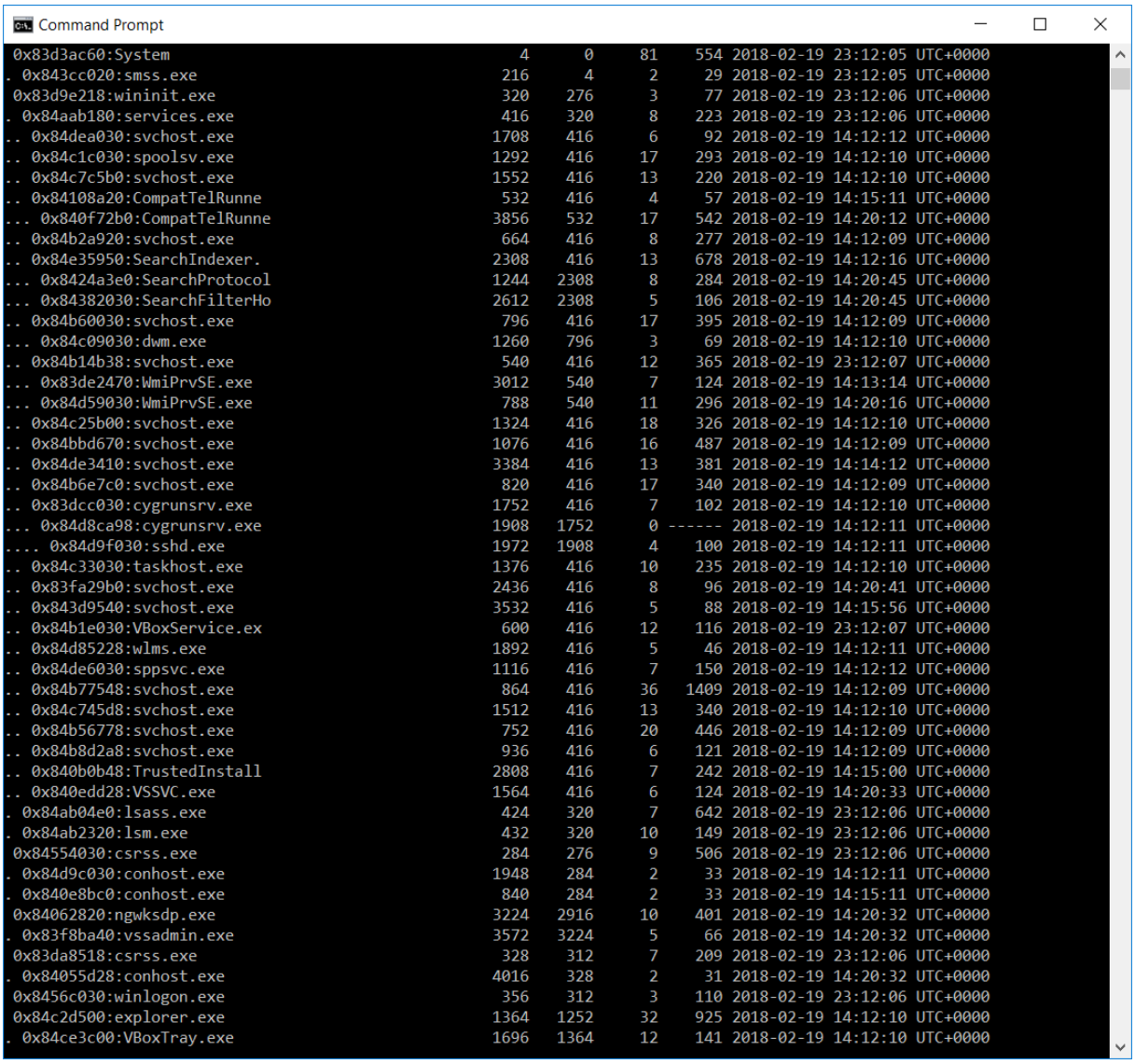
U narednim primjerima sve naredbe izvršene su iz direktorija *C:\volatility* u kojem se nalazila izvršna datoteka alata Volatility te datoteka sa slikom memorije naziva *infected_teslacrypt.elf.*

3.1 Popis procesa

Jedna od prvih stvari koje forenzičar u ovakvoj situaciji želi saznati o stanju sustava je popis pokrenutih procesa. U prethodnom dokumentu o alatu Volatility opisana je naredba *pslist*. 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.

Kao i u ostalim pokretanjima alata Volatility, potrebno je alatu proslijediti ime datoteke u kojoj se nalazi slika memorije te inačicu operacijskog sustava na kojem je snimljena slika memorije. Parametrom **-f** postavlja se ime datoteke slike memorije (*infected_teslacrypt.elf*), a parametrom **--profile** ime sustava na kojem je slika nastala (*Win7SP1x86*, što označava 32-bitnu verziju Windows 7 Service Pack 1 sustava).

```
volatility –f infected_teslacrypt.elf --profile=Win7SP1x86 pstree
```



Slika 3 – Popis procesa dobiven pokretanjem naredbe *pstree*

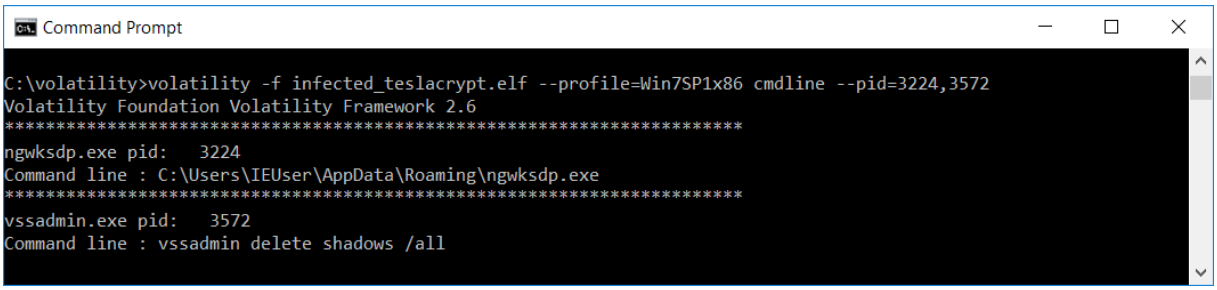
Na popisu je moguće primijetiti veći broj procesa, no proces *ngwksdp.exe* izgleda neobično zbog svojeg imena koje izgleda kao da je nasumično generirano. Proces *ngwksdp.exe* ima jedan potproces, tj. proces dijete, imena *vssadmin.exe*. Kratkim istraživanjem moguće je otkriti da je to alat za administraciju Windows mehanizma za stvaranje sigurnosnih kopija (eng. *backup*) datoteka naziva *Volume Snapshot Service* ili *Volume Shadow Copy Service*. Zbog ovakve kombinacije neobičnog imena procesa i korištenja alata za administraciju sigurnosnih kopija, procesi *ngwksdp.exe* i *vssadmin.exe* će biti detaljnije analizirani.

