

GLAVNI FAKTORI UTICAJA VIRTUELIZACIJE TIP I NA FORENZIČKU ISTRAGU

Gojko Grubor
Univerzitet Singidunum
e-mail: ggrubor@singidunum.ac.rs

Angelina Njeguš,
Univerzitet Singidunum
e-mail: anjugus@singidunum.ac.rs

Nebojša Ivaniš, dipl. inž. master

Apstrakt: Distribuirano Internet računarstvo (*Cloud Computing, CC*) donosi nove servise, ali i nove tipove ranjivosti koje unosi virtuelno okruženje klijentske i serverske strane. Bezbednost CC sistema je kritičan faktor, a zahteva primenu svih poznatih servisa zaštite, ali i specifičnih rešenja za pokrivanje novih tipova ranjivosti. Literaturni podaci sugerišu da politika zaštite u virtuelnom okruženju zavisi od ugovora o nivou servisa (*Service Level Agreement, SLA*) između davaoca i korisnika CC servisa; da virtuelna mašina ima prednosti u odnosu na fizičku, u procesu digitalne forenzičke istrage prisustva malicioznih programa i da su poznate neke prednosti virtuelne mašinske introspekcije – VMI, kao alata u procesu forenzičke istrage. Malo je dostupnih radova o glavnim faktorima uticaja virtuelizacije tipa I na proces forenzičke istrage. U ovom radu su eksperimentalno verifikovani glavni faktori uticaja virtuelizacije tipa I na digitalnu forenzičku istragu u ograničenom virtuelnom okruženju *MS servera 2008 R2* i *Hyper-V* programa koji omogućava podizanje VM sa različitim operativnim sistemima. Neke pretpostavke ukazuju da je potrebno dublje istraživanje značaja virtuelizacije tipa II za digitalnu forenzičku istragu.

Abstract: The Cloud Computing brings the new services, but the new types of vulnerabilities, too, that virtual environment of the server and client sides introduces. The security of cloud computing becomes a critical factor and it requests implementation of the all known security services, but some specific solution to cover the new vulnerabilities, too. Some references suggest that security policy in a virtual environment mainly depends on the SLA between a vendor and the user of cloud computing services. The VM has some advantages against a physical machine regarding forensic testing bad for malware investigation, as well as some advantages of the VMI has been suggested, too. However, there are quite few works on the impact of virtualization type I to the process of the digital forensic investigation. In this piece of paper the main impact factors of the virtualization type I to the digital forensic investigation are verified through an experiment in limited virtual environment by MS Server R2 and Hyper-V that enables installation of the VM with the different operation systems. Some assumptions show that a deeper investigation of the virtualization type II importance for the digital forensic investigation should be conducted.

1. Uvod

Pojava virtualizacije serverske i klijentske strane na globalnom tržištu unela je velike promene u arhitekturi sistema i dovela do značajne uštede materijalnih sredstava za nabavku

hardvera, programa i infrastrukture. Virtuelizacija je klijentska i serverske hardverske resurse zamenila fajlovima u folderima koji opisuju virtuelne mašine (VM) sa virtuelnim hardverom i funkcionalnostima. Virtuelizovani sistemi distribuiranog Internet računarstva - CC (*Cloud Computing*) prodaju firmama softver, hardver i mrežnu infrastrukturu kao servise. U virtuelnom okruženju, sistem CC može da ponudi različite funkcionalnosti brojnim klijentima, sa različitim zahtevima, bezbednosnim ciljevima i politikama zaštite, ali i nove tipove ranjivosti [4, 5], brojne zloupotrebe i kriminalne aktivnosti. Za kompanije je atraktivna adaptivnost (fleksibilnost) virtuelnog okruženja CC sistema, jer omogućava jednostavno i brzo prilagođavanje dizajna i arhitekture sistema specifičnim potrebama određene kompanije.

