



Univerzitet
Singidunum

UNIVERZITET SINGIDUNUM
SAVREMENE INFORMACIONE TEHNOLOGIJE

MASTER STUDIJE

Master rad:
**Digitalna forenzička istraga u
virtuelnom okruženju**

MENTOR:
Docent dr. Gojko Grubor

KANDIDAT:
Nebojša Ivaniš

Beograd, februar 2011.

Abstract:

The master paper deals related to digital forensic investigations in a virtual environment. The first part deals with the approach of digital forensics in a virtual environment, known as cloud computing. While the second part deals with a topic related to anti-forensic capabilities that provide a virtual environment. Access to digital forensics virtual machine differs greatly from access to physical machines, and these differences are described. Virtual machines use hardware servers completely, as do guest accommodation. Communication between virtual machines and servers is implemented over a bus driver and the hypervisors that communicate via hyper call. The processor allows the calls to its operations are carried out at the privileged ring 0 processor that was used by the kernel. The importance of virtual environment driven by a hardware server, allowing virtual machines to feel as if they were physical. This information is essential for digital forensics to know that access to the start of the investigation to locate and access server running virtual machines. Access live digital forensic investigation of suspect virtual machines on a server, is very useful because it can be collected ample evidence, while the server is turned on. All evidence must have weight, must be preserved, should not be changed and the entire investigation must be conducted through an open case. Forensic tools must support and work correctly in a virtual environment as well as in newer operating systems because the possibility of manipulation of evidence by the suspect in this environment is great, so the job of collecting evidence and more complex and difficult.

Key words: *Cloud Computing, BUS driver, hypervisor, hipercalls, Hyper-V host, child, migration, live migration, anti-forensic activities, Evidence Eliminator, viruses, worms, Trojan horses*

Abstrakt:

U master radu obrađena je tema vezana za digitalnu forenzičku istragu u virtuelnom okruženju. Prvi deo rada obrađuje pristup digitalnog forenzičara u virtualnom okruženju, poznatijem kao *Cloud Computing*. Dok drugi deo rada obrađuje temu vezanu za anti forenzičke mogućnosti koje virtuelno okruženje pruža. Pristup digitalnog forenzičara virtuelnim mašinama se u mnogome razlikuje od pristupa fizičkim mašinama i te razlike su opisane. Virtualne mašine koriste hardver servera u potpunosti, kao što to rade gosti kod domaćina. Komunikacija između virtualnih mašina i servera se sprovodi preko *BUS driver-a* i hipervizora koji komuniciraju preko hiper poziva. Procesor dozvoljava ovim pozivima da svoje operacije sprovode na privilegovanom prstenu 0 procesora koji je do sada koristio kernel. Značaj virtualnog okruženja koga pokreće hardverski server, omogućava virtuelnim mašinama da se osećaju kao da su fizičke. Ove informacije su bitne za digitalnog forenzičara kako bi znao da pristup istrazi počne od lociranja i pristupa serveru koji pokreće virtualne mašine. Živi pristup digitalnog forenzičar u istrazi nad osumnjičenim virtuelnim mašinama na nekom serveru, je od velike koristi zato što se mogu skupiti brojni dokazi, dok je server uključen. Svi dokazi moraju imati težinu, moraju biti sačuvani, ne smeju biti menjani i celokupna istraga se mora voditi kroz otvoreni slučaj. Forenzički alati moraju podržavati i korektno raditi u virtuelnom okruženju kao i u novijim operativnim sistemima jer mogućnost manipulacije dokaza od strane osumnjičenog u ovakvom okruženju je velika, pa je tako i posao prikupljanja dokaza složeniji i teži.

Ključne reči: *Cloud Computing, BUS driver, hipervizor, hipercalls, Hyper-V, host, child, migracija, živa migracija, anti forenzičko delovanje, Evidence Eliminator, virusi, crvi, trojanski konji*

Sadržaj:

1. Metodologija istraživačkog projekta.....	6
1.2. Predmet istraživanja	7
1.3. Ciljevi i zadaci istraživanja.....	8
1.4. Hipotetički okvir istraživačkog rada.....	8
1.5. Metodi, tehnike i tok istraživačkog procesa	9
 2. Digitalna forenzička istraga u virtuelnom okruženju	11
2.1. Teorijske osnove.....	11
2.2. Specifičnosti forenzičke istrage u virtuelnom <i>hyper-V</i> okruženju.....	15
2.3. Pristup mestu osumnjičene virtualne mašine	17
2.4. Cloud Computing	19
2.5. <i>Hyper-V</i> virtualizacija tipa 1.....	19
2.6. Hardverska pomoć virtualizaciji	19
2.7. <i>Hyper-V</i> host i child	26
2.8. Sistemski zahtevi <i>hyper-V</i>	30
2.9. Zahtevnost <i>hyper-V</i> kod operativnih sistema i korišćenja procesora	30
2.10. Hardversko podešavanje <i>hyper-V</i>	31
2.11. Memorijski zahtevi <i>hyper-V</i>	31
2.12. Mrežni zahtevi <i>hyper-V</i>	32
2.13. Instalacija <i>hyper-V</i> na operativni sistem kao i forenzičko delovanje na isti.....	33
2.14. Instalacija <i>hyper-V</i> iz komandne linije.....	33
2.15. Konzola za upravljanje <i>Hyper-V</i>	34
2.16. Arhitektura i razumevanje virtualnih mreža	37
2.17. Vrste virtuelnih mreža.....	38
2.18. Kreiranje virtualnih mašina na <i>hyper-V</i>	41
2.19. Dodeljivanje memorije na virtualnoj mašini	42
2.20. Podešavanje mrežnog adaptera na virtualnoj mašini	43
2.21. Podešavanje virtualnog <i>hard disc-a</i> na virtualnoj mašini.....	43
2.22. Instaliranje i pokretanje operativnih sistema na virtuelnim mašinama	45
2.23. Konekcijski alat između virtualnih mašina i <i>hyper-V</i>	47
2.24. Kreiranje i upravljanje <i>hyper-V Snapshots</i>	48
2.25. Razumevanje i instalacija <i>hyper-V</i> usluga integracije.....	50
2.26. Pristup forenzičkim alatima na <i>hard disc</i> virtualne mašine	55
2.27. Uticaj antiforenzičkih aktivnosti u virtuelnom <i>hyper-V</i> okruženju na digitalnu forenzičku istragu.....	62
2.28. Migracije unutar <i>hyper-V</i> okruženja	63
2.29. Mogućnosti i ograničenja virtuelne mašinske migracije.....	63
2.30. Izvoz virtuelne mašine u <i>hyper-V</i> okruženju.....	64
2.31. Anatomija izvoza virtuelnih mašina u <i>hyper-V</i>	66
2.32. Uvoz virtuelnih mašina u <i>hyper-V</i> okruženje.....	67
2.33. Živa migracija u <i>hyper-V</i> okruženju	67
2.34. Konfiguracioni zahtevi za živu migraciju u <i>hyper-V</i> okruženju	68
2.35. Proces žive migracije	68
2.36. Konfigurisanje virtuelne mašine kako bi bila stalno dostupna	69

2.37. Podešavanje virtuelne mašine za automatski start	69
2.38. Izvođenje žive migracije pomoću <i>Failover Cluster Manager</i>	70
2.39. Izvođenje žive migracije pomoću programa <i>Windows PowerShell</i>	70
2.40. Kreiranje i upravljanje slikama stanja virtuelnih mašina u <i>hyper-V</i> okruženju.....	70
2.41. Slika stanja u <i>hyper-V</i> okruženju.....	71
2.42. Uzimanje slike stanja virtuelnim mašinama.....	71
2.43. Hijerarhijsko drvo snimka stanja za virtuelnu mašinu u <i>hyper-V</i> okruženju.....	72
2.44. Upravljanje slikama stanja.....	72
2.45. Anatomija slike stanja u <i>hyper-V</i> okruženju	73
 3.Studije slučajeva.....	75
3.1.Studija slučaja 1: Snapshots.....	75
3.1.1. Praktični primer slike stanja na virtuelnoj mašini.....	75
3.2.Studija slučaja 2: Zombiranje.....	87
3.2.1. Zombirana virtuelna mašina u <i>hyper-V</i> okruženju	87
3.3.Studija slučaja 3: Kloniranje.....	99
3.3.1. Anti forenzičko delovanje kloniranja operativnog sistema.....	99
3.4.Studija slučaja 4: <i>Evidence Eliminator</i>	108
3.4.1. Antiforenzičko delovanje na digitalne dokaze sa alatom <i>Evidence Eliminator</i>	108
3.5.Studija slučaja 5: <i>Malveri</i>	112
3.5.1. Virusi, trojanski konji i crvi	112
 4.Diskusija.....	114
 5.Zaključak.....	117
 6.Literatura.....	118

Zahvalnost

Prvi korak u dvokoraku, koji me vodi do postizanja cilja i uspešnog završetka doktorskih studija jesu završene master studije. Kako bi zaokružio svoje životno školovanje i stekao odgovarajuće titule i zvanja, moja velika želja je bila da pristupim istraživanju master studija iz oblasti digitalne forenzike u virtuelnom okruženju. Zbog toga, ovim putem želim da se zahvalim meni dragim osobama koji su mi na direktan ili indirektan način dali podršku da završim diplomske i master studije. Među prvima je moja supruga Zoka koja je trudna i nosi malu ćerkicu Smu kao i moji roditelji otac Duško i majka Nadežda koji su mi davali neizmernu moralnu podršku tokom studiranja i bili uvek od pomoći kada je bilo najteže. Moj brat Ljubomir kao i prijatelj Slobodan Kundadžija koji su mi davali uvek korisne stručne savete iz oblasti informacionih sistema i sistema zaštite. Želeo bih ovim putem da se zahvalim profesorima Milanu Milosavljeviću, Mladenu Veinoviću i mentoru Gojku Gruboru na čijim konsultacijama sam kroz diskusiju uvek dobijao konkretne i precizne informacije vezane za predmete koje sam pohađao.

Nebojša Ivaniš

1. Metodologija istraživačkog projekta

1.1. Uvodne napomene i obrazloženje rada

Pojavom računarskih mreža, njihovim razvojem i umrežavanjem u sistem globalne mreže Interneta, dolazi do zloupotrebe i narušavanja osnovnih funkcionalnosti – komunikacije i prenosa informacija, kao i do sve većeg broja napada sa Interneta, bilo nekim malicioznim programima ili od strane čoveka – hakera, krakera, vandala i kompjuterskog teroriste.

Razlozi za pojavu ovih napada su različiti. Najčešći razlog je sticanje finansijske dobiti, ali i drugi motivi, kao što su izazov, znatiželja, samopotvrđivanje, krađa informacija, špijunaža i drugi oblici kompjuterskog kriminala. "Pod kompjuterskim kriminalom u najširem smislu podrazumevaju se krivična dela prema krivičnom zakonu nacionalne države, u kojoj su na bilo koji način uključeni računarski sistemi i mreže. Glavni cilj istrage kompjuterskog kriminala je, kao i u slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv, ili čvrst dokaz, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela."¹ Da bi se obezbedio takav dokaz, u slučaju kompjuterskog kriminala, potrebno je, nizom posrednih dokaza, doći do informacija u digitalnom obliku koje imaju verodostojnu vrednost, a koja je uskladištena ili prenesena u takvom obliku. Ovakve informacije su digitalni dokazi.

U zvaničnoj istrazi kompjuterskog kriminala, u toku prikupljanja, analize i prezentacije digitalnih dokaza, mora se pridržavati određenih principa. Najbolja forenzička praksa dokazala je da je najbolje formirati tim od tri profesionalca: zvaničnog organa istrage, tužioca i eksperta u oblasti Informaciono komunikacionog sistema. U slučaju kompjuterskog kriminala česta je praksa da se zahteva ekspertsko svedočenje ili veštačenje pred sudom.

Pojavom virtuelnog okruženja, koje je usledilo razvijanjem i stalnim napredovanjem tehnologija, koje se koriste u Informaciono komunikacionom sistemu, otvorio se veliki spektar pravaca korišćenja računara. Njihova primena, koja se uvek može smatrati napretkom i pozitivnom novinom za društvo u globalnu, isto tako može ponuditi i mogućnost velikih zloupotreba i nanošenje materijalne i moralne štete kako društvu tako i pojedincu.

Smisao upotrebe virtuelizacije računara u današnje vreme vezan je, prvo zbog finansijskog momenta i odbacivanja velikog broja hardverskih uređaja, koje su koristili klijenti. Usmeravanje ka serverskom okruženju, centralizovano nadgledanje, kao i jednostavnija i fleksibilnija upotreba računara za različite uloge, ponudiće klijentu jednostavniji, sigurniji, moderniji i brži rad ali pod uslovom da svoj računar koristi u legalne i društveno korisne svrhe. Tačnije, klijentski računari na globalnom nivou trošili su puno energije i resursa, i plus zahtevali velike troškove samih klijenata koji su morali kako tehnologija napreduje da svoje personalne računare s vremena na vreme poboljšavaju kako bi pravili korak sa novim i zahtevnijim operativnim sistemima. Tako da pokušaj IBM-a, da napravi terminale kojima bi klijenti pristupali, još 60-tih godina prošlog veka, mogao je dati neke pretpostavke stvaranja virtuelnog računarskog okruženja. Ali sve do pre dve godine, nije mogla ni da se zamisli sama snaga virtuelizacije i budućeg okruženja *Cloud Computinga*, koje će dejstvovati na društvo sa svojim pozitivnim i negativnim svojstvima.

Kako je sam proces virtuelizacije računarskog okruženja predložen javnosti, odmah je nekolicina firmi startovala i krenula u proces stvaranja aplikacija koje bi ponudile velikom broju korisnika, a koje će simulirati virtuelno okruženje. Takve aplikacije se sada mogu naći i preuzeti sa Internet

¹ Milosavljević M., Grubor G., *Digitalna forenzika*, Univerzitet Singidunum, Beograd 2008, str. 12

stranica proizvođača besplatno, a neke od poznatih aplikacija su: *Citrix*, *VMware* i *Sun Microsystems*. I to su samo neki od proizvoda koji se nude korisniku. Kako se i računarski virtuelni svet razvija, tako i razvoj aplikacija prati u stopu i pokušava da omogući jednostavniji i lakši rad, a da korisnik i ne primećuje da se nalazi u takvom virtuelnom okruženju. Ali, proizvođači u početku su ušli samo ponudom aplikativnog virtuelnog okruženja, što nije bilo dovoljno za korporacijsko tržište. Sve dok Microsoft kompanija nije ponudila operativni sistem *Windows Server 2008* Cora 2 ediciju i pokrenula tektonske poremećaje na svetskom korporativnom tržištu. U 2008. godini, Microsoft kompanija je izbacila *Windows Server 2008* cor 2 i veoma brzo je dobio pozitivne kritike. Koncept samog operativnog sistema zamišljen je tako da virtuelne mašine koriste hardvere *host-a* i da pri tom budu smeštene na određenoj lokaciji na tom *host-u* gde će zauzimati određeni deo prostora za skladištenje, tj. čvrstog diska. Korisnici pristupaju virtuelnim mašinama sa udaljenog pristupa kroz *remote desktop*. Sama konekcija i pristup korisnika ka serveru ne zahteva veliku propusnu moć kabla. Može se koristiti obični *dial up* od 64kb, što je jednom rečju prevaziđeno u celom svetu, jer je ponuda Internet provajdera postala daleko bolja i srazmerno jeftinija sa cenom.

U master radu obrađena je tema digitalne forenzičke istrage u virtuelnom *hyper-V* okruženju. Dati su primeri u pristupu digitalnog forenzičara na virtualnu mašinu ali i odnos dosadašnjeg pristupa fizičkim mašinama u odnosu na virtualne. Pošto virtualno okruženje pruža jednostavniji rad administratora kao i korisnika u korišćenju samog okruženja sa zakonskim propisima ali isto tako i sa ne zakonitim postupcima. Predstavljena su i delovanja anti forenzičkih aktivnosti vezanih za virtuelno *hyper-V* okruženje, kao i šta sve samo okruženje može da ponudi hakerima da svojim delovanjem izvrše uklanjanje dokaze o incidentima koje vrše ili su ih izvršili.

1.2. Predmet istraživanja

U ovom radu, predmet istraživanja je specifičnost operativnog sistema ali i virtuelnog okruženja koje može da ponudi moguća anti forenzička delovanja na dokaze, ali i da prikaže različitost u pristupu digitalnog forenzičara na fizičku i na virtualnu mašinu. Celokupno virtuelno okruženje ima svoje specifičnosti i projektovano je tako da omogući jednostavan rad administratora, da određenom brzinom, kao i uštedom vremena deluje na određene virtuelne mašine, operativne sisteme pa sve do samih foldera i fajlova. Postoji mogućnost da virtuelnim okruženjem upravlja i lice koje čini određena ne zakonita dela, tako da može da koristi mogućnosti celokupnog sistema kako bi vršio manipulaciju virtuelnim mašinama, operativnim sistemima pa i samim fajlovima. Primenom pravila pristupa istrazi određenog incidenta u virtuelnom okruženju i forenzičkim alatima za pristup u digitalnoj istrazi kao i pronalaženju čvrstih digitalnih dokaza, stavlja se pred digitalnog forenzičara jedan veliki zadatak borbe protiv osoba koje zloupotrebljavaju virtuelno okruženje koje je napravljeno za dobrobit kako kompanijama pa tako i pojedinaca. Zato digitalni forenzičar mora biti obazriv jer istraga može da ga odvede u pravom pravcu ali i u pravcu zablude i skretanje sa pravog puta.

U master radu korišćeno je virtuelno okruženje koje je pokrenuto na *host-u* uz pomoć *Hyper-V* i hardverskom podrškom hipervizora. Korišćeni su forenzički alati za istragu osumnjičene virtuelne mašine kao i servera na kome je virtuelna mašina instalirana. Od forenzičkih alata korišćeni su *FTK Imager*, *X-Way Forensic*. Za digitalni forenzički pristup korišćeni su svi alati koji pomažu u radu administratoru sistema, a koji su sastavni deo *Windows* operativnog sistema. Serverska mašina koristi *Windows Server 2008* operativni sistem, dok klijentske virtuelne mašine kao i jedna fizička sa kojom se vršilo poređenje, koristile su *Windows 7* operativni sistem.

1.3. Ciljevi i zadaci istraživanja

Glavni cilj ovog rada je da se prikaže digitalna forenzička istraga u virtuelnom *hyper-V* okruženju ali i moguće manipulacije koje umesto pozitivne i legalne primene mogu za cilj imati zloupotrebu i nanošenje štete pojedincima ali i velikom broju korisnika. Obezbediti dokaze da je incident na virtuelnoj mašini postojao, ali i izvrši poređenje sa mogućim obmanama i anti forenzičkim radnjama.

1.4. Hipotetički okvir istraživačkog rada

Sa obzirom na temu rada, moraju se postaviti četiri opšte hipoteze sa radnim hipotezama.

Opšta hipoteza 1: Za forenzičku analizu virtualnog okruženja potrebno je dobro poznavanje samog virtualnog okruženja, jer ono može nuditi velike mogućnosti korišćenja koje pozitivno utiču na okruženje ali i na rad korisnika, mada virtualno okruženje može ponuditi i brojne negativne primere koje utiču loše na korisnike kao i na društvo u kome se koristi.

Radna hipoteza 1.1: Od posebnog značaja za pristup digitalnog forenzičara virtualnom okruženju je da pristupi serveru, tj. *host-u*, na kome su instalirane i pokrenute virtualne mašine. Pristupom serveru od strane digitalnog forenzičara, mogu se prikupiti značajne informacije vezane za dokaze o nekom delu. Sa prikupljenim dokazima kreira se slučaj događaja koji mora imati čvrste dokaze koji će potom biti predstavljeni pred sudom ili menadžmentom kompanije. U zavisnosti o kojem incidentnom događaju se radi, istragu mogu pokrenuti javna bezbednost koju predstavlja tužilaštvo, policija, bezbednosne agencije, vojska ili korporacijska istraga koju predstavlja menadžment same kompanije.

Hipoteza 2: Digitalna forenzika virtualnih mašina ima specifičnosti u odnosu na fizičku mašinu. Specifičnosti su opisane u master radu i predstavljaju razliku pri pristupu digitalnog forenzičara koji mora biti dobro pripremljen za prikupljanje dokaza iz virtualnog okruženja.

Radna hipoteza 2.1: Od posebnog značaja je pristup serveru ili *host-u* na kome se nalaze sve informacije. Istraga počinje fizičkim pristupom lokalitetu, potom prikupljanjem fizičkih dokaza i sve do trenutka kada digitalni forenzičar mora da izvrši istragu nad digitalnim podacima.

Hipoteza 3: Za borbu protiv hakera i lica koja nanose štetu u virtuelnom *hyper-V* okruženju, potrebno je dobro poznavanja, kao i analiza virtuelnog okruženja. Jer može nuditi velike mogućnosti pozitivnog korišćenja koje utiču na rad korisnika, mada virtuelno okruženje može ponuditi i brojne negativne primere koje utiču loše na korisnike kao i na društvo u kome se koristi.

Radna hipoteza 3.1: Od posebnog značaja je to što *hyper-V* virtuelno okruženje nudi razne operacije koje mogu biti zloupotrebljavane. Te operacije su migracija ili premeštanje virtuelnih mašina, manipulacija slikama stanja virtuelne mašine. Postoje i manipulacije u živoj migraciji ali i mogućnosti preuzimanja kontrole virtuelne mašine od strane ne ovlašćenog ili zlonamernog lica. Sve ove aktivnosti mogu biti zabeležene na *host-u* kao i na *chil-u* ali isto tako ti dokazi mogu biti uklonjeni ako digitalni forenzičar ne pristupi istrazi i prikupljanju dokaza na način koji

se kreira po profilu istrage, u zavisnosti od situacije i incidenta. U zavisnosti o kojem incidentnom događaju se radi, istragu mogu pokrenuti javna bezbednost koju predstavlja tužilaštvo, policija, bezbednosne agencije, vojska ili korporacijska istraga koju predstavlja menadžment same kompanije.

Hipoteza 4: Postoje i alati koji omogućavaju uklanjanje dokaza i sprovode anti forenzičke aktivnosti. Te alate koriste lica koja vrše ne zakonite aktivnosti, a mogu ih kreirati i programirati u zavisnosti kakvu posledicu za sobom žele da ostave. Lica koja koriste anti forenzičke alate isto tako koriste za napade maliciozne softvere.

Radna hipoteza 4.1: Od posebnog značaja je pristup serveru ili *host-u* na kome se nalaze sve informacije. Istraga počinje fizičkim pristupom lokalitetu, potom prikupljanjem fizičkih dokaza i sve do trenutka kada digitalni forenzičar mora da izvrši istragu nad digitalnim podacima. Tada mora voditi računa o svim mogućim manipulacijama od strane lica koja je incident izazvao, kako ne bi bio doveden u zabludu.

1.5. Metodi, tehnike i tok istraživačkog procesa

Metoda naučnog istraživanja je sistematski, kritički, kontrolisani i ponovljivi proces sticanja novih znanja, neophodnih za identifikovanje, određivanje i rešavanje naučnog problema. U naučnom istraživanju glavni principi su:

- *sistematičnost* - dobra uređenost istraživanja i obezbeđivanje prirodnog i logičkog sleda procesa,
- *kontrolisanost* - sprovođenje istraživanja u što moguće boljim i nadziranim uslovima, kako bi se isključila alternativna rešenja i
- *kritičnost* - sve važne tvrdnje o pojavama, procesima, odnosima i svojstvima moraju se ozbiljno, iskreno i strogo procenjivati, proveravati i obrazložiti.

Na osnovu podele naučnog istraživanja, a prema prirodi istraživanja postoje: teorijska i empirijska, a prema cilju istraživanja na: fundamentalna i primenjena. Prema funkciji istraživanja na: eksplorativna i usmerena na proveravanje hipoteza. U ovom istraživačkom radu primenjena su: uglavnom *fundamentalna* i *primenjena* istraživanja. Fundamentalna istraživanja koriste se radi sticanja novih znanja o ovoj oblasti, a primenjena radi sticanja novih znanja i rešavanja hipotezom postavljenih problema u ovoj naučnoj oblasti.

Na početku istraživanja identifikovan je problem, definisan kao kompjuterski incident i opisan u scenariju studije slučaja. Takođe, definisan je cilj istraživanja, kao verifikacija dela teorije virtuelnog digitalnog računarskog sistema, sa pristupom forenzičkoj istrazi. Istraživanje je izvršeno kroz faze *pristupa slučaju*, uglavnom teorijskog i opisnog karaktera, *prikupljanja i obrade podataka na incidentnom virtuelnom računaru i izvođenje zaključaka*.

U ovom istraživačkom radu korišćene su različite metode istraživanja i verifikacije procesa digitalne forenzičke istrage da bi se došlo do određenih saznanja, otkrili i izložili naučni principi, koji se primenjuju u digitalnoj forenzici.

Od *opšte naučnih metoda* korišćene su statistička metoda, metoda modelovanja i analitičko-deduktivna metoda. Takođe, su korišćene *osnovne, opšte metode društvenih nauka*: pozitivistička metoda, metoda razumevanja, komparativna metoda, metoda idealnih tipova, metodološki funkcionalizam i strukturalizam i dijalektičke metode.

Od *posebnih naučnih metoda i tehnika* primenjene su: analitičko-sintetička metoda, metoda apstrakcije i konkretizacije, metoda generalizacije i specijalizacije, metoda klasifikacije, logičke metode indukcije i dedukcija, kao i metoda spoznaje i dijalektičkog jedinstva indukcije i dedukcije.

Tehnike istraživanja predstavljaju sistematsko i svrsishodno jedinstvo postupaka i instrumenata. Ovaj deo naučnog metoda podrazumeva: *ocenu, sređivanje, obradu podataka i zaključivanje* na osnovu njih. U tom smislu, postoji povezanost i međuzavisnost između metoda prikupljanja i obrade podataka, odnosno dokaznih materijala i informacija do kojih se došlo istraživanjem.

Tok istraživanja, kao prvi logični korak uključuje *prikupljanje literature* o metodologiji naučnog istraživanja u digitalnoj forenzičkoj istrazi sa težištem na virtuelno okruženje u svetu Informaciono komunikacionih tehnologija, *Cloud Computing-a*, klasičnoj forenzičkoj istrazi i digitalnoj forenzičkoj istrazi, ali i anti forenzičkim radnjama u samom virtualnom okruženju. Zatim, istraživanje literaturnih podataka i materijala preuzetih iz raznih izvora, kroz faze otkrivanja, opisivanja i objašnjavanja određenih faza digitalne forenzičke istrage u zavisnosti od situacije i primene. Rad je struktuiran u određene celine i svaka od njih konkretno objašnjava glavne faze i procese pristupa digitalne forenzičke istrage u virtuelnom okruženju koje je pokrenuto uz podršku hipervizora.

2. Digitalna forenzička istraga u virtuelnom okruženju

2.1. Teorijske osnove

Digitalna forenzika kao mlada nauka jer je nastala sa postojanjem računara, bori se da nađe mesto među ostalim naukama i da se razvija rame uz rame sa njima. Od kako su nastali računari a sa njima i međusobno povezivanje, došlo je do stvaranja informacionog i globalnog okruženja koje je namenjeno ljudskoj populaciji u celini. Namenjeno je boljoj, bržoj, jednostavnijoj kao i još mnogo pozitivnih mogućnosti u korist komunikacije između ljudi ma gde god se nalazili na planeti Zemlji. Ali sa rastom pozitivnog korišćenja računara ali i mrežnog okruženja, pojavile su se i zloupotrebe. Jedan deo ljudske populacije počeo je da koristi na ne zakonit način računare ali i Internet kao Globalnu mrežu. Tada je stupila na scenu digitalna forenzika kao nauka, jer je morala da dokaže koja su to ne zakonita dela učinjena ali i koji su počinioci tih dela. Pošto je do sadašnja forenzika raznoraznih prekršaja i zločina moga da se oseti ljudskim čulima ona nije mogla da se suprostavi ovakvoj vrsti kriminala koja se odvijala na Internetu ali i na računaru. Zato je morala da se pojavi nauka koja će umesto opipljivog dokaza da ponudi digitalni ali i apstraktni dokaz koji je u prvom momentu bio ne shvatljiv ljudima koji su od njega i zavisili. Kako su se računari razvijali ali i njihovo međusobno umrežavanje, tako se i nauka digitalna forenzika razvijala. Moralo se voditi računa da se istražitelji koji se bave digitalnom forenzikom svakodnevno edukuju jer je razvoj Informacionih sistema ali i tehnologija imao vrtoglavo brz razvoj, pa su se i proporcionalno tome edukovali digitalni forenzičari. Ali i to nije ponekad bilo dovoljno pa je edukacija digitalnih forenzičara zahtevala još brži razvoj, pretpostavke ali i saznanja o mogućim ne zakonitim radnjama i na taj način bi bili ispred lica koji su svoje aktivnosti rešavali da sprovedu na računarima ali i na Globalnoj mreži u suprotnosti sa zakonima i odredbama zemalja u kojima se nalaze ali i zemalja u kojima vrše svoje ne zakonita dela. Zato se digitalna forenzika i danas razvija i kaže se da je mlada nauka, jer svakodnevnim koraćanjem kroz informacione sisteme i tehnologije napreduje, prikuplja razna saznanja, prati anti forenzičke delatnosti kako bi mogla lakše, brže i jednostavnije uz prikupljanje mnoštva čvrstih dokaza da stane na put osobama koje čine ne zakonite radnje.

U osnovne elemente kompijuterskog i Internet kriminala svrtavaju se događaj koji se desio od strane lica koje ga je počinila, ali i okolnosti pod kojim je taj događaj počinjen. U ovom radu se opisuje virtualno okruženje i primena forenzičkih ali i anti forenzičkih aktivnosti u tom okruženju. Okruženje je specifično pa samim tim i pristup digitalnog forenzičara istrazi je specifičan, jer sa druge strane može imati osobu koja je incident i izazvala a koja može biti ne edukovana ali i dobro edukovana kako bi sve svoje aktivnosti sakrila, uklonila i dovela digitalnog forenzičara u stanje obmane i time celokupni slučaj odbacila od sebe. Tome u prilog ide i mentalno stanje počinioca dela koje je iniciralo određeni događaj.

Kada se spomenu kategorije kompjuterskog kriminala, onda se može reći da su to sredstva kojima se napad izvršio i raznorazna tehnička i informaciona pomagala od hardverskih uređaja pa sve do softverskih rešenja nekih programera koja napad mogu da olakšaju i koja isto tko mogu i da nanesu štetu pojedincu ali i kompaniji. Uvek je bitna i informacija o cilju napada ali i veza ili povezanost direktna ili indirektna sa klasičnim kriminalom što može biti trgovina drogama, trgovina ljudima, oružjem, decom itd. Svaki digitalni forenzičar mora da obrati pažnju i na još jednu kategoriju kompjuterskog kriminala a to je skladištenje informacija kod osumnjičenog kako bi mogao da izvuče potrebne informacije o delu koje bi kasnije moglo biti i čvrsti dokaz pred sudom i porotom.

Sve je više tipova kompjuterskog kriminala jer se sve više ljudi u njega i upušta radi ostvarivanja dobitka, nanošenja štete drugom ili konkurenciji ali i nekada iz čiste radoznalosti ili dokazivanja pred drugom osobom. Neki od tipova kompjuterskog kriminala mogu biti neovlašćen pristup drugom računaru ili bazi podataka, ali i zloupotreba ukradenih lozinki kao i kompanijska špijunaža radi sputavanja i onesposobljavanja za normalan i korektan rad konkurencije. Krađa autorskih prava ili kako je još zovu piraterija može naneti štetu pojedincu u materijalnom ali i moralnom pogledu. A što se tiče morala još jedan od tipova kompjuterskog kriminala može biti i iznuđivanje i kompromitovanje osobe ili kompanije od strane lica koje štetu nanaosi.

Predhodno navedene informacije o kompjuterkom kriminalu su veoma bitne i moraju se shvatiti ozbiljno ako neka osoba ukaže na njih. Zato je potrebno dobro razvijeno pravno društvo kao i zakoni na koje će državni aparat reagovati. Reagovaće zvanični organi koje predstavljaju policija, tužilaštvo, sudstvo ali i organi odbrane ako se nekim delom nanosi šteta ne samo pojedincu nego i celokupnoj državi. Ti organi odbrane su vojska i bezbednosne agencije. Pošto se i kompanije uključuju u korišćenje Interneta radi bolje reklame ali i ponude svojih usluga klijentima ili drugim firmama, njihova ranjivost postaje sve veća od mogućih napada i špijunaže. Takvim istragama će se interesovati timovi u korporacijama ako se incident odigrao u kompanijskim okvirima i nije narušio bezbednost države. Tada se vodi kompanijska istraga koja nema mogućnosti određivanja mera represije na pojedince i njegovo lišavanje slobode, već se radi unutar kompanije i ima za mogućnost da određenu osobu izvede pred komisiju za određivanje mere u toj kompaniji.