Svaki proces ima svoj jedinstveni identifikator – PID (od eng. *process id*) pomoću kojeg se može jedinstveno identificirati taj proces iz liste pokrenutih procesa na računalu. Identifikatori procesa *ngwksdp.exe* i *vssadmin.exe* su 3224 i 3527, što je korisno zabilježiti za sljedeće naredbe čiji je rad moguće ograničiti na određene procese kako bi se smanjila količina ispisanih rezultata i ubrzao rad alata Volatility.

3.2 Argumenti naredbene linije

Kako bi znali što je učinjeno pomoću alata *vssadmin.exe*, potrebno je saznati s kojim argumentima naredbene linije je program pozvan, a upravo to je moguće saznati naredbom **cmdline**. Argumentom **--pid=3224,3527** moguće je ograničiti njen rad samo na prethodno navedene procese koje želimo detaljnije istražiti, kako bi se smanjila količina ispisanih podataka. Potpuna naredba izgleda ovako:

```
volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 cmdline
--pid=3224,3572
```



Slika 4 – Informacije o argumentima naredbene linije procesa dobivene pokretanjem naredbe *cmdline*

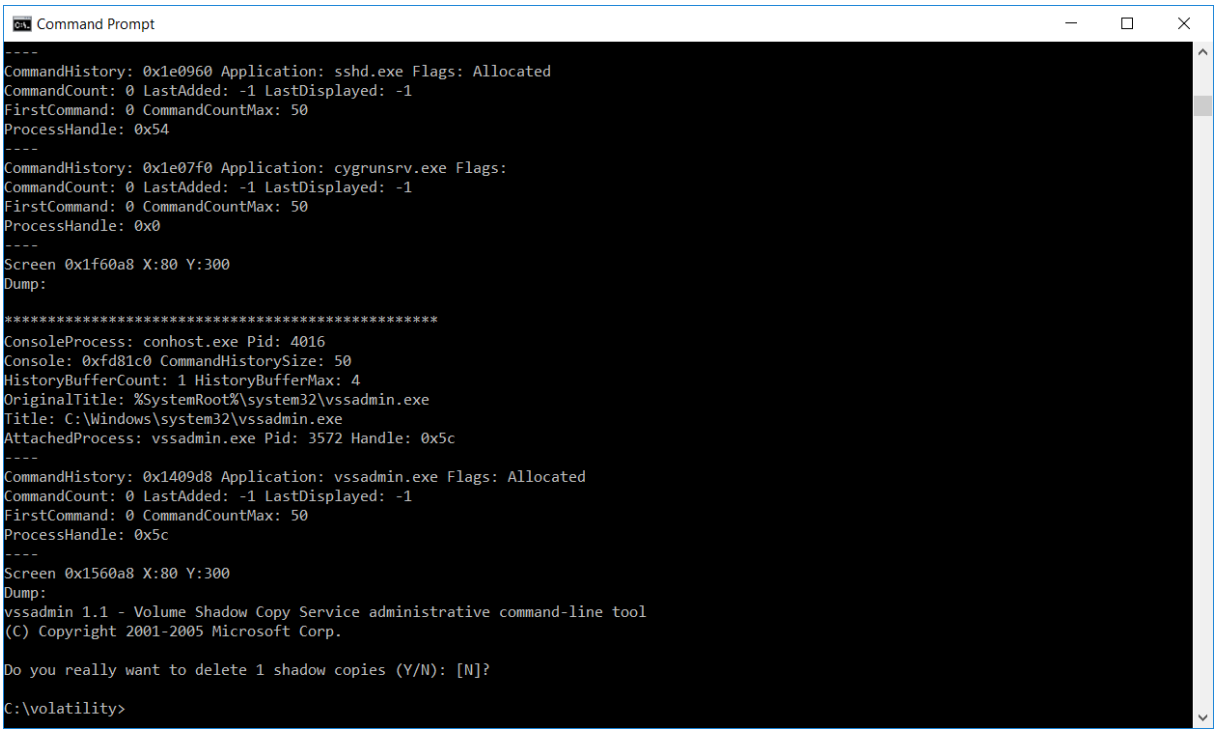
U ispisu naredbe moguće je vidjeti da je puni poziv alata *vssadmin* bio:

```
vssadmin delete shadows /all
```

Kratkim istraživanjem moguće je saznati da se takvim pozivom brišu sigurnosne kopije datoteka stvorene *Volume Shadow Copy* sustavom. Istražiteljima koji su se prethodno susretali s *ransomwareom* će već ovo biti izrazito sumnjivo – ovo je uobičajena tehnika *ransomwarea* za brisanje sigurnosnih kopija kako se ne bi lako mogle povratiti šifrirane datoteke.

Također, u alatu Volatility postoji i naredba **consoles**, kojom se mogu vidjeti upisane naredbe i njihov ispis, kao i neki dodatni detalji o pokrenutom naredbenom retku. U ovom slučaju pomoću naredbe *consoles* se ne dolazi do novih tragova, no pri kraju ispisa naredbe može se potvrditi kako su zaista alatom *vssadmin* brisane sigurnosne kopije.

```
volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 consoles
```



Slika 5 – Ispis sadržaja naredbenog retka dobiven poretanjem naredbe *consoles*

3.3 Ručke (eng. *handles*) procesa

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.