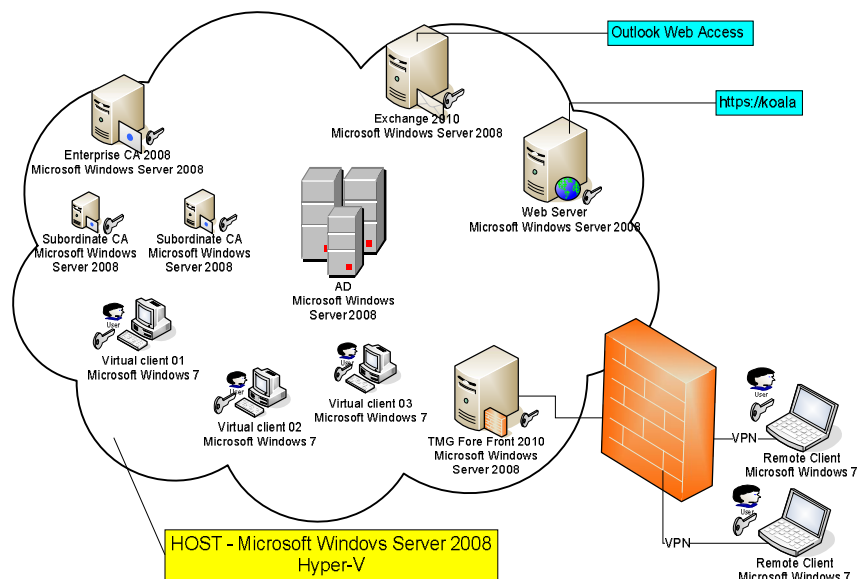
Bezbednost informacija u virtuelnom okruženju postaje kritičan faktor za praktičnu primenu brojnih funkcionalnih prednosti CC sistema. Dostupna istraživanja sugerišu novu paradigmu zaštite u CC sa: primenom tradicionalnih servisa zaštite; ugradnjom umesto naknadnom instalacijom mehanizama zaštite u sistemski hardver i softver; praćenjem toka osetljivih informacija u virtuelnom okruženju kroz intranet, ekstranet i privatne virtuelne mreže; primenom distribuiranih i inovativnih mehanizama zaštite i deljenjem odgovornosti za zaštitu između vendora i klijenta CC servisa, potpisivanjem detaljnog sporazuma o nivou usluga - SLA [2,3]. Izbor politike zaštite CC sistema, najviše zavisi od SLA [6]. Dokazana je i korisna primena VM za ispitivanje prisustva malicioznih programa u ispitivanoj mašini [1], kao i primena VMI za forenzičku akviziciju i analizu [4,1]. Manje su poznata istraživanja glavnih faktora uticaja tipa virtuelizacije na digitalnu forenzičku istragu.

U radu je opisano eksperimentalno istraživanje glavnih faktora uticaja tipa I virtuelizacije na digitalnu forenzičku istragu, izvedeno na serveru MS 2008 2R sa *Hyper-V* programom [11] koji kontroliše VM (*child*) smeštena na domaćinu (*host*) - hardverskoj fizičkoj mašini. Ispitivan je uticaj antiforenzičkog napada u virtuelnom okruženju na forenzičku istragu

2. Eksperimentalna verifikacija glavnih faktora uticaja virtuelizacije na forenzičku istragu

Fleksibilnost virtuelnog sistema u CC omogućava centralizovano upravljanje od strane administratora sistema. Virtuelni sistem može digitalnom forenzičaru omogućiti lakši proces akvizicije i skladištenja podataka sa digitalnog mesta krivičnog dela kompjuterskog kriminala. Pregled i analiza velikih log fajlova mogu se obavljati na jednostavniji i brži način. Takođe, digitalni forenzičar, slučaj istrage može otvoriti na jednostavan način, jer kopiju sistema koji je predmet istrage sa lakoćom može instalirati na forenzičku radnu stanicu, na jednostavniji način izvršiti rekonstrukciju osumnjičenog okruženja i sprovesti forenzičku istragu do kraja [10].

Međutim, virtuelno okruženje nudi neke određene aktivnosti koje se mogu smatrati anti forenzičkim. Tako se pristup digitalnog forenzičara osumnjičenim virtuelnim mašinama mora sprovesti pažljivo i sa obaveznom pred istražnom radnjom, odnosno ispitivanjem virtuelnog sistema na prisustvo malicioznih programa. Prisustvo trojanca prikrivenog rutkit tehnikom u ispitivanom virtuelnom sistemu može ukloniti digitalni dokaz ili obmanuti digitalnog forenzičara [8]. Specifičnosti pristupa digitalnog forenzičara u istrazi digitalnih dokaza u virtuelnom okruženju, na koje je moguće delovanje antiforenzičkih aktivnosti, vezane su za dobro poznavanje sistema kao i celokupne arhitekture koja se pokreće pomoću servera [6]. U ovom istraživačkom eksperimentu, instaliran je operativni sistem *Microsoft Server 2008 R2* u konfiguraciji sistema prikazanoj na Slici 1.

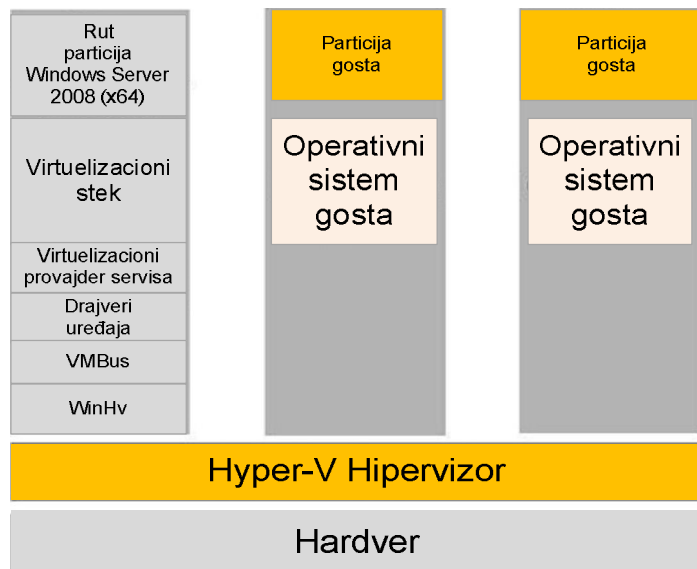


Slika 1. Konfiguracija sistema za eksperimentalnu verifikaciju uticaja virtuelizacije na forenzičku istragu