Ako se digitalna forenzika ne koristi kao nauka, ali i ako se digitalni forenzičarai dovoljno ne edukuju imaće velikih problema oko prikupljanja dokaza koji su u većini slučajeva apstraktni. Ti dokazi su uglavnom binarni 0 i 1. Skup binarnih brojeva čini niz a njime mogu da se opišu razni fajlovi, folderi koji u sebi sadrže određene aplikacije, slike, dokumenta a svi ti dokazi mogu da se uklone ali isto tako i da se izvuku ako je digitalni forenzičar spreman da u odnosu događaja reaguje pravovremeno.

Digitalni dokaz je svaka informacija koja ima dokazujuću vrednost a koja je uskladištena ili snimljena u digitalnoj, tačnije, binarnoj formi. Digitalnim dokazom se smatraju i informacije koje mogu biti i prenešene sa jednog na drugi računar ili sa nekog prenosivog i spoljnog uređaja na računar.

Postoji i originalni digitalni dokaz a on je svaka informacija koja se nalazi snimljena na računaru koji je fizički privremeno oduzet dok istraga traje i biće iznešen pred sud kada za to dođe vreme. Postoji još i duplikat digitalnog dokaza, a za njega se smatraju svi digitalni dokazi koji su kopirani sa originalnih digitalnih dokaza koji su predhodno spomenuti.

Kada se izlazi pred sud i porotu moraju se pokazati digitalni dokazi i to po mogućnosti u originalnom zapisu, tačnije da nisu menjani i da nad njima dok je istraga trajala nisu vršeni nikakvi opiti i testiranja radi sprovođenja istrage. Zato postoje i kopije digitalnih dokaza na kojima se može sprovoditi istraga od strane digitalnog forenzičara i koji neće biti iznešeni pred organe suda.

Postoje i fizički dokazi koji mogu biti prikupljeni na licu mesta gde se odvijao incident i koji mogu imati dokazujuću vrednost da se na tom mestu nalazio osumnjičeni kao i da dokažu sa kojim je to uređajima osumnjičeni to ne zakonito delo sprovodio. Kombinovanjem dokaza mora se voditi računa da se celokupan slučaj incidenta opiše, kako bi imao čvrst i ne oboriv stav pred sudom. Kada se pristupi mestu od strane digitalnog forenzičara na kome se odigrao incident, mora se voditi računa da se fizičko mesto incidenta ogradi i da se omogućiti pristup samo onim istražiteljima koji neće svojom ne pažnjom ili namerom kompromitovati ali i uništiti dokaze.

Bitno je raći da se svi dokazi koji su originalni moraju čuvati u skadištima ili sefovima u zavisnosti koliko je incident opipljiv i najbitnije je da se ne dozvoli ne ovlašćen pristup istim kako ne bi došlo do kvarenja dokaza a samim tim bi i slučaj izgubio na težini. Svi dokazi moraju biti dokumentovani ali i lica koja mogu da im pristupaju moraju imati i određenu odgovornost kada nad njima vrše ispitivanje.

Postoje uslovi pod kojima sud može priznati digitalni dokaz a to su analiza, čuvanje i ponovljivost kompletne procedure istrage ako to sud zahteva od digitalnog forenzičara. Tako da postoji procedura pri čuvanju dokaza kako bi imali sve potrebne attribute. Atributi koji opisuju glavne elemente standardne operativne procedure digitalne forenzičke istrage su naslov koji opisuje ime procedure, namena koja opisuje zašto se neki digitalni dokaz koristi, kao i kada se koristi ali i ko ga koristi kako bi osoba koja ga koristi imala punu odgovornost da ne utiče na dokaza kako istraga ne nalaže. Bitne su i oprema, materijal, kontrole i standardi pod kojim se digitalno dokaz ispituje. Opis procedure mora imati svaki digitalni dokaz koji opisuje korake i mere opreza pod kojima se digitalni dokaz koristio u istrazi. Atributi mogu biti još i kalibracija koja opisuje korake kod kojih se zahteva tačnost u istrazi i kalkulacija koje opisuje matematičke operacije ako su korišćene. Ostaju još ograničenja koja opisuju opremu koje nije korektna kada se ispitivanje vrši, sigurnost i reference koje indentifikuju interna i eksterna dokumenta.

Jedan od principa koji su prihvatljivi pred sudom a tiču se digitalnog dokaza je i *Doubert-ov* sistem. U svim dosadašnjim sudskim parnicama a tiču se procedura u kojima se koriste digitalni dokazi jesu alati kojima su digitalni dokazi i dobijeni ili izvučeni sa osumnjičene mašine. Forenzički alati moraju biti prihvatljivi kao merodavni pred sudom i zato su u USA još 2004.god odlučili da za forenzičke alate koji su merodavni su *EnCase* i *FTKImager*. U suprotnom sud može da prihvati ili odbaci digitalne dokaze koji su prikupljeni forenzičkim alatima i zato u svetu u parnicama koje su vezane za Internet kriminal mogu da variraju. Da bi forenzički alati mogli biti prihvatljivi pred sudskim organima moraju imati poznat stepen greške ali i moraju ga prihvatati i relevantni naučni skupovi. Isto tako digitalne dokaze sud može verifikovati i ako je digitalni dokaz kao određeni fajl ali i forenzički alat mogu biti prihvatljivi pred sudom ako su objavljeni u nekim naučnim časopisima. Međutim, konferencijski radovi nisu prihvatljivi.

Postoje i tri grupe ljudi koji su korisnici forenzičkih alata, a to su:

- Istražitelj - koristi brojne forenzičke alate kao i tehnike i mogu dolaziti iz redova kontrolnih organa ili inspekcija.
- IKT Profesionalac – koriste mali broj forenzičkih alata i tehnika i to uglavnom iz njima bliske oblasti. Deo su osoblja tehničke podrške.
- Tim – koriste veliki broj alata i tehnika, sposobni su da odgovore na različite kompjuterske incidente

Glavni pravosudni zahtevi za prihvatljivost digitalnih dokaza su:

- Ako se koristi kopija, tada kopija mora biti najbolja, ali isto tako može biti korišćena ako postoji na oduzetom računaru isti takav originalan fajl
- Ako se koristi original, tada kopija ne važi

Kada se pokrene istraga incidenta koji je učinjen delom kompjuterskog kriminala tada su bitna pitanja koje digitalno forenzičar treba da postavi. Svi tipovi kompjuterskog kriminala zahtevaju odgovore na određena pitanja. Pitanja su početna osnova za svaku istragu digitalnog forenzičara, a ta pitanja su:

- Ko?
- Šta?
- Gde?
- Kada?
- Zašto?

Kada se dobije odobrenje za sprovođenje zvanične izjave vezane za kompjuterski kriminal, tada se otvaraju faze inicijalne istrage, ulaska u trag napadača, otkrivanje indentiteta napadača ili osumnjičenog, kao i njegovo lišavanje slobode ako je to potrebno, da ne bi izvršio ponovo isto delo i onemogućiti mu uništavanje dokaza.

Istraga zahteva korišćenje forenzičkih alata i njihovu primenu u celokupnom toku istrage. Forenzički alati, kao i tehnike digitalnog forenzičara, koriste se u slučajevima kada treba da se eliminiše očiglednost, postavljanje hipoteza o napadu, rekonstrukcije krivičnog dela i otkrivanje traga do osumnjičenog računara. Vršiti se analiza ciljnog, ali i računara od kojih su pokrenute ne zakonite aktivnosti, ali i onih računara koji su ne posredno korišćeni u toku ne zakonite operacije. Bitno je prikupiti sve dokaze bili oni fizički ili digitalni i celokupan materijal predati zvaničnim organima ako je ugrožena javna i državna bezbednost, ali i kompanijskim organima ako je ne zakonita aktivnost počinjena u okvirima kompanije.

Pošto je digitalni dokaz apstraktan i sa njime se može lako manipulirati raznoraznim operacijama koje mogu da ga dupliraju ili uklone sa računara vrlo je bitno da se znaju informacije na koji se *hard disc-ovima* sačuvani. Ali i u trenucima kada digitalni forenzičar pristupi digitalnom dokazu može ga sačuvati na svojoj radnoj stanici i sa njim dalje manipulirati u cilju istrage. Da bi računar postao deo istrage i da bi postao sumnjičav mora se na njemu predhodno odigrati neka radnja koja je ne zakonita a koja za rezultat ima neku razmenu fajlova ili podataka sa jednog računara na drugi i ako to nije kopiranje. Jer kako Lokardova teorija govori, da princip razmene materije uvek postoji, u slučaju digitalnih dokaza misli se na fajlove i mora da se dogodi kada dva objekta dođu u kontakt.

Kada se digitalni dokaz preuzme prave se kopije od kojih jedna mora biti šifrovana algoritmom kako se sadržaj digitalnog dokaza ne bi promenio. Algoritam za šifrovanje je SHA256 jer se u paksi najčešće koristi. Do sada su uglavnom pravljene tri kopije *hard disc-a* ali od pojave virtualnog okruženja počinje da se pravi i četvrta kopija. Četvrta kopija ima za ulogu da se pokrene na forenzičkoj radnoj stanici i da se nad njom vrši istraživanje kao da se radi na osumnjičenoj mašini.

2.2. Specifičnosti forenzičke istrage u virtualnom hyper-V okruženju

U ovom delu master rada se obrađuje forenzički pristup osumnjičenoj virtualnoj mašini koja radi u *hyper-V* okruženju i koju pokreće hipervizor, ali i poređenje forenzičke istrage na fizičkoj mašini. Pristup fizičkom mestu, na kome se odvija neka kriminalna radnja vezana za digitalni svet u kome su pojedinci sami ili ne u zavisnosti od slučaja pa sve do situacije, svesno ili nekada i ne svesno, mora pratiti određena predpripremna radnja kao i operativna saznanja o potencijalnom osumnjičenom. Ali i o mestu i računaru sa koga se vrše te kriminalne ili incidentne radnje. Svaka operacija koja je protiv prava i ustava zemlje, regiona ili oblasti u kojoj se operacija izvrši, smatraće se potencijalnim izvršenjem krivičnog dela po zakonu te zemlje. U digitalnom svetu i korišćenju Interneta kao Globalnog okruženja postoji veliki broj mogućih

izvršenja krivičnih dela ili incidenata. U tim slučajevima uglavnom korisnici i nisu ni svesni da ga vrše, ali i mnogi korisnici svesno pristupaju ne zakonitim delima. Postoji mogućnost da korisnik bude obmanut od strane trećeg lica i da bude izložen nekom incidentu, a da, pri tom toga nije ni svestan. Dolaskom *Cloud Computinga* i primene virtualnih računara u korporacijske i komercijalne svrhe, mogućnosti zloupotrebe su dostigle najveće moguće eskaliranje i zahtevaju temeljan, organizovan pristup i veliko zalaganje istražnih organa na svakom slučaju koji je okarakterisan od istih kao sumnjiv. Digitalni forenzičar tada mora da primeni sva svoja znanja i veštine kako bi izgradio čvrst i valjan dokaz za sudstvo. U modernom društvu se javljaju prepreke oko razumevanja dokaza od strane sudskih organa. Digitalni dokazi koji su prikupljeni na mestima gde su se incidenti dogodili moraju imati sve potrebne elemente kako bi imali merodavno i čvrsto objašnjenje pred organima sudstva ali i organima kompanije ako se incident odigrao u njoj. Problemi koji se javljaju oko razumevanja digitalnih dokaza su edukativne prirode, jer se malo ljudi iz sveta forenzike angažuje na stalnom radu u sudu. Postoje situacije kada forenzičar iznosi prikupljene dokaze, a sudija ne može da ih razume i omogući okrivljenom da vrlo lako prevari zakon i sudiju. Isto to se može desiti u suprotnom smeru, kada forenzičar dokazuje nevinost osumnjičenog kao njegov branilac. Zato se forenzičke aktivnosti progresivno šire i zahtevaju svakodnevni rad, usavršavanje i praćenje Informacionih komunikacionih tehnologija. To će omogućiti digitalnom forenzičaru da uvek bude ispred potencijalnih osumnjičenih. Jer, ako se taj korak u svakodnevnoj trci izgubi, forenzičar vrlo lako može biti obmanut, a osumnjičeni može da nastaviti da radi ne zakonita dela i nanositi štetu pojedincu ali i društvu u globalu. Digitalna forenzika se smatra mladom naukom, jer je od nastajanja digitalnih podataka koji su počeli da se koriste u svakodnevnoj primeni u društvu, javila se mogućnost za zloupotrebu, a tada je potrebno da se izvrši prikupljanje dokaza i da se uradi rekonstrukcija incidenta događaja. Veliko zalaganje od strane istražnih organa daje se na pred pripremu i prikupljanje podataka o određenom krivičnom delu. Informacije o određenom incidentu mogu se dobiti na različite načine, preko prijave, dojava, praćenja i još mnogo slučajeva, ali bitno je svaku informaciju proveriti i shvatiti je ozbiljno jer se u digitalnom svetu kriminala, forenzičar mora suprostaviti visoko edukovanoj osobi koja dobro zna da sakrije informacije, a te informacije ga mogu dovesti u vezu sa incidentom. Osobe koje se sumnjiče za određena ne zakonita dela u kompjuterskom kriminalu, se svakodnevno edukuju, razmenjuju podatke i informacije na određenim forumima koja se lako mogu kreirati i ukloniti kada se dijalog na neku temu završi. Polazi se od pretpostavke, ali i ne mora da znači, da takve osobe dobro poznaju programiranje i da su sposobne da naprave anti forenzičke programe samostalno, u kućnoj varijanti, *Home made*, i da ih potom primenjuju na Internetu. Zato je bitan svakodnevni pristup edukaciji u praćenju noviteta i lakom i brzom snalaženju sa forenzičkim alatima jer se informacije u digitalnom formatu mogu veoma brzo i lako ukloniti i njima se može manipulirati u delićima sekunde a onda i cela akcija pristupa mestu na kome se dogodio incident može biti dovedena u pitanje. Zato svaki forenzičar koji se bavi digitalnom forenzikom mora imati u vidu moć virtualnih računara i samog virtualnog okruženja koje pored pozitivnih i dobrih stvari za primenu i korišćenje može imati isto tako i širok spektar negativnih primena. Veoma je bitno da se razume virtualno okruženje kao i sama arhitektura, kako bi se pred pripreme radnje prikupljanja dokaza sprovele u što kraćem vremenskom periodu i omogućilo brže sprovođenje istrage. U odnosu na klasičnu digitalnu forenziku, virtualna forenzika mora imati veći broj dokaza jer se u startu, pristup razlikuje, a gde forenzičar mora da prikupi informacije o paketima i komunikacijama između okrivljenog i oštećenog korisnika. Tu se sve incidentne radnje i akcije dešavaju na Internetu. Time je omogućena lakša transakcija digitalnih podataka i sama

manipulacija. U virtualnoj forenzici sve se dešava na virtuelnim prostorima koji su smešteni fizički na serverskim stanicama tj. serverskim mašinama, a koriste se u Internet prostoru i mogu virtualno biti bilo gde. To zapravo i dovodi do razlike, gde će se potencijalni osumnjičeni računari uvek tražiti na centralnom mestu, tačnije serveru, koji u sebi nosi mnoštvo informacija koje mogu biti korišćene kao dokazni materijal.

2.3. Pristup mestu osumnjičene virtualne mašine

Kada se pristupi na mesto incidenta određene krivične radnje koju je počinio osumnjičeni izvršilac, a koji je koristio virtualnu mašinu, mora se ispoštovati redosled operacija prikupljanja dokaza. Redosled je veoma bitan kao i procedure prikupljanja i čuvanja fizičkih i digitalnih dokaza. Svaki dokaz koji ima veze sa incidentom mora biti čuvan i ne sme biti menjan kao što je preuzet u datom trenutku sa mesta incidenta od strane digitalnog forenzičara.

Prvo se mora pristupiti fizičkoj istrazi koja podrazumeva, lišavanja slobode osumnjičenog kao i njegovo uklanjanje od delovanja ili pokušaja uklanjanja mogućih dokaza, ako predhodno nije pobeo. Zato treba osumnjičenog ukloniti od potencijalnih elektronskih uređaja u prostoriji, da ne bi izvršio nasilno uklanjanje dokaza. Primer ovakvog uklanjanja dokaza, je namerno dejstvovanje električnog napona na osumnjičeni računar koje za delovanje ima kao rezultat momentalni prestanak rada *hard* diskova, koji u sebi mogu imati najbitnije informacije o dokazima izvršenja incidenta. Ako je osumnjičeni uhvaćen, obavezno ga fotografisati, kao dokaz njegovog prisustva mestu na kome je izvršen incident. To može biti jedan od dokaza da je osumnjičeni prisustvovao mestu na kome je incident izvršen.

Pogledati, da li je serverski fizički računar, prisutan u prostoriji, na kome je pokrenuta virtualna mašina i proveriti prostoriju tako da se vidi da li postoje određeni svičevi ili habovi, kablovi, koji mogu biti veza sa nekom udaljenom lokacijom. Proveru nastaviti tako, što je potrebno uvideti, kakva je konekcija servera prema Internetu, da li je bežična ili žična. U predhodna dva koraka pristupa forenzičara mestu na kome se incident desio, nema razlike u pristupu kod fizičkih i virtualnih mašina. Zato je ovaj deo fizičke istrage isti. Potom, fotografisati prostoriju kao i sve elektronske uređaje predhodno navedene, a koji se smatraju potencijalnim dokazima, jer je bitno slikati i specifikacije, brend imena kao i modele uređaja. Te informacije su veoma bitne, jer se na Internet stranicama proizvođača mogu naći informacije o uređajima kao i uputstva koja mogu potvrditi da taj uređaj može da izvrši određenu aktivnost koja je u datom trenutku ne zakonita. Ovo je još jedan od potencijalnih dokaza pred sudom, jer mogu se smatrati saučesnicima u izvršenju incidenta, zato što su omogućili ili olakšali osumnjičenom da svojim delovanjem izvrši određene ne zakonite radnje.



Slika1. Mesto incidenta, osumnjičeni, uređaji

U toku prikupljanja fizičkih dokaza treba obezbediti mesto incidenta zbog toga da ne ovlašćena lica ne bi narušila određene dokaze. Kada se ove rednje istražnog fizičkog forenzičkog zadatka obave, mora se pristupiti računar ili serveru koji je potencijalni osumnjičeni. U ovom radu tema se obrađuje na osnovu pretpostavke da je računar u toku pristupa forenzičara na mesto incidenta ostao u radu, kako bi se pristupilo živoj forenzičkoj istrazi u digitalnom okruženju. Pretpostavka da je uključen računar ili server na kome je pokrenut virtualni računar, vodi put digitalnog forenzičara na različitu stranu u odnosu ako bi pristupao istrazi na fizičkom računaru. Ako bi koji slučajem osumnjičeni računar bio isključen ili ga je osumnjičeni isključio prilikom upada istražitelja na mesto incidenta, procedura prikupljanja dokaza sa računara bi išla u pravcu vađenja *hard disc-a* i priključenja na forenzički računar kako bi se napravila slika diska, a potom bi se fotografisalo kućište računara, da se vidi od kojih je hardverskih komponenti sastavljeno, ali i sve specifikacije tih komponenti bi bile slikane.

Do sada, predhodno navedene radnje digitalnog forenzičara su se podudarale kako kog pristupa fizičkom računaru, tako i kog pristupa virtualnom računaru, jer se radilo o istrazi fizičkih uređaja kao i samog računara. Sada forenzičar ulazi u digitalno okruženje koje je veoma kompleksno i može biti u određenom trenutku i nepoznanica ako forenzičar nije izvršio dobru pripremu praćenja i skeniranja delovanja osumnjičenog.

U nastavku rada, biće objašnjena veza između virtualizacije *hyper-V* i hardverske podrške od strane hipervizora, ali i sve operacije unutar operativnog sistema Windows Server 2008, a vezane su za virtualno okruženje i mogu ponuditi određene dokaze. Bitno je da forenzičar dobro vlada i poznaje softversko okruženje unutar koga sprovodi istragu, ali i kako je izgrađena arhitektura

virtualnog okruženja unutar sistema, jer *Cloud Computing* postaje stvarnost kako u svetu pa tako i u našem okruženju.

2.4. Cloud Computing

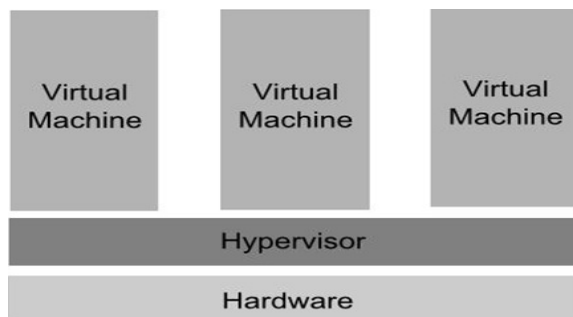
Da bi forenzičar mogao da prikuplja dokaze sa osumnjičenog virtualnog računara koji se nalazi na fizičkom serveru, mora dobro razumeti arhitekturu i princip rada hardverske virtualizacije koja se opisuje u ovom radu. Veoma je bitno da se sada sve informacije nalaze na fizičkom serveru, u odnosu na klasičnu digitalnu forenziku gde su se informacije nalazile na klijentskim računarima. Nepotrebno je juriti lokaciju virtualnog računara, jer on može biti postavljen bilo gde u virtualnom prostoru.

U odnosu na fizički računar do koga se moglo doći fizičkim putem, pristup kod virtualnih računara se svodi na traganje za fizičkom lokacijom servera na kojem su pokrenute virtualne mašine i onda mu treba pristupiti fizički. Zbog toga, bitno je znati koje sve vrste virtualizacija postoje, ali i koje virtualne usluge mogu biti pružene i ili omogućene virtuelnim mašinama od strana host-a.

2.5. Hyper-V virtualizacija tipa 1

Ovo je tip 1 virtualizacije gde virtualna mašina koristi hardver *host-a* na kome je instaliran operativni sistem za serversku podršku. Sam *host* je odgovoran za deljenje resursa za virtualne mašine.

Koncept je prikazan na slici:



Slika2. Koncept virtualizacije

Princip je da se omogući virtualnoj 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 Slika2 prikazuje da virtualna mašina koristi resurse fizičkog *host-a*. Informacije koje forenzičar može da prikupi i koristi, mogu biti dostupne na fizičkom *hard disc-u* kao i u RAM memoriji *host-a*. Što predstavlja ekvivalent pristupa digitalnog forenzičara fizičkoj mašini ali samo iz ovog trenutnog pogleda na hardver *host-a* i korišćenje istog od strane virtualne mašine, kao što trenutna situacija pokazuje. U nastavku rada, biće predstavljeno da ipak postoje velike razlike u pristupu istrazi digitalnog forenzičara u odnosu virtuelne i fizičke mašine.

2.6. Hardverska pomoć virtualizaciji

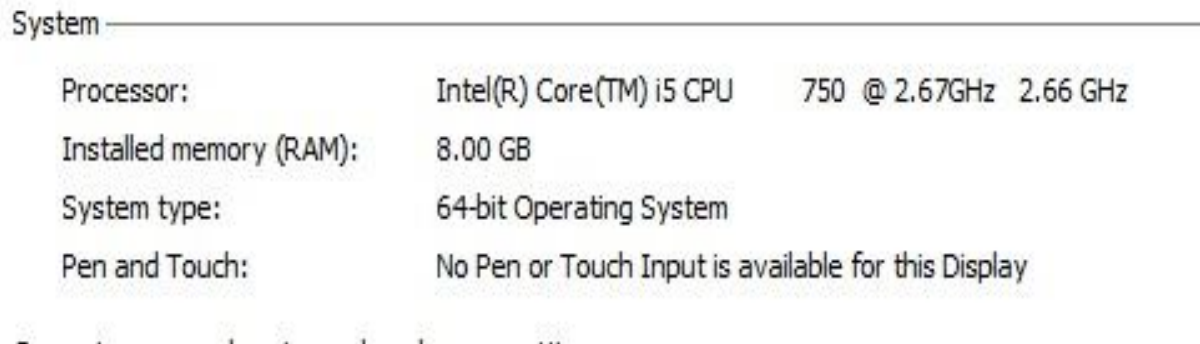
Hyper-V koncept Clouding Computinga će raditi samo na hardverski predefinisanim i kompatibilnim procesorima nove generacije koji podržavaju proces rada sa hipervizirom. Podrazumeva se da na matičnoj ploči računara ili servera postoji procesor koji podržava hipervizor. Hipervizor uspostavlja komunikaciju 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 određenim prstenovima 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 virtualnog klijenta koji koristi *host* i hardverske fizičke resurse *host-a*, među kojima je i procesor. Tim napadom bi se srušio server na kome je Cloud pokrenut i automatski bi prestale da rade i sve virtualne mašine koje su gosti na *host-u*. Antivirusi na procesorima su novina u svetu industrije Informacionih tehnologija i trebalo bi da spreče ovakve napade, kao i da obezbede miran rad klijentskim virtuelnim mašinama.

Kada se kernel kod izvršava, kaže se da radi u prostoru jezgra ili supervizor modu. Tada procesor radi na prstenu 0. Prsten 0 se zove još prsten privilegije operativnog sistema. A aplikacije u sistemu rade na prstenu 1, 2 ili 3. Hipervisor, na matičnoj ploči, na kojem je instaliran *hyper-V* podrška za rad virtualnih mašina, radiće na privilegovanom prstenu 0. Takav rad će mu omogućiti da može da rukuje operacijama na samom procesoru i RAM memoriji samog *host-a*. Isto tako, hipervizor, i na sledećim nivoima će morati da omogući rad u menadžerisanju aplikacijama u virtualnom okruženju.

Pošto su kod proizvođača uvek na prvom mestu procesori, njihova arhitektura, funkcionalnost ali i izvršenja operacija, koja su od vitalnog značaja za rad računara, pojavio se problem oko korišćenja prstena 0. Pojavom hipervizora, koji mora da koristi isti prsten 0, privilegija izvršavanja operacija, a da se pri tom operacije na samom procesoru ne dovedu u pitanje, kao i njihovo izvršenje, oduzimalo bi procesorske resurse i vreme. Taj problem je rešen, na način na koji su proizvođači postavili *Hypercall-s*, pozive hipervizora ka procesoru. Tako da te pozive procesor beleži kao veoma bitne. Procesor omogućava hipervizoru opciju gosta na privilegovanom prstenu 0, što je i bukvalno dovelo do mogućnost da virtualna mašina ima nesmetano korišćenje fizičkih resursa. Korisnik u ovakvom okruženju ima osećaj da koristi fizičku mašinu. Postoji i drugo rešenje problema oko korišćenja privilegovanog prstena 0, kao što je pojava novih procesora AMD-V i Intel VT chipset-a, kod kojih je kreiran prsten -1. Taj prsten omogućava nesmetan rad hipervizora, a operacijama na procesoru se ostavlja nesmetan rad na prstenu 0.

Forenzički pristup na fizički *host*, na kome je osumnjičena virtualna mašina, od velike koristi je dokaz postojanja ovakvih procesora, koji podržavaju hardversku virtualizaciju. To može dovesti do dokaza da na tom serveru postoji mogućnost postojanja virtualnih mašina i da se sa njega ili njih, misleći na virtualne mašine, mogu voditi operacije koje su u toku fizičkog ispitivanja dovele do sumnje da su izvršene neke ne zakonite radnje. Time će svrstati *host* u potencijalne osumnjičene.



Slika3. Computer properties

Kao što se može videti sa Slike 3, do koje se došlo pristupom na *host*, tako što se klikne desnim tasterom miša na Computer, pa Properties, dobija se informacija o *host-u*. Može se videti model procesora, kao i koliko RAM memorije *host* koristi, što je dovoljno hardverske podrške za jedan manji domen od par virtualnih mašina. Ovaj deo istrage se vodi pod digitalnim forenzičkim pristupom osumnjičenom računaru. Mora se predhodno pristupiti čulom vida, na vidljivu površinu ekrana, tako što forenzičar mora izvršiti istragu trenutnog stanja operativnog sistema i time otpočeti digitalni slučaj. Slučaj se mora voditi, jer pred sudom se mora izneti studija retrospektive događaja, kako bi dokazi imali svoju snagu, jer u suprotnom sud može da ih odbaci. Pristup istrage na operativnom sistemu počinje od utvrđivanja o kom operativnom sistemu je reč, kao i verziji tog sistema. Iskusni forenzičar neće gubiti vreme oko saznanja o kom se operativnom sistemu radi, jer u Properties-u, desnim klikom na Computer, dobiće informacije o operativnom sistemu. Sada kada ima informacije o operativnom sistemu, kao i o hardverskoj podršci, može sa sigurnošću da pretpostavi da se na ovom *host-u* nalaze virtualne mašine. Ovaj postupak se može voditi i u istrazi nad fizičkim mašinama.



Intel® Core™ i5-750 Processor (8M Cache, 2.66 GHz)

SPECIFICATIONS

COMPATIBLE PRODUCTS

BLOCK DIAGRAMS

ORDERING / SPEC / STEPPING

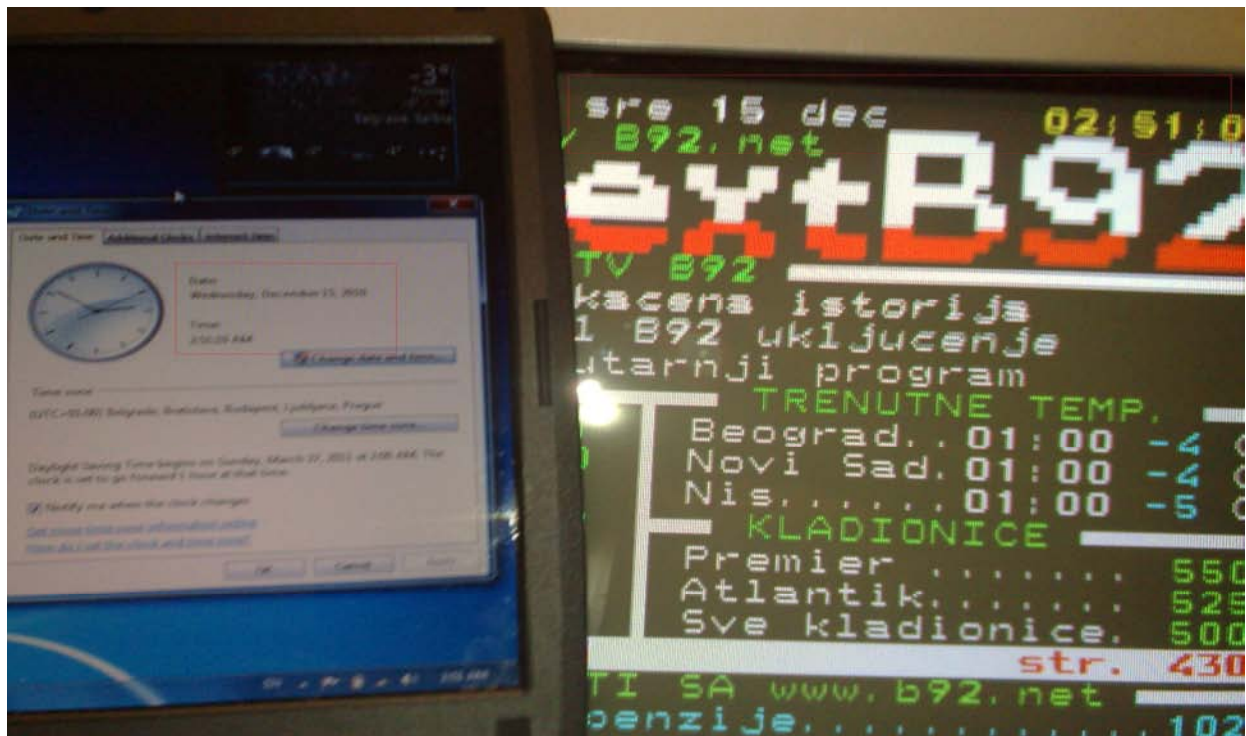
SPECIFICATIONS

Status	Launched
Launch Date	Q3'09
Processor Number	i5-750
# of Cores	4
# of Threads	4
Clock Speed	2.66 GHz
Max Turbo Frequency	3.2 GHz
Intel® Smart Cache	8 MB
Bus/Core Ratio	20
DMI	2.5 GT/s
Instruction Set	64-bit
Instruction Set Extensions	SSE4.2
Embedded Options Available	Yes
Supplemental SKU	No
Lithography	45 nm
Max TDP	95 W
VID Voltage Range	0.6500V-1.4000V
Tray 1ku Budgetary Price	\$196.00
Max Memory Size (dependent on memory type)	16 GB
Memory Types	DDR3-1066/1333
# of Memory Channels	2
Max Memory Bandwidth	21 GB/s
Physical Address Extensions	36-bit
Integrated Graphics	No
PCI Express Revision	2.0
PCI Express Configurations	1x16, 2x8
# of PCI Express Ports	1
Max CPU Configuration	1
T _{case}	72.7°C
Package Size	37.5mm x 37.5mm
Processing Die Size	296 mm²
# of Processing Die Transistors	774 million
Sockets Supported	LGA1156
Halogen Free Options Available	Yes
Intel® Turbo Boost Technology	Yes
Intel® Hyper-Threading Technology	No
Intel® Virtualization Technology (VT-x)	Yes
Intel® Trusted Execution Technology	No
AES New Instructions	No

Slika4. Informacije sa Internet sajta proizvođača

Pošto je forenzičar prikupio saznanja oko postojećeg procesora, može pristupiti ovlašćenom Internet sajtu proizvođača prikazanog na slici4. Tamo može pogledati da li takav procesor podržava hipervizor i hiperpozive, što u studiji slučaja o incidentu može predstavljati čvrst dokaz, a da osumnjičeni ne može da ospori da na *host-u* takva mogućnost postoji.