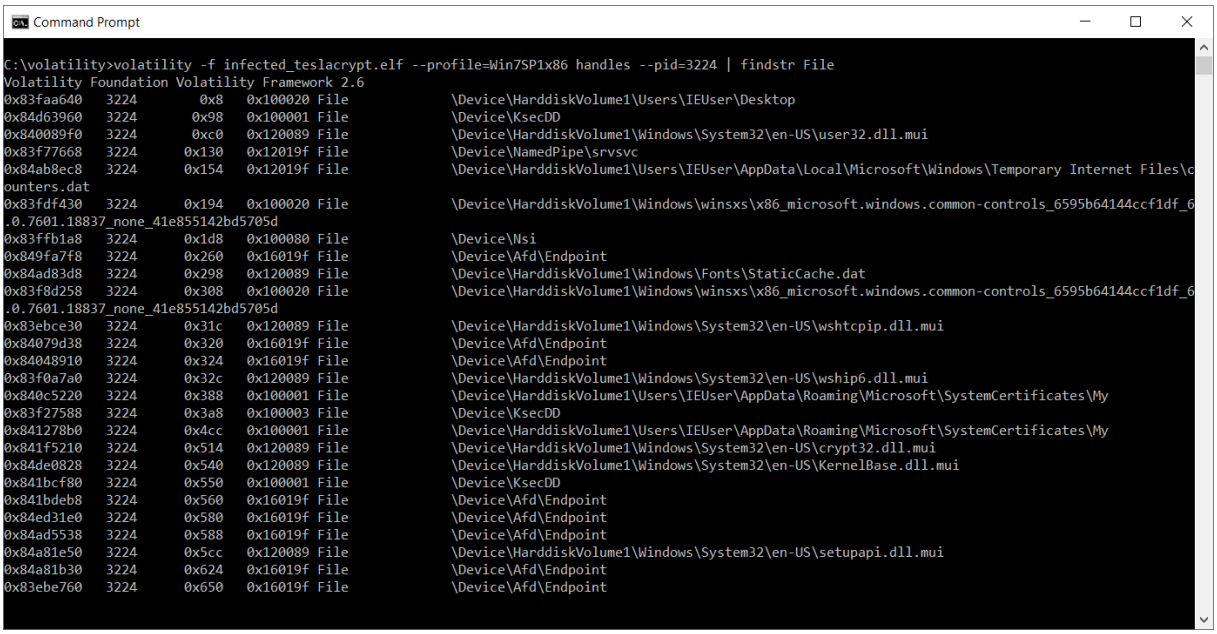
Sada kada je poznato što je radio proces *vssadmin.exe*, potrebno je detaljnije istražiti proces *ngwksdp.exe*. Pokretanjem sljedeće naredbe dobiva se popis ručki procesa *ngwksdp.exe* (s identifikatorom 3224):

```
volatility –f infected_teslacrypt.elf --profile=Win7SP1x86 handles
--pid=3224
```

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.

Kako bi ispisali samo ručke koje služe za datoteke moguće je koristiti sljedeću naredbu:

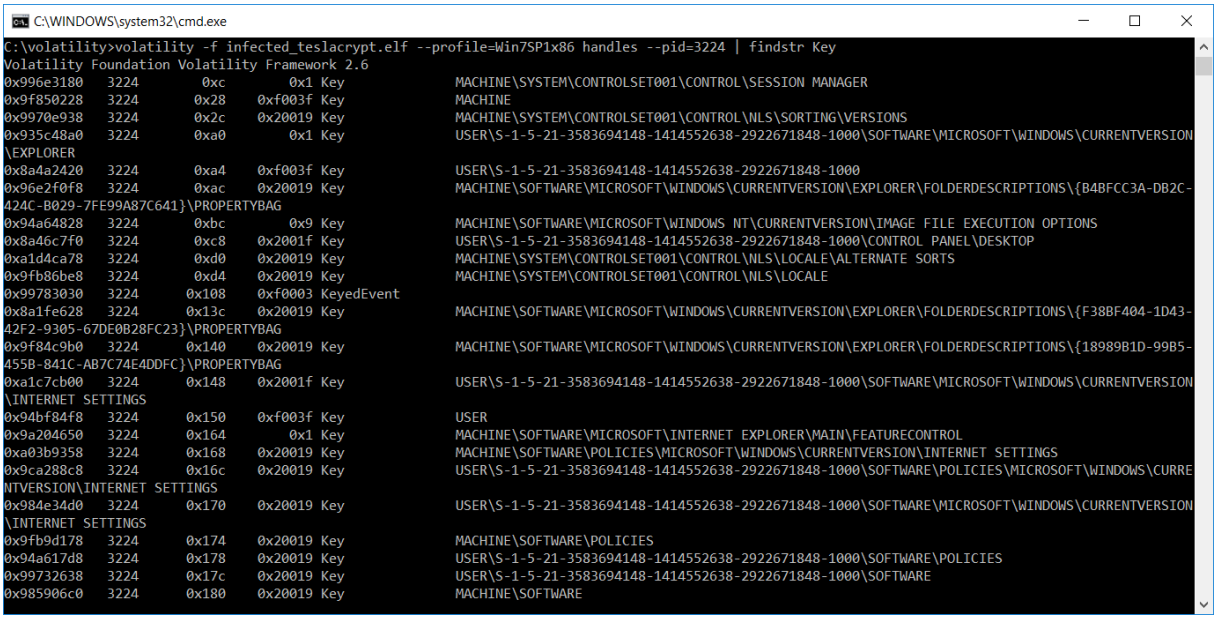
```
volatility –f infected_teslacrypt.elf --profile=Win7SP1x86 handles
--pid=3224 | findstr File
```



Slika 6 – Ispis ručki otvorenih datoteka dobivenih pokretanjem naredbe *handles* i filtriranjem po ključnoj riječi „File“

U ovom slučaju, u trenutku snimanja slike memorije ovaj proces nije imao nikakve posebno zanimljive otvorene datoteke. Sada, moguće je filtrirati ispis i po drugom tipu objekta – ključevima registra:

```
volatility –f infected_teslacrypt.elf --profile=Win7SP1x86 handles
--pid=3224 | findstr Key
```

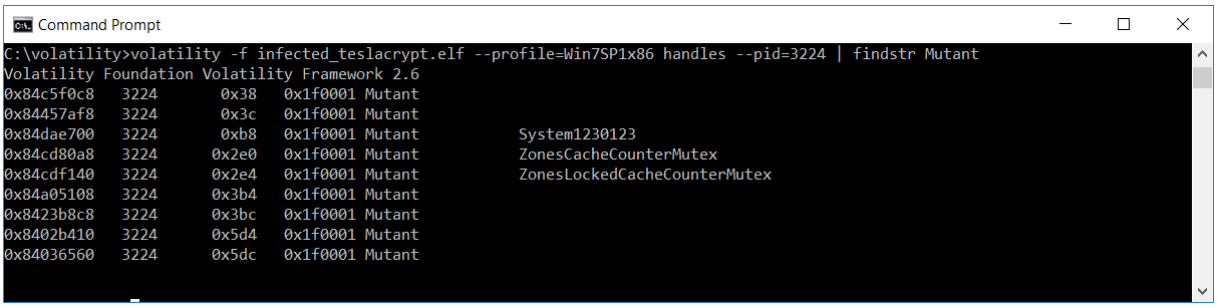


Slika 7 – Ispis ručki otvorenih registarskih ključeva dobivenih pokretanjem naredbe *handles* i filtriranjem po ključnoj riječi „Key“

Nažalost, ni u slučaju ključeva registra nema zanimljivih tragova.