Instalirane virtuelne mašine u potpunosti koriste hardver servera, kao što to rade gostujuće (*child*) mašine na domaćinu (*host-u*). Hardverski server i instalirani operativni sistem omogućavaju virtuelno okruženje u kojem se virtuelne mašine ponašaju *kao da su fizičke*. Ove informacije su bitne za digitalnog forenzičara, kako bi istragu počeo od lociranja i pristupa *osumnjičenom* serveru koji pokreće virtuelne mašine. Od velike je koristi aktivna (*live*) digitalna forenzička istraga osumnjičene virtuelne mašine, koja se nalazi na nekom serveru u radu, zato što se mogu skupiti brojni dokazi (aktivni procesi, mrežne konekcije, sadržaj RAM-a itd.) [9]. Međutim, ako se kojim slučajem server isključi, uticaj na virtuelne mašine zavisi od stanja procesa rada u kojima su se virtuelne mašine nalazile pre isključenja. Na primer, ako je neka VM u određenom procesu rada, a *host* se u tom trenutku resetuje, VM bi i posle uključivanja ostali u tom istom procesu rada. Poznato je da svi dokazi u forenzičkoj istrazi moraju biti relevantni, sačuvani nepromenjeni, neborivi i prihvatljivi na sudu, a celokupna istraga se mora voditi dokumentovano i transparentno za sudski proces [9].

Sistem CC digitalnom forenzičaru omogućava da, pored uzimanja dva imidža čvrstog diska (HD) osumnjičene mašine, sada može uzeti i dve kopije VM. Jednu kopiju VM treba sačuvati sa heš algoritmom (npr. SHA-256) do suđenja, kao referentni dokazni materijal, a na drugoj sprovesti forenzičku analizu na forenzičkoj radnoj stanici. Korišćeni forenzički alati moraju podržavati i korektno raditi u virtuelnom okruženju, kao i sa novijim operativnim sistemima, jer su velike mogućnosti antiforenzičkih aktivnosti. Prikupljanje i akvizicija digitalnih dokaza u virtuelnom okruženju je mnogo složenija i teža, nego sa statičke fizičke mašine. Eksperiment je potvrdio da je, od forenzičkih alata u virtuelnom okruženju, moguće koristiti *EnCase*, *X-Ways Forensic*, *FTK Imager* i *Whireshark*. Ovi alati su naučno ispitani i rad u CC sistemima im nije nepoznat, dok njihova efektivnost može zavisiti samo od operativnih sistema instaliranih na virtuelnim sistemima. Da bi forenzičar mogao da prikuplja dokaze sa osumnjičene VM koja se nalazi na fizičkom *host-u*, mora dobro poznavati arhitekturu i princip rada hardverske virtuelizacije koja opisuje sistem [10]. Veoma je bitno da se sada sve informacije nalaze na fizičkom serveru, u odnosu na klasičnu digitalnu forenziku, gde su se informacije nalazile na klijentskim računarima. Nepotrebno je juriti lokaciju VM, osim ako se

ne traga za osobom koja je osumnjičena, što je posao organa javne bezbednosti, a ne digitalnog forenzičara. Osumnjičeni se može nalaziti bilo gde u fizičkom prostoru, jer pristupa virtuelnoj mašini kroz *remote desktop* sa udaljene lokacije. Virtuelna mašina koja se nalazi u virtuelnom CC sistemu ima stvarnu lokaciju na hardverskom *host-u*. U odnosu na fizički računar do koga se moglo doći fizičkim putem, pristup VM se svodi na traganju za fizičkom lokacijom *host-a*, na kojem su pokrenute virtuelne mašine. Kada se *host* locira tada mu treba fizički pristupiti, zbog čega je bitno znati, koje sve vrste virtualizacija postoje, ali i koje virtuelne usluge mogu biti omogućene ili pružene virtualnim mašinama od strane *host-a*. U eksperimentu je korišćena virtualizacija tipa I.