Kako bi proces istrage bio nastavljen, na forenzičaru je da utvrdi da li se vreme i vremenska zona operativnog sistema poklapa sa okruženjem u kome se nalazi osumnjičeni računar.



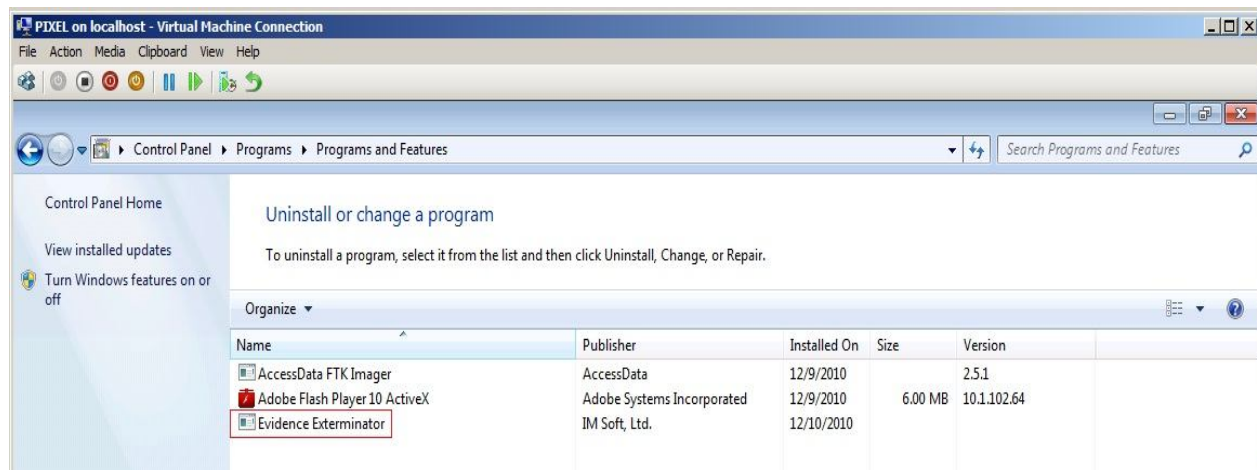
Slika 5. Fotografija upoređivanja datuma i vremena

Najbolje je fotografisati sat na *host-u* sa datumom i pored monitora posaviti, na primer, televizor, kao što je prikazano na Slici 5, na kome će biti program neke nacionalne televizije koji ima informacije o vremenu i datumu. Može se i iskoristiti i teletekst koji daje sve ove informacije.

Forenzičar će nastaviti sa prikupljanjem informacija o *host-u*. Pristupiće START opciji i uočiti koje su aplikacije instalirane i koje su poslednje pokretane, što može usmeriti tok istrage prema tim aplikacijama, kao na primer *Office* paketu. *Word* dokumenta mogu kriti veoma bitne informacije, ali i aplikacije koje pokreću slike, kao i specifični softveri.

Predpostavka da na *host-u* neće biti puno informacija oko pokretanih aplikacija i korišćenja tekstualnih dokumenata, jer se uglavnom sve dešava na virtualnom računaru ne treba da obeshrabri digitalnog forenzičara, ali nikada ne treba ni preskakati neku od operacija pristupa istage, jer tamo gde se najmanje očekuje otkrivanje dokaza, praksa pokazuje da se tu dokazi i nalaze. Pregledati da li osumnjičeni koristi neki od chat aplikacija, ako koristi pristupiti kontroli i pronalaženju *history-a* ako nije izbrisan jer može imati više informacija o *chat* prijateljima, nekim statusima vezanim za prijateljstva ili ljubavne veze, kao i poslednje o čemu su pričali ili vršili razmenu nekih fajlova. Nastavlja se, pogledom *host-a*, pristupanjem u opcije *Uninstal* konzolu, da se vide moguće instalirane aplikacije. Postoji mogućnost da osumnjičeni ima

pomagača koji može pristupiti *host-u* i pokrenuti određenu aplikaciju koja će uklanjati dokaze, kao na primer, *Evidence Eliminator* (Slika 6.).



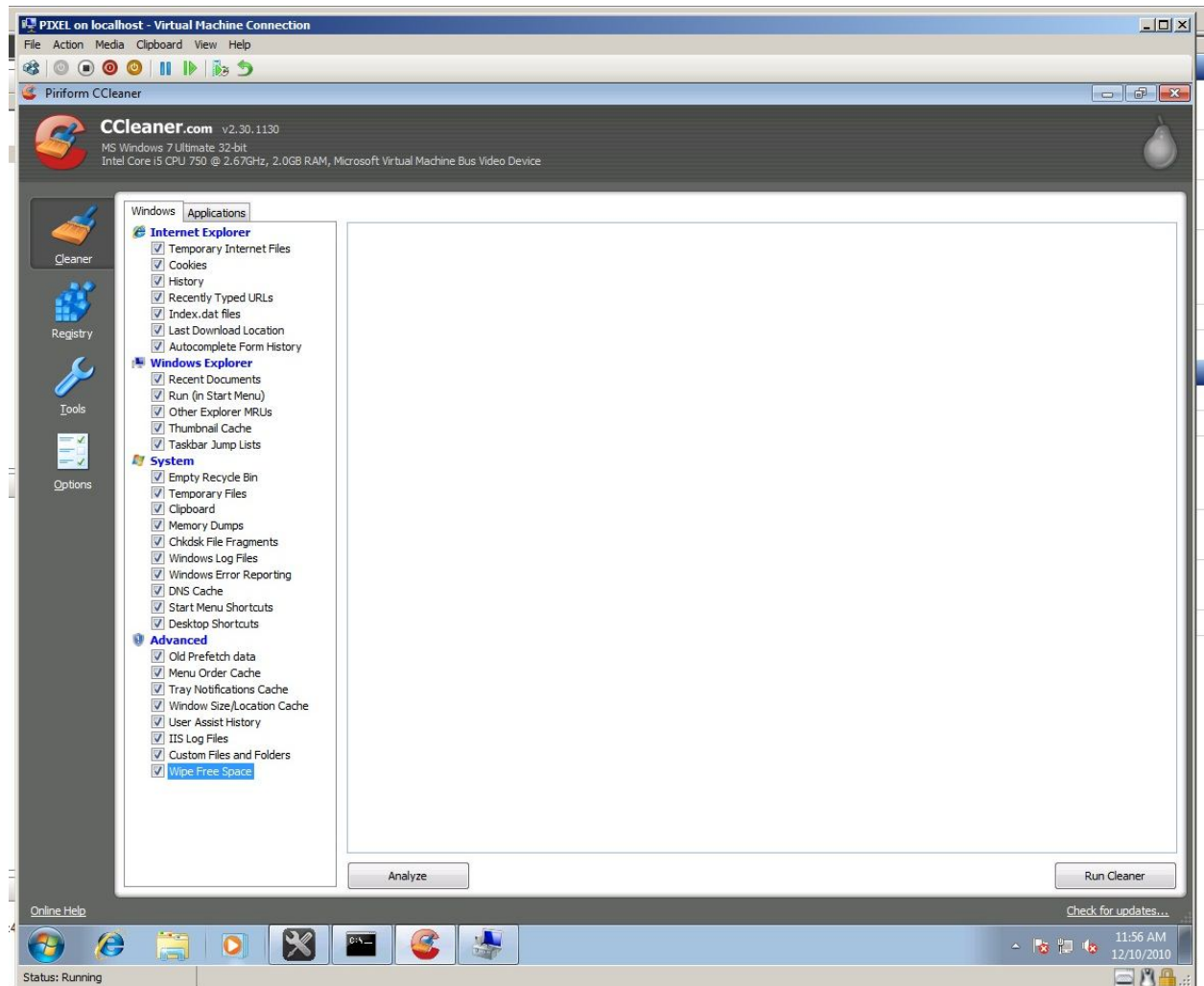
Slika 6. Uninstal konzola

Ova operacija forenzičara, kao što je prikazano na Slika6 pokazuje postojanje softvera koji eliminiše moguće dokaze. Ovakav pristup digitalnog forenzičara može nastupiti i među prvim radnjama u pristupu mestu incidenta. Tada bi trebalo videti da li postoje moguće konekcije ka drugim korisnicima na drugim lokacijama. Fizičkim isključivanjem *host-a* sa konekcije prema Internetu, može se sprečiti ovakav napad sa udaljenog pristupa ako osumnjičeni ima pomagača. Pošto je pristup virtualnoj forenzici specifičan i zahteva dobru pripremu pred pristupa mestu incidenta, kao i veliku brzinu delovanja, te se mora voditi računa, da se određeni detalji istrage ne previde, ali i da se istraga ne dovede u pitanje ako se mesto digitalne istrage računara ne obezbedi. Time se otklanja mogućnost udaljenog delovanja na *host*. Primera radi, pomagač osumnjičenog može da sedi u prostoriji pored ili drugoj stambenoj jedinici koja je u blizini mesta incidenta, čuje upad istražitelja na mesto incidenta i jednostavnim pristupom *host-u* pokrene uklanjanje dokaza. Najbolje rešenje je izvaditi mrežni kabl is *host-a* ili ugasiti bežični uređaj u zavisnosti šta *host* koristi za komunikaciju ka Internetu ili intranetu.

Sledeće što forenzičar treba da pogleda su *Temporary* folder kao i folder *System32* u kojima treba uočiti da li je neka aplikacija aktivna. U folderu *System32*, proveriti da li je kopiran sadržaj nekog trojanskog virusa. To bi osumnjičeni mogao da iskoristi kroz pravdanje i odbranu da je njegov *host* ili virtualna mašina zloupotrebljena od strane trećeg lica. Postoji veliki broj alata koji simuliraju *rootkit*, a to su fajlovi koji se ostavljaju na računaru koji je zombiran i omogućavaju trećem licu da izvrši ponovni pristup. Iskusni forenzičar će pokušati da izvrši brzu pretragu sa nekoliko aktuelnih *rootkit-ova* o čijim informacijama može da konsultuje Internet sajtove antivirusnih kompanija. Antivirusne kompanije ostavljaju ove informacije kako bi pospešile borbu protiv zlonamernog pristupa hakera na klijentske računare.



Slika7. Haker



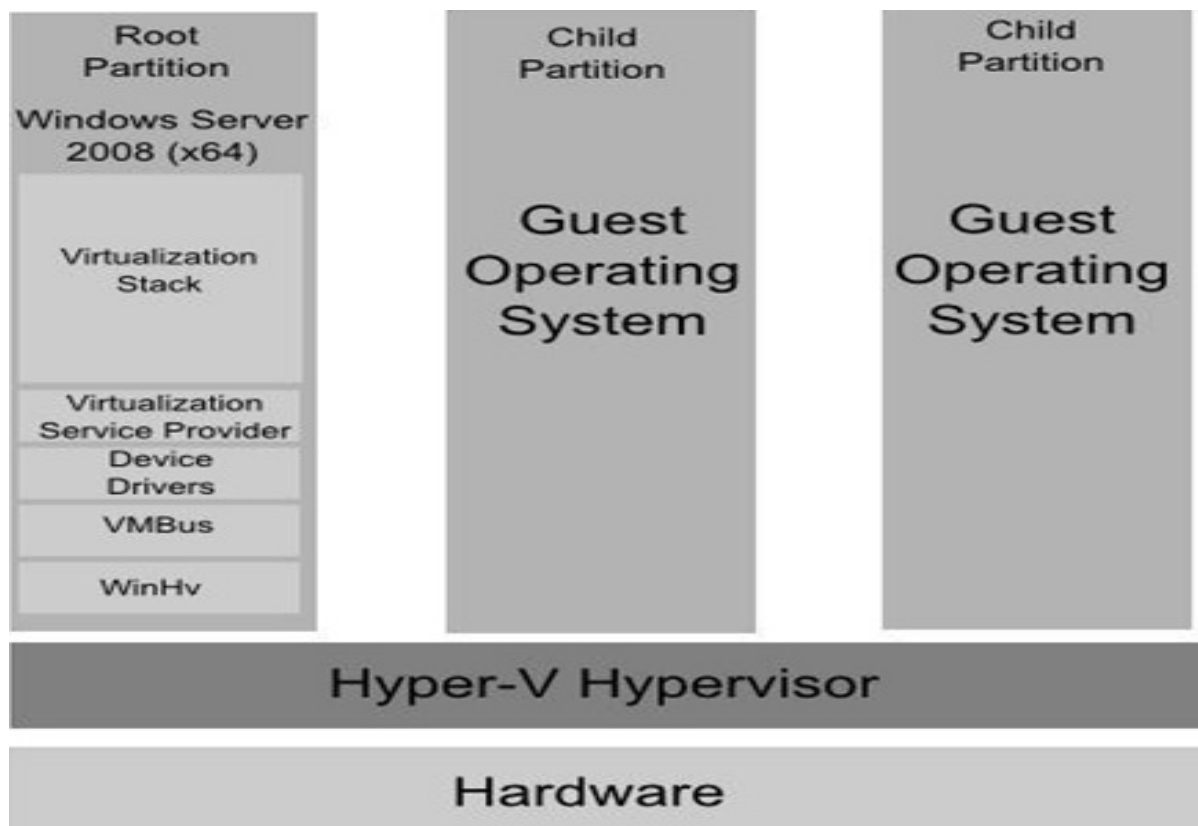
Slika 8. Alat CCleaner

Slika 7. slikovito prikazuje šta se dešava kada neko neovlašćeno pristupi vašem računaru. Bukvalno umesto korisnika preuzima funkcionalnost celog operativnog sistema i šalje poruku svima da je to pravi korisnik računara, što se još zove zombiranje računara. Ovakva zloupotreba računara može da se lako primeni u virtuelnom okruženju, jer samo okruženje dozvoljava veliku fleksibilnost u ne zakonitim radnjama i tada lice, koje zloupotrebljava tuđi računar, želi da svoje

tragove prisustva ukloni. Slika 8. pokazuje koliko bitnih dokaza može da izbriše jedan običan alat, a pri tom ga je moguće besplatno preuzimanje sa Internet stranica.

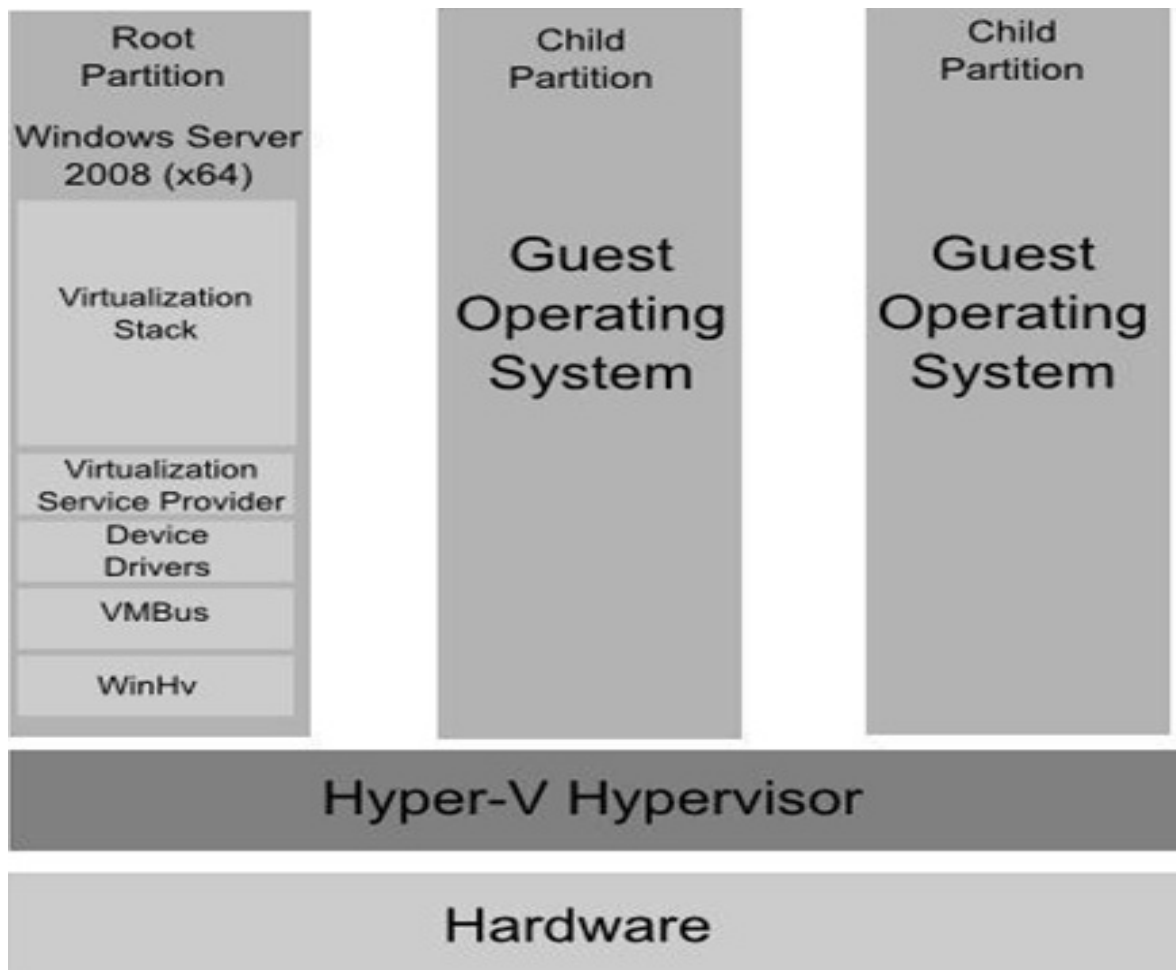
2.7. Hyper-V host i child

Host, na kome je hipervizor kao i procesor sa podrškom za hipervizor, radi tako što se pokreće 64bitni operativni sistem Windows Server 2008, koji je bukvalno domaćin svim budućim, tj. novim virtuelnim mašinama. *Host* je kao otac deci što je i prikazano na Slika9, koju predstavljaju nove virtualne mašine. *Host* im obezbeđuje upravljanje strujom, obezbeđuje hardver, prati, upravlja događajima i evidentira ih.



Slika 9. Host i child

Virtualno skladište je skup komponenti koje sadrže podršku za *hyper-V* funkcionalnost. Forenzičar mora znati kako je složeno virtualno skladište na osumnjičenom *host-u*. Na slici10 je prikazano standardno virtualno skladište koje se koristi kod *Cloud Computing-a* podržanog hardverskim hipervizorom:



Slika10. virtualno skladište kod Cloud Computing-a

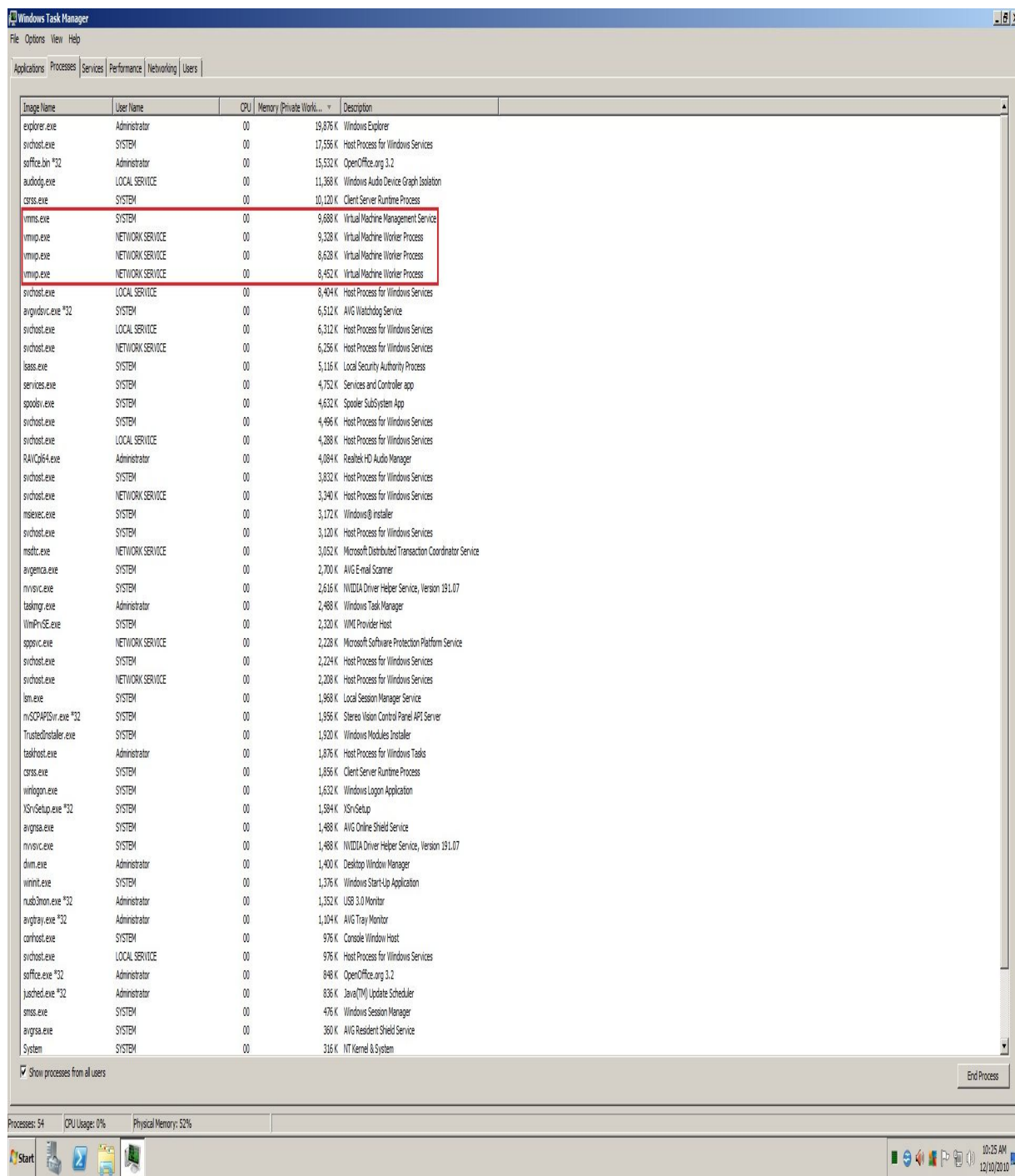
Na Slika10, prikazano je virtualno skladište sa svim elementima podrške i funkcionalnostima vezanim za hardverski *Cloud Computing-a*. Opisi servisa koji funkcionišu u ovom virtualnom skladištu mogu biti od velike koristi digitalnom forenzičaru i dati mu opisnu sliku okruženja.

VMM Service – Virtual Machine Management Service, upravlja stanjem virtualnih mašina, koje još nazivamo *decom* ili *child*. Servis može biti aktivan ili ne aktivan ili zaustavljen. Upravlja operacijama na virtualnoj mašini na osnovu trenutnog stanja. Isto tako može obezbediti dodavanje ili uklanjanje uređaja. Kada se virtualna mašina startuje, tada je VMM servis odgovoran za stvaranje *Virtual Machine Worker Process-a*.

Virtual Machine Worker Proces – u procesima u operativnom sistemu pojaviće se egzekutivni fajl **vmwp.exe**. Kreira se na svakoj virtualnoj mašini i odgovoran je za veliki broj interakcija između operativnog sistema Windows Servera 2008 na *host-u* i virtualnih mašina ili kako se još zovu *child-ovi*. Dužnost VMWP je da kreira, konfiguriše, pokreće, pauzira, startuje, nastavlja rad sa poslednje sačuvanog setovanja, čuva, vrši povraćaj i snima stanja operacija na virtualnoj

mašini. Pored ovih operacija, upravlja IRQ-om, memorijom i I/O tj ulazno/izlaznim portom na matičnoj ploči.

VMWP servis može se zabeležiti *printscrean* operacijom, pritiskom na taster na tastaturi, što forenzičaru daje još jedan od dokaza da su na *host-u* pokrenute virtualne mašine i da reaguje pravovremeno na njih.



Slika11. Procesi na host-u

Slika11 prikazuje da postoje procesi koji ukazuju na pojavu virtualnih mašina, redom nabrojani, a to su: vmms.exe vezan za sistem SYSTEM, kao i vmwp.exe NETWORK SERVICE.

Virtualni uređaji – ove virtualne uređaje kontroliše virtualna matična ploča koja se nalazi u okviru VMWP-a. Virtualna matična ploča se dodeljuje po jedna za svaku virtualnu mašinu.

Virtual Infrastructure Driver – radi u režimu jezgra procesora na *host-u*. Radi u privilegovanom prstenu 0, kao i vid.sys *driver*, koji omogućava komunikaciju virtualizacionog skladišta gore navedenog i objašnjenog hipervizora.

Windows Hypervisor Interface Library – to je .dll fajl koji se još zove WinHv.sys. Nalazi se na matičnoj ploči, na kojoj je podignut operativni sistem Windows Server 2008. Može se i naći na bilo kom drugom operativnom sistemu koji može biti gost na *host-u*. Njegovog prisustva je svestan i *hyper-V*. DLL fajl omogućava *driver-ima* operativnog sistema da pristupe procesoru preko API poziva, a ne preko Hypercall-s koji su deo najnovije izrade tehnologije procesora.

VMBus Driver – omogućava visoko optimizovanu komunikaciju između *host-a* i gosta tj. *child-a*. Isto tako je i sastavni deo *Hyper-V Integration Service*.

Virtualization Service Providers – nalazi se na *host-u* i pruža usluge, preko sintetičkih uređaja koji koriste VMBus *driver* pa sve do *Virtual Service Client-a* koji radi kod *child-a*.

Virtualization Service Clients – su sintetički uređaji smešteni u *child-u*. Komuniciraju sa predhodno pomenutim VSP servisom, kako bi nakon toga Virtualization Service Provider ispunio zahteve *Virtualization Service Clients-ima*.

Pogledom na funkcionalnosti operacija gore pomenutih servisa, može se razumeti funkcionisanje hipervizora u potpunosti, kao i *driver-a* ali i ostalih uređaja. Bitno je da se napomene, da *hyper-V* može da primi na svojim *child-ovima* i različite verzije kao i različite celokupne operativne sisteme, ne mora funkcionisati samo sa Microsoft proizvodima iako je u ovom radu za primer uzet Microsoft Server 2008 kao operativni sistem na *host-u*. U zavisnosti od operativnih sistema, ponašanje komunikacije između hipervizora i procesora će se menjati, u zavisnosti od oblika poziva za komunikaciju. Koristiće se *Hypercall-ovi* ako operativni sistemi na *child-u* nisu iz Windows lepeze operativnih sistema.

Ovo poglavlje u kome je opisivan *host* i *child-ovi* i servisi koji rade unutar *hyper-V* su novina za digitalne forenzičare, jer nemaju možda direktnog uticaja na istražni postupak ali moraju se poznavati svi procesi i koje mogućnosti nude u hardverskoj komunikaciji između *host-a* i *child-a* tj. između hardverskog dela *host-a* a to su procesor i hipervizor. Kao što je u uvodu navedeno, oblast virtualizacije u pristupu digitalnog forenzičara kod pristupa nekom mestu na kome je izvršen neki incident, se u mnogome razlikuje od klasičnog pristupa fizičkoj mašini, pa čak i ako je toj fizičkoj mašini uloga servera u nekom domenu, okruženju na intranetu ili Internetu. Zato se ovakav pristup digitalnog forenzičara smatra novim pravcem u kome digitalna forenzika kao nauka mora da se razvija.

2.8. Sistemski zahtevi hyper-V

Virtualizacija, kao i sama zahtevnost *hyper-V* otvara pitanja za svakog arhitektu Informacionog sistema u Cloud okruženju. Prvo se mora napraviti studija slučaja, u kojoj će se razmatrati, koliki je to obim informacija i pristupa korisnika ka Cloud sistemu. Postaviti pitanje koji operativni sistem treba da učestvuje u Cloud sistemu i kakva će biti iskorišćenost hardvera koju zahtevaju ti operativni sistemi. Postavlja se pitanje koliko *child-ova* treba biti u Cloud sistemu u odnosu na prohteve klijenata. Sledeće pitanje je, koje operacije će biti izvršavane u samom sistemu, ali i kojom brzinom sistem mora da odgovori na te zahteve. Stvar pripreme i samog kreiranja sistema zahteva veliki napor za svakog IT arhitektu. Ali isto tako digitalni forenzičar ili tim sačinjen od istražnog organa, tužioca i tima digitalnih forenzičara treba da pristupi u pred priprema prikupljanja informacija pre nego se upusti na upad na lokaciju za koju se smatra da je mesto izvršenja incidenta. Priprema IT arhitekta je od velikog značaja za kompaniju u kojoj će postaviti Cloud okruženje, ali isto tako se može pripremati potencijalni osumnjičeni i za izvršenje neke ne zakonite radnje koja može za posledicu imati nanošenje velike materijalne i moralne štete. Razumevanje Cloud sistema je veoma bitno, jer digitalni forenzičar koji treba da pristupi mestu incidenta u kojem je korišćeno virtualno okruženje, mora razumeti sve moguće posledice, mogućnosti primene forenzičkih alata. Neki od forenzičkih alata se ne mogu u potpunosti primeniti u virtualnom okruženju, jer ne podržavaju novije operativne sisteme, ali i sam hardver na *host-u* je toliko razvijen, kako dinamički tako i prostorno, kao na primer, hard diskovi na *host-u* koji idu i do nekoliko desetina ili stotina terabajta što bi primenom dosadašnjih forenzičkih alata za pravljenje slike diska, usporilo celokupnu istragu. Zato je bitno raditi u živoj forenzici kada se pristupa virtualnom okruženju i praviti slike diskova samo onih particija ili delova hard diska koji se smatraju osumnjičenim. Kao i u nekoliko prethodnih slučajeva i u ovom pristupu digitalnog forenzičara mestu incidenta razlikuje se pristup prikupljanja podataka između fizičke mašine i virtualne mašine koja se nalazi u oblaku.

2.9. Zahtevnost hyper-V kod operativnih sistema i korišćenja procesora

Zahtevnost nad operativnim sistemima koju zahteva *hyper-V* je bitan faktor koji svaki digitalni forenzičar mora da razume. Zahtevnost na *host* računaru u slučaju koji je obrađen u ovom radu je operativni sistem *Windows Server 2008* i koji se isporučuje u verzijama, *Standard*, *Enterprise* i *Data* centar kao i u verzijama *Windows Server 2008 FULL* i *CORE* koje su se najbolje pokazale u Cloud sistemima. Ostale verzije operativnih sistema od Microsoft proizvoda nisu u mogućnosti da podrže zahteve *hyper-V*, što je i podrazumevano jer tada kada su razvijane, virtualizacija nije bila razvijena kao ni mogućnosti korišćenja *Cloud Computing* sistema. Procesor mora biti 64bitni, kao što su pomenuti modeli Intel VT i AMD-V, ali i hardverska zahtevnost da procesor podržava hipervizorske pozive koji će raditi na privilegovanim prstenovima 0 i -1. Ove informacije se mogu potvrditi kada digitalni forenzičar pristupi *host-u* i u Computer Properties-u uoči o kom operativnom sistemu se radi ali i koji procesor koristi, što i prikazuju predhodno pomenute Slika3 i Slika4.