No, ima još jedan zanimljivi tip ručke u ovom kontekstu, a to su mehanizmi međusobnog isključivanja, takozvani *mutexi* (skraćeno od eng. *mutual exclusion)*. Zlonamjerni softver 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:

```
volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 handles
--pid=3224 | findstr Mutant
```



Slika 8 – Ispis ručki *mutex* objekata dobivenih pokretanjem naredbe *handles* i filtriranjem po ključnoj riječi „Mutant“

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 su:

- System1230123
- ZonesLockedCacheCounterMutex
- ZonesCacheCounterMutex

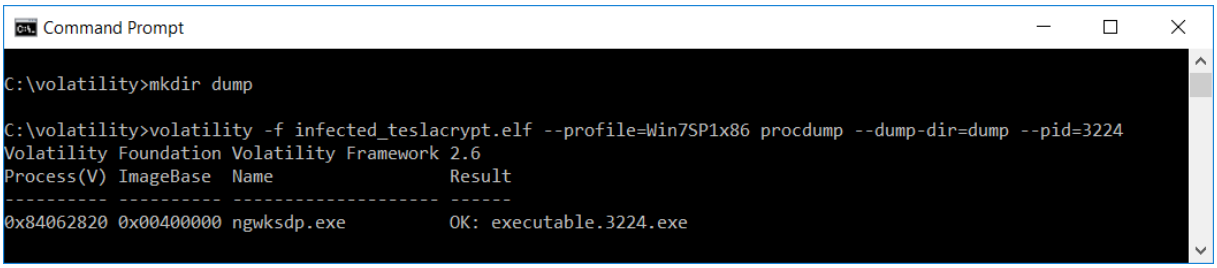
Iako na prvi pogled imena možda i ne izgledaju sumnjivo, korisno je internetskim tražilicama pretražiti jesu li se ta imena pojavljivala kod drugih zlonamjernih softvera. Kratkim istraživanjem moguće je otkriti da se prvi *mutex*, imena *System1230123*, pojavljuje kod *ransomwarea* zvanog TeslaCrypt, dok se druga dva imena *mutexa* pojavljuju kod TeslaCrypta, ali i kod nekih drugih zlonamjernih programa.

3.4 Rekonstrukcija izvršne (*.exe*) datoteke

Naredbom ***procdump***, Volatility može iz procesa pokušati rekonstruirati izvršnu (*.exe*) datoteku. Rezultat rekonstrukcije gotovo nikada neće savršeno odgovarati izvornoj izvršnoj datoteci. Primjerice, sadržaj podatkovnih sekcija datoteke će gotovo zasigurno biti promijenjen, no sadržaj samog strojnog koda često će biti isti kao i u izvršnoj datoteci.

Naredbi *procdump* je, uz identifikator procesa za rekonstrukciju, potrebno zadati i argument *–dump-dir=<direktorij>*, gdje je *<direktorij>* putanja do direktorija u koji će biti spremljena datoteka. Potrebno je stvoriti taj direktorij, primjerice naredbom *mkdir* ili uobičajenim stvaranjem direktorija u grafičkom sučelju, te pokrenuti naredbu:

```
volatility –f infected_teslacrypt.elf --profile=Win7SP1x86 procdump
--dump-dir=dump --pid=3224
```

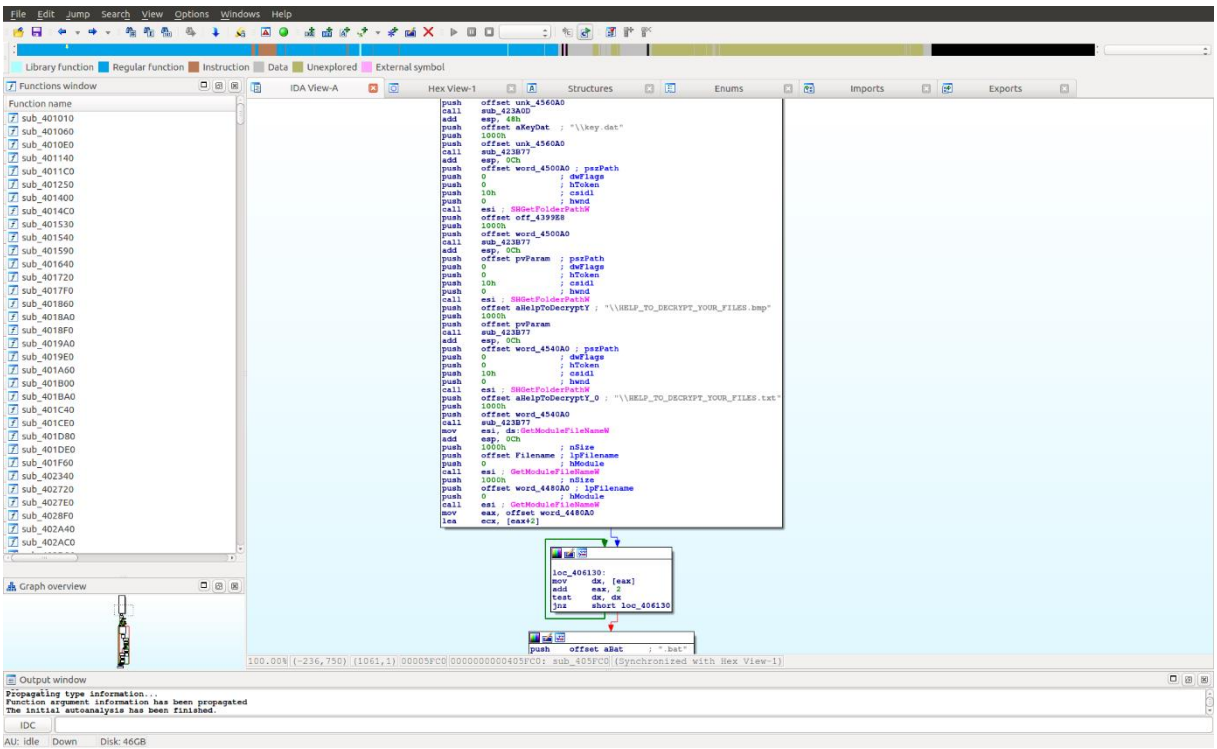


Slika 9 - Stvaranje direktorija i rekonstrukcija izvršne datoteke procesa pomoću naredbe *procdump*

Na ovaj način ponekada je moguće dobiti izvršnu datoteku i u korisnijem obliku za analizu od izvornog oblika, primjerice ako je izvorna datoteka bila zapakirana (eng. *packed*). Tzv. pakiranje izvršnih datoteka je česta tehnika zlonamjernog softvera u kojem je sadržaj izvršne datoteke komprimiran i/ili šifriran te se tek prilikom pokretanja programa dešifrira i/ili dekomprimira unutar radne memorije računala.