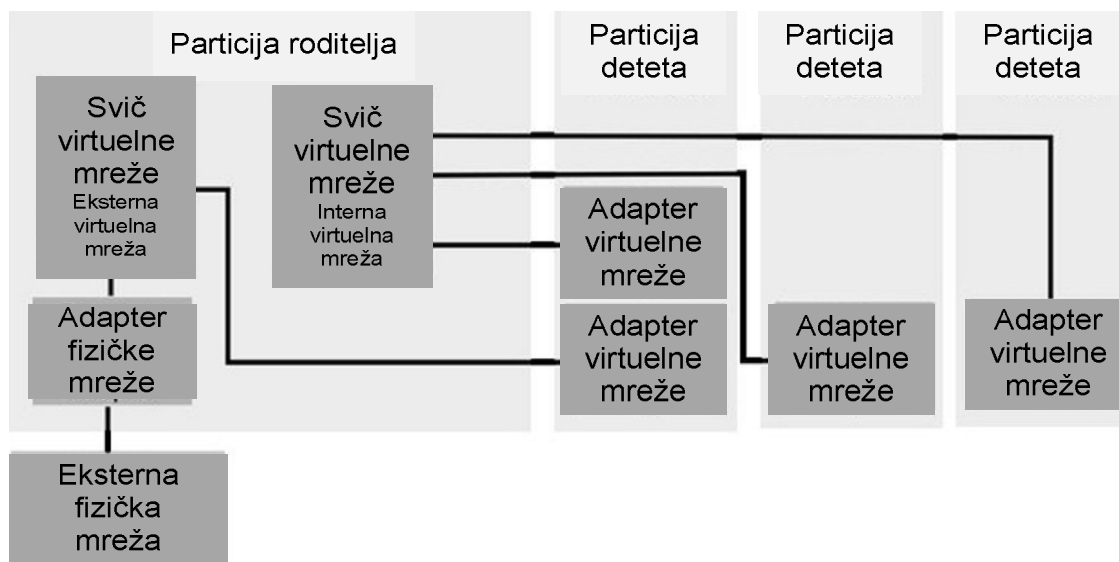
Slika 2. Tip 1 virtualizacije

Na Slici 2. je predstavljen tip 1. virtualizacije, gde virtualna mašina koristi hardverske resurse *host-a* na kome je instaliran operativni sistem za serversku podršku. Sam *host* je odgovoran za deljenje resursa gostujućih mašina (*child-ova*) koji se nalaze na njemu. Princip virtualizacije je da se omogući virtuelnoj mašini da koristi fizički procesor i RAM memoriju na *host-u*. Može se smatrati da razlika između forenzičkog pristupa virtuelnoj i fizičkoj mašini ne postoji, jer slika prikazuje da virtuelna mašina koristi resurse fizičkog *host-a*. Informacije koje digitalni forenzičar može da prikupi i koristi, mogu biti dostupne na fizičkom *hard disc-u* kao i u RAM memoriji *host-a*. Ekvivalent predstavlja pristup digitalnog forenzičara fizičkoj mašini, ali samo iz ovog trenutnog pogleda na hardver *host-a* i uz korišćenje istog od strane virtuelne mašine.

Međutim, ipak postoje velike razlike u pristupu digitalnoj forenzičkoj istrazi virtuelnih mašina. *Hyper-V* koncept koji pokreće CC sistem radi samo na hardverski predefinisanim i kompatibilnim procesorima nove generacije koji podržavaju proces rada sa hipervizirom. Podrazumeva se da na matičnoj ploči računara ili servera postoji procesor koji podržava hipervizor. Hipervizor uspostavlja komunikaciju sa *VMBus driver-om* koji dalje komunicira sa virtuelnim mašinama. Tipovi procesora koji podržavaju hardversku virtualizaciju su: *AMD-V* i *Intel VT chipset*. Bitno je da procesori rade na određenom prstenu jezgra procesora, jer taj prsten jezgra omogućava određenu zaštitu koda. Tako da su se pojavili i procesori od istih

proizvođača koji nude i antivirusnu zaštitu na samom procesoru. Postoji mogućnost da hakeri izvrše napad na takt procesora koji je na *host-u*, a da se napad izvrši preko virtuelnog klijenta koji koristi *host*. Hardverski resursi *host-a*, među kojima je i procesor, mogu biti izloženi napadima hakera, ali samo ako se koriste interna mreža koja koristi virtuelni mrežni adapter ili eksterna mreža koja koristi hardverski mrežni adapter, između *host-a* i *child-ova*. Tim napadom bi se srušio server na kome je CC sistem pokrenut i automatski bi prestale da rade i sve virtuelne mašine koje su gosti na *host-u*.