2.10. Hardversko podešavanje hyper-V

BIOS opcije su od velike važnosti za virtualizaciju, možda i ne toliko bitni za digitalnog forenzičara ali indirektno može uticati na ispitivanje i prikupljanje dokaza. Kada se startuje računar, *host*, pritisnuti taster DEL ili F2 na tastaturi, ili neki drugi taster kojim se pozivaju BIOS opcije u zavisnosti od proizvođača matičnih ploča. Dva navedena tastera su standardna za poziv BIOS opcija kod velikog broja proizvođača matičnih ploča. Kada uđete u BIOS opcije naći će te podešavanja za virtualizaciju i uključiti opciju. Ovo se radi jer proizvođači matičnih ploča, prave, kreiraju, fabrički podešavaju ploče za komercijalnu prodaju korisnicima koji ih kupuju u većinu slučajeva za svakodnevnu ličnu upotrebu. Kod ploča koje koštaju više i koje su predefinisane u fabričkom podešavanju za serverske stanice, opcija virtualizacije u BIOS-u je po *default-u* uključena. Još jedna ključna stvar je da pri izboru matične ploče, koja će se koristiti za potrebe virtualizacije, mora se voditi računa o samoj arhitekturi Cloud sistema. Zašto je to bitno? Odgovor je, da se mora misliti na broj slotova u koje će se stavljati RAM memorija i na kom taktu radi magistrala te matične ploče u memorijskom slotu. Primera radi, ako će na toj matičnoj ploči biti pokrenuto dvadeset virtualnih mašina i na svakoj instaliran operativni sistem Windows7, kao klijentski, koji zahteva minimum 1Gb RAM memorije po *child-u*. U zbiru će biti 20Gb RAM memorije potrebno i na tu memoriju moramo dodati od 512Mb pa do 4Gb RAM memorije ili više za operativni sistem na *host-u*. U specifikaciji za korisnike koja se može pre nabavke pročitati sa sajta proizvođača, može se zaključiti da li ima dovoljno memorijskih slotova, kao i da li ti slotovi podržavaju određeni takt memorije koja bi bila postavljena u njih. Isto tako mora se videti kolika je maksimalna memorija po svakoj memorijskoj pločici i onda napraviti račun celokupnog procesa prikupljanja hardvera za potrebe *host-a*. Ove informacije su bitne za digitalnog forenzičara, kako bi imao u vidu koliko ima RAM memorije i kolika je njena iskorišćenost od strane virtualnih mašina koje je i koriste.

2.11. Memorijski zahtevi hyper-V

Kada se krene u razmatranje potrebne količine memorije za operativni sistem na kome će biti pokrenut *hyper-V* na *host-u*, mora se uzeti u razmatranje arhitektura Cloud sistema, odnosno potreba sistema i broja virtualnih mašina koje će raditi na njemu. Tada se memorija uzima proporcionalno sa zahtevima Cloud sistema. Taj odnos je jednostavan, jer ako se na primer, koriste virtualne mašine na kojima će biti pokrenut operativni sistem Windows7, onda svakom *child-u* treba obezbediti minimum 1GB RAM memorije. Ali mora se voditi računa da *host* mora imati obezbeđenu memoriju na kojoj će se pokrenuti operativni sistem Windows Server 2008, jer bez njega celokupna virtualizacija neće raditi. Minimum RAM memorije za *host* ide od 512 MB pa sve do 4GB RAM memorije i da pri tom na tu veličinu memorije mora da se dodaju memorije za buduće *child-ove* posebno.

2.12. Mrežni zahtevi hyper-V

Kada je u pitanju mrežna kartica na *host-u*, ona je po standardu fabrike uvek na matičnoj ploči integrisana, što je postalo standard u izradi matičnih ploča u zadnjih par godina ne vezano za virtualizaciju. Postoji mogućnost da se dokupi nova mrežna kartica ili više njih, koja će biti instalirana, tačnije, ubačena u PCI slot na matičnoj ploči i time omogućiti da se *host-u* pristupa i sa udaljene lokacije, ili da *host* ima ulogu rutera što će omogućiti da komunicira između više različitih domena i mreža. Integrisanu mrežnu karticu koriste i *child-ovi* ovog *host-a*. Ali ovo nije definicija, već postoji više opcija u zavisnosti od upotrebe *host-a* u virtualnom okruženju. Postoje i mrežne kartice koje simuliraju predajnik za bežičnu komunikaciju, *access point-i* i ruteri, pa se kombinovanje ostavlja arhitektama sistema. Sve ove informacije vezane za mrežne adaptere, koji se fizički koriste na *host-u*, a različitost je velika u zavisnosti od modela i funkcionalnosti od internih, eksternih, bežičnih, različitih tipova konekcija prema *host-u*, od TCP kablova pa do USB priključaka, imaju veliku važnost za digitalnog forenzičara. Informacije koje one pružaju su bitne u potvrdama sa uporednim korišćenjem forenzičkih alata za praćenje koje digitalni forenzičar može koristiti u pred istrazi i u toku žive istrage. Bitne informacije su o proizvođačima mrežnih adaptera, kao i MAC adresama koje definišu svaku mrežnu karticu kao jedinstvenu. Postoje i mrežne kartice kojima sami dodeljujemo MAC adrese jer su u masovnoj proizvodnji stvorene i imaju veoma nisku cenu.

```
C:\Windows\system32\cmd.exe
C:\Users\Radni>ipconfig/all

Windows IP Configuration

Host Name . . . . . : Radni-PC
Primary Dns Suffix . . . . . : 
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : domain.invalid

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : domain.invalid
Description . . . . . : Atheros AR5007EG Wireless Network Adapter
Physical Address . . . . . : 00-1D-D9-07-44-D6
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::40a9:5aa2:462:591b%126(Prefe
IPv4 Address. . . . . : 192.168.1.5(Prefered)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Wednesday, December 15, 2010 11:37:57 AM
Lease Expires . . . . . : Saturday, January 21, 2147 9:11:31 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 Iaid . . . . . : 218111447
DHCPv6 Client DUID . . . . . : 00-01-00-01-14-99-0C-C2-00-1B-38-D9-F6-05
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Local Area Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Broadcom NetLink (TM) Fast Ethernet
Physical Address . . . . . : 00-1B-38-D9-F6-05
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter isatap.domain.invalid:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : domain.invalid
Description . . . . . : Microsoft ISATAP Adapter
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . : 
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : 2001:0:5ef5:79fd:3c53:674:b050:8447(Prefe
Link-local IPv6 Address . . . . . : fe80::3c53:674:b050:8447%13(Prefered)
Default Gateway . . . . . : 
```

Slika12. komandna linija

Sa slike, Slika12, može se videti ime *host-a*, kao i informacije o brendu mrežne kartice, i uočljivo je da se radi o bežičnom mrežnom adapteru. Može se uzeti informacija o MAC adresi i uporediti je sa istražnim informacijama, kao i adrese *Geteway-a* i *DHCP-a*, ali može postojati mogućnost da se MAC adresa promeni jer se može podešavati na aplikativnom nivou.

Sve ove informacije važe za mrežne adaptere koje su fizički na *host-u* i kojima se može pristupiti direktno na *host-u*, što je ekvivalentno operaciji pristupa digitalnog forenzičara kod fizičke osumnjičene mašine. Moguće je postojanje i virtualnih mrežnih adaptera, što može zakomplikovati stvar u toku prikupljanja digitalnih dokaza, ako se ne poznaje dovoljno dobro arhitektura Cloud sistema. O mogućim virtuelnim mrežnim adapterima i njihovoj primeni, biće dato objašnjenje u nastavku rada.

2.13. Instalacija hyper-V na operativni sistem kao i forenzičko delovanje na isti

Kao što je predhodno navedeno, potrebno za pokretanje *hyper-V*, mora biti obezbeđen 64bitni procesor i operativni sistem napisan za takav procesor. Prilikom instaliranja operativnog sistema neće biti uključena opcija *hyper-V*, po default-u, već sam korisnik ili administrator sistema mora da podesi virtualno okruženje. Podsećanja radi, sistemski zahtevi su objašnjeni u prethodnom poglavlju. Isto tako moraju biti obezbeđeni svi hardverski resursi za početak instalacije operativnog sistema na *host-u*.

2.14. Instalacija hyper-V iz komandne linije

Proces instalacije *hyper-V* može se pokrenuti posle instalacije operativnog sistema na *host*. Dodeljivanjem svih *driver-a* za korektan rad operativnog sistema na *host-u*, kao što se može proveriti pritiskom desnog tastera miša na Computer opciju, pa opcija Manage. Otvoriće se prozor u kome će biti opcija na hijerarhijskom stablu sa leve strane, *Device Manager*, i onda će se pojaviti u glavnom prozoru svi uređaji koje je BIOS pokrenuo kada se *host* uključio u rad. Ako je ova stavka ispoštovana i *Device Manager* ne prijavljuje da za neki određeni uređaj nije korektno instaliran *driver*, administrator sistema može pristupiti instalaciji *hyper-V*. Proces instalacije *hyper-V* može se pokrenuti na dva načina, i to preko *Server Manager tool-a* ili preko komandne linije koju pokrećemo pritiskom desnog klika na taster miša na Start opciju, jer želimo da pokrenemo komandnu liniju sa privilegijom administratora operativnog sistema. Potom, u prostoru za pokretanje unosi se naredba CMD. Kada se pokrene komandna linija, tada u njoj se unosi sledeća naredba:

```
C:\Users\Administrator>servermanagercmd -install hyper-v
..
Start Installation...
Warning: [Installation] Succeeded: [Hyper-V]. You must restart this server to
finish the installation process.
<100/100>
Success: A restart is required to complete the installation.
```

Slika13. Instalacija Hyper-V preko komandne konzole

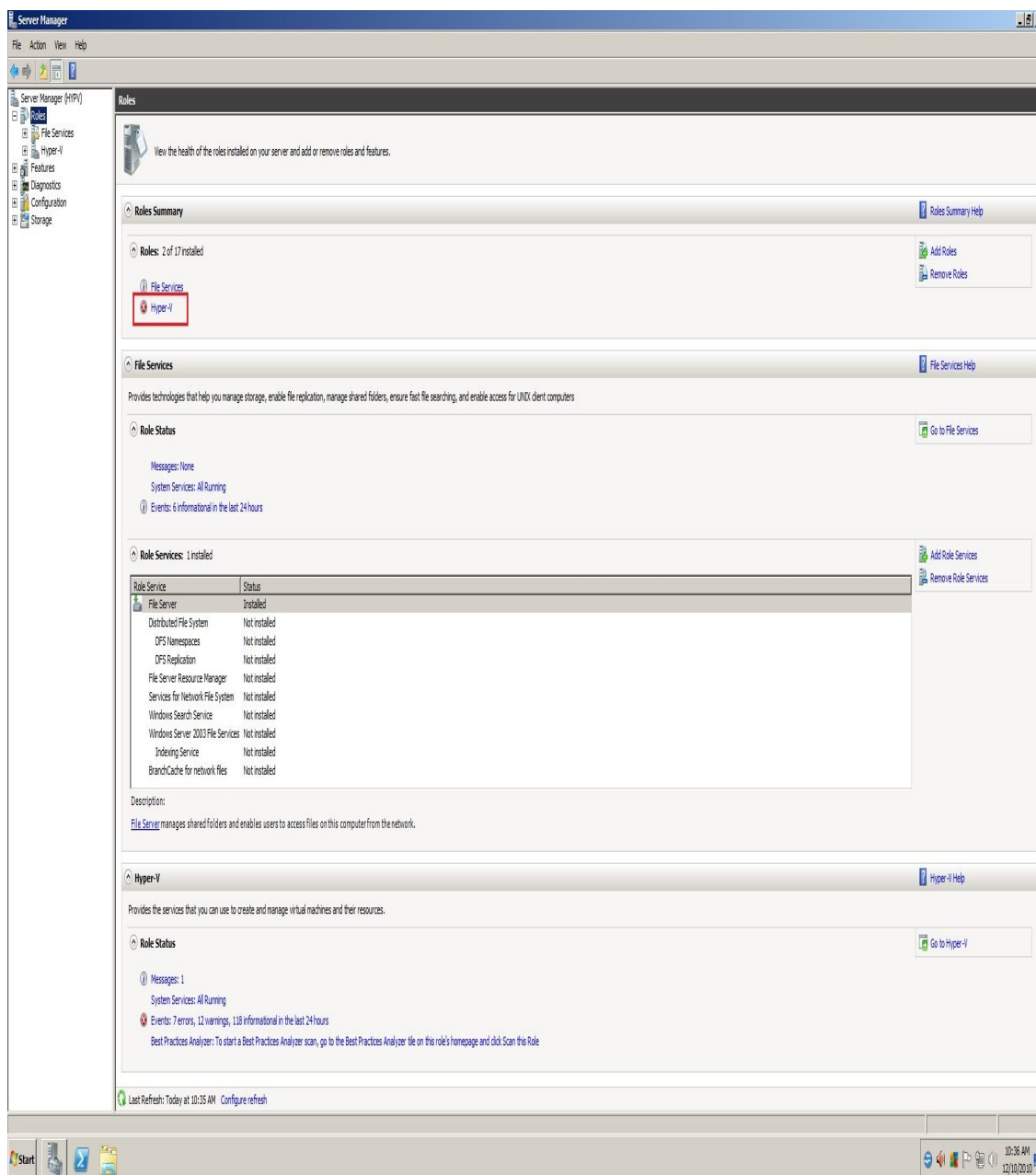
Kao što je na slici prikazano, Slika13, posle instalacije, koja je uspešno izvedena, potrebno je restartovati *host* računar, radi kompletiranja instalacije *hyper-V*. Po završetku prethodne operacije iz komandne linije i restartovanja sistema, ponovo će biti potrebno pokretanje komandne linije. Tada se unosi naredba koja glasi:

start /w ocsetup Microsoft-Hyper-V

Posle toga se instalacija *hyper-V* završava. Preporuka je da se još jednom restartuje računar, da bi se stanje poslednje promene zabeležilo. Potom, pri sledećem startovanju operativnog sistema može se pokrenuti konzola *Hyper-V Manager*. Do konzole se dolazi preko Start-a, pa *Administration Tools*-ova, pa *Hyper-V Manager*. Tu se može proveriti uspešnost cele instalacije. Kada se računar, tj. *host*, na kome je pokrenuta instalacija *hyper-V*, prvi put se resetovao, tada se dogodila promena u softverskoj podršci vezana za uređaj hipervizor koji komunicira sa procesorom, a koji je opisan u prethodnom poglavlju. Instalira se *BUS driver*. Kao što se *hyper-V* može instalirati na računar tj. *host*, isto tako se može i instalacija ukloniti. Ovo je bitan podatak za digitalnog forenzičara, ukoliko pristupa *host-u* na kome je podignut CC servis, tj. virtualno okruženje. Jer u oblaku može biti podignut virtualni domen sa aktivnim direktorijumom kojeg pokreće neki serverski operativni sistem, ali iskusni hakeri će obrisati za sobom ostatke od aktivnog direktorijuma jer u operativnom sistemu Microsoft Windows 2008 postoji wizard u kome na jednostavan način može čekirati sve opcije koje želi da ukloni. Wizard će pitati da li administrator želi da ukloni DNS jer u njemu se beleže sve promene u aktivnom direktorijumu i pošto je domen koji se uklanja na virtualnom serveru, biće zabeleženo da se neka aplikacija instalirala, radila i uklonila što bi se manifestovalo u log fajlovima. Ali iskusni forenzičar uvek treba da pokuša sve moguće opcije istrage jer uvek može postojati trag koji može postati i potencijalni dokaz u istrazi, pa makar samo ostali profili korisnika domena. Za pretragu profila potrebno je posedovati administratorsku privilegiju za pristup istom.

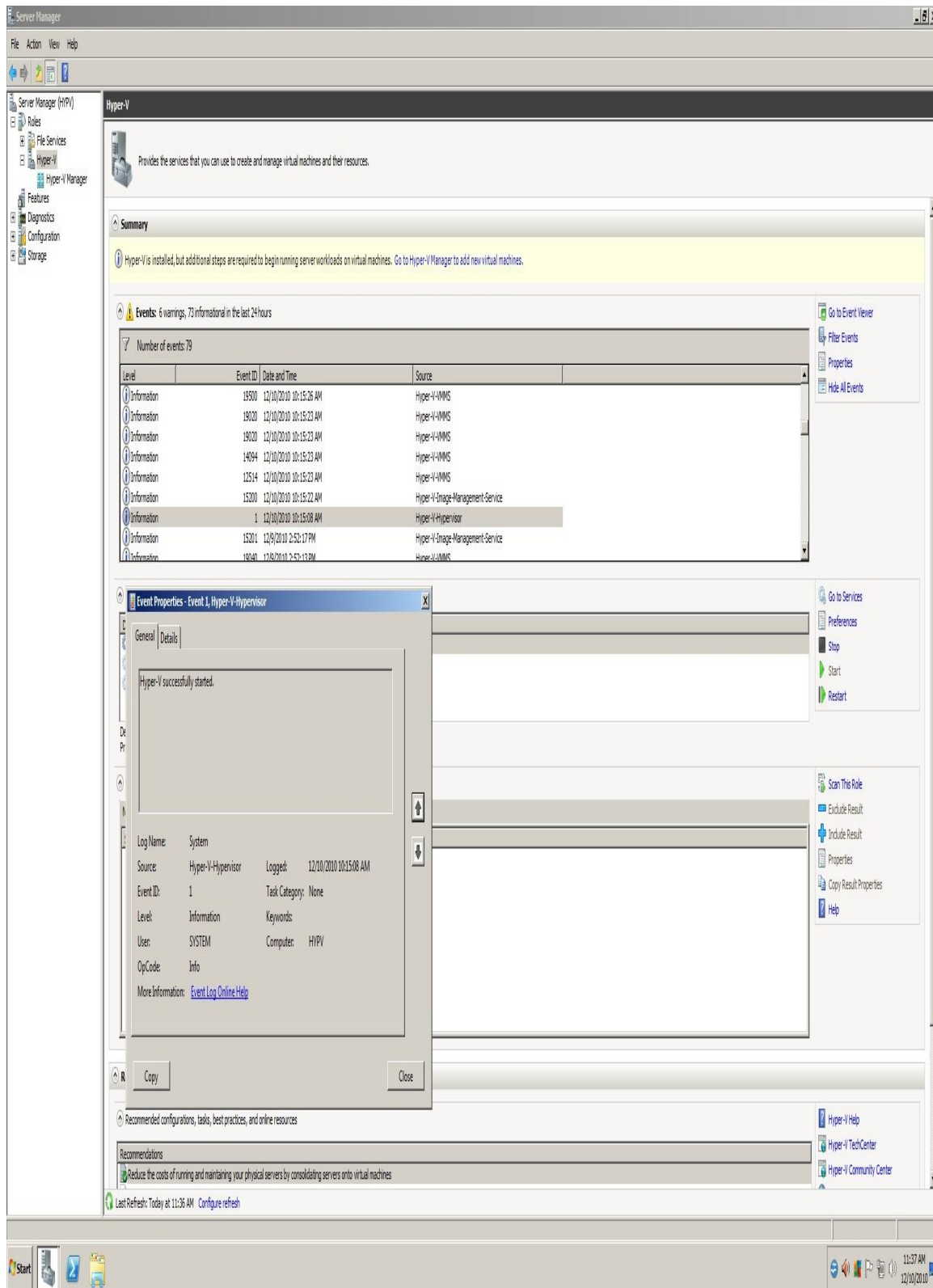
2.15. Konzola za upravljanje Hyper-V

Kada se instalira i pokrene *hyper-V Manager*, konzola u kojoj će se vršiti kreiranje, servisiranje i celokupno korišćenje virtualnih mašina, stiče se utisak kod menadžerisanjem *hyper-V*, da će sa ovim alatom provoditi najviše vremena. Alat *Administrative Tools Menu* u kome su još pored *Hyper-V Managera*, dodatni alati, za administraciju samog *host-a* računara najviše se koristi u administraciji operativnog sistema Windows Server 2008. Konzola *Hyper-V Manager* koristan je alat za digitalnog forenzičara koji može izvršiti živi monitoring i informisanje o virtuelnim mašinama.



Slika 14. Uloga host-a, instaliran Hyper-V

Slika14. pokazuje da u prozoru *Server Manager* vidimo ulogu *host-a*. Uloga pokazuje da se na *host-u* nalazi, tačnije je instaliran je *hyper-V* i samim tim i to je jedna od bitnih informacija za digitalnog forenzičara da ima u vidu da se nalazi na mestu sa koga se pokreće Cloud sistem, tj. virtualno okruženje. Ali i postoji mogućnost provere da li je ranije bio startovan *hyper-V* na *host-u* i tu informaciju digitalni forenzičar može izvući iz log fajlova.

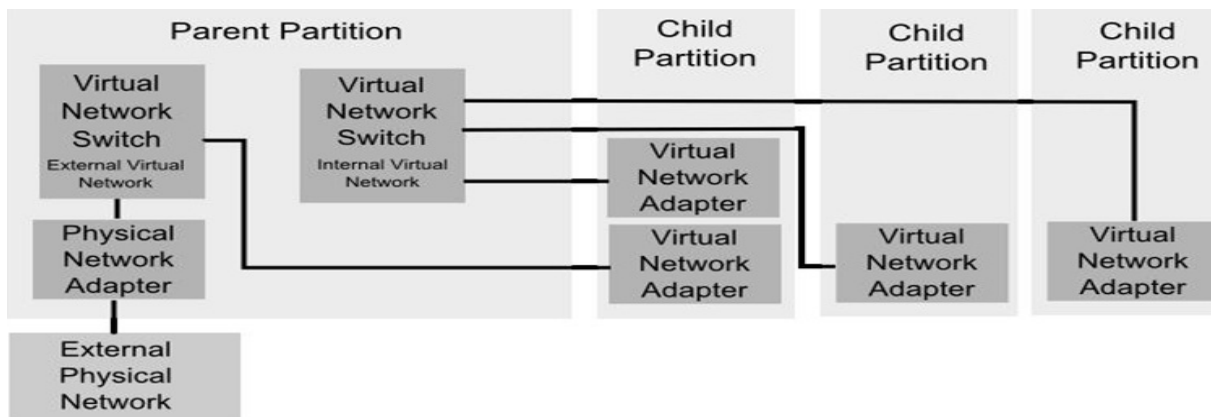


Slika 15. Pregled događaja na host-u

Kao što se može videti sa slike, Slika15, zabeležen je proces startovanja *hyper-V* na *host-u* što može biti od velike važnosti digitalnom forenzičaru kada beleži u beleškama o istražnim radnjama u određenom incidentu.

2.16. Arhitektura i razumevanje virtuelnih mreža

Svaki iskusni arhitekta Informacionih komunikacionih sistema, a koji se bavi i kreiranjem virtualnih mreža, prvo će se uvek pozabaviti pretpostavkama mogućih problema u logici, funkcionalnosti i organizaciji same virtualne mreže, ali i kako će okruženje reagovati na korisnika i obratno. Mora se voditi računa o bezbednosnim aspektima i ulogom virtualne mreže koju projektuje na Globalnu Internet mrežu. Ova oblast je veoma bitna za svakog digitalnog forenzičara, zbog toga što mora poznavati suštinu Cloud sistema, ali i uočiti detalje vezane za stvaranje jedne ili više digitalnih virtualnih ili realnih mreža koje koriste Cloud sistem. Virtualne mašine se uvek kreiraju na kraju, kao i što se krov kuće uvek postavlja posle izgrađenog temelja, kao i same konstrukcije. Arhitektura podrazumeva proces događaja koji moraju biti ispoštovani, kao i ispunjeni za stvaranje dobrog virtualnog okruženja. Razumevanje da je *host* domaćin za *child-ove* ili goste kojih može da bude više u zavisnosti od potreba Cloud sistema. Potrebe povlače hardverske resurse u bitnom ali i većem obimu, jer od potreba zavisi i odgovor arhitekta na sam virtualni sistem. O tim potrebama treba da razmišlja i digitalni forenzičar ako se bavi istragom nekog virtualnog okruženja. Postoji mogućnost da ima određena saznanja ili pretpostavke, što mu može pomoći o pravcu kretanja kroz slučaj istražnog procesa, pod pretpostavkom da je arhitekta virtualnog okruženja sa druge strane zakona. Zna se, da je *host* kao domaćin, podržan Windows Server 2008 operativnim sistemom, jer se u ovom radu obrađuje tema vezana za Cloud sistem, podržan sa *hyper-V* i da je sposoban da omogući prijem *child-ova* različitih operativnih sistema. Evo jednog arhitektonskog visokog pogleda na domen virtualnog okruženja:



Slika16. Arhitektonsko rešenje Cloud sistema

Kao što je prikazano na slici, Slika16, svaka virtualna mašina ima jedan ili više konfigurisanih mrežnih kartica. Može se primetiti da *child* može biti povezan na virtualnu mrežnu karticu *host-a*, ali i biti u intranetu koji može simulirati domen virtualnih mašina. Isti taj *child*, može biti povezan na fizičku mrežnu karticu na *host-u*, kojom može biti izveden na neku eksternu mrežu

ili Internet. Najbolja arhitektura virtualnih sistema je takva, kada postoji jedan izlaz na Internet preko na primer *Proxy* servera. Taj server će biti podešen kao usluga na operativnom sistemu Windows Server 2008. Time će biti kontrolisan celokupni saobraćaj, od korisnika virtualnih mašina ka Internetu i nazad, a bezbednost od spoljnih upada će obezbediti *Firewall*. Paketi koji koriste takav saobraćaj koristiće fizičku mrežnu karticu, dok na istom *host-u* će biti preko *Hyper-V Manager* dodata još jedna ili više virtualnih mrežnih kartica, kojima će uloga biti da se *child-ovi* konektuju na *host* i komuniciraju međusobno. Ovakve arhitekture su korektne jer smanjuju konfuziju kod administratora mreže. On je najbitnija osoba u celokupnom sistemu, od kreiranja mreže, pa preko implementacije i sve do puštanja u rad celokupnog virtualnog sistema, ali i implementacije korisnika u isti. Ovakva arhitektura je predložena od strane Britanskog standarda *StandardBS10008:2008* kojim se može obezbediti visok nivo stepena bezbednosti virtualnog okruženja. Još se mogu podesiti grupne polise i na njima obezbediti prava i privilegije korisnika u celom virtualnom sistemu i smanjiti neželjena dejstva zloupotreba virtualnog okruženja. Ali, ne i maksimalan stepen bezbednosti, jer takav stepen nije moguće postići na Globalnoj mreži dok god u procesu bezbednosti najslabiju kariku čini ljudski faktor. Ovakve informacije su korisne za digitalnog forenzičara, naročito ako se radi o korporacijskoj istrazi jer administratori korporacijskih virtualnih okruženja žele da imaju uređen sistem. Upadi od strane zlonamernih hakera u dobro obezbeđen virtualni sistem mogu se lako zabeležiti na Firewall-u, log fajlovima i monitoringu mrežnog saobraćaja. Ali ako se vrši istraga na virtualnom okruženju pod hakerskom upotrebom, biće mnogo manje dokaznih informacija jer hakeri za sobom neće ostavljati tragove. Postoji mogućnost dokaza protiv takvih sistema jer se mora vršiti pred priprema prikupljanja dokaza i potom pristupu na odgovarajući osumnjičeni server ili *host*, vršiti poređenje i dokazivanje.

2.17. Vrste virtuelnih mreža

Omogućeno je da se koriste tri kategorije različitih virtualnih mreža u kojima će se koristiti virtualne mašine. Te tri vrste mreža su:

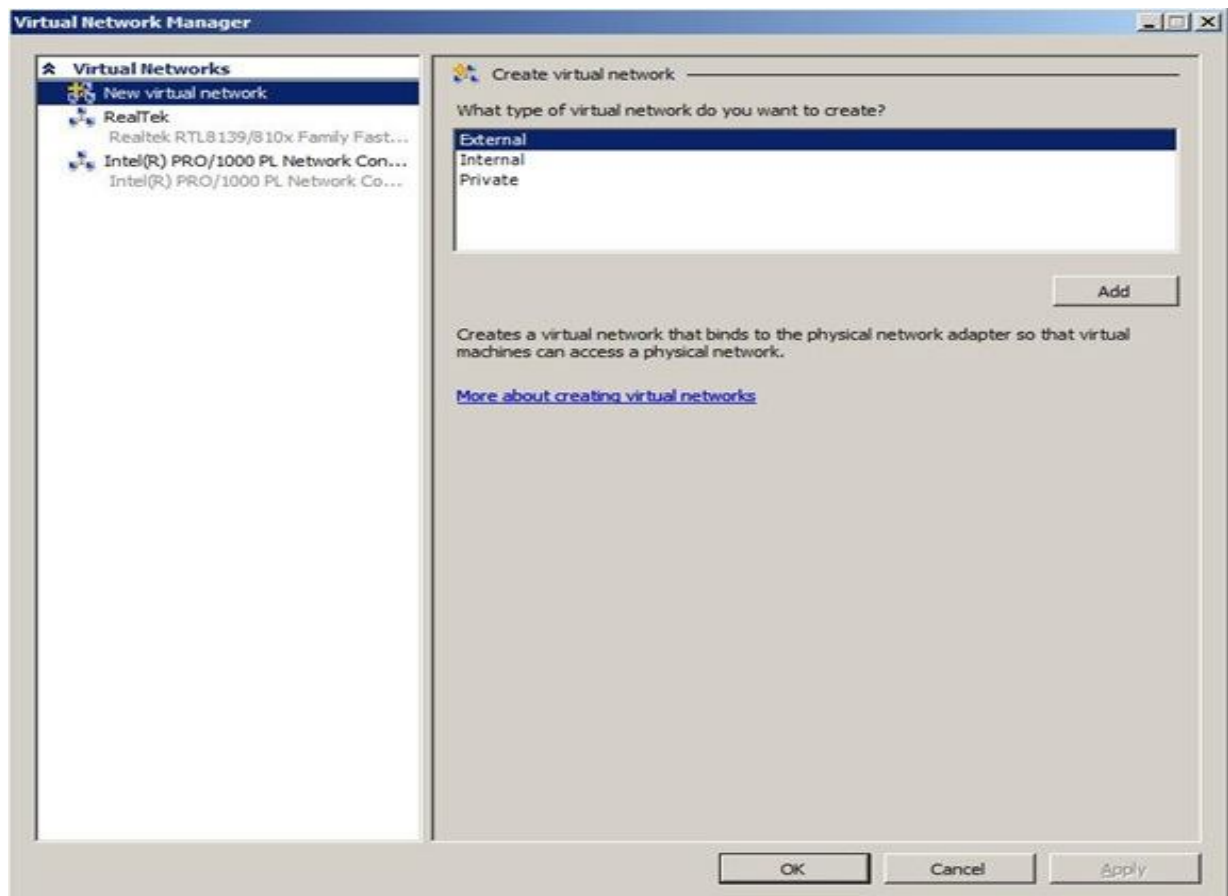
Spoljna virtualna mreža – koristi fizički mrežni adapter i omogućava nesmetanu komunikaciju sa fizičkim ali i virtuelnim mašinama, kako u intranetu pa tako i ka Internetu. Otvorena je mogućnost napada zlonamernih hakera na *host* preko virtualnih klijenata tj *child-ova*, jer je komuniciranje na relaciji *host-child* moguće kao i kod fizičkih računarskih mreža. Digitalni forenzičar pristupa prikupljanju dokaza isto kao i kod fizičkih mreža.

Interna virtuelna mreža – 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*. Pošto je omogućeno komuniciranje sa *host-om* od strane *child-a*, znači da i ovde postoji mogućnost upada zlonamernih hakera na *host* uz korišćenje *child-a*.