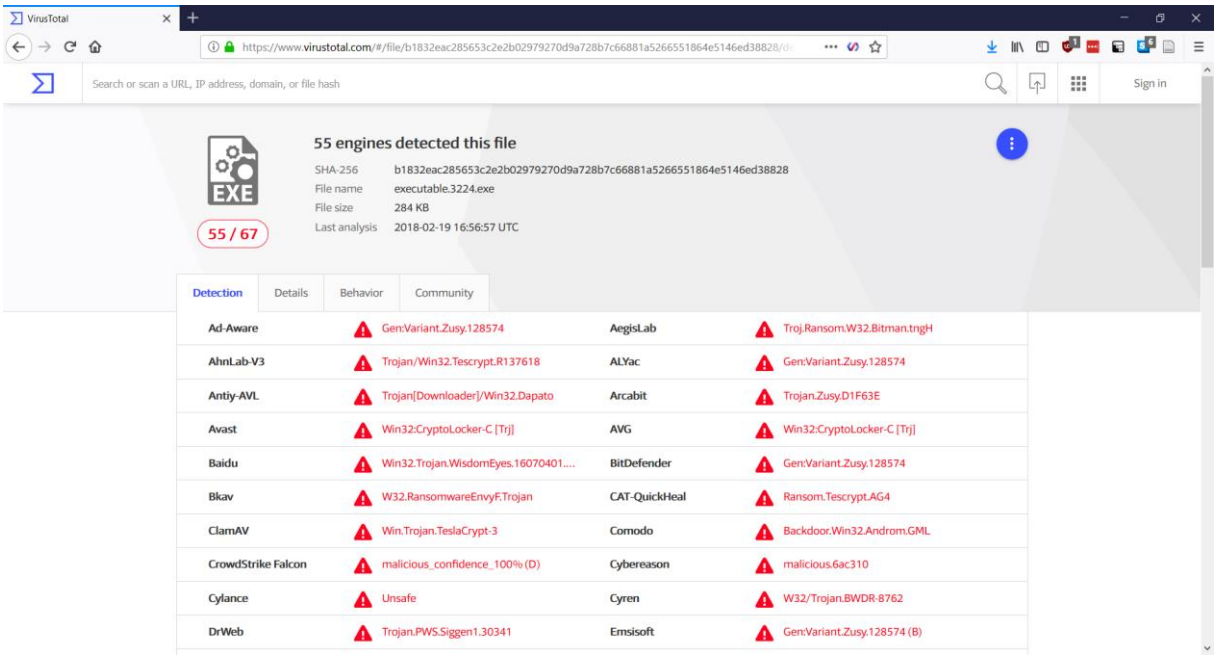
Kako rekonstruirana datoteka potencijalno sadrži zlonamjeran kod, moguće je da na računalu istražitelja antivirusni alat to prepozna i automatski obriše datoteku.

Rekonstruiranu izvršnu datoteku moguće je otvoriti u drugim alatima za analizu izvršnih datoteka, primjerice u alatu za reverzni inženjering IDA, kao što je prikazano na slici 10.



Slika 10 – Rekonstruirana izvršna datoteka otvorena u alatu IDA

Također, rekonstruiranu izvršnu datoteku moguće je učitati na 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.



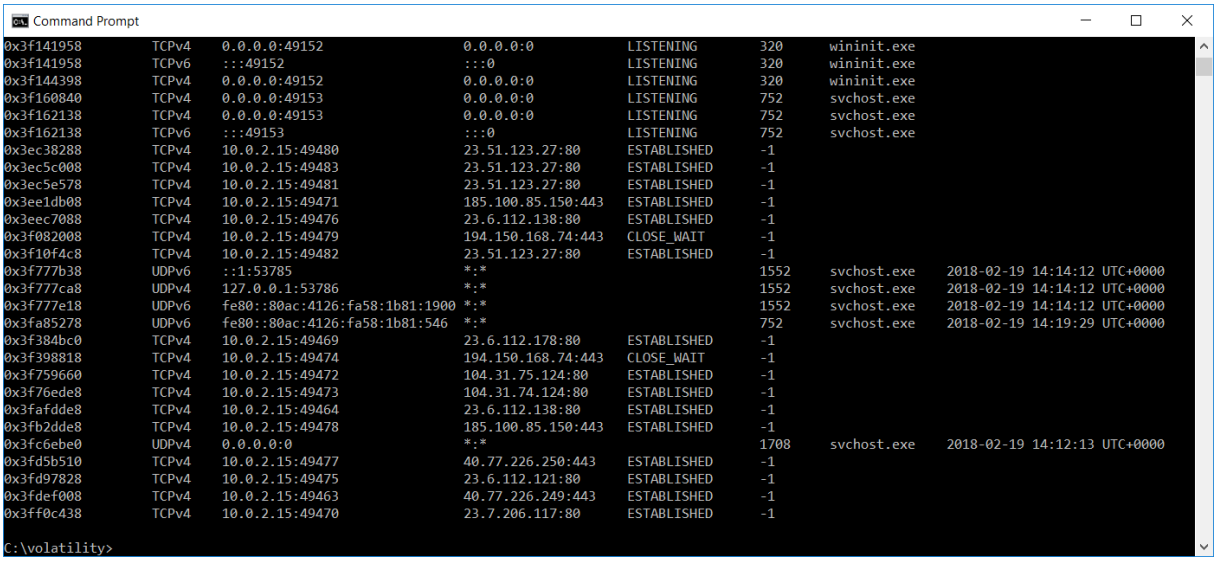
Slika 11 – Dio rezultata analize rekonstruirane izvršne datoteke na Web stranici *VirusTotal*

U ovom slučaju, moguće je vidjeti kako brojni antivirusni alati svojim detekcijama upućuju na **TeslaCrypt** (imena *tescrypt*, *teslacrypt*), no ima i alata koji upućuju na druge zlonamjerne programe (*cryptolocker*, *zusy*).

3.5 Mrežne veze

Još jedan bitan korak u forenzici radne memorije je analiza mrežnih veza. Kako je na računalu bio pokrenut operacijski sustav Windows 7, potrebno je koristiti naredbu ***netscan*** za analizu mrežnih veza. Format naredbe je:

```
volatility –f infected_teslacrypt.elf --profile=Win7SP1x86 netscan
```



Slika 12 – Popis mrežnih veza dobiven pokretanjem naredbe *netscan*

Iz navedenog popisa, računalo je bilo spojeno na sljedeće IP adrese i odgovarajuće TCP priključke (eng. *port*):

- 104.31.74.124:80
- 104.31.75.124:80
- 185.100.85.150:443
- 194.150.168.74:443
- 23.51.123.27:80
- 23.6.112.121:80
- 23.6.112.138:80
- 23.6.112.178:80
- 23.7.206.117:80
- 40.77.226.249:443
- 40.77.226.250:443

Korišteni TCP priključci 80 i 443 upućuju na HTTP i HTTPS protokole, odnosno spajanje na Web servise. Volatility nije uspio povezati mrežne veze s procesom (PID = -1), no već i ovakav popis je korisna informacija. Navedene IP adrese moguće je dalje istražiti na nekoliko načina, opisanih u narednim potpoglavljima. Bit će opisani primjeri istraživanja pojedinih IP adresa s popisa, no u sklopu sveukupne analize je korisno proučiti sve IP adrese.