Ugrađeni antivirusni programi na procesorima su novina u industriji informacionih tehnologija i trebalo bi da spreče ovakve napade, kao i da obezbede miran rad klijentskim virtuelnim mašinama. Novina je i opcija *hipertrade* koja omogućava, na primer, da *host* izabere jedno od dva, četiri ili šest jezgara procesora za svoj rad, a da klijentima ili *child-ovima* ponudi ostala jezgra procesora. Predhodno pomenuti napad na procesor ne bi bio moguć, jer su procesi podeljeni između *host-a* i *child-ova* i ne utiču jedni na druge, ako bi se koristila usluga *hipertrade-a*. Postoje i procesori sa šest jezgara tako da se hardverska infrastruktura sve više razvija da odgovori potrebama CC sistema. Kada se kernel kôd operativnog sistema izvršava, kaže se da radi u oblasti jezgra ili supervizor modu. Tada procesor radi na prstenu „0“. Prsten „0“ se još zove privilegovani prsten operativnog sistema. Aplikacije u sistemu rade na prstenovima „1, 2 ili 3“. Hipervizor, na matičnoj ploči, na kojoj je instalirana podrška za *hyper-V* i koja pokreće rad virtuelnih mašina, radiće na privilegovanom prstenu „0“. Takav rad omogućava da *hyper-V* može da upravlja operacijama na samom procesoru i RAM memoriji *host-a*. Isto tako, hipervizor će na ostalim nivoima prstenova procesora omogućiti upravljanje aplikacijama u virtuelnom okruženju. Svaki iskusni projektant informaciono komunikacionih sistema koji se bavi kreiranjem virtuelnih mreža, prvo će se uvek pozabaviti pretpostavkama mogućih problema u logici, funkcionalnostima i organizaciji same virtuelne mreže. Takođe, mora da obrati pažnju, kako će okruženje reagovati na korisnika i obrnuto, odnosno, na bezbednosne aspekte i ulogu virtuelne mreže koja se projektuje na globalnu Internet mrežu. Ova oblast je veoma bitna za svakog digitalnog forenzičara, zbog toga što mora poznavati suštinu CC sistema, ali i da uočava detalje vezane za stvaranje jedne ili više digitalnih virtuelnih ili realnih mreža koje koriste CC sistem. Digitalni forenzičar mora razumeti proces istrage nad *host-om*, koji može imati više gostujućih VM, zavisno od potreba CC sistema. Potrebe CC sistema zahtevaju proširivanje hardverskih resursa u većem obimu na samom *host-u*, jer od potreba zavisi i arhitektura virtuelnog okruženja. O tim potrebama treba da razmišlja i digitalni forenzičar, u procesu forenzičke istrage u virtuelnom okruženju. Postoji mogućnost da digitalni forenzičar ima određena saznanja ili pretpostavke o hardveru *host-a*, što mu može pomoći u izboru pravca istrage, pod pretpostavkom da je projektant virtuelnog okruženja sa druge strane zakona i samim tim osumnjičen. U eksperimentu je *Host* podržan operativnim sistemom *Windows Server 2008 R2*, a *hyper-V* omogućava podizanje VM (*child-ova*) sa različitim operativnim sistemima, bezbednosnim ciljevima i politikama zaštite. Primer jednog arhitektonskog pogleda na domen virtuelnog okruženja prikazan je na Slici 3.



Slika3. primer jedne mrežne strukture u virtuelnom okruženju

2.1. Vrste virtualnih mreža

Struktura virtualnih mreža mora biti dobro poznata digitalnom forenzičaru, kako ne bi postao žrtva obmane osumnjičenog koji koristi sistem CC u ne zakonite svrhe. Sistem CC omogućava primenu tri različite kategorije virtualnih mreža u kojima se koriste VM-e [1,3]:

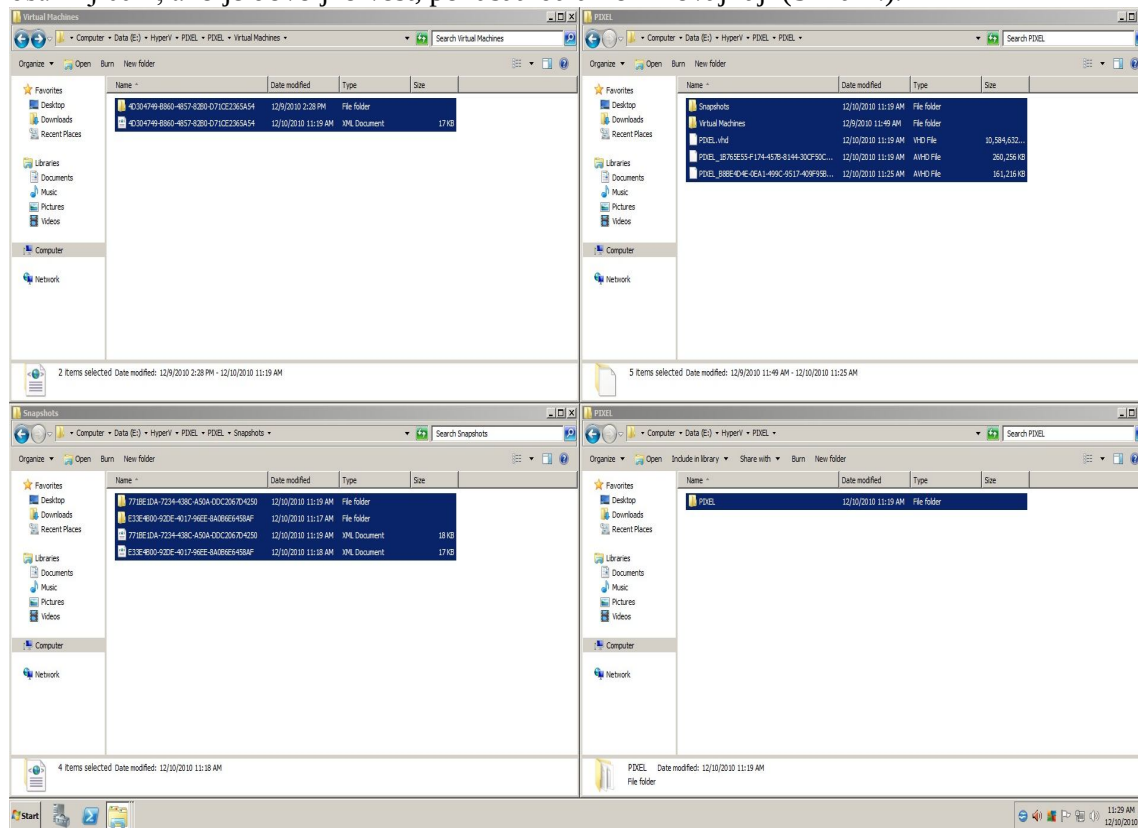
1. **Spoljna virtuelna mreža** (eksterna) – koristi fizički mrežni adapter i omogućava nesmetanu komunikaciju sa fizičkim, ali i VM, kako u intranet mreži tako i na Internetu. Otvorena je mogućnost napada zlonamernih hakera na *host* preko virtualnih klijenata tj. *child*-ova, jer je komuniciranje na relaciji *host-child* moguće kao i kod fizičkih računarskih mreža [12]. Digitalni forenzičar pristupa prikupljanju dokaza isto kao i kod fizičkih mreža.
2. **Unutrašnja virtuelna mreža** (interna) – ova kategorija mreže ne zahteva fizički mrežni adapter, već je dovoljno da koristi virtualni mrežni adapter. Omogućava komunikaciju između virtualnih mašina u intranetu, ali i mogućnost komuniciranja sa *host*-om. Ako *host* ima ulogu rutera može se obavljati komunikacija i sa članovima koji su van interne virtualne mreže, jer bi tada u komunikaciju bio uključen i fizički mrežni adapter sa *host*-a. Pošto je omogućeno komuniciranje sa *host*-om od strane *child*-a, znači da postoji mogućnost upada zlonamernih hakera na *host* uz korišćenje *child*-a.
3. **Privatna virtuelna mreža** (*private*) – funkcioniše slično kao i interna virtuelna mreža. Ne zahteva fizički mrežni adapter, ali ne dozvoljava pristup gostima u virtualnu privatnu mrežu, jer nisu članovi te mreže. Isto tako ni *host* ne može da komunicira sa tom mrežom. Ovakva vrsta virtualne mreže ne dozvoljava upad zlonamernih hakera kao i mogućnost napada na *host*, jer nema direktne komunikacije na relaciji *host-child*.

2.2. Struktura virtualne mašine

Svaki *child* na *host-u*, mora negde da beleži svoje podatke. Zato se mora odrediti veličina prostora virtuelnog *hard disc-a* (VHD), kao i njegova lokacija na *HD-u host-a*. U pogledu smeštaja i čuvanja podataka na *hyper-V*, postoje nekoliko mogućnosti, kao što su:

- *Hyper-V Supports Direct Access Storage* (DAS) drajveri koji uključuju IDE, SATA, SCSI, SAS i
- *Storage Area Network* standarde koji koriste *fiber channel* i iSCSI.

VHD fajl ima ekstenziju **.vhd** i igra ulogu *HD-a* virtuelne mašine. Razumljivo je da sa ovim fajlom osumnjičeni može lakše da manipuliše, nego sa HD fizičke mašine; može ga prekopirati na neku udaljenu lokaciju, obrisati ili izmeniti i na brz i jednostavan način ukloniti dokaze koji ga terete. Takođe, osumnjičeni može **.vhd** fajlu pristupiti i kroz mrežu sa nekog udaljenog *host-a*, koji nije u fizičkom okruženju osumnjičenog, tako što će prekonfigurisati fajl sa ekstenzijom **.xml**. U fajlu **.xml** biće upisana putanja do fajla **.vhd**, gde je stvarna lokacija virtuelnog *HD-a* na kome se fajl **.vhd** stvarno i nalazi. Fajl **.bin** simulira virtuelnu RAM memoriju i može biti veoma bitan digitalnom forenzičaru u procesu istrage, jer se u njemu mogu naći određeni dokazi koji terete osumnjičenog. Treba očekivati da će osumnjičeni, ako je dovoljno vešt, pokušati da ukloni i ovaj fajl (Slika 4.).