Privatna virtuelna mreža – slično kao i interna mreža, isto 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 i mogućnost napada na *host*, jer nema direktne komunikacije na relaciji *host-child*. Postoji teoretska mogućnost napada *host-a* preko *child-ova* tako što će preko

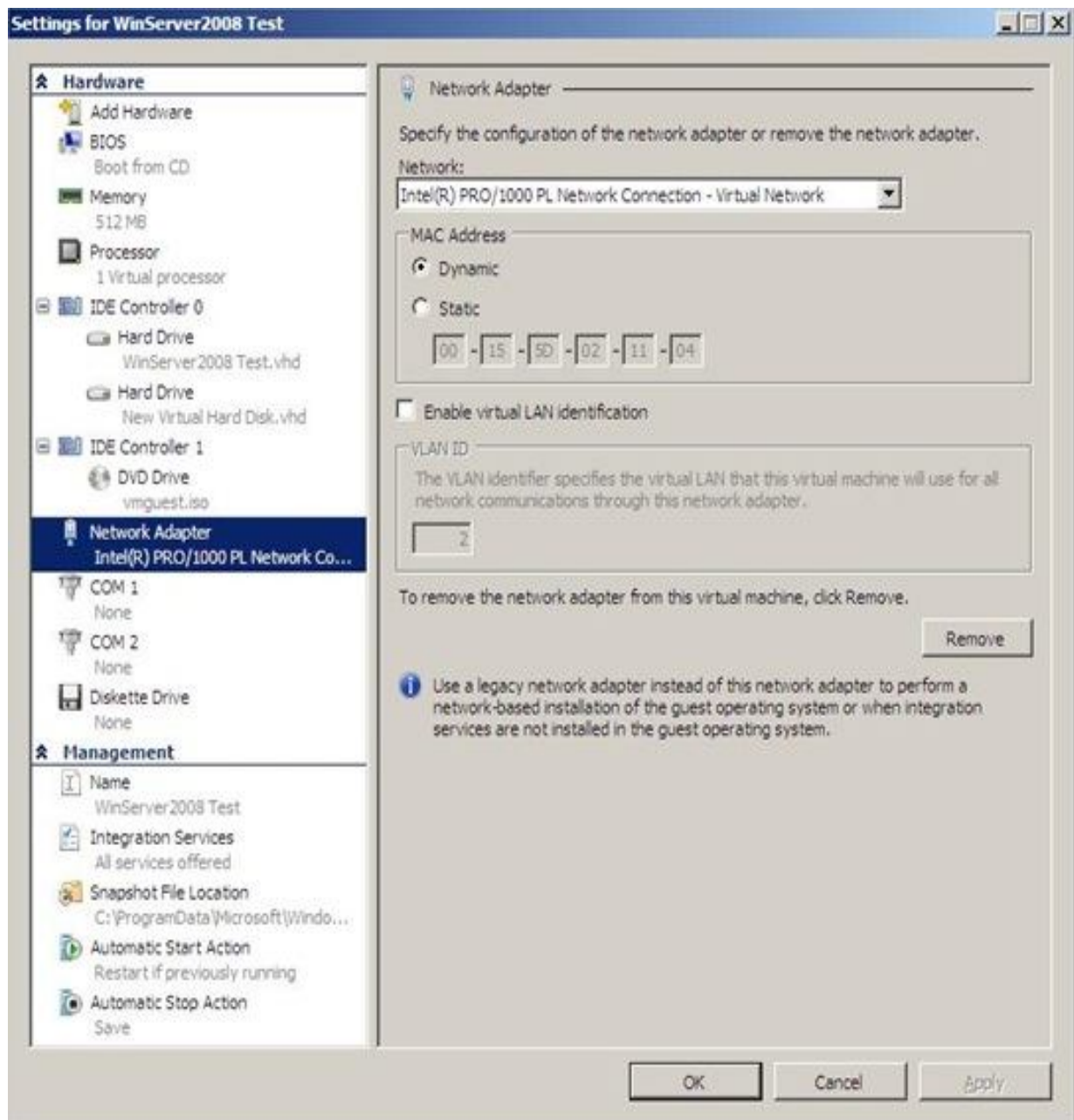
određenog impulsa oboriti fizički procesor kojeg koriste virtualne mašine kao gosti i time napasti sada hardverski deo *host-a*, a ne kao u prethodne dve mogućnosti kod spoljne i interne virtualne mreže, da izvrše napad na softversku oblast i time obore virtualne mašine ili ih zloupotrebe.

Kreiranje virtualnih mreža može se izvršiti preko wizard-a koji se pokreće iz *Hyper-V Manager* konzole:



Slika17. Virtual Network Manager

Kao što se može videti sa slike, Slika17, u prozoru se bira da li se pravi nova virtualna mreža ili koristi već postojeći fizički mrežni adapter. Ako se izabere kreiranje nove mreže, pojaviće se prozor sa desne strane i time omogućiti izbor kategorija mreža koje su opisane na početku pasusa. Kada se izabere, onda pritiskom na taster *Next* kreira se virtualna mreža. Postoji opcija da se izvrši izbor kreiranja nove virtualne mreže uz korišćenje fizičke mrežne kartice i tada se bira jedna kombinacija od tri predhodno navedene kategorije virtualnih mreža. Ali ako je potrebna još jedna virtualna mrežna kartica, izvršiće se izbor opcije predstavljene na slici:



Slika18. Dodavanje virtualnog mrežnog adaptera

Kao što je na prikazano na slici, Slika18, očigledno je kako se izbor vrši. Pored izabrane virtualne mrežne kartice, može se podesiti dinamička ili statička IP adresa, u zavisnosti od podrške DHCP servisa.

Sada se već nazire moć i jednostavnost u brzini kreiranja celokupne virtualne mreže. Postoji mogućnost kreiranja i cele šume domena, ako se poseduje dovoljno hardverskog resursa, koji će se kontrolisati i pratiti sa centralizovanog mesta tj *host-a*. Na istoj slici je predstavljena i mogućnost kreiranja celokupne virtualne mašine, što se može videti izborom određenih podešavanja, tačnije hardvera virtualnih mašina koji se povlači od resursa *host-a*. Tako da se na veoma jednostavan i lak način može podesiti virtualna mašina. U poglavlju Arhitektura virtualnih mašina navedeno da se mora voditi računa o hardverskoj iskorišćenosti *host-a*, kako ne bi došlo do preopterećenja procesora i RAM memorije, što bi dovelo u pitanje celokupno virtualno okruženje.

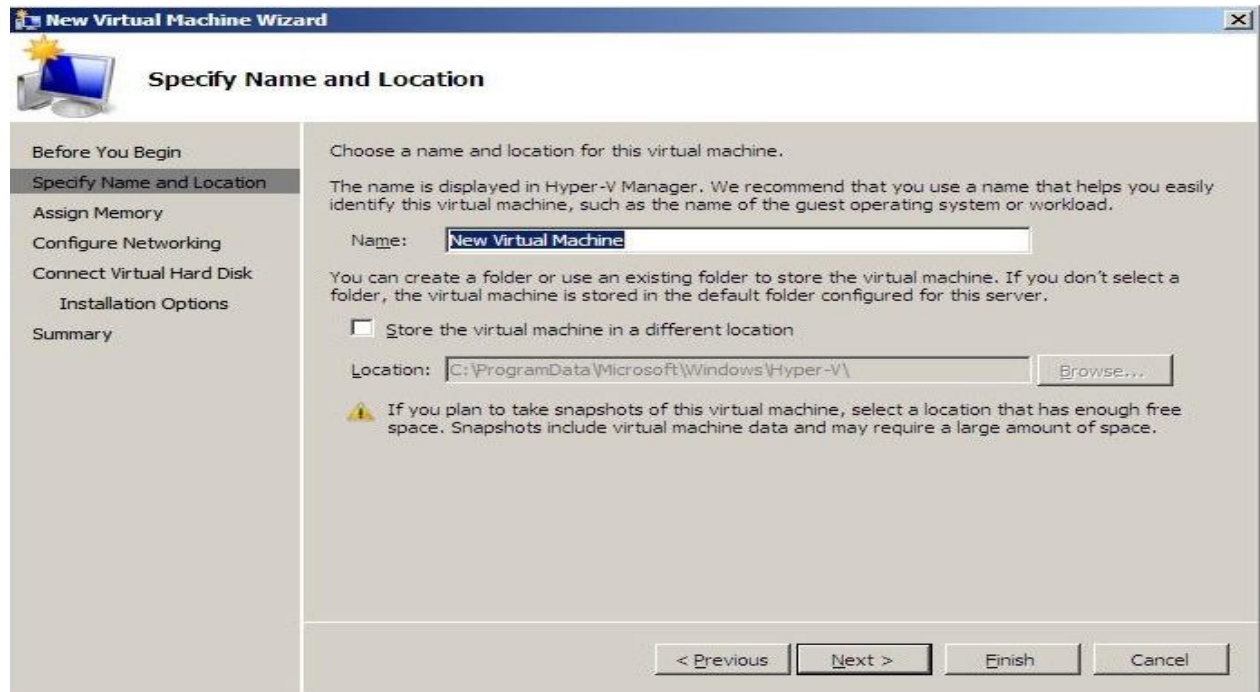
2.18. Kreiranje virtualnih mašina na hyper-V

Ključ rešenja, kako virtuelizacije, pa tako i *Cloud Computinga* omogućići će korisniku da pristupa računaru koji će biti smešten na serveru na udaljenoj lokaciji. Sistem mora korisniku da omogućiti nesmetan rad i ugodno okruženje koje će imati kod korisnika osećaj sigurnosti, što je jedno od bitnih stavki koje firma mora da ponudi korisnicima na Globalnom tržištu. Isto tako korisnik ne treba da razmišlja gde mu se njegov računar nalazi i da ne treba da ima gomilu gvožđa koje će da buči zbog rada hladnjaka i izmučenih i ne defragmentovanih hard diskova. Jednostavno sa *thin* klijentom koji otvara konekciju prema serveru i koji je priključen na javnu mrežu, korisnik će uspostaviti konekciju prema serveru na kome će se nalaziti virtualna mašina. Korisnik u veoma kratkom roku, izuzevši kucanje autentifikacije ili korišćenjem smart kartice, pristupa svojoj virtuelnoj mašini na određenom serveru. Arhitektura virtuelnih mreža je detaljno objašnjena u prethodnom poglavlju. Pravljenje virtuelnih mašina koje će biti prilagođene prohtevima korisnika, a koji će te svoje prohteve plaćati prema odluci tima menadžmenta kompanije koja pruža usluge *Cloud Computinga*. Primer dolazi iz najrazvijenije zemlje na planeti, kako informacionim tehnologijama, pa tako i u marketing sferi i pretpostavlja se da će početna cena za virtuelni klijentski računar prosečnih performansi klijent moći da priušti po mesečnoj ceni od 40\$, što za uslove te zemlje i nije velika cena. Naravno sa povećanjem broja kompanija koje će nuditi usluge *Clouding Computinga* i zdrave tržišne konkurencije, cena će naravno biti manja a srazmerno će usluga rasti u što bolje, sigurnije i stabilnije korišćenje virtuelnih mašina u jednoj Globalnoj džungli kakav je Internet.

Ovo je jedan od dodatnih problema vezanih za bezbednost korisnika u kiber prostoru, jer dozvolom pristupa još većeg broja korisnika na Globalnu mrežu, a da pri tom nije razvijen i globalni plan i strategija koja će vremenom izrasti u neki zakon u zavisnost od države do države, otvoriće se velika rupa koju neće moći da kontrolišu organi bezbednosti i tada red neće postojati. Ovo nije pitanje samo za digitalne forenzičare, već je ovo pitanje vlasti država gde će se *Cloud* sistemi primenjivati.

Kada se pristupi wizard-u za kreiranje virtuelnih mašina, može se birati nekoliko opcija hardvera same virtuelne mašine. Pritiskom na dugme *Finish* završiće se rad sa wizard-om, tada će se kreirati virtuelna mašina po setovanjima tj. podešavanjima koja su postavljena od strane administratora. Ali ako se kreira virtuelna mašina bez podešavanja administratora, kreira će se po default-na sa 512Mb RAM memorije, VHD-virtuelnim *hard disc-om* koji će biti smešten na

default-nu lokaciju na *hard disc-u host-a*. CD ili DVD drive biće dodeljen u zavisnosti koji je fizički uređaj na *host-u* i što važi za mrežni adapter.



Slika19. Ime i lokacija virtuelne mašine

Kao što se može videti sa slike, Slika19, izborom opcije za dodeljivanje imena i lokacije virtuelnih mašina, dobija se mogućnost dodele iste. Najbolje je, da se odredi u toku arhitekture Cloud sistema, kako će se definisati davanje imena virtuelnim mašinama kao i određivanje lokacije na kojoj će biti smeštene, sve zbog toga kako bi se izbegla konfuzija u administraciji sistema.

Digitalni forenzičar ovu putanju do foldera će iskoristiti kako bi došao do određene virtuelne mašine koju želi da kontroliše. U istrazi je bitno da se pristupi *host-u*, jer se sa njega može kontrolisati celo virtuelno okruženje.

2.19. Dodeljivanje memorije na virtuelnoj mašini

Memorijska zahtevnost je objašnjena u prethodnim poglavljima, tako da, ako se dobro napravi arhitektura sistema neće se javiti problem oko definisanja virtuelne memorije na virtuelnoj mašini, ali to je samo deo RAM memorije *host-a* koju sam *host* deli sa virtuelnim mašinama.

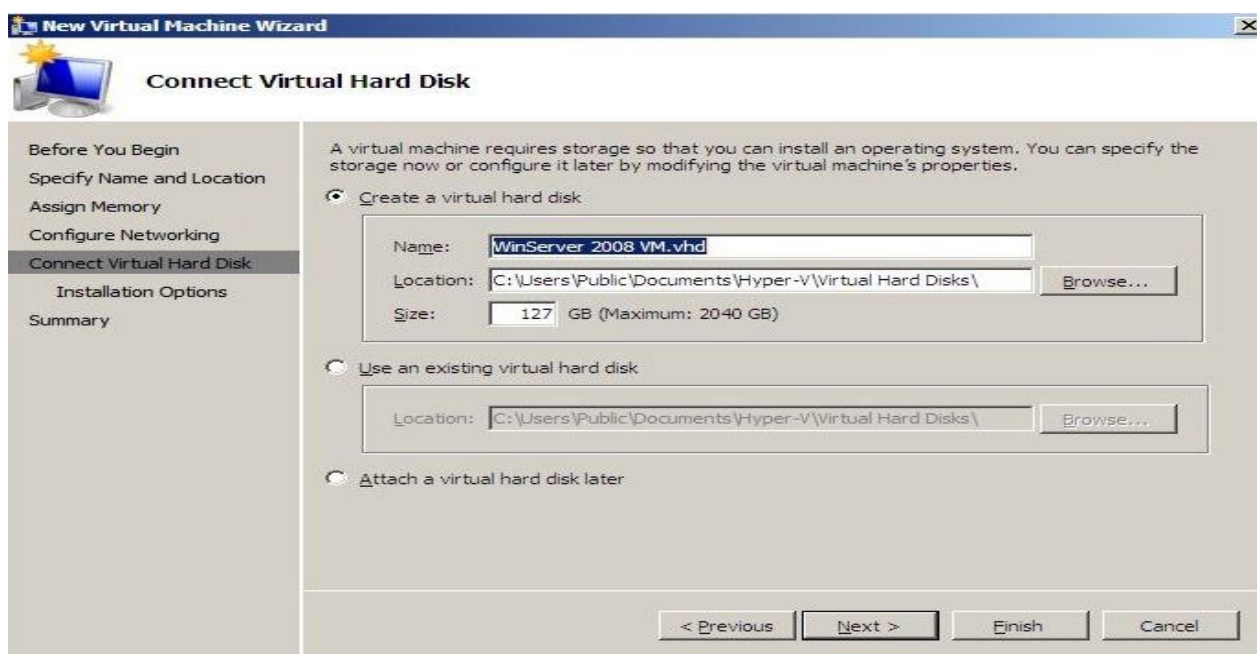
Digitalni forenzičar može vršiti vađenje informacija iz RAM memorije *host-a*, ali pod uslovom da koristi forenzičke alate za digitalno pristupanje informacijama od kojih značaju ulogu u istrazi imaju *FTK Imager*, *X-Way Forensic*. Ovim alatima je moguće pregledati RAM memoriju *host-a* pod uslovom da se pristupa živoj forenzici i da predhodno *host* nije bio isključen.

2.20. Podešavanje mrežnog adaptera na virtualnoj mašini

Kao i za podešavanje virtualne memorije na virtualnoj mašini, isto važi i za podešavanje korišćenja mrežnog adaptera na novo kreiranoj virtualnoj mašini. Mogu se koristiti već postojeći jedan ili ako ima više fizičkih mrežnih adaptera, ali i postoji mogućnost da se napravi nov virtualni mrežni adapter ili više njih.

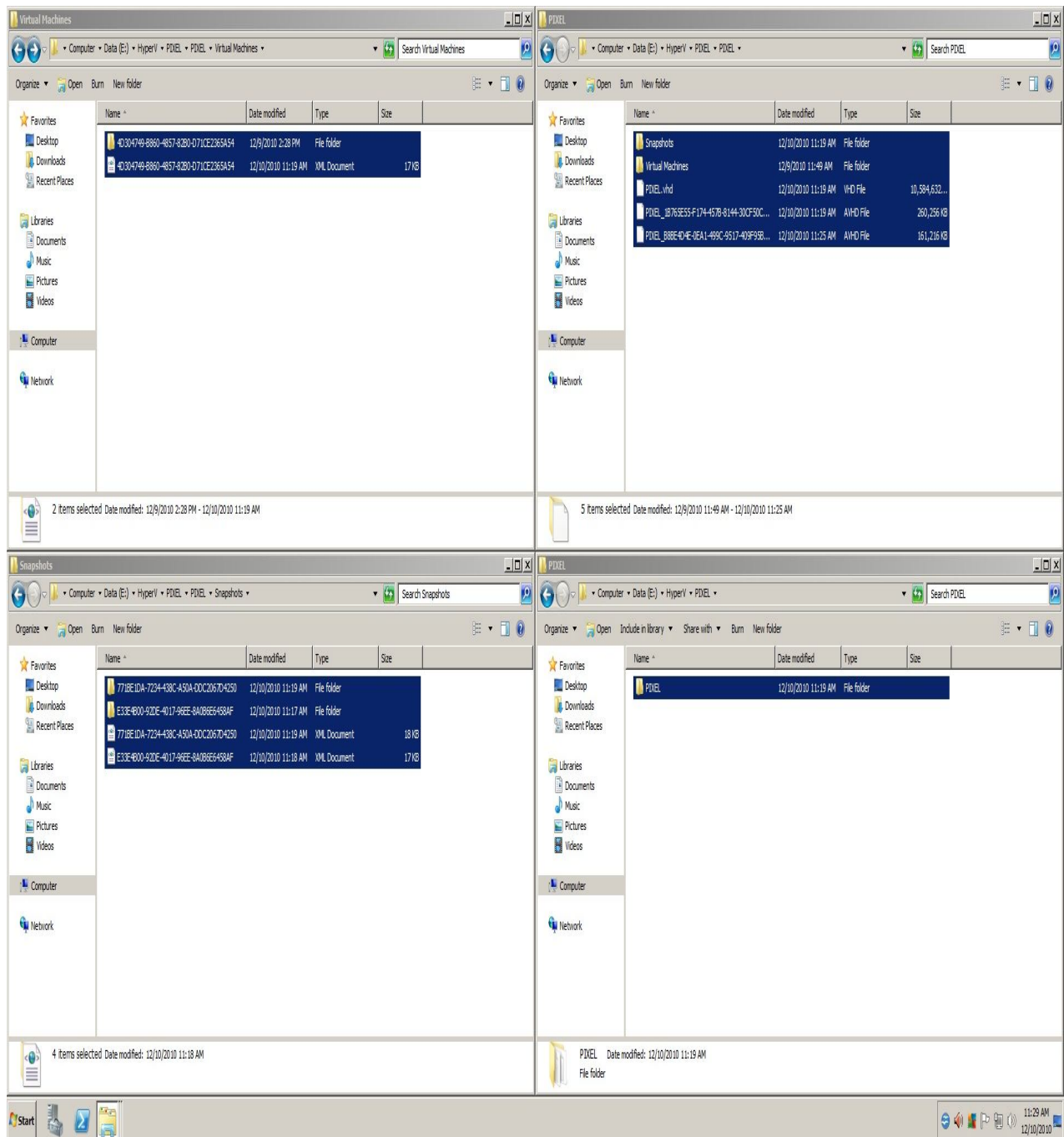
2.21. Podešavanje virtuelnog hard disc-a na virtualnoj mašini

Svaki *child* na *host-u*, mora negde da beleži svoje podatke. Zato se mora odrediti veličina prostora VHD-virtuelnog *hard disc-a*, kao i njegova lokacija. U pogledu smeštanja 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.



Slika 20. Kreiranje VHD-virtuelnog hard disc-a

Kao što se može videti na Slici 20, radi se o wizardu koji je pokrenut kada se kreira nova virtualna mašina. Ovo je jedan deo procesa kreiranja VHD-a u sklopu kreiranja nove virtualne mašine. Bitan je izbor imena VHD-a iza koga će stajati ekstenzija *.vhd*, izbor lokacije kao i veličina VHD-a. Ove informacije su veoma bitne za digitalnog forenzičara jer je bitan pristup *hard disc-ovima* na kojima se nalazi sadržaj koji se sumnjiči. Može se iskoristiti već postojeći VHD-ovi ili fizički *hard disc-ovi* ili se može kreirati i kasnije. Informacija o veličini VHD-a je isto tako bitna kako bi digitalni forenzičar mogao da organizuju prepisivanje slike *hard disc-a* na svoj medij sa koga će vršiti ispitivanja.



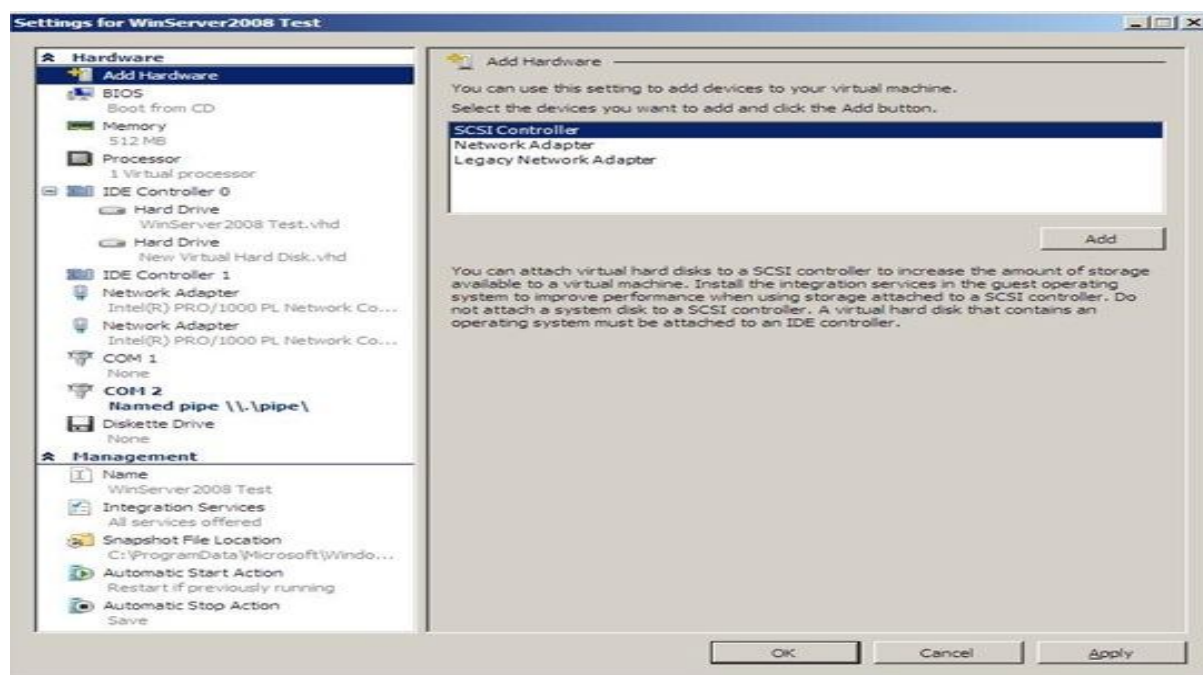
Slika21 lokacije fajlova VHD i slike stanja kao i konfiguracionog fajla virtuelne mašine

Slika21 daje četiri prikaza koji opisuju virtuelnu mašinu kroz fajlove. Prikaz dole desno daje informaciju na kojoj lokaciji na *host-u* se nalazi virtuelna mašina. Prikaz gore desno pokazuje fajlove sa ekstenzijom .vhd i dva fajla sa ekstenzijom .avhd što govori da osumnjičena virtuelna

mašina ima dva stanja ili *snapshot-a* što je isto bitna informacija za digitalnog forenzičara. Na istom prikazu imamo i postojanje pod foldera. Prikaz gore levo pokazuje unutrašnjost malo pre spomenutih podfoldera, tačnije fajl sa ekstenzijom .xml, a taj fajl nosi informacije o konfiguraciji osumnjičene virtuelne mašine, kao i o svim konekcijama sa VHD-ovima, o njihovim lokacijama i o *snapshot-ovima*. Prikaz dole levo daje informacije o *snapshot-ovima*. Za forenzičara ove informacije su bitne, jer ako sazna lokaciju ili više lokacija na *hard disc-u host-a* može lako da uradi sliku *hard disc-a host-a* jer se pretpostavlja da su u pitanju diskovi velikog kapaciteta. Sam proces pravljenja slike disc-a osumnjičenog trajao bi možda i nekoliko dana što nije izvodljivo, zato je bitno uvideti na kojim particijama se nalaze fajlovi virtuelnih mašina i time skratiti vreme pravljenja kopija. Isto je važno, da digitalni forenzičar izvrši kopiranje fajlova koji opisuju virtuelnu mašinu, kao sa slike, Sliak21 i onda ih pokrene na svojoj forenzičkoj mašini. VHD-ovi mogu biti diferencirani, dinamički i sami povećavati svoju veličinu u zavisnosti od potreba, ili već definisane veličine koji se još zovu i statički VHD-ovi. Najveći prostor za VHD može biti 2040Gb što je veoma velika količina prostora. Postoje još i pet radnji koje se mogu izvršiti na VHD-ovima kao što su: **Compact**-opcija koja smanjuje veličinu VHD-a i uklanja iza sebe ne iskorišćeni prostor, a prostor na *host-u* se neće smanjiti jer će biti ispisan nulama, **Convert**-opcija koja omogućava prebacivanje rada dinamičkih i fiksni VHD-a u proširive, **Expand**-opcija koja dodatno povećava proširivost VHD-a, **Merge**-opcija koja omogućava spajanje VHD-a ali i spajanje VHD-a i fizičkog *hard disc-a host-a* u novi VHD, a sadržaj *hard disc-a host-a* ostaće ne promenjen, **Reconnect**-opcija koja služi da poveže diferencijalni VHD sa *host-om*.

2.22. Instaliranje i pokretanje operativnih sistema na virtuelnim mašinama

Kada se napravi virtuelna mašina očekuje se i završna faza kreiranja, kao što je instalacija operativnog sistema na *child-u*. Mora se birati opcija između fizičkog optičkog uređaja koji mogu biti CD ili DVD rom. Virtuelni optički uređaj, sa koga korisnik može instalirati operativni sistem na *child-u*, može se pokrenuti i sa imidž fajla koji je smešten na nekoj lokaciji *hard disc-a*, a kreiranje virtuelnog optičkog uređaja može predhodno izvršiti u wizardu podešavanja virtuelne mašine. Kada se instalacija operativnog sistema završi, jednostavnim odabirom opcije koja pokazuje na virtuelnu mašinu koja je instalirana, sa desne strane pojaviće se opcija Start, tada se virtuelna mašina uključuje i dešava se približno slična procedura kao i kada se uključuje fizički računar. Isto kao što je rečeno u prethodnom poglavlju oko kreiranja virtuelnih mašina, postoje i mogućnosti podešavanja u toku korišćenja, što daje administratoru velike mogućnosti za fleksibilnost u radu. Opciji, koja se najviše koristi za podešavanje virtuelnih mašina, posle instalacije može se prići sa desnim klikom na biranu virtuelnu mašinu koja treba da se podesi. Onda se može birati opcija *Setings*, kao što se može videti na sledećoj slici:



Slika 22. Podešavanja virtuelnih mašina

Slika 22. pokazuje da se mogu vršiti podešavanja hardvera virtuelnih mašina i ono što je bitno je da se bilo koja promena može izvršiti ako je virtuelna mašina isključena i njeno stanje snimljeno. Postoji mogućnost pomeranja VHD-a po particijama *host-a*, ali mora se voditi računa o konekcijama između virtuelnih mašina i VHD-ka koji se mogu podesiti u *Setings* opciji *Hyper-V Managmenta*. Ovo je veoma bitno, jer na jednostavan i lak način dozvoljava se promena VHD-ova u zavisnosti od potreba ali isto tako mogu da se menjaju i konekcije kao što su IDE na SCSI.

Kod pristupa digitalnog forenzičara *host-u* na kome je osumnjičena jedna ili više virtuelnih mašina, lokacije kao i setovanja virtuelnih mašinama su od velike važnosti u istrazi. U wizardu u kome se može podešavati virtuelna mašina, mogu se naći informacije o veličini memorije, procesoru i koliko ih ima, broju VHD-ova i o lokacijama, IDE kontroleru, mrežnom adapteru, kao i kojoj mreži pripadaju, snimljenim promenama stanja i njihovim lokacijama, jer mogu raspolagati sa velikim brojem dokaza o instalacijama određenih aplikacija i o korišćenju istih. Ovo predstavlja veliku razliku kod pristupa digitalnog forenzičara u istrazi virtuelnih mašina i servera tj. *host-a* na kome se virtuelne mašine nalaze u odnosu na fizičke mašine ili server, jer ovakve informacije se ne mogu naći u fizičkom digitalnom okruženju.

2.23. Konekcijski alat između virtuelnih mašina i hyper-V

Kako bi se virtuelna mašina mogla videti na desktop-u *host-a* mora se instalirati *Virtual Machine Connection tool* i to kroz nekoliko koraka:

1. Start Server Manager
2. Select *Features* from the left hand panel
3. Click on the *Add Features* link in the main panel to invoke the *Add Features Wizard*
4. Locate the *Remote Administration Tools* category in the list of features and click on the + to unfold the sub-categories.
5. Click on the + next to *Role Administration Tools* to unfold the list of features in that category.
6. Select *Hyper-V Tools*.
7. Click on *Install* to install the feature.

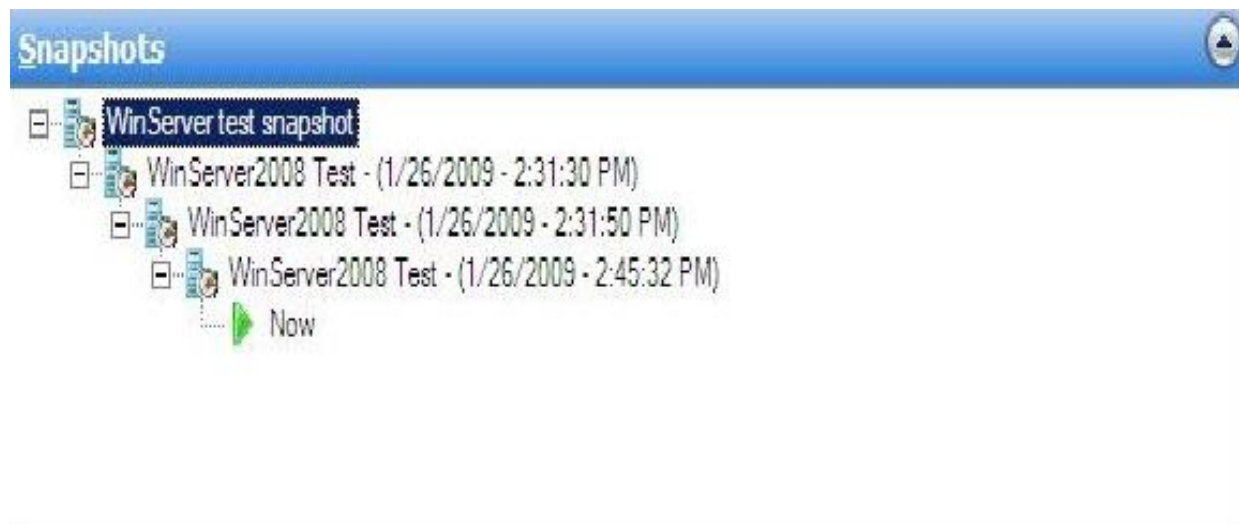
Posle instalacije će se omogućiti puna kontrola nad virtuelnim mašinama i administratoru će biti mnogo lakše u radu. Jedan od problema koji se mogu desiti posle instalacije, je da se miš zaglavljuje u desktop prozoru virtuelne mašine. Instalacijom ovog alata dobiće se još nekoliko pogodnosti koje omogućavaju fleksibilan i korektan rad administratora. Pri tom, administrator nema osećaj da radi na drugom računaru. Postoje i komande sa tastature kojim administrator ili klijent pritiskom na njih, sprovodi određene operacije nad ovim konekcionim alatom, a te naredbe su (Slika 23.):

Windows Accelerator	Virtual Machine Connection Mapping	Description
Ctrl+Alt+Del	Ctrl+Alt+End	Switches to the security screen providing options to lock, switch user, change password, log off or run the Windows task manager.
Alt+Tab	Alt+Page Up	Switches between running desktop applications
Alt+Esc	Alt+Insert	Switches between running applications in launch order
Ctrl+Esc	Alt+Home	Invokes the Windows Start menu
None	Ctrl+Alt+Pause	Switch Virtual Machine Connection Tool to and from full screen mode
None	Ctrl+Alt+Left Arrow	Releases the mouse and keyboard focus from the Virtual Machine Connection Tool.

Slika 23. Komande sa tastature za delovanje na virtuelne mašine

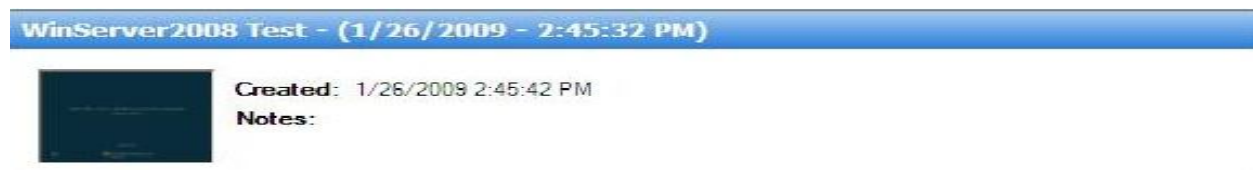
2.24. Kreiranje i upravljanje hyper-V Snapshots

Slikanje stanja virtuelnih mašina, poznatije pod nazivom *snapshots*, kreira fajl sa ekstenzijom .avhd. „Snimaju se samo one promene koje se dogode ako korisnik promeni konfiguraciju operativnog sistema ili instalira neku aplikaciju.