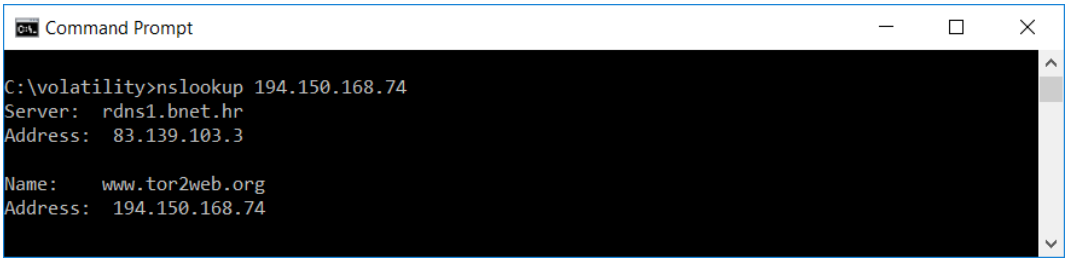
3.5.1 Obrnuti DNS (eng. *reverse DNS)*

DNS (eng. *Domain Name System*) sustav je koji povezuje simbolička imena s numeričkim IP adresama. Pomoću DNS-a korisnik može primjerice koristiti simboličko ime *carnet.hr* umjesto IP adrese *161.53.160.25* koju je teško zapamtiti.

Manje je poznato da je pomoću DNS-a moguće napraviti i obrnuti postupak, tj. povezati IP adresu sa simboličkim imenom. Taj postupak naziva se obrnuta DNS pretraga (eng. *reverse DNS lookup*) te ga je moguće napraviti pomoću alata ***nslookup***, dostupnog na Windows i Unix računalima ili korištenjem besplatno dostupnih Web alata, primjerice MxToolbox Reverse Lookup alata.

Kako bi se izvršila obrnuta DNS pretraga pomoću alata *nslookup*, potrebno mu je kao argument dati IP adresu za koju se traži simboličko ime, u ovom primjeru jedna od IP adresa iz popisa veza dobivenih naredbom *netscan*:

```
nslookup 194.150.168.74
```



Slika 13 – Ispis obrnutog DNS zapisa IP adrese 194.150.168.74

U ispisu naredbe vidi se kako postoji obrnuti DNS zapis za tu IP adresu, te je on jednak *www.tor2web.org*. Kratkim istraživanjem moguće je saznati da je ta stranica zapravo most koji omogućava pristup skrivenim servisima Tor mreže. U ovom kontekstu, iz toga je moguće posumnjati da je zlonamjerni softver kontaktirao poslužitelje unutar Tor mreže, na Tor skrivenim servisima.

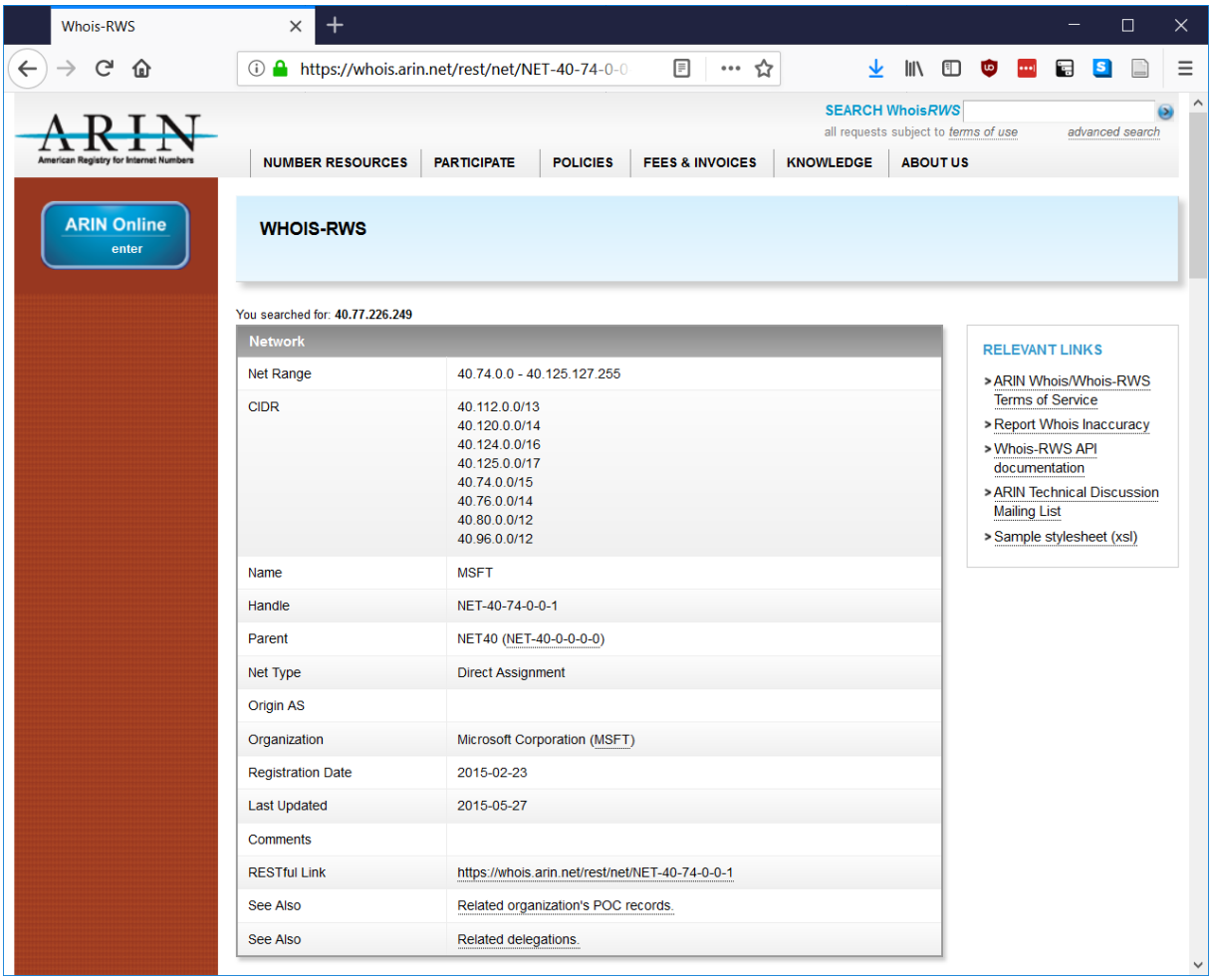
Problem s obrnutim DNS zapisima je to što:

- oni ne moraju uvijek postojati,
- ne moraju čak biti ni točni,
- a i jednostavno više simboličkih imena može pokazivati na istu IP adresu – u tom slučaju obrnuti DNS zapis može dati informacije o samo jednom imenu.