Slika 4. Folderi i fajlovi koji su sastavni deo svake virtuelne mašine

2.3. Eksperimentalna verifikacija forenzičke analize u virtuelnom okruženju

U eksperimentu je izveden potencijalni scenario antiforenzičkog napada osumnjičenog, koji pokušava da ukloni dokaze sa kompromitovane VM tehnikom kloniranja. Osumnjičeni prvo

klonira legalan sistema koji nije kompromitovan (osumnjičen). Potom izvrši određene nezakonite radnje, npr. skida nelegalan sadržaj sa *web* stranica i smešta ga na VM, razmenjuje putem mreže ilegalne slike i nove slike smešta na VM i virtuelni *HD* (fajl **.vhd**) itd. Osumnjičeni vrši nezakonite radnje u određenom vremenskom periodu, a onda uplašen od moguće istrage primeni klon koji je predhodno napravio. Kopiranjem klona bit po bit preko kompromitovanog sadržaja nastoji da ukloni sve dokaze iz **.vhd** fajla ili virtuelnog *HD-a*. Posle operacije kloniranja operativnog sistema sa ranije, legalno napravljenim klonom prividno uklanja sve dokaze, jer legalan klon prekopira celokupni kompromitovani **.vhd** fajl. Međutim, podaci su otkriveni uzimanjem imidža virtuelnog *HD-a* osumnjičene virtuelne mašine, sa forenzičkim alatom *FTK Imager*. Sve aktivnosti osumnjičenog su zabeležene u fajlu *pagefile.sys*, koji koristi RAM memorija, tačnije fajl **.bin**, počevši od konekcija sa *web* stranicama kojima je pristupao, do fajlova i foldera koje je kreirao. Ovo je još jedna novina u forenzičkoj istrazi u virtuelnom okruženju, koje može biti korisna za digitalnog forenzičara, ali i iskoristiva za antiforenzički napad. Kada se administrator sistema odluči da omogući korisniku VM da na nju instalira određenu aplikaciju, za koju smata da može ugroziti korektnost rada VM, onda treba da napravi sliku trenutnog stanja VM - *snapshots*, pre nego što korisnik pokrene instaliranje aplikacije. Od trenutka kada se, kao kod foto aparata, „okine“ slika stanja VM, dolazi do kreiranja fajla **.avhd**, koji počinje da beleži sve moguće operacije korisnika u radu, ali i korišćenje operativnog sistema VM. Kako raste broj zabeleženih operacije, srazmerno se povećava fajl **.avhd**. Kada se „okine“ još jedna slika stanja VM, napraviće se novi fajl **.avhd**, koji od tog trenutka počinje sa beleži operacije korisnika, dok predhodni fajl ostaje sačuvan. Standardni tragovi zapisa ovih fajlova su *ime mašine*, *datum i vreme kreiranja*, ali se može izmeniti ime slike stanja VM. Primenom forenzičkog alata *X-Way Forensic* na fajl **.avhd** izvučene su sve informacije iz virtuelne RAM memorije, jer je fajl **.avhd** u sprezi sa fajlom **.bin**, koji beleži sve što se našlo u memoriji od „okidanja“ slike stanja VM, pa sve do trenutka novog „okidanja“. Tačnije, sve što je jednim slikanjem stanja VM zabeleženo u određenom trenutku, ostaće zapamćeno u fajlu **.bin**, čak i ako se *host* restartuje. Ako osumnjičeni ukloni fajlove koji ga mogu povezati sa dokazom da je izvršio „okidanje“ slike stanja VM, a pritom da negira tu radnju, digitalni forenzičar će pronaći informacije o „okidanju“ slike stanja VM u registrima *host-a* sa datumom i vremenom događaja.

Dakle, ovo je još jedan novi faktor uticaja virtuelizacije na digitalnu forenzičku istragu. Kod klasične forenzičke istrage fizičke mašine ova situacija u virtuelnom okruženju može se uporediti sa zaštitom *HD-a* kod fizičkih desktop i laptop mašina. Kada se isključi fizička mašina kod koje je primenjena ovakva zaštita, nije moguće izvući informacije sa takvog *HD - a*. Kod VM se ne primenjuje takva praksa i ne postoji takva vrsta zaštite nad fajlovima **.vhd** i **.avhd**, osim ako *host* nema zaštitu fizičkog *HD-a*. Postoji mogućnost da osumnjičeni u antiforenzičkom napadu primeni određeni kriptološki algoritam (npr. AES) i šifruje pristup folderu u kome su smešteni fajlovi **.vhd**, **.avhd**, **.bin** i **.xml**. Time bi mogao da napravi problem digitalnom forenzičaru. Ipak, ovaj primer nema direktnu vezu sa uticajem virtuelnog okruženja na forenzičku istragu, ali omogućava korisniku u virtuelnom okruženju da šifruje samo određene foldere i fajlove koje želi da zaštiti [7].