Slika 24. Slike stanja virtuelne mašine

Sa Slike 24, se vidi da *WinServer test snapshot* ima zabeležene tri slike stanja. Zabeležio je određene promene u operativnom sistemu, što je isto bitno kod pristupa digitalnog forenzičara. Forenzičar mora napraviti slike tih stanja koje će istraživati na forenzičkom računaru. Pošto su mogućnosti administratora da vratiti prethodno ili stanje pre toga, to može dodatno napraviti problem u istrazi. Zato forenzičar kreće sa vraćanjem poslednjeg stanja po datumu i vremenu, tako vidi poslednje promene i ima mogućnost istraživanja pokretanja virtuelnih mašina na forenzičkom računaru. Nekada je dobro napraviti simulaciju celokupnog virtuelnog okruženja, ako kompleksnost istrage to zahteva.



Slika 25. Pokretanje virtuelne mašine iz prethodne slike stanja

Slika 25 predstavlja vraćanje operativnog sistema virtuelne mašine u predhodno stanje od moguća tri. Kada se pride mišem na određeno birano stanje, desnim klikom miša dobiće se mogućnost startovanja tog stanja. Uključiće se virtuelna mašina u stanju pre nekog incidenta. Ovde se može iskoristiti i pregled RAM memorije, jer pokretanjem određene slike stanja na *host-u* će se videti upamćeno sve što se nalazilo tog trenutka u RAM memoriji. Digitalni forenzičar mora imati orijentaciju u vremenu i kretanju kroz slike stanja i sa informacijama iz RAM memorije kao i svim drugim informacijama koji mogu biti na raspolaganju. Digitalni forenzičar može napraviti scenario događaja nekog incidenta koji mora biti podržan sa digitalnim ali i fizičkim dokazima.

Pored startovanja u padajućem meniju, pokrenut desnim klikom miša, postoje još neke operacije koje mogu biti izvršene. Te akcije su predstavljene u tabeli:

Action	Description
Apply	Applies the snapshot to the virtual machine from which it was taken. The virtual machine will revert to the exact state it was in when the snapshot was taken. Any changes made to the virtual machine since the snapshot was taken will be lost. Hyper-V will provide the option to take a new snapshot of the virtual machine's current state before applying the old snapshot.
Rename	Allows the name assigned to the snapshot to be changed.
Delete Snapshot	Deletes the snapshot and all associated files from the system. This action is irreversible.
Delete Snapshot Subtree	Deletes the currently selected snapshot and all other snapshots which are located beneath it in the tree.
Settings	Allows the settings of the virtual machine at the time of the snapshot to be viewed. Modification of settings is disabled.

Slika 26. Spisak mogućih naredbi nad virtuelnim mašinama

Dešavanja na VHD-u posle kreiranja slika stanja se menjaju i kreiraju se određeni fajlovi koji u sebi nose veliki broj informacija, ti fajlovi su:

- **Configuration file** - An XML file containing the current configuration settings of the virtual machine.
- **Saved state file** - A .vsv file containing virtual machine state information.
- **Differencing disk image file** - A .avhd differencing disk.
- **Memory image file** - A .bin file containing an image of the virtual machine's memory at the point the snapshot was taken.

Fajlovi u sebi nose informacije i od velike su važnosti administratoru, kao i digitalnom forenzičaru. Sa tim fajlovima se može lako manipulirati, što opet daje mogućnost fleksibilnosti u radu sa virtuelnim mašinama u Cloud sistemima.

2.25. Razumevanje i instalacija hyper-V usluga integracije

Ono što je bitno u *hyper-V* okruženju je odnos između *host-a* i *child-a*, kao i o mogućim delovanjima na *child*. Usluge se nalaze i na *host-u*, ali i na *child-u*, a opisane su na sledećoj strani rada i one su:

- **Virtual Machine Connection Enhancements** - When the console of a guest operating system without Hyper-V Integration Services installed is accessed using the Virtual Machine Connection, clicking in the Virtual Machine Connection dialog locks the mouse pointer into that window. Focus may only be released by initiating a keyboard sequence (the default being Ctrl+Alt+Left Arrow). With Integration Services installed, however, the pointer focus is automatically assigned to and released from the Virtual Machine Connection window as the mouse pointer passes in and out of the window. This avoids the necessity to click in the window to assign focus and then press the keyboard sequence to subsequently return the focus to the local desktop.
- **Virtual drivers and Hypervisor-aware Kernel** - Allows the guest operating system to communicate directly with the parent partition over the VMBus when accessing devices and making I/O requests, thereby increasing performance of the guest operating system.
- **Hyper-V Time Synchronization Service** - The purpose of this service is to synchronize the system time between Hyper-V child and parent partitions (for a detailed description of child and parent partitions, read the chapter entitled [An Overview of the Hyper-V Architecture](#)). This synchronization is important to avoid potential time drift between the guest operating systems running in a child partitions and the Hyper-V parent partition.
- **Hyper-V Heartbeat Service** - The heartbeat service allows the parent partition to detect when a virtual machine has locked up, crashed or otherwise ceased to function. The parent partition sends heartbeat messages to the guest operating system at regular intervals. It is then the job of the Hyper-V Heartbeat Service installed on the guest operating system to send a response to each of these heartbeat messages. When the parent partition fails to receive responses from the child partition, it assumes that the child's Heartbeat Service, and therefore the guest operating system on which it is running, has encountered problems. The administrative services on the parent partition will subsequently log the event accordingly such that it is brought to the attention of a system administrator for corrective action to be taken.
- **Hyper-V Shutdown Service** - The Hyper-V Shutdown Service allows the guest operating system to be shut down cleanly using Hyper-V management interfaces (such as the Hyper-V Manager console and the Virtual Machine Manager), thereby avoiding the necessity to log into the guest operating console and manually initiate the shutdown procedure. As a typical example, when an administrator selects the *Shutdown* action for a virtual machine from with Hyper-V Manager, the parent partition communicates with the Hyper-V Shutdown Service running on the selected guest operating system to notify it of the request. The Shutdown Service then initiates the guest operating system's shut down process by making (in the case of Windows guests) standard Windows Management Instrumentation (WMI) calls.
- **Hyper-V Volume Shadow-Copy Requestor** - The Hyper-V Volume Shadow-Copy Service provides Volume Shadow Copy integration between Volume Shadow Copy enabled guest operating systems and the parent partition.
- **Hyper-V Key/Value Pair Exchange** - Provides the ability for the child and parent partitions to exchange configuration information through pre-defined registry entries in the guest operating system. In the case of the parent partition, it is able to view, set and delete registry entries in the child partition's guest operating system. In addition, the parent partition configures a number of registry entries into the guest's registry which serve to provide the guest with information about the parent partition and host system configuration. Additional information on the Hyper-V Key/Value Pair Exchange service is covered later in this chapter.

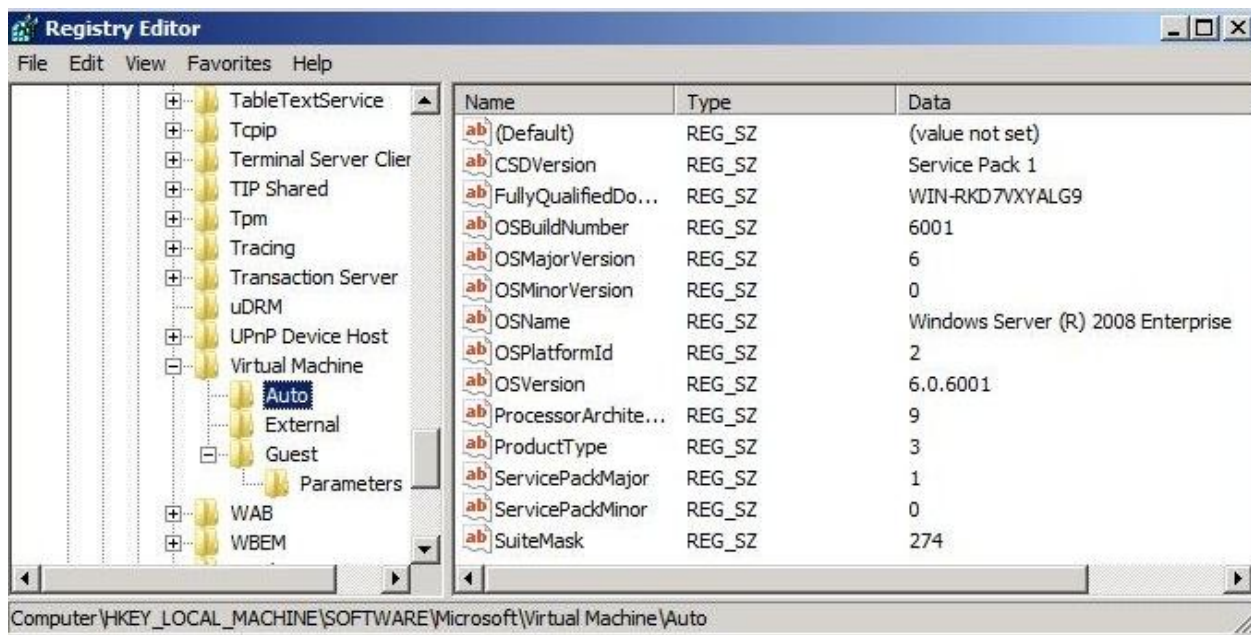
Svaka promena vezana za virtuelnu mašinu se beleži u registru u operativnom sistemu *child-a* i te informacije se nalaze kada pritiskom na Start meni, unesemo u polje za startovanje aplikacija naredbu *regedit* i potom pristupimo registru. Sve bitne informacije se nalaze na lokacijama koje su date na sledećoj slici:

```
* HKEY_LOCAL_MACHINE\Software\Microsoft\Virtual Machine\Auto
* HKEY_LOCAL_MACHINE\Software\Microsoft\Virtual Machine\External
* HKEY_LOCAL_MACHINE\Software\Microsoft\Virtual Machine\Guest\Parameters
```

Registry Key	Description
OSMajorVersion	The guest operating system's major version number.
OSMinorVersion	The guest operating system's minor version number.
OSBuildNumber	The guest operating system's build number.
OSVersion	The guest operating system's version number.
OSPlatformId	The guest operating system's platform ID value.
CSDVersion	The most recent Service Pack applied to the guest operating system (e.g. Service pack 1)
ServicePackMajor	The major version number of the most recent Service Pack applied to the guest operating system (e.g. 1).
ServicePackMinor	The minor version number of the most recent Service Pack applied to the guest operating system (e.g. 0).
SuiteMask	The product suites installed on the guest system.
ProductType	Numerical value indicating the guest operating system product type installed in the child partition.
OSName	The name of the guest operating system installed in the child partition (e.g. Windows Server (R) 2008 Enterprise).
ProcessorArchitecture	Numerical value indicating processor architecture identifier
FullyQualifiedDomainName	The fully qualified DNS name that uniquely identifies the guest operating system's fully qualified domain DNS name.

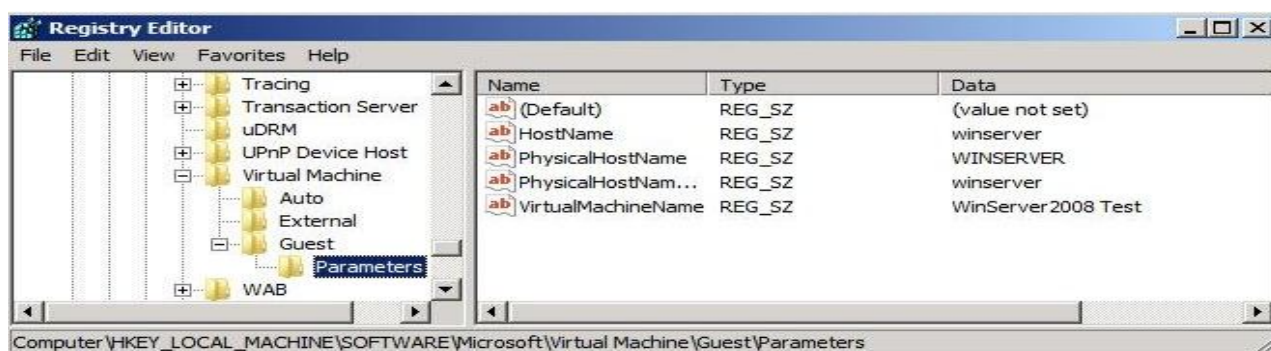
Slika 27. Registry ključevi

Slika 27. pokazuje ključeve registara i objašnjenja u kojima se beleže promene, a sledeće slike 28 i 29, pokazuju navedene ključeve i tačne lokacije u registru gde se nalaze:



Slika 28. Lokacija registry ključeva

Informacije koje obezbeđuje *host* prema *child-u*, su takve da omoguće gostu da vidi osnovne informacije o sredini na kojoj je pokrenut. Te informacije se nalaze na:
HKEY_LOCAL_MACHINE\Software\Microsoft\Virtual Machine\Guest\Parameters



Registry Key	Description
HostName	The domain name system (DNS) name of the operating system running in the Hyper-V parent partition.
PhysicalHostName	The non-fully qualified name of the operating system running in the Hyper-V parent partition.
PhysicalHostNameFullyQualified	The fully qualified name of the operating system running in the Hyper-V parent partition.
VirtualMachineName	The name of the virtual machine used by the virtualization stack.

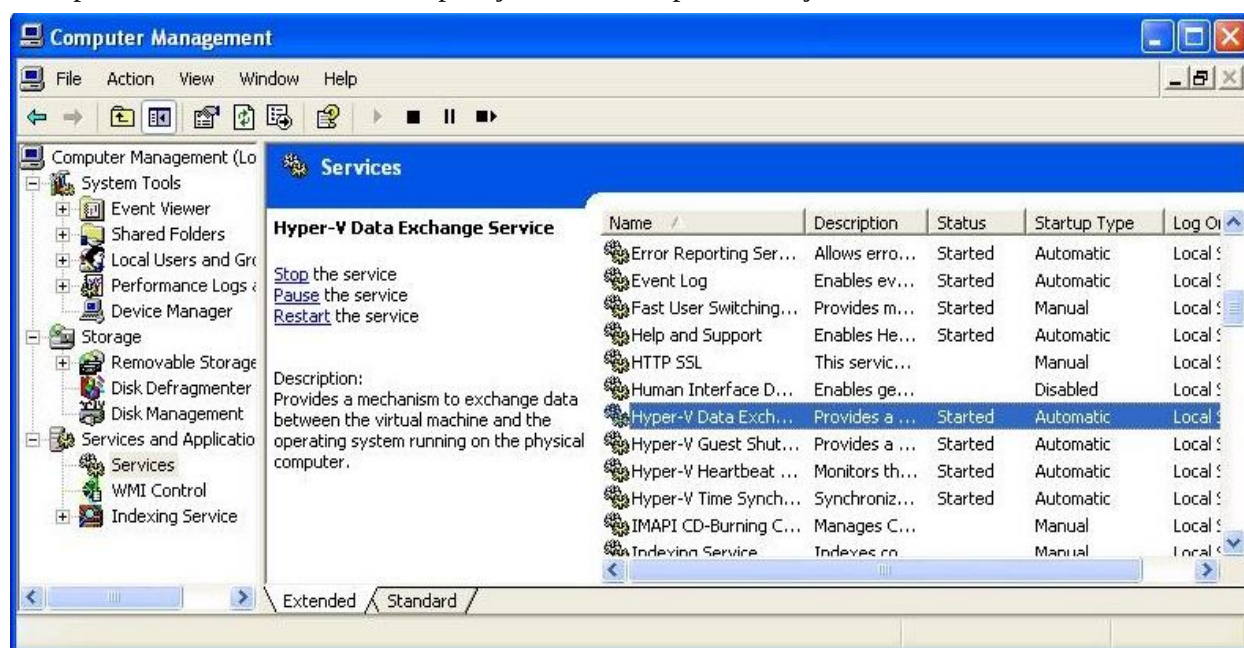
Slika 29. Prikaz informacija registra na *host-u* od *child-a*

Na sledećoj slici, Slika30, su predstavljeni svi Microsoft operativni sistemi koji podržavaju *hyper-V* i servisi koji podržavaju njihovo korišćenje:

Platform	Supported Services
Windows Server 2008 x64	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange, VSS
Windows Server 2008 x86	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange, VSS
Windows Server 2003 x64 (SP2)	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange, VSS
Windows Server 2003 x86 (SP2)	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange, VSS
Windows 2000 Server (SP4)	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange
Windows 2000 Advanced Server (SP4)	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange
Windows Vista x64 (SP1)	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange, VSS
Windows Vista x86 (SP1)	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange, VSS
Windows XP x86 (SP2/SP3)	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange
Windows XP x64 (SP2)	Time Synchronization, Heartbeat, Shutdown, Key/Value Pair Exchange

Slika30. Microsoft operativni sistemi koji podržavaju hyper-V

Ako bi trebalo da se instalira neka od starijih verzija operativnih sistema iz lepeze Microsoft-ovih proizvoda, trebalo bi obratiti pažnju na dodatna podešavanja.



Slika 31. Instalacija za podršku hyper-V na child-ovima

Dodatna podešavanja vrše se oko rešavanja problema kod instalacije starijih operativnih verzija sistema. Tada se mora instalirati podrška za hipervizor na *child-u* i potom će biti omogućeno korišćenje *host-ovih* usluga kao servera. Novije verzije su predefinisane da prepoznaju hipervizor. Podešavanja na *child-u* se nalaze, kada se pristupi na Computer ili MyComputer u zavisnosti od verzije operativnog sistema, pa desni klik i u opciju Computer Manager, kao što slika, Slika31, pokazuje da se mogu videti, u opciji *Service and Application* setovanja za podršku i podešavanje *hyper-V*.

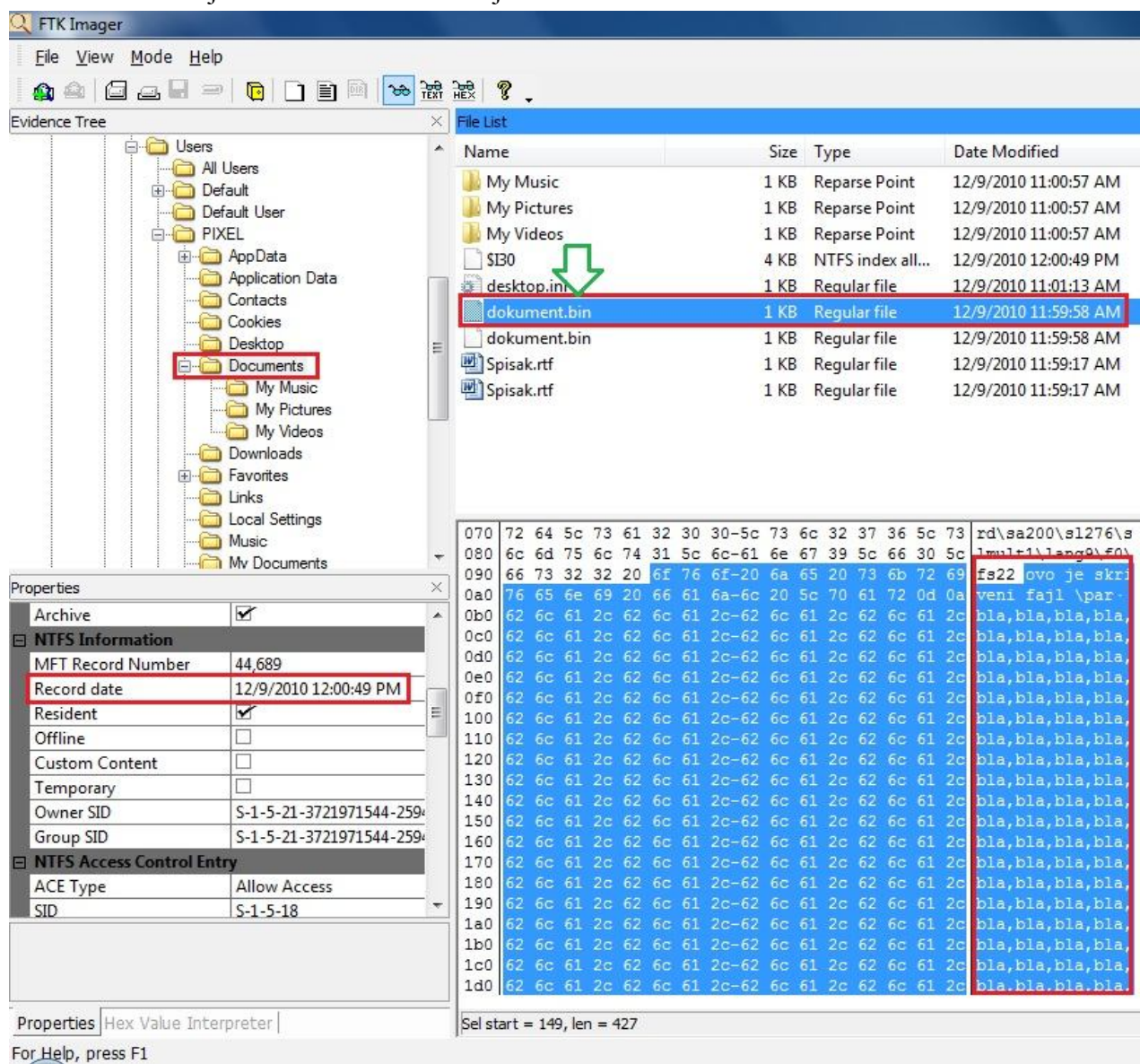
2.26. Pristup forenzičkim alatom na hard disc virtualne mašine

Kada digitalni forenzičar napravi kopiju virtuelnog *hard disc-a* na svoj medij uz korišćenje nekog forenzičkog alata, tada taj fajl treba da pokrene na svojoj forenzičkoj mašini na kojoj će vršiti istragu. Bitno je napomenuti da su se do sada uvek pravile dve kopije *hard disc-a* osumnjičene fizičke mašine. Jedna kopija se uvek šifrovala sa MD5 ili SHA256 algoritmom kako bi bila čuvana do pojavljivanja dokaza pred sudom i tada bi bila dešifrovana. Ovim se dokazuje da nije bilo promena u toku istrage nad osumnjičenim podacima na *hard disc-u*. Dok bi druga kopija bila korišćena u forenzičkoj istrazi na forenzičkom računaru. Ali pojavom virtuelnih mašina javila se potreba za pravljenjem i treće kopije osumnjičenog *hard disc-a*. Ta treća kopija, u kojoj bi se nalazili i VHD-ovi kao i *snapshot-ovi* i konfiguracioni fajlovi osumnjičene virtuelne mašine, bi se koristila u forenzičkoj virtuelnoj mašini i bila bi pokrenuta u okruženju sličnom u kojem ga je koristio i osumnjičeni.



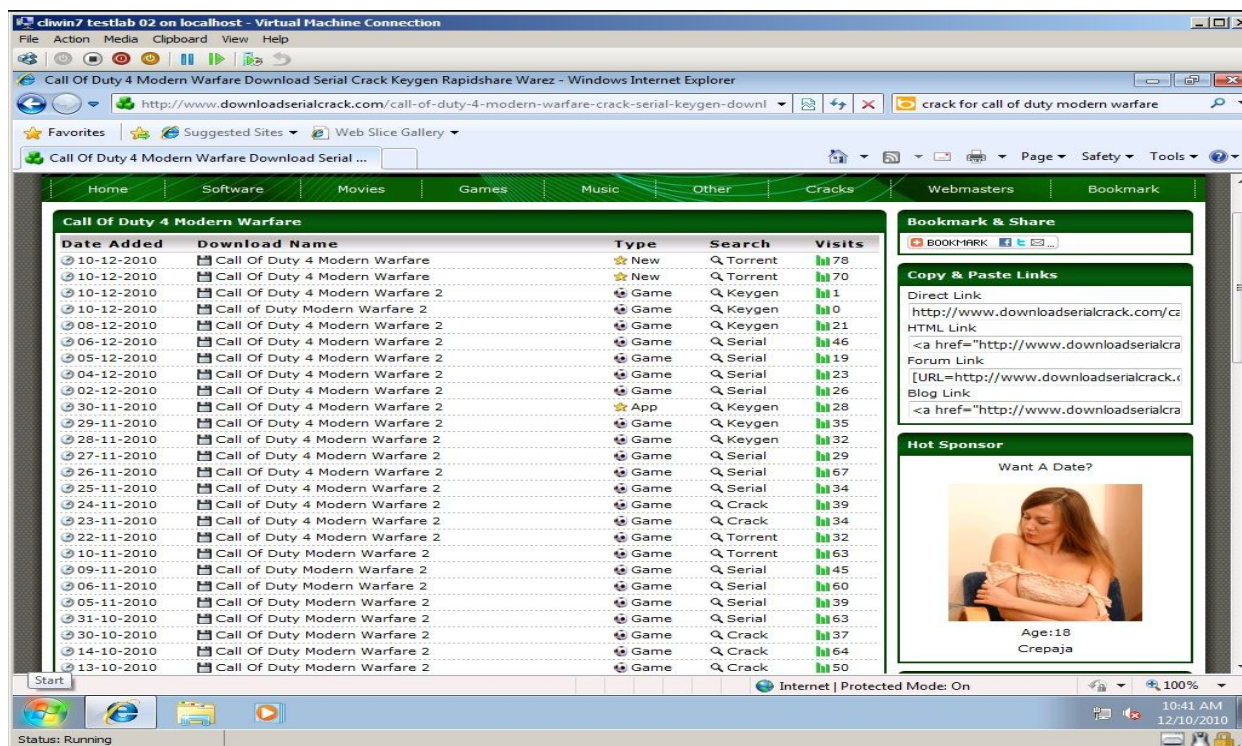
Slika 32. Pristup Heliks-om na virtuelnu mašinu

Slika 32. prikazuje pristup forenzičkog alata na osumnjičenu virtuelnu mašinu. Informacije koje digitalni forenzičar može da vidi vezane su za korisnika virtuelne mašine, adresu mrežne kartice, organizacije u kojoj se operativni sistem koristi, pripadnost domenu, veličini VHD-a i o postojanju optičkog drajva ali po informaciji *error* pretpostavka je da se radi o virtuelnom drajvu. Postojanje pravljenje slike operativnog sistema sa forenzičkim alatom je opipljiv proces jer pri toj operaciji ne sme biti narušena konfiguracija kao ni podaci na osumnjičenom *hard disc-u*. Najbolje je koristiti butabilan CD ili DVD medij na kome je forenzički alat i koristiti spoljni ili eksterni uređaj sa koga se neće ništa upisati na osumnjičeni računar. Napravljenju sliku *hard disc-a* osumnjičenog računara koja je sačuvana na *hard disc-u* digitalnog forenzičara, treba prekopirati na forenzički računar i izvršiti detaljnu analizu fajlova koji deluju sumnjivo. Prikupljene dokaze treba beležiti u knjigu u kojoj je otvoren novi slučaj, ali postoje i programski softverski alati kojima se može voditi slučaj.



Slika 33. Istraga incidenta na virtuelnoj mašini sa alatom FTKImager

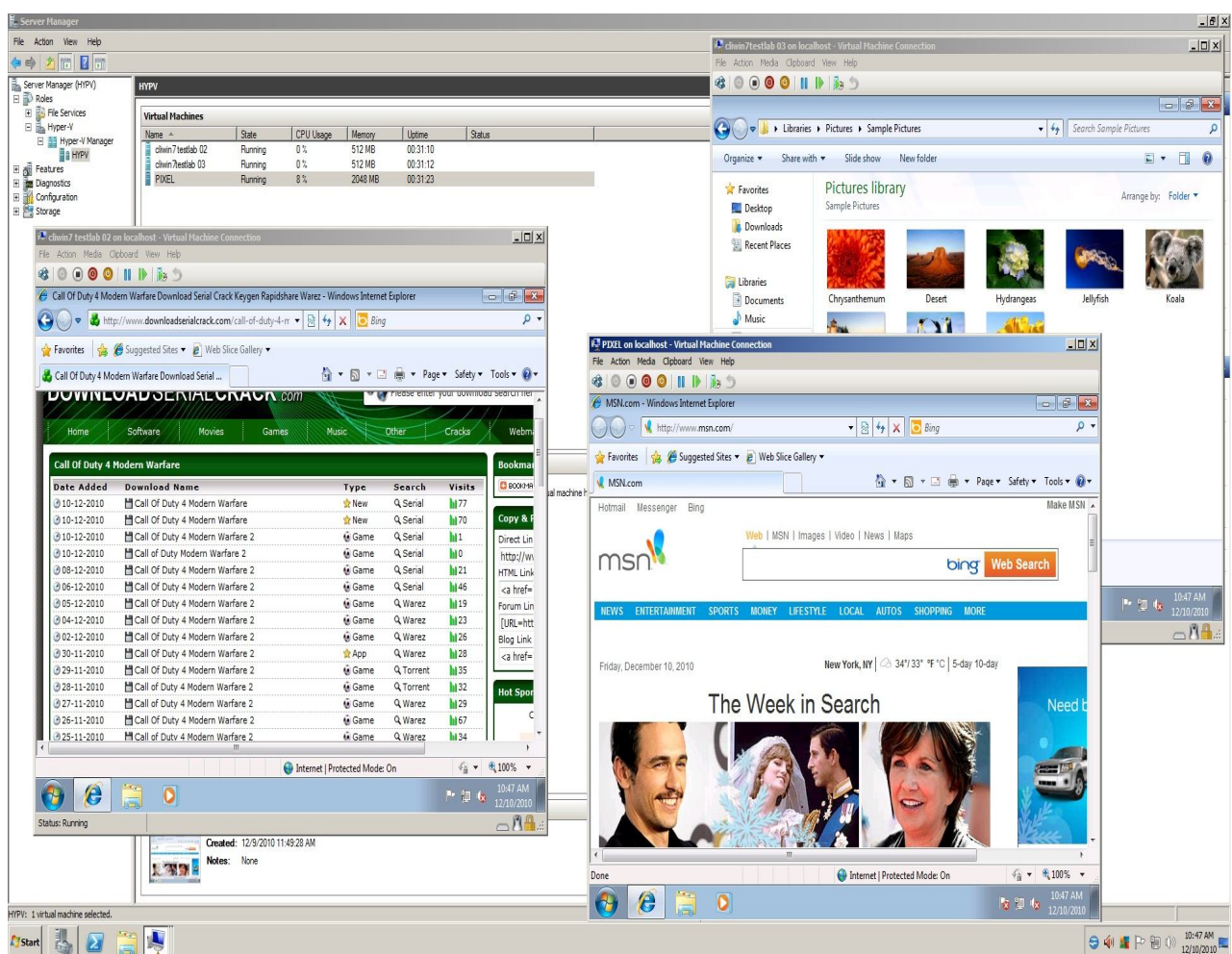
Sa Slike 33, može se videti da je osumnjičeni pokušao da promeni ekstenziju fajla *dokument* u ekstenziju koju operativni sistem ne zadaje po kreiranju tekstualnog fajla. Ali pošto je operativni sistem takav da fajlove uvek potpisuje pravilno sa već određenim ekstenzijama, a koje su mu programirane u kernel-u, digitalni forenzičar će uvek gledati binarni zapis koji počinje karakterima *6f 76...* koji govore da se radi o tekstualnom fajlu sa ekstenzijom *.txt*. Kada se uoči ovakva nepravilnost odmah postoji sumnja da se nešto krije u ovakvim fajlovima tekstualne prirode. Tekst koji se nalazi u fajlu *document.bin* a koji bi po pravilu trebao da bude sa punim imenom i ekstenzijom *document.txt*, vidi se sa desne strane forenzičkog alata i glasi *ovo je skriveni fajl....* Pošto je lociran fajl koji tereti osumnjičenog, treba snimiti sliku fajla i datum, kako bi se videlo kada je fajl kreiran od strane osumnjičenog i obratila pažnja na akcije osumnjičenog u tom vremenskom intervalu na osumnjičenoj virtuelnoj mašini. U istom forenzičkom alatu se vidi kada je kreirana slika *hard disc-a* od strane digitalnog forenzičara. Može se pogledati da li je osumnjičeni slao ovaj fajl nekom preko email-a ili nekog Internet komunikacionog kanala. Može se još pogledati u folderima gde su smešteni kolačići od Web stranica, da nema zabeležena neka konekcija sa koje može biti preuzet fajl. Ovaj detalj je bitan kako bi slučaj bio vođen u jednom pravcu i kako osumnjičeni ne bi mogao da se pravda kako mu je taj fajl podmetnut, jer je njegovu mašinu zauzelo treće lice. Ovaj deo digitalne forenzičke istrage nad virtuelnom mašinom se u potpunosti poklapa sa klasičnom digitalnom forenzikom istragom koja se sprovodi nad fizičkim mašinama. Isti je jer su napravljene slike *hard disc-a* i binarno su upisane na treću lokaciju tj. forenzički *hard disc*. Testirana je i ova opcija, a upoređivanjem se zaključilo da su slike *hard disc-a* sa virtuelne mašine i fizičke mašine iste. Ako se sazna konekcija ka nekoj Web stranici, forenzičar će pristupiti toj stranici sa svog forenzičkog računara.