3.5.2 WHOIS servis

WHOIS je servis pomoću kojega je moguće saznati informacije o organizaciji koja je registrirala određenu domenu ili blok IP adresa. Za slanje WHOIS upita, na Unix sustavima obično je dostupan alat *whois* koji se pokreće iz naredbenog retka, dok je na Windows sustavima potrebno dodatno instalirati takav alat, dostupan ovdje. Alternativno, moguće je koristiti neki od Web alata za slanje WHOIS upita, primjerice ovaj alat.

Na slici 14 prikazan je ispis rezultata WHOIS upita na navedenom Web alatu za jednu od IP adresa s popisa naredbe *netscan* – 40.77.226.249. IP adresa je registrirana na tvrtku Microsoft, te se zbog toga ne čini sumnjivom – vjerojatno ju je kontaktirao neki dio operacijskog sustava Windows, primjerice servis za ažuriranje.

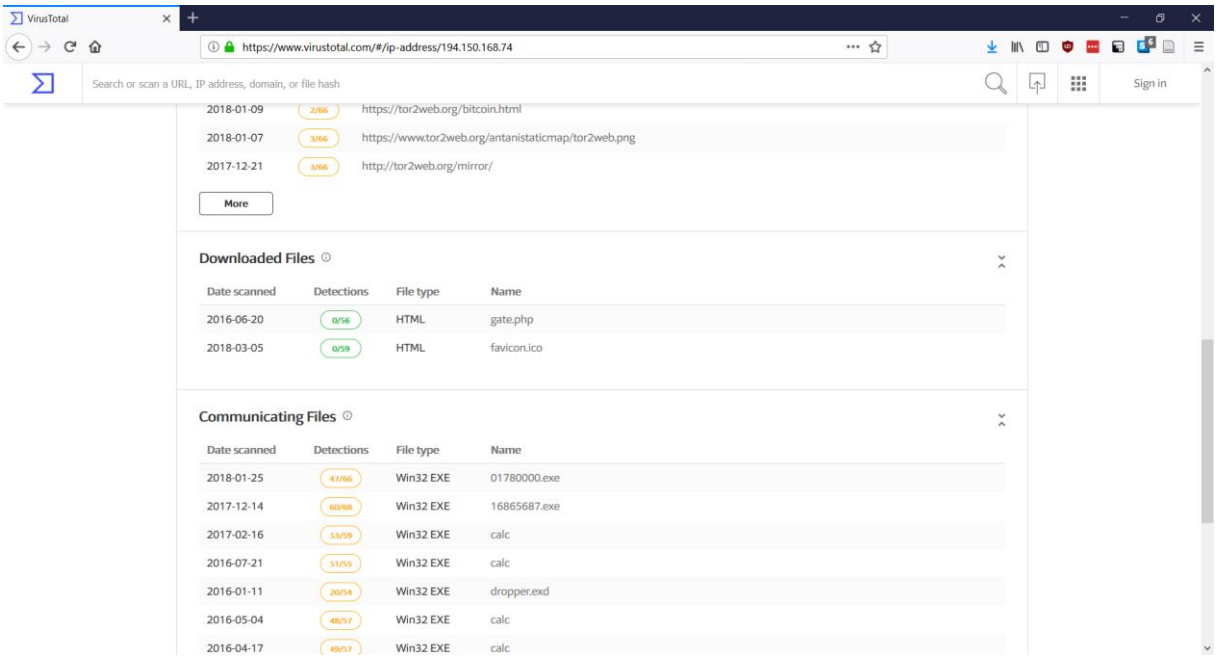


Slika 14 – WHOIS zapis za IP adresu 40.77.226.249 na vanjskom Web alatu

3.5.3 Ostale baze informacija o IP adresama

Od ostalih baza informacija o IP adresama korisno je znati za servise s tzv. pasivnim DNS bazama. U takvim bazama zapisane su povijesne informacije o povezanosti IP adresa i simboličkа imena. Upitom na takve servise moguće je otkriti i druge domene koje su bile povezane s određenom IP adresom. Jedna od takvih javno dostupnih baza s mogućnošću pretraživanja nalazi se na ovoj poveznici.

Još jedna korisna baza u ovom kontekstu je baza servisa VirusTotal, koje se može pretraživati ovdje. VirusTotal kao cijeli servis specijaliziran je za zlonamjerni softver, tako da je u njegovoj bazi moguće naći informacije o datotekama koje su preuzete s tražene IP adrese te informacije o izvršnim datotekama koje, jednom kada su pokrenute, komuniciraju s tom IP adresom. U primjeru na slici 15 u tražilicu alata VirusTotal upisana je adresa 194.150.168.74, za koju je ranije ustanovljeno da odgovara Web stranici *www.tor2web.com*. Na slici je moguće vidjeti kako je veći broj zlonamjernog softvera komunicirao s tim poslužiteljem.



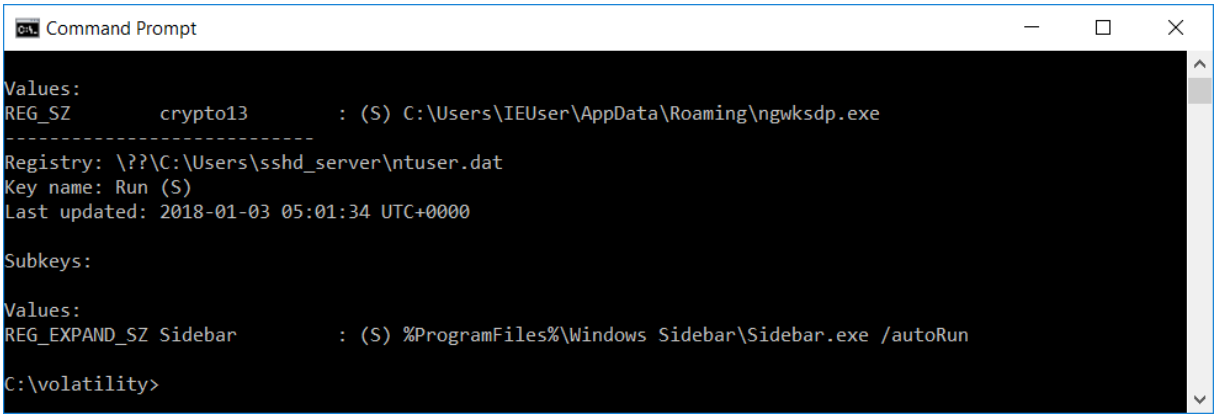
Slika 15 – Pretraživanje informacija o IP adresi u bazi Web stranice VirusTotal

3.6 Windows registar (eng. *registry*)

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 ovdje.