3. Zaključak

U virtuelnom okruženju kompjuterski incidenti su ekvivalentni krivičnom delu (zločinu) u realnom životu. Digitalnoj forenzičkoj istrazi treba pristupiti drugačije nego istrazi u fizičkom svetu koju ljudska čula rezonuju i osećaju. U poređenju sa dlakom osumnjičenog ili čaurom metka kojim je izvršeno ubistvo, kod digitalne forenzičke istrage u virtuelnom okruženju

moraju se razumeti apstraktne pojave VM-a, servera, mreža, fajlova itd. Ovde su dokazi binarne 0 i 1, kao i velika lepeza fajlova različitih funkcionalnosti. Informacije mogu biti promenjene u deliću sekunde i sa jednim ili par klikova miša, tako da digitalni forenzičar lako može ostati bez dokaza.

Moguće zloupotrebe ili antiforenzičke aktivnosti u virtuelnom okruženju, ne mogu se uvek kontrolisati, a kada se dogode, mogu naneti veliku materijalnu i moralnu štetu pojedincu i društvu. Apsolutna bezbednost u virtuelnom okruženju ne postoji. Posebno se mora voditi računa o faktoru ljudske greške, koja bi mogla dovesto do zombiranja virtuelnog sistem i posrednog napada na neki društveno značajniji sistem. Preuzimanjem softvera sa inficirane web stranice i instaliranjem na virtuelnu mašinu, može se preuzeti trojanac sa rutkit tehnikom za skrivanje. Za forenzičku istragu u virtuelnom okruženju, bitno je imati dobru IDPS zaštitu od upada u sistem, antirut i antivirusnu zaštitu na bazi kombinovacije heuristike i digitalnog potpisia. Na ovaj način se može onemogućiti tzv. „trojanska odbrana“ osumnjičenog [8, 12]. Digitalna forenzička istraga u virtuelnom okruženju ima brojna otvorena pitanja. Posebno je značajno istražiti uticaj virtulizacije tipa II na forenzičku istragu, gde se monitor VM nalazi iznad sloja aplikacija. i ulascima u diskusiju sa kolegama iz naučne oblasti digitalne forenzike, moraju se nalaziti odgovori za određene situacije i probleme u istrazi. Svako novo saznanje i rešenje u sferi digitalne forenzičke istrage u virtuelnom okruženju, može dati veliki doprinos u rešavanju potencijalnih slučajeva kompjuterskog kriminala u CC okruženju. Funkcionalne prednosti CC za poslovne sisteme očekivano šire primenu CC servisa, ali i novi tipovi ranjivosti virtuelnog okruženja povećavaju rizike od napada i zahtevaju specifični pristup forenzičkoj istrazi, na koju utiču novi faktori svojstveni virtuelnom okruženju.

Literatura

- [1] Barrett, D., Kipper, G., *Virtualization and Forensics a digital forensic investigator's guide to virtual environments*, Elsevier Inc., Burlington, MA 01803, USA, 2010.
- [2] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, December 2009.
- [3] Garrison, C., *Digital Forensics for Network, Internet, and Cloud Computing a forensic evidence guide for moving target and data*, Elsevier Inc., Burlington, MA 01803, USA, 2010.
- [4] Grubor, G., Njeguš, A., *Paradigma zaštite distribuiranog računarstva*, Naučni skup Sinergija 10, Bijeljina, 2010.
- [5] [IBM, IBM X-Force 2008 Annual Report, www.ibm.org](http://www.ibm.org), 2008.
- [6] [Mather T.](#), [Kumaraswamy S.](#), [Latif S.](#), *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) (Paperback)*, O'Reilly, 2009.
- [7] Meisel A., *Art of Defence*, Security News, 23.7. 2009.
- [8] Milosavljević, M., Grubor, G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Beograd, 2009.
- [9] Milosavljević, M., Grubor, G., *Istraga kompjuterskog kriminala – metodološko tehnološke osnove*, Univerzitet Singidunum, Beograd, 2010.
- [10] Sun Microsystems, *Advanced cloud security tools*, CSA Security News, decembar 2009

Web izvori:

- [11] http://www.virtuatopia.com/index.php/Hyper-V_Essentials
- [12] http://www.symantec.com/security_response/writeup.jsp?docid=2005-081910-3934-99