Slika 34. Web stranica sa ne zakonitim trgovanjem fajlova koji se mogu preuzeti

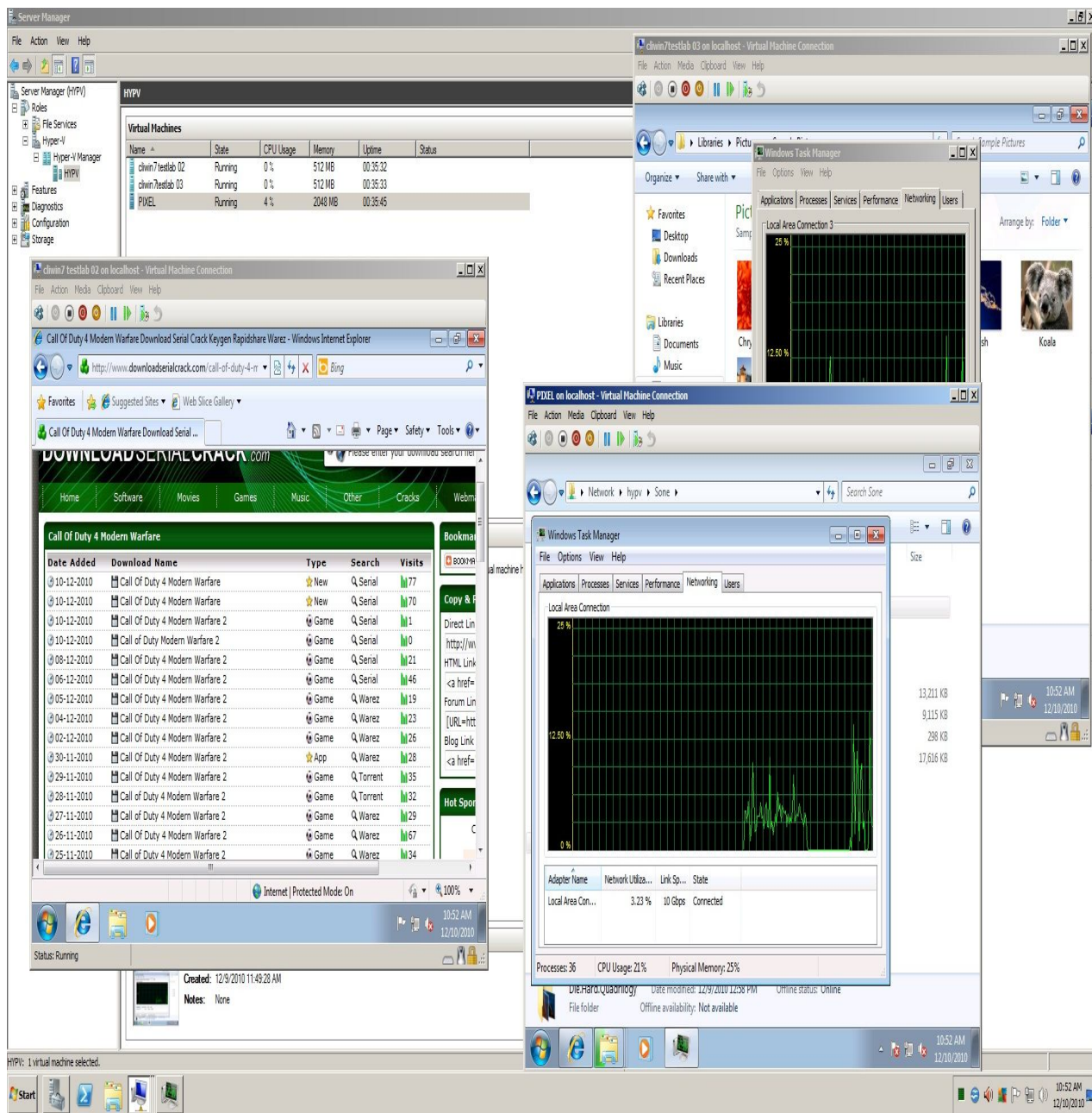
Slika 34. nudi prikaz jedne Web stranice koja daje mogućnost preuzimanja ne zakonitih fajlova jer krši autorska prava proizvođača.

Pošto je rad baziran na pristup virtuelnom okruženju, informacije o tome da li još neka virtuelna mašina vrši neku ne zakonitu radnju može se proveriti pokretanjem svih mašina na forenzičkoj mašini. Ova operacija može da se uradi i pri živoj istrazi nad osumnjičenim serverom na kome su virtuelne mašine. Operacija se izvodi jednostavnim putem tako što se pristupa konzoli *Server Manager* koja ima mogućnost pokretanja i kontrolisanja virtuelnih mašina. Postoji informacija o virtuelnim mašinama koje su u procesu rada i o isključenim virtuelnim mašinama. Isto tako mogu se videti informacije o imenu virtuelne mašine, kao i o opterećenju procesora, zauzeću RAM memorije i o vremenu od kada su uključene. procesu rada i o isključenim virtuelnim mašinama. Isto tako mogu se videti informacije o imenu virtuelne mašine, kao i o opterećenju procesora, zauzeću RAM memorije i o vremenu od kada su uključene.



Slika 35. Virtuelne mašine i Server Manager

Prethodni opis je prikazan na slici, Slika35, gde se vidi i osumnjičena virtuelna mašina sa leve strane slike. Ostale dve virtuelne mašine na prvi pogled ne rade ni jednu ne zakonitu radnju, ali moraju biti ispitane jer postoji sumnja pošto se nalaze u mreži sa osumnjičenom virtuelnom mašinom, ali za sada samo kao pretpostavka.



Slika 36. Snimanje mrežnog saobraćaja na virtuelnim mašinama

Sa Slike 36, mogu se videti informacije o opterećenosti mrežnog adaptera na virtuelnoj mašini kako vizuelno tako i u obliku cifara. Vidi se da virtuelna mašina koristi lokalni mrežni adapter i da je priključena na mrežu. Prozoru se pristupa desnim klikom miša na *Tool* bar pa na opciju *Start Task Manager*. U ovom wizardu postoji mogućnost uvida koje su aplikacije trenutno pokrenute na virtuelnoj mašini, koji su procesi instalirani i koliko opterećuju procesor, opterećenje procesora i RAM memorije, opterećenje na mrežnom adapteru i informacije o

korisnicima koji koriste sistem. Ovo može biti bitno za digitalnog forenzičara, kako u klasičnom pristupu fizičkoj mašini, tako i pristupu virtualnoj mašini.

Mogućnost forenzičkih alata omogućava i pristup memoriji, a kada je u pitanju pristup virtualnoj mašini, digitalni forenzičar će pristupiti onom delu RAM memorije na *host-u* koliko je određeno prilikom kreiranja virtualne mašine.



Slika 37. Prikaz pristupa RAM memoriji korišćenjem forenzičkog alata X-Ways Forensic

Kao što Slika 37 prikazuje, kada digitalni forenzičar pristupi virtuelnoj mašini uz pomoć forenzičkog alata, postoji mogućnost pristupa RAM memoriji ali samo pod uslovom ako virtuelna mašina nije isključivana jer se onda sadržaj RAM-a briše i kreira novi sadržaj koji opisuje one aplikacije koje su pokrenute ili pokretane od uključivanja virtuelne mašine. A kako slika pokazuje, može se videti da su pokretani fajlovi sa ekstenzijom .jpg, što je ekstenzija za slike, kao i u koje je vreme pokretano što je pokazano žutom strelicom i datum koji je pokazan zelenom strelicom. Sama lokacija fajla .jpg uokvirena je crvenim pravougaonikom. Isto tako u dnu slike može se videti da je osumnjičeni pristupao određenoj Web stranici, a informacija o tome je uokvirena braon pravougaonikom, ali i informacija za vreme i datum kada je pristupano. Sa desne strane slike braon pravougaonikom je uokvirena informacija o folderu kojem se pristupalo sa forenzičkim alatom, kao i veličina particije na kojoj se folder nalazi.

Sve ove informacije digitalni forenzičar može da iskoristi za kreiranje slučaja o incidentu koji se dogodio i nad kojim se istraga sprovodi. Ostalo je još reći da se svi dokazi moraju označavati unapred definisanim oznakama kao bi se znalo o kojim dokazima se radi i kako ne bi došlo do zamene, gubitka ili iznošenja pogrešnog dokaza pred sudske organe.

Svaki digitalni dokaz kojeg prikupi digitalni forenzičar ili neki tim digitalnih forenzičara mora biti **relevantan** - da pokaže koliku štetnost nanosi; **autentičan** - da ima razumnu verodostojnost o incidentu za koji se vezuje; **posrednost** - da je dokaz moguće dokazati, kao i u razmatranju ići na naučnu ali i na tehničku stranu; **prihvatljiv na sudu** - svi dokazi koji se prikupe tokom istrage moraju biti potkrepljeni čvrstim dokazima vezanim za incident za koji se vezuju i obavezno je dobro se pripremiti sa uvodnom reči pred porotom. Dokaze treba predložiti tužiocu ili menadžeru u zavisnosti da li se vrši istraga za javnu bezbednost ili korporaciju, ali i postoji mogućnost zastupanja tužene strane u ulozi branioca. Obraćanje mora biti na edukacionom, ali i na razumnom nivou izneseno pred porotu da bi razumela kompleksnost incidenta i ne koristiti previše stručnih termina da ne bi bili ne prihvaćeni, tačnije ne shvaćeni od strane porote i suda. Ali isto tako treba voditi računa da ne budete previše nonšalantni i blagi jer sa druge strane može sedeti visoko edukovana osoba koja želi da opovrgne te digitalne i fizičke dokaze. Ovaj deo pripreme za iznošenje prikupljenih dokaza sa mesta na kome se dogodio incident je isti i kod mašina fizičkih ali i virtuelnih.

Digitalni forenzičar mora postati deo svakog administratorskog tima ili kao deo istražnih organa, u zavisnosti da li se radi o kompaniji ili organima vlasti tj. javne bezbednosti. Mora postojati pozitivna nota za prihvatanje stručnjaka iz oblasti digitalne forenzike u javnoj bezbednosti kao i u korporacijskoj, jer Cloud sistemi su novina ali i napreduju velikom brzinom što otvara pozitivne ali i negativne mogućnosti svetske populacije koja ih koristi.

2.27. Uticaj anti forenzičkih aktivnosti u virtuelnom hyper-V okruženju na digitalnu forenzičku istragu

U ovoj studiji slučaja obrađuje se pristup digitalnog forenzičara na virtuelnu mašinu u *Cloud Computing* sistemu koji je podržan *hyper-V*, a pokrenut na operativnom sistemu Microsoft Windows 2008. Kada forenzičar treba da pristupi osumnjičenoj virtuelnoj mašini ili celokupnom virtuelnom okruženju kojeg pokreće hipervizor, tada se javlja mogućnost da osumnjičena strana želi da deluje anti forenzički i ukloni sve dokaze koji se mogu upotrebiti protiv njih. Svaka operacija koja je protiv prava i ustava zemlje, regiona ili oblasti u kojoj se operacija izvrši, smatraće se potencijalnim izvršenjem krivičnog dela po zakonu te zemlje. U digitalnom svetu, i korišćenju Interneta kao Globalnog okruženja postoji veliki broj mogućih izvršenja krivičnih dela ili incidenata, a da pri tome korisnici i nisu ni svesni da ga vrše, ali i mnogi svesno pristupaju tim delima. Postoji mogućnost da korisnik bude obmanut od strane trećeg lica i da bude izložen nekom incidentu, a da pri tom toga nije ni svestan. Dolaskom *Cloud Computinga* i primene virtuelnih računara u korporacijske i komercijalne svrhe, mogućnosti zloupotrebe su dostigle najveće moguće eskaliranje i zahtevaju temeljan, organizovan pristup i veliko zalaganje istražnih organa na svakom slučaju koji je okarakterisan od istih kao sumnjiv. Tada forenzičar mora da primeni sva svoja znanja i veštine kako bi izgradio čvrst i valjan dokaz za sudstvo. Jer ako digitalni forenzičar ne prikupi dokaze koji su merodavni pred sudom i porotom, neće moći nikako da dokaže da se ne zakonito delo dogodilo i biće obmanut od strane osumnjičenog lica. Zato svaki digitalni forenzičar mora dobro poznavati celokupno virtuelno okruženje ako se u njemu odvija neka ne zakonita radnja ali i mogućnosti virtuelnog sistema koji olakšavaju skrivanje dokaza. Takve mogućnosti virtuelno okruženje pruža ali i samo virtuelno okruženje je kreirano tako da ih pruži. Vrlo lako u virtuelnom okruženju se mogu sakriti određeni dokazi jer je okruženje napravljeno da se njime lako manipuliše ali ne u svrhu sakrivanja dokaza, već u svrhu lakšeg rada administratora koji takvo okruženje kontroliše.

U modernom društvu javljaju se prepreke oko razumevanja dokaza koji su prikupljeni na mestima gde su se incidenti dogodili od strane sudskih organa. Problemi su edukativne prirode jer se malo ljudi iz sveta forenzike angažuje na stalnom radu u sudu. Ali i u suprotnom smeru kada forenzičar dokazuje nevinost osumnjičenog kao njegov branilac. U oba slučaja, osumnjičeni će ako je i malo edukovan o okruženju koje koristi, primeniti delovanje određenih anti forenzičkih alata ili iskoristiti sve mogućnosti manipulacije virtuelnih mašina kako bi određene dokaze koji ga terete, uklonio. Anti forenzički alati mogu se besplatno preuzeti sa Interneta ali oni koji se predstavljaju kao najbolji od svih alata koji uklanjaju digitalne dokaze, kao što je *Evidence Eliminator*, potrebno je platiti kako bi se preuzela celokupna verzija. Kod alata *Evidence Eliminator-a* postoje verzije od dva proizvođača, razlikuju se ali rade istu stvar, a to je uklanjanje dokaza. Zato forenzičke aktivnosti moraju da se progresivno šire, kako bi zahtevale svakodnevni rad i usavršavanje u praćenju Informacionih komunikacionih tehnologija. Zbog toga, digitalni forenzičar i celokupna istraga morale bi biti ispred potencijalnih osumnjičenih lica. Ako se taj korak u svakodnevnoj trci izgubi, digitalni forenzičar vrlo lako može biti obmanut, a osumnjičeni može da nastaviti da radi ne zakonita dela i nanositi štetu pojedincu ali i društvu u globalu.

2.28. Migracije unutar *hyper-V* okruženja

Jedno od mogućih delovanja na uklanjanje dokaza u virtuelnom *hyper-V* okruženju na kome je kao *host* instaliran operativni sistem Microsoft Windows 2008, može biti i operacija koju podržava malopre pomenuti operativni sistem a to je premeštanje iliti migracija virtuelnih mašina. Ova operacija je donela velike povoljnosti za rad administratora virtuelnog sistema jer mu daje mogućnost da sa nekoliko operacija premesti lokaciju VHD-virtuelnog hard disc-a kojem je ekstenzija .vhd i slike stanja ili AVHD kojem je ekstenzija .avhd. Naravno ta operacija je pojednostavljena za administratora virtuelnog sistema ali za osobu koja se može baviti ne zakonitim radnjama daje veliku mogućnost delovanja da prikrije dokaze o svom ne zakonitom delovanju. Ovo mora da zainteresuje svakog digitalnog forenzičara jer ovo nije alat koji omogućava anti forenzičke aktivnosti, nego je sastavni deo *hyper-V* okruženja koji je instaliran na operativnom sistemu Microsoft Windows 2008.

Može se uzeti kao problem kod pristupa istrazi osumnjičenog servera premeštanje lokacije virtuelne mašine u okviru samog servera kao *host-a*, ali i premeštanju jedne ili više virtuelnih mašina na drugi fizički ili virtuelni *host*. Ovo može dodatno otežati istragu ako *host* ima ulogu klastera, tačnije dva servera rade iste operacije i ako postoji problem kod jednog *host-a* i desi se da prestane sa radom, sav saobraćaj kao i izvršenje svih operacija premestiće se na drugi *host*.

2.29. Mogućnosti i ograničenja virtuelne mašinske migracije

Pre nego što se pokrene migracija ili uvoz/izvoz virtuelnih mašina moraju se poštovati određena pravila.

Prvo i osnovno pravilo je da virtuelna mašina mora biti stopirana u radu, tačnije da je off ili isključena, jer virtuelna mašina koja je u procesu rada ili *running* ili *pause* koja je pauzirana mora biti prethodno isključena jer se sa njom ne može vršiti migracija. Microsoft kompanija radi na dodatku ili zakrpi koja će omogućiti da se migracija vrši u toku rada virtuelnih mašina i bez prekida ali to je u procesu razvoja. Virtuelna okruženja kao što su *Xen* ili *Vmware* omogućavaju migraciju virtuelnih mašina u toku rada.

Drugo pravilo, skup kompresovanih fajlova kada se izvozi neka virtuelna mašina može se kopirati, uvesti i smestiti samo jednom na *hyper-V host*. Razlog ove tvrdnje je da će importovane virtuelne mašine biti sačuvane na *host-u* i pokrenute sa lokacije sa koje su izvezene. Ključna prednost ove konstatacije jeste da izvozni proces može potrajati puno vremena i time naneti nestabilan rad virtuelnog okruženja kao i preopterećenje *host-a*, a dok uvozna operacija u migraciji protiče veoma brzo i završava se u jednoj sekundi. Ako međutim izvezena virtuelna mašina bude uvezena u više *hyper-V* okruženja koje podržavaju više *host-ova*, odvojene kopije izvezenih foldera i fajlova će morati da se koriste za svaki uvoz pojedinačno na svaki *host*, što može izazvati gubljenje vremena kao i pravljenje greške ako prethodno arhitektonsko rešenje virtuelnog okruženja nije dovoljno dobro urađeno. Zato se mora voditi računa o organizaciji lokacija kao i smeštanje virtuelnih mašina na *host* ali i o numeraciji virtuelnih mašina.

Treće pravilo govori da je moguće napraviti jednu virtuelnu mašinu koja će biti osnov za pravljenje klonova takve virtuelne mašine što bi omogućilo korisnicima da sami mogu da kreiraju virtuelnu mašinu kakvu žele. Tačnije podesi se hardverska konfiguracija i instalira operativni sistem i takva virtuelna mašina se potom klonira u određeni broj kopija koji nam je potreban. Zato drugo pravilo govori da ako se napravi više kopija virtuelnih mašina mogu se staviti na *host* i to izgleda da se virtuelna mašina stavlja načelno više puta a ne samo jednom, ali

pošto će te virtualne mašine koristiti različiti korisnici ili čak isti moraju postojati i različiti folderi tih kopija virtualnih mašina jer promene se dešavaju na njima i ne postoji mogućnost sinhronizacije tih promena ali i sami korisnici ne bi želeli da im neko drugi menja podatke na virtualnom *hard disc-u* kao i na setovanju same virtualne mašine. Zato drugo pravilo i govori da mora postojati za svaku virtualnu mašinu i njegova kopija foldera za migraciju koja se uvozi na *host*.

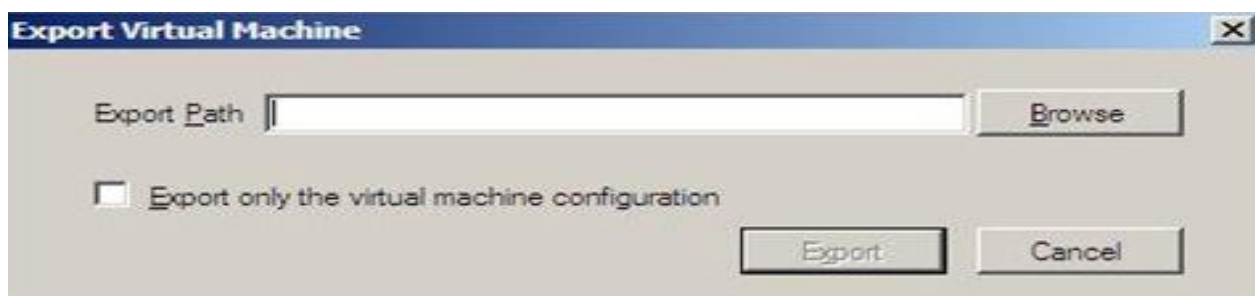
Ovo su bitne informacije za digitalnog forenzičara koji vrši istragu na osumnjičenom serveru tj. *host-u*. Mora se voditi računa o lokacijama foldera gde su smešteni konfiguracioni fajlovi virtualnih mašina, ali i gde su smešteni fajlovi virtualnih *hard disc-ova* i ako postoje slike stanja virtualnih mašina i ti fajlovi mogu biti od velikog značaja digitalnom forenzičaru, a ti fajlovi su .avhd.

Pošto je kroz ova tri pravila ograničen rad migracije u *hyper-V* okruženju na *host-u* na kome je instaliran operativni sistem *Microsoft Windows 2008*, mora se napomenuti i snaga kao i moguće operacije koje čine ovu vrstu migracije u *hyper-V* okruženju veoma bitnom u svetu *Cloud Computing-a*. Mogućnosti su velike ali bitno je napomenuti da virtualne mašine mogu da migriraju sa bilo kog *host-a hyper-V* okruženja na bilo koji drugi *host* u *hyper-V* okruženju. Postoji mogućnost migracija virtualnih mašina i sa *VirtualPC-a* kao i sa *Vmware-a* na *hyper-V* okruženje u instalaciju određene podrške. Bitno je napomenuti da kada virtualna mašina migrira, da mogu biti prenete informacije o konfiguraciji samo koje mogu biti korišćene za dupliranje ili pravljenje većeg broja kopija virtualnih mašina. Kada se radi operacija izvoza virtualne mašine tada će biti prenete sve informacije pa čak i slike stanja te virtualne mašine ako su postojale. Sada je jasno da proces migracije može uticati na obmanjivanje digitalnog forenzičara u procesu istrage osumnjičenog *host-a* ako prethodno nije napravio određene radnje praćenja celokupnog virtualnog okruženja.

2.30. Izvoz virtualne mašine u *hyper-V* okruženju

Kada se pristupi operaciji izvoza virtualne mašine koja treba da se premesti na drugu lokaciju moraju se ispoštovati koraci procesa operacije, radi uspešnosti obavljanje izvoza virtualne mašine. Prvo treba pokrenuti *Hyper-V Manager* konzolu, a koja se pokreće pritiskom na *Start meni*, potom *Administration Tools* pa *Hyper-V Manager*. Veoma je bitno da se proverí da li je virtualna mašina koja je izabrana za migraciju, u *Off-isključenom* stanju ili je u stanju *Save-sačuvanom* jer se tada može izvršiti migracija. Stanje virtualne mašine se može videti u okviru konzole ili ako je potrebno promeniti stanje, može se desnim klikom miša na određenu virtualnu mašinu izvršiti promena stanja. Ove informacije su bitne za digitalnog forenzičara jer time kontroliše virtualnu mašinu i pristupa istoj u stanju u kome želi da obavi istragu, a može je obaviti u uključenom ili *Run* stanju ili slici određenog stanja, kao i u isključenom stanju.

Kada se virtualna mašina pripremi za operaciju izvoza a u isključenom je ili sačuvanom stanju, onda treba pozvati vizard za izvoz virtualne mašine koji je predstavljen na sledećoj slici:



Slika38. Vizard za izvoz virtuelne mašine

Kada se pojavi ovaj vizard, kao što je prikazan na slici, Slika38, potrebno je izabrati lokaciju preko dugmeta *Browse* gde treba smestiti fajlove za izvoz. Moguće je i uneti direktnu lokaciju. Izborom pritiska na dugme *Browse* sigurnost u biranju tačne lokacije je veća. Postoji mogućnost da se izostavi određen karakter i da se izvoz virtuelne mašine obavi na lokaciju koja je neželjena, ako se vrši unos lokacije. Što se tiče izvozne lokacije, ona može biti bilo koja lokacija na kojoj je sistem *host-a*, kao što može biti sistemska lokacija na *hard disc-u*, ali i lokacije na ostalim particijama *host-a*, kao i prenosni *hard disc-ovi* koji su u *hyper-V* okruženju. Isto tako mogu biti i virtuelni *hard disc-ovi* ako ih *host* koristi. Jedini bitan razlog za brigu administratora koji izvozi virtuelnu mašinu je da na novoj lokaciji ima dovoljno prostora da se smeste konfiguracioni fajlovi virtuelne mašine kao i VHD i AVHD. Postoji opcija koja je prikazana na slici, Slika38, da se čekira izvoz samo konfiguracionog fajla virtuelne mašine. Tada će na mesto na koje je odabrano da se izvoz izvrši biti kreiran pod folder sa imenom virtuelne mašine koji će u sebi imati informacije o izvezenoj virtuelnoj mašini. Sada, može se pritiskom na dugme *Export* izvršiti operacija izvoza virtuelne mašine. Nakon pritiska na dugme *Export* pojaviće se informacija za koliko vremena će se izvoz virtuelne mašine obaviti. Ovaj vremenski period može zavistiti od faktora koji utiču na operativni sistem *host-a*. Faktori su zavisnost da li su na *host-u* postoje aktivne virtuelne mašine, kao i koliko ima raspoložive RAM memorije koje koristi sam *host*. Bitno je, da li su na *host-u* pokrenute neke operacije a opterećenje procesora tada može biti veliko, pa ovi faktori utiču na brzinu obavljanja operacije izvoza virtuelne mašine. Jedan od najbitnijih faktora, koji utiču na vremenski period završetka procesa je i veličina VHD fajlova kao i njihov broj. Virtuelna mašina može da ima jedan ili više virtuelnih *hard disc-ova*. Isto tako je i bitan broj snimaka stanja, jer ako je veliki broj snimaka stanja, vreme izvršenja operacije će biti srazmerno veće. Ove informacije mogu bitno da utiču na pred istražni rad i prikupljanje informacija kod digitalnog forenzičara kako bi znao kada i u koliko brzoj meri da reaguje na mesto gde se obavlja neka ne zakonita radnja. Naj bitnije je digitalni forenzičar istragu izvrši na *host-u* koji je u stanju rada i da prikupi sve informacije o slikama stanja virtuelne mašine koja je osumnjičena. Kada digitalni forenzičar pokrene virtuelnu mašinu iz neke određene slike stanja, može da izvrši živu istragu na toj mašini, što mu obezbeđuje veliki broj informacija.

2.31. Anatomija izvoza virtuelnih mašina u *hyper-V*

Kada se završi operacija izvoza određene virtuelne mašine, tada se kreiraju određeni fajlovi i folderi na izabranoj lokaciji koja je u prethodnom poglavlju objašnjena.

- *config.xml* – je fajl koji se kreira po završetku operacije izvoza virtuelne mašine i on je konfiguracioni fajl koji u sebi nosi informacije o konfiguraciji virtuelne mašine kao i o lokacijama VHD-a i AVHD-a. Ako je izabrana opcija kao na slici, Slika1, da se izveze samo konfiguracioni fajl onda će *config.xml* biti jedini kreiran fajl u folderu. Kada se izvrši otvaranje *config.xml* vide se sledeće informacije.

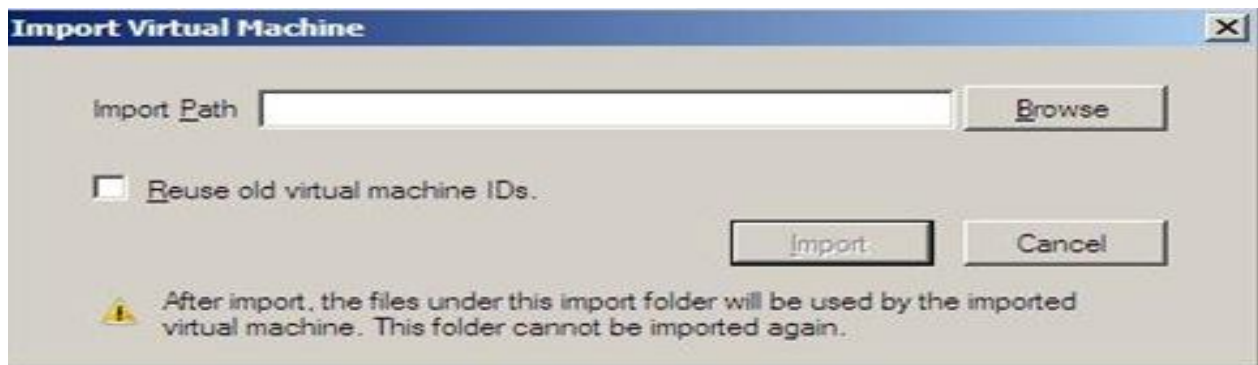
```
<?xml version="1.0" encoding="UTF-16" standalone="yes" ?>
- <configuration>
  <SnapshotDataRoot type="string" />
  <ExternalDataRoot type="string" />
- <vhd>
  <source type="string">C:\Users\Public\Documents\Hyper-V\Virtual hard disks\User Data Hard Disk.vhd</source>
  <target type="string" />
</vhd>
- <vhd>
  <source type="string">C:\Users\Public\Documents\Hyper-V\Virtual hard disks\WinServer2008 Test.vhd</source>
  <target type="string" />
</vhd>
  <VmStateCopied type="bool">true</VmStateCopied>
</configuration>
```

Slika39. Konfiguracioni fajl *config.xml*

Vidi se lokacija VHD fajla na slici, Slika39, što je veoma bitna informacija da se zna lokacija fajla .vhd. Ovaj fajl može biti kopiran od strane digitalnog forenzičara i pri tom pokrenut na radnoj stanici kod digitalnog forenzičara i potom biti ispitan celokupan virtuelni *hard disc*.

- *Virtual Machines* – je folder koji u sebi nosi informacije o konfiguraciji virtuelne mašine koja je izvezena ali u binarnom formatu, kao i o GUID- u i fajlu sa ekstenzijom .exp. Kada se izvrši operacija uvoza u ciljni *host*, ovaj fajl prelazi u ekstenziju .xml. Ove informacije ostavljaju trag koji je bitan za digitalnog forenzičara jer su u binarnom obliku koji je prihvatljiv kao dokaz pred sudom.
- *Virtual Hard Drives* – je folder koji u sebi nosi informacije o svim VHD-ovima kao i o slikama stanja virtuelne mašine koja je izvezena.
- *Snapshot* – ovaj folder sadrži informacije o slikama stanja i promenama na VHD-u.

2.32. Uvoz virtuelnih mašina u *hyper-V* okruženje



Slika40. Vizard za uvoz virtuelne mašine

Kada se završi uspešno izvoz virtuelne mašine na izabranu lokaciju i kada se izvrši provera fajlova i foldera koji su izvezeni, treba pristupiti uvozu virtuelne mašine na željeni *host*. Preko *Start* menija pa *Administrative Tools* izabrati *Hyper-V Manager* i opcija *Import Virtuel Machines* dobiće se vizard kao na slici, Slika40. Kao što se može videti sa slike, mora se dati putanja do lokacije na kojoj se nalaze folderi i fajlovi izvezene virtuelne mašine ili jednostavnim klikom na dugme *Browse* izvršiti izbor lokacije. Kada se izvrši izbor lokacije potrebno je pročitati upozorenje koje govori da ista lokacija i folderi na njoj se ne mogu uvesti ponovo posle ove operacije. Pritiskom na dugme *Import*, obaviće se operacija uvoza koja će trajati u vremenskom periodu oko jedne sekunde i posle toga virtuelna mašina je sprema za rad na novom *host-u*.

Snaga migracije omogućava veoma fleksibilan rad administratora virtuelnog sistema jer u određenom vremenskom periodu može da menja lokacije virtuelnih mašina. Ovo otvara nove mogućnosti anti forenzičkog delovanja na virtuelno okruženje ako se koristi u ne zakonite svrhe, ali i virtuelne mašine kao pojedinaca ako se samostalno koristi ili čak izvrši moguće zombiranje od strane trećeg lica. Digitalni forenzičar mora da ima saznanja o arhitekturi virtuelnog okruženja jer postoje mogućnosti da se klasteri nalaze kao fizički ali i kao virtuelni *host-ovi*, kao i da se proveriti ako su fizički na kojim lokacijama se nalaze. U opciji podešavanja DNS servisa na serveru može se videti ime *host-a* i potom u *Server Manager* konzoli u opcijama se može videti da li je podešen *host* koji je osumnjičen kao *klaster*. Ove informacije odmah otvaraju sumnju da postoji još jedan *host* koji može nositi određene informacije kao i *host* kome je digitalni forenzičar prvobitno pristupio. Tako da se istraga treba sprovesti i na drugi *host*.