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"
```



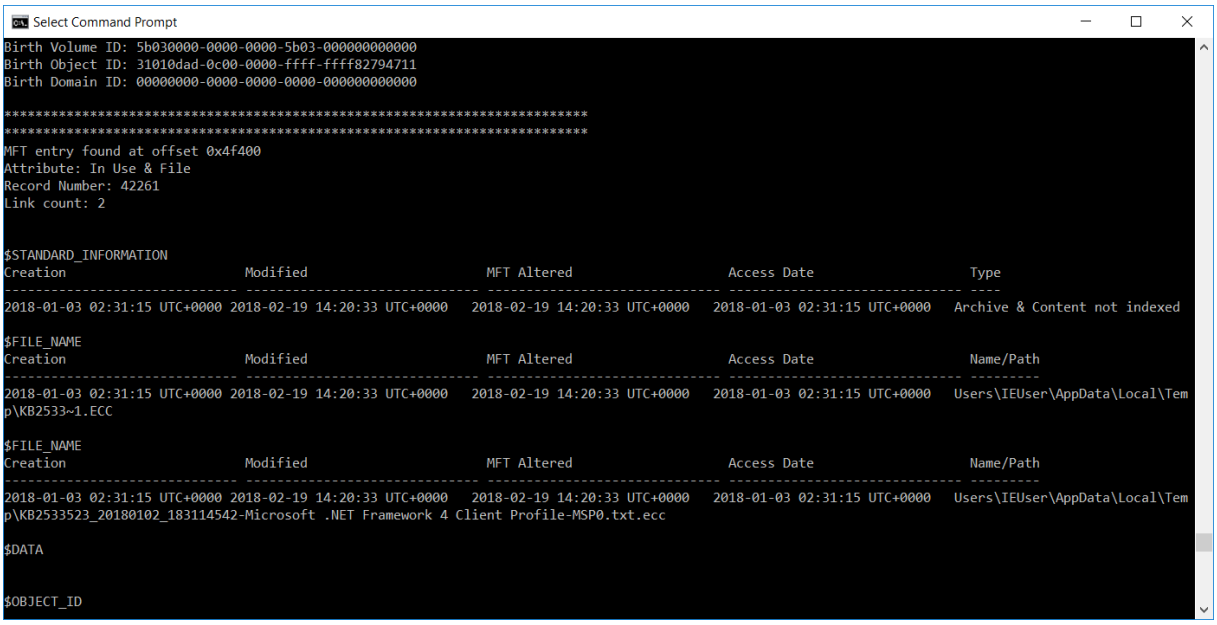
Slika 16 – Ispisivanje vrijednosti ključa registra pomoću naredbe *printkey*

U ispisu naredbe moguće je vidjeti vrijednost povezanu sa sumnjivim *ngwksdp.exe* procesom. Konkretnije, moguće je vidjeti ime ključa (*crypto13*) te putanju do izvršne datoteke (*C:\Users\IEUser\AppData\Roaming\ngwksdp.exe*).

3.7 Datotečni sustav

Datotečni sustav opisuje na koji način se pohranjuju datoteke u trajnu memoriju te opisuje njihovu hijerarhiju, tj. u kojem se direktoriju nalazi koja datoteka. Operacijski sustav Windows koristi datotečni sustav pod nazivom NTFS. Datotečni sustav NTFS koristi datotečnu tablicu zvanu MFT (eng. *Master File Table*) u koju su zapisani detalji svake od datoteka u sustavu. Naredba ***mftparser*** potražit će datotečne tablice u slici memorije te ispisati neke od informacija sadržanih u njoj:

```
volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 mftparser
```



Slika 17 – Informacije iz datotečne tablice dobivene naredbom *mftparser*

U ispisu naredbe moguće je vidjeti kako primjerice druga datoteka u tablici ima nastavak od dva dijela: *.txt.ecc*. Neobično je vidjeti takav oblik nastavka, te je istraživanjem moguće saznati da neke inačice *ransomwarea* TeslaCrypt koriste taj nastavak za označavanje šifriranih datoteka. U ovom slučaju, šifrirana je tekstualna datoteka s originalnim nastavkom *.txt*. U ispisu naredbe je moguće pronaći veći broj datoteka s nastavkom *.ecc* te je tako moguće i saznati koje su datoteke šifrirane.

4 Zaključak

U ovom dokumentu opisano je kako alatom Volatility forenzički analizirati sliku radne memorije računala zahvaćenog stvarnim zlonamjernim softverom. Znanja usvojena kroz ovaj primjer moguće je općenito primijeniti za detaljniju analizu procesa, mrežnih veza, Windows registra i podataka o datotečnom sustavu koji se nalaze u radnoj memoriji.

U kontekstu forenzičke analize računala zahvaćenog zlonamjernim softverom, bitno je imati na umu da je forenzikom radne memorije moguće otkriti neke tragove koje druge grane računalne forenzike jednostavno ne mogu otkriti. Primjerice, neki podaci nikada neće biti zapisani na disk ili poslani preko mreže ili ako i hoće, tada će biti šifrirani. U tom slučaju, jedino mjesto gdje ih je moguće pronaći u otvorenom, nešifriranom obliku će biti radna memorija.

No i dalje, forenzika radne memorije je samo jedna grana forenzike, tako da daljnji koraci u ovakvoj analizi bi svakako uključivali i forenziku diska, snimke mrežnog prometa (ako je ona dostupna) te po potrebi i detaljan reverzni inženjering zlonamjernog programa.

5 Literatura

1. **Martinez, Emiliano.** VirusTotal += Passive DNS replication . [Mrežno] 1. 4 2013. [Citirano: 7. 3 2018.] http://blog.virustotal.com/2013/04/virustotal-passive-dns-replication.html.
2. **Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters.** *The Art of Memory Forensics.* s.l. : Willey, 2014.
3. **Microsoft.** *MSDN - Handles and Objects.* [Mrežno] [Citirano: 8. 3 2018.] https://msdn.microsoft.com/en-us/library/windows/desktop/ms724457(v=vs.85).aspx.
4. **-.** Command Reference. *Volatility Wiki.* [Mrežno] [Citirano: 8. 3 2018.] https://github.com/volatilityfoundation/volatility/wiki/Command-Reference.
5. **Russinovich, Mark.** Pushing the Limits of Windows: Handles. [Mrežno] 29. 9 2009. [Citirano: 8. 3 2018.] https://blogs.technet.microsoft.com/markrussinovich/2009/09/29/pushing-the-limits-of-windows-handles/.
6. **Roussey, Benjamin.** What is passive DNS? [Mrežno] 8. 7 2017. [Citirano: 8. 3 2018.] http://techgenix.com/what-passive-dns/.
7. **-.** DNS and WHOIS - How it Works. [Mrežno] ICANN, 7 2017. [Citirano: 8. 3 2018.] https://whois.icann.org/en/dns-and-whois-how-it-works.
8. **Seals, Tara.** Anti-Forensic Malware Widens Cyber-Skills Gap. [Mrežno] 9. 8 2015. [Citirano: 8. 3 2018.] https://www.infosecurity-magazine.com/news/antiforensic-malware-widens/.