2.33. Živa migracija u *hyper-V* okruženju

Kako je u prethodnom poglavlju objašnjena migracija u *hyper-V* okruženju gde su morala da se ispoštuju određena pravila. Morala je biti isključena virtuelna mašina ili u stanju sačuvana, a tek potom je trebalo vršiti izvoz. Izvoz virtuelne mašine je imao određeni vremenski period koji je bio varirajući u zavisnosti od faktora, a tek posle toga je mogla biti izvršena operacija uvoza virtuelne mašine. Ovo je ne prihvatljivo za korporacije koje daju klijentima korišćenje virtuelnih mašina a naročito onih virtuelnih mašina kojima je funkcija, celodnevni rad. Ako bi došlo do prestanka rada *host-a*, to bi moglo izazvati jednom rečju haos, u korporaciji ali i među

klijentima. Zato postoji i živa migracija koju omogućava operativni sistem *Microsoft Windows 2008* u kome je pokrenuto *hyper-V* okruženje. Živa migracija virtuelnih mašina koje su smeštene na *hard disc* jednog *host-a* mogu se prebaciti bez isključivanja ili snimanja stanja na drugi *host*, što je omogućio prethodno pomenuti operativni sistem iz lepeze *Microsoft* proizvoda.

2.34. Konfiguracioni zahtevi za živu migraciju u *hyper-V* okruženju

Pre nego što određenu virtuelnu mašinu koja je u stanju *running*, premestite sa jednog *host-a* na drugi, potrebno je da se ispune određeni zahtevi, kao što su:

- Prvo mora da se operativni sistem, kao i *hyper-V* okruženje instaliraju i pokrenu na oba *host-a*. Prva verzija operativnog sistema *Microsoft Windows 2008* nema ovu mogućnost, tek kasnije verzije su dobili mogućnost za živu migraciju
- Izvori i odredišta *hyper-V host-a* moraju biti konfigurisani kao *Failover Cluster* sa deljenim i omogućenim za korišćenje *hard disc-ovima*
- Izvor i odredište moraju da koriste deljenu lokaciju na *hard disc-u* koji moraju biti iSCSI ili viaSAN i tako biti konfigurisani
- Oba *host-a* moraju imati isti procesor koji ih pokreće jer nije moguće da na jednom *host-u* bude *Intel procesor* a na drugom *host-u* bude AMD
- Virtuelna mašina na kojoj se vrši živa migracija mora stalno biti dostupna i mora biti podešena kao *Cluster Shared Volumes*
- *Automatic Start Action* opcija na virtuelnoj mašini na kojoj se vrši živa migracija mora biti setovana na *Nothing*
- Svi *hyper-V host-ovi* koji su podešeni u *Failover cluster*, moraju biti podešeni da imaju isto ime particije sa koje se pokreću virtuelne mašine na kojima se vrši živa migracija. Tačnije, ne može se na jednom *host-u* pokrenuti živa migracija na virtuelnoj mašini sa C particije, a da se ista vrši na drugom *host-u* na D particiji, naprimer.

2.35. Proces žive migracije

Kao i svaki proces, tako i proces žive migracije mora da prođe kroz određene poslove kako bi bio uspešno izvršavan. A ti procesi su:

- *Configuration transfer* – prenos konfiguracionih fajlova virtuelnih mašina sa izvora na odredište na *host-u*
- *Destination VM creation* – na osnovu informacija iz konfiguracionog fajla stvara na odredišnom *host-u* uslove hardverskog tipa i najbitnije je da obezbeđuje dovoljno RAM memorije za rad virtuelne mašine
- *Transfer of memory pages* – ove informacije se prenose sa *host-a* izvora na *host* odredišta memorije virtuelne mašine. Tokom rada virtuelne mašine sve informacije koje su u memoriji beleže se u ovom fajlu koji je prvobitno na *host* izvoru a potom se prebacuju na *host* odredište. Takve promenjene informacije o memoriji virtuelne mašine se beleže na *host* odredište
- *Transfer of state* – beleži se stanje na *host* izvoru a potom se takvo zabeleženo stanje šalje *host* odredištu
- *Transfer of storage* – prenosi informacije o VHD na *host* izvoru i takve informacije prenosi na deljeni prostor koji mora imati isto ime particije na *host-u* odredišta, kako bi virtuelna mašina mogla da radi neometano

- *VM brought online* – ovo je informacija koja je migriranu virtuelnu mašinu sa *host* izvora dovela na *host* odredišta
- *Network Re-direction* – mrežno usmerenje ili tačnije preusmeravanje treba biti takvo da se i *host* odredište konfiguriše kao i *host* izvor jer virtuelna mašina mora neometano da radi

Kao što se može videti, omogućeno je funkcionisanje virtuelne mašine da stalno i neometano radi i funkcioniše čak i ako jedan *host* prestane sa radom. Sve potrebne informacije o konfiguraciji i podešavanju virtuelne mašine ima drugi *host*. Virtuelno okruženje koje je arhitektuirano u radu žive migracije virtuelnih mašina ili čak servera može biti korisno i postojano. Ali isto tako, ovakve informacije mogu imati težinu u dokazivanjima digitalnog forenzičara pred sudom, ako je virtuelno okruženje u kojem je urađena neka ne zakonita radnja, jer na oba *host-a* postoje iste informacije o virtuelnim mašinama. Ako ipak neko pribegne anti forenzičkim radnjama u ovakvom virtuelnom okruženju, ostaviće za sobom veliki broj tragova i dokaza koji mogu biti upotrebljeni u istrazi, ali i posle toga pred sudom.

2.36. Konfigurisanje virtuelne mašine kako bi bila stalno dostupna

Kako bi bilo ispoštovano da virtuelna mašina bude stalno dostupna što je jedan od preduslova za izvršenje operacije žive migracije mora se pristupiti *Failover Cluster Manager-u*. Do *Failover Cluster Manager-a* se dolazi preko *Start* menija, pa *Administrative Tools*, pa *Failover Cluster Manager*. Kada se pristupi konzoli *Failover Cluster Manager* potrebno je pritisnuti *Services and Applications* opciju pa potom izabrati *Configure a Service or Application* opciju koja je unutar *Action pane*. Posle ovih odabira potrebno je pratiti vizard i izvršiti izbor konfigurisanja da je mašina stalno dostupna iliti *highly available*. Kada se vizard završi i dođete do dugmeta *Finish* potrebno je proveriti spisak svih podešenih opcija koje ste izabrali prilikom konfiguracionog vizarda i tek onda pritisnete dugme *Finish*.

Poglavlje vezano za stalnu dostupnost nema neke određene anti forenzičke radnje kao ni informacije za digitalnog forenzičara koje mu direktno govore o nekom ne zakonitom delu. Ali mora se znati da je virtuelna mašina korišćena na klasteru, tj. na dva *host-a* kako bi se istraga proširila na oba *host-a*.

2.37. Podešavanje virtuelne mašine za automatski start

Prvo treba pristupiti *Hyper-V Manager* konzoli i izabrati virtuelnu mašinu nad kojom će se sprovoditi operacija žive migracije i potom izabrati opcija *Setings link* u okviru *Action pane*. U levom prozoru pojaviće se opcija *Automatic Start Action* i potom će imati pod odeljak u kome će biti pitanje:

What do you want this virtual machine to do when the physical computer starts?

Pitanje glasi: Šta želite da uradi virtuelna mašina kada se fizički kompjuter pokrene tj. startuje. Logično, pošto ne treba ništa da radi jer je između dva *host-a* i mora da prati sva prethodna podešavanja koja su navedena u prethodnim poglavljima odgovor je da, ne želimo da se automatski startuje tj. ništa. A na to pitanje se odgovara sa *Nothing*. I pritiskom na *Apply* dugme završava se podešavanje.

2.38. Izvođenje žive migracije pomoću *Failover Cluster Manager*

Prethodni zahtevi za živu migraciju koji su navedeni u prethodnim poglavljima moraju biti ispoštovani. Tek posle toga može se pokrenuti živa migracija iz menija *Failover Cluster Manager* ili iz konzole *Windows PowerShell*. *Failover Cluster Manager* može se izabrati virtuelna mašina nad kojom se sprovodi operacija žive migracije. Desnim tasterom na virtuelnu mašinu i potom se bira opcija *Live migrate virtual machine to another node* – što znači da se virtuelna mašina prebacuje na drugi čvor što u prevodu znači klaster.

2.39. Izvođenje žive migracije pomoću programa *Windows PowerShell*

Može se koristiti skripta koja se programira iz komandne linije ako određeni administratori tako žele da pokreću živu migraciju. To se radi na sledeći način jer je potrebno otvoriti *PowerShell* prozor, preko *Start* menija, pa *All Programs*, pa *Accessories*, pa *Windows Powershell*. U okvir ovog prozora instalira se *Failover Clustering* funkcija na sledeći način, kuca se naredba:

Import-Module FailoverClusters

a potom se unosi naredba za izvršavanje operacije žive migracije koja glasi:

***Get-Cluster "<cluster>" | Move-ClusterVirtualMachineRole
-Name "<vm group>" Node "<destination node>"***

Gde će se u polja koja su pod uglastim zagradama unositi određene informacije koje su date u sledećem nabrajanju:

- *<cluster>* - sadrži ime klastera koji sadrži virtuelne mašine koje treba da budu premeštene
- *<vm group>* - predstavlja grupu virtuelne mašine, a ta grupa sadrži određene virtuelne mašine
- *<destination node>* - predstavlja ime *host* odredišta ili čvora. Može se još nazvati *host* sa *Failover cluster* na koga treba da se preseli virtuelna mašina

Zanimljivo je da preko konzole *Windows Powershell*, mogu se vrlo lako vršiti manipulacije virtuelnih mašina što može izazvati prikrivanje tragova osumnjičene virtuelne mašine ili celog *host-a* i biti deo anti forenzičkog delovanja. Ali može ponuditi i informacije koje mogu biti od koristi digitalnom forenzičaru ako pristupi *Windows Powershell* konzoli, jer u njemu može dobiti ime čvora na kome će biti ili je smeštena osumnjičena virtuelna mašina.

Sve prethodne informacije mogu uticati na anti forenzičke radnje ponekad direktno a nekada i indirektno u zavisnosti od situacije u kojoj se osumnjičene virtuelne mašine nalaze. Raspolaganjem ovih informacija, kao i poznavanjem podešavanja i korišćenje virtuelne migracije virtuelnih mašina u *hyper-V* okruženju pojednostavljuje se borba digitalnog forenzičara u virtuelnom okruženju koje postaje svakodnevnica u svetskoj populaciji.

2.40. Kreiranje i upravljanje slikama stanja virtuelnih mašina u *hyper-V* okruženju

Izraz slike stanja će biti korišćen u daljem tekstu, ili kako im je ime *snapshots*, virtuelnih mašina su sačuvana stanja određene virtuelne mašine koja je od nekog trenutka izvršavala određene funkcije i potom sve te funkcije bivaju zabeležene i sačuvane u određenom fajlu koji se kreira po izvršenju slikanja tog određenog stanja. Postavlja se pitanje zašto su bitne slike stanja, tačnije, fajlovi u kojima su zabeležena stanja. Odgovor će biti dat na kraju poglavlja, jer je veoma bitno znati koji su fajlovi u pitanju, kakve informacije nose, kada se prave slike stanja i šta sve u sebi nose.

2.41. Slika stanja u *hyper-V* okruženju

Slika stanja na virtualnoj mašini u *hyper-V* okruženju koje je pokrenuto na operativnom sistemu *Microsoft Windows 2008*, je slikano okruženje celog operativnog sistema *child-a* koji je pokrenut na *host-u*. Čuva se celokupno podešavanje operativnog sistema *child-a*, kao i hardversko podešavanje. Slika može biti pokrenuta kasnije u budućnosti i pri tom se može vratiti neko stanje iz prošlosti kao i celokupno okruženje koje je bilo zabeleženo u datom trenutku. Ali pošto je stanje reč za trenutno, a slike stanja mogu se praviti ne samo jednom nego ih može imati više, pa tako se slika stanja određene virtualne mašine ne odnosi samo na jedan trenutak kada je slika okinula već i na celokupni vremenski period od prethodnog okidanja slike pa do sledećeg. Ovde se mogu naći veoma bitna informacije za digitalnog forenzičara ali i sa slikama stanja se može manipulirati i mogu se brisati ako se deluje anti forenzički u cilju uklanjanja dokaza o ne zakonitim radnjama. Bitno je da se slike stanja mogu uzimati ako je virtualna mašina u stanju rada, stanju čuvanja ili isključenom stanju, ali se ne mogu uzimati ako je virtualna mašina u pauziranom stanju. Bitno je napomenuti i da se čuvaju informacije o pokrenutim aplikacijama pa čak i aplikacije će ostati u onom statusu izvršenja kada je napravljena slika stanja, ali i o virtualnoj RAM memoriji. Kada posle određenog vremena pokrenemo sliku stanja, imaćemo utisak kao da smo vratili vreme. Informacije iz RAM memorije nose veliki broj dokaza pa tako ako se izvrši pokretanje određene slike stanja onda će i informacije biti dostupne digitalnom forenzičaru kao dokazni materijal, ali isto tako i otvoriti mogućnost uklanjanja dokaza iz RAM-a ako se radi o anti forenzičkom delovanju.

2.42. Uzimanje slike stanja virtualnim mašinama

Što se tiče uzimanja slike stanja na određenoj virtualnoj mašini, može se uraditi na jednostavan način tako što se izabere *Hyper-V Manager* konzola. Izborom *Start* menia, pa potom *Administrative Tools*, da bi se došlo do *Hyper-V Manager* konzole, pojaviće se instalirane virtualne mašine i imaće informacije koje su u procesu rada ili su isključene. Kao što je prethodno bilo napomenuto, bitno je da virtualna mašina ne može biti u stanju pauziranom da bi se uzela slika stanja, ali u svim ostalim stanjima može biti, kao što su stanje rada, stanje čuvanja i stanje isključene virtualne mašine. Kada se izabere virtualna mašina čije stanje je potrebno slikati, desnim klikom miša na izabranu virtualnu mašinu, potom iz padajućeg menia izabrati opciju *snapshots* i pritiskom na nju dobićemo pitanje da li sigurno želimo da napravimo *snapshot* i izborom dugmeta *Apply*, slika stanja biće izvršena. Pošto je moguće izvršiti više od jednog slikanja stanja virtualne mašine pojaviće se i mogućnost reimenovanja slika stanja ako korisnik želi da ima svoju numeraciju. Ali ako ne želi da pravi svoju numeraciju, osnovna numeracija će imati informacije o imenu virtualne mašine, datumu i vremenu kada je izvršeno okidanje slike. Datum, vreme i ime virtualne mašine mogu imati dokaznu vrednost kada se ispituje osumnjičena virtualna mašina, zato se mora voditi računa da se ovi dokazi uvek uporede sa relevantnim dokazima o osumnjičenoj virtualnoj mašini. Pošto postoji mogućnost da se napravi više slika stanja, ako se tako nešto i uradi, pojaviće se hijerarhijsko drvo svih slika stanja počevši od vrha ka dnu od prvog po vremenu i datumu pa sve do poslednjeg i to sve vezano za samo jednu virtualnu mašinu. Takve informacije daju preglednost jer su vezane za pojedinačne virtualne mašine, a pošto je moguće da ih ima više slika bi bila haotična da ne postoji hijerarhijsko stablo, tako da za svaku virtualnu mašinu može se izvršiti uvid u to koliko ima slika stanja i kada su kreirane.

2.43. Hijerarhijsko drvo snimka stanja za virtuelnu mašinu u *hyper-V* okruženju



Slika41. Hijerarhijsko drvo slika stanja jedne virtuelne mašine

Kao što se može videti sa slike, Slika41, urađene su tri slike stanja virtuelne mašine pod nazivom WinServer test i to u istom danu ali u tri različita vremenska perioda. Svako sledeće stanje biće dodato na hijerarhijsko stablo ispod poslednje slike stanja sa istim imenom jer se radi o istoj virtuelnoj mašini ali sa drugim datumom i vremenom. Stanje Now, kao što se može videti na slici, predstavlja da je virtuelna mašina aktivna trenutno. Ali i da se može ako je to potreba vratiti u prethodno stanje kao što se može videti:



Slika42. Pokretanje virtuelne mašine iz slike stanja

Može se videti sa slike, Slika42, da se pokreće stanje koje je predstavljeno kao poslednje na slici, Slika41. Vidi se tačan datum i vreme kada je slika stanja slikana i da će se posle ovog prozora pojaviti prozor operativnog sistema *Microsoft Windows* gde će korisnik ostaviti svoje korisničko ime i lozinku. Ali slike stanja se mogu praviti i u toku rada operativnog sistema, pa kada se pokrene ta slika stanja korisniku će biti otvoren direktno operativni sistem u onom trenutku kada je slika stanja i urađena.

2.44. Upravljanje slikama stanja

Kada se desnim klikom miša pristupi na odgovarajuću virtuelnu mašinu, dobija se padajući meni sa operacijama kojim može da se deluje na slike stanja na virtuelnoj mašini. Sledeća slika govori o operacijama.

Action	Description
Apply	Applies the snapshot to the virtual machine from which it was taken. The virtual machine will revert to the exact state it was in when the snapshot was taken. Any changes made to the virtual machine since the snapshot was taken will be lost. Hyper-V will provide the option to take a new snapshot of the virtual machine's current state before applying the old snapshot.
Rename	Allows the name assigned to the snapshot to be changed.
Delete Snapshot	Deletes the snapshot and all associated files from the system. This action is irreversible.
Delete Snapshot Subtree	Deletes the currently selected snapshot and all other snapshots which are located beneath it in the tree.
Settings	Allows the settings of the virtual machine at the time of the snapshot to be viewed. Modification of settings is disabled.

Slika43. Operacija nad slikama stanja

Kao što se može videti sa slike, Slika43, mogu se uraditi brojne operacije nad slikom stanja jedne virtuelne mašine. Bitno je to što se mogu izmeniti imena slikama stanja u opciji *Rename*, kao i da se mogu izbrisati, jedna slika stanja ali i celo hijerarhijsko stablo. Ove informacije su bitne za digitalnog forenzičara koji treba da usmeri istragu na detalje i da uoči stanja u kojima se nalazi osumnjičena virtuelna mašina. Ako bi digitalni forenzičar pokretao slike stanja na svojoj forenzičkoj radnoj stanici, od kraja ka početku ili čak ako bi ima pred istražna saznanja, kada se određena ne zakonita radnja desila, mogao bi lako da izvrši pregled virtuelne mašine u tom periodu i da izvlači informacije iz RAM memorije i da napravi kopiju *image-a hard disc-a*. Ali iste informacije daju mogućnost uklanjanja dokaza od strane osumnjičenog pri anti forenzičkom delovanju, pri čemu bi mogao da izbriše slike stanja ako ih je i pravio, ili da ih reimenjuje i tako dovede u zabludu digitalnog forenzičara. Može da im promeni lokaciju ili jednostavno pošto je svaka slika stanja novi fajl koji se kreira, može da izvrši kopiranje fajla na neki prenosivi *hard disc*.

2.45. Anatomija slike stanja u *hyper-V* okruženju

Svaki put kada se desnim klikom miša na virtuelnu mašinu izabere snimanje slike stanja, kreira se novi fajl u određenom folderu. Ako se lokacija ne definiše po želji administratora ili korisnika virtuelne mašine, standardna lokacija će biti:

%SystemRoot%\ProgramData\Microsoft\Windows\Hyper-V\Snapshots

Ova informacija može biti od koristi digitalnom forenzičaru ali samo pod uslovom da osumnjičeni nije menjao lokaciju, što je malo verovatno ali nikada ne treba odustajati od potrage za dokazima kada pristupate istrazi kao digitalni forenzičar. Ovako kreirani fajlovi i folder su po standardu operativnog sistema nevidljivi tj. *Hidden*, ali ako se uključi prikazivanje skrivenih fajlova i foldera postaće vidljivi. Svaki snimak se sastoji od sledećih fajlova:

- **Configuration file** - An XML file containing the current configuration settings of the virtual machine.
- **Saved state file** - A .vsv file containing virtual machine state information.
- **Differencing disk image file** - A .avhd differencing disk.
- **Memory image file** - A .bin file containing an image of the virtual machine's memory at the point the snapshot was taken.

Slika44. Fajlovi od kojih se sastoji slika stanja

Slika44 pokazuje četiri fajla sa ekstenzijama **.xml** – konfiguracioni fajl podešavanja virtuelne mašine, **.vsv** – fajl koji sadrži informacije o stanju virtuelne mašine, **.avhd** – fajl koji se kreira kad i slika stanja i sadrži samo one informacije koje su nanele promenu kako operativnom sistemu pa tako i virtuelnom *hard disc-u*. Početno stanje virtuelne mašine a koje se odnosi na celokupan virtuelne *hard disc* snimljeno je na virtuelni *hard disc*, ali i same promene u slici stanja u trenutku okidanja pa sve do sledećeg okidanja slike stanja biće zabeležene u .avhd. **.bin** – fajl koji nosi informaciju o sadržini virtuelne RAM memorije koja je zabeležena od trenutka okidanja slike stanja.

3. Studije slučajeva

Rad se bavi pristupom digitalnog forenzičara na mestu gde se nalazi *host* i *childo-ovi* koji koriste taj *host* kao domaćina. Na *host-u* je instaliran operativni sistem Microsoft Windows 2008 core2 i naknadno pokrenut posle instalacije *hyper-V* servisa. Na *child-ovima* koji se koriste u slučajevima opita su instalirani operativni sistemi Microsoft Windows 7.

Slučajevi opita treba da prikažu ali i opišu dešavanja digitalne forenzičke istrage u virtuelnom okruženju koje pokreće predhodno spomenuti *host*, ali i da pokaže i anti forenzička delovanja koja mogu uticati na isto virtuelno okruženje.

3.1. Studija slučaja 1: *snapshots*

Snapshots – slike stanja operativnog sistema su postala sastavni deo ponude virtuelne mašine koja se koristi u Cloud sistemu. Mogu imati široku primenu u korišćenju, od čuvanja promena koje su nastale na operativnom sistemu u nekom vremenskom intervalu preko mogućnosti ako se određena aplikacija instalira i kao rezultat promeni rad operativnog sistema ali i cele virtuelne mašine na gore, da olakša administratoru Cloud sistema da vrati virtuelnu mašinu u predhodno stanje i time omogući korisniku normalan rad na virtuelnoj mašini. Ali slike stanja mogu imati i ulogu u zoupotrebama od strane korisnika koji žele da nanesu štetu korisniku ili društvu u celini.

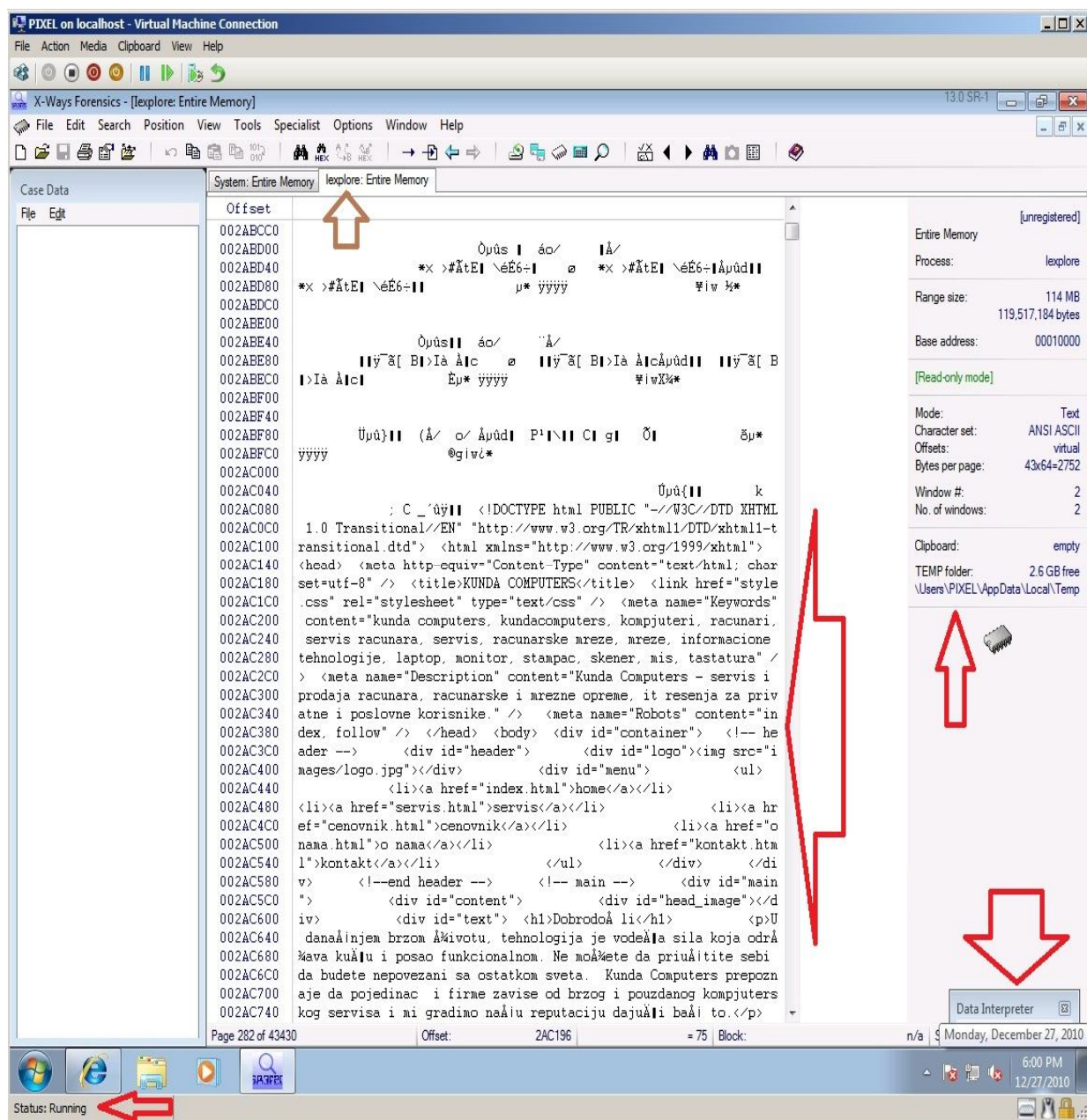
3.1.1. Praktični primer slike stanja na virtuelnoj mašini

Slike stanja koje se u praksi kreiraju, imaju ulogu uglavnom da zabeleže određene promene ako se instaliraju aplikacije koje mogu da ugroze rad operativnog sistema kao i celokupne virtuelne mašine. Slike stanja beleže sve promene, kao i informacije koje ostaju u virtuelnoj RAM memoriji, što je i objašnjeno u prethodnim poglavljima. Digitalni forenzičar treba da pokrene određenu sliku stanja na svojoj radnoj stanici i da primenom forenzičkog alata izvuče informacije o delovanju osumnjičene virtuelne mašine na virtuelno i realno okruženje vezano za internu ili javnu mrežu. Fajl .bin u sebi čuva informacije o RAM memoriji virtuelne mašine i bitno je da se taj fajl startuje kada se izvrši pokretanje stanja virtuelne mašine. Tako da digitalni forenzičar ako želi da prenese virtuelnu mašinu na svoju radnu stanicu u kojoj će vršiti ispitivanje, mora voditi računa o svim fajlovima koji se prenose iliti migriraju. Kada se pristupi istrazi virtuelnog digitalnog okruženja, potrebno je uzeti dve kopije *hard disc-a* osumnjičene virtuelne mašine, ali i dve kopije svih foldera i fajlova koji opisuju virtuelnu mašinu a u prethodnim poglavljima je bilo reči o njima. Od dve kopije *hard disc-ova* jedna se sa SHA algoritmom čuva i numeriče sve do izlaska pred sud i porotu kako bi se dokazalo da nije bilo promene u bitovima, a drugu kopiju digitalni forenzičar koristi za istragu. Isto važi i za kopije virtuelnih mašina, jer jedna je kao dokazni materijal a druga se koristi na radnoj stanici digitalnog forenzičara.

Kada se virtuelna mašina smesti na *hard disc* radne stanice i digitalni forenzičar tada otvara slučaj u kome će voditi beleške o svim dokazima koji će biti pronađeni tokom istrage nad

digitalnim osumnjičenim klijentom. U nastavku rada biće reči o primeru koji je sproveden da se pokaže koje informacije se čuvaju u virtuelnoj RAM memoriji pre i posle pravljenja slike stanja, ali i kada se slika stanja kreira, pa se virtuelna mašina isključi, a potom se pokrene poslednja ili izabrana slika stanja i dobije se mogućnost pristupu svim informacijama u virtuelnoj RAM memoriji te virtuelne mašine. Sve ovo ima veliku ulogu u istrazi u virtuelnom okruženju jer postoji mogućnost da osumnjičeni deluje anti forenzički na virtuelnu mašinu sa kreiranjem slika stanja koja mogu da dovedu u zabludu digitalnog forenzičara. Ali isto tako mogu imati veliku dokaznu moć jer nose veliki broj informacija o radnjama osumnjičenog.

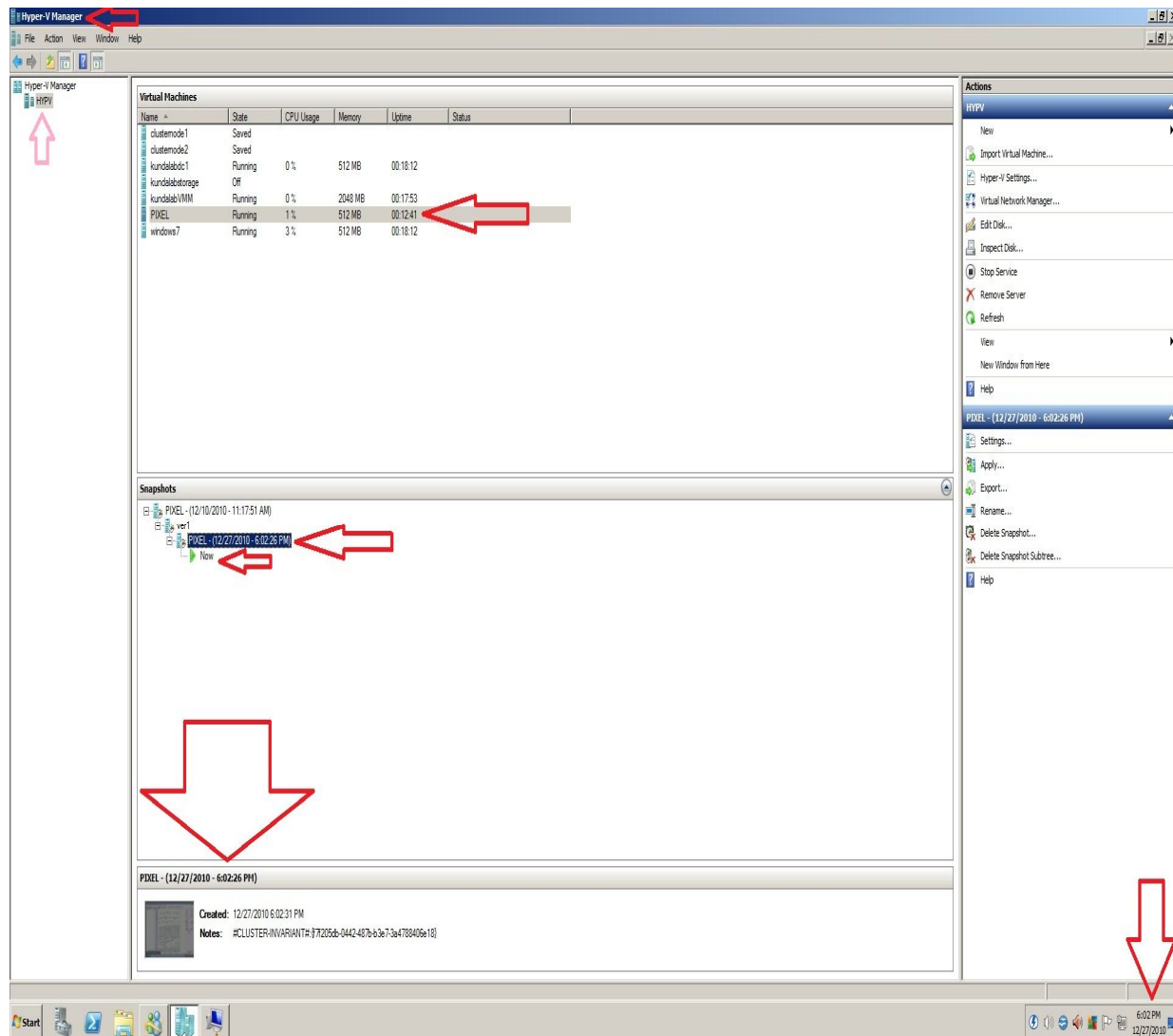
Korisnik je prvo posetio određeni *Web* sadržaj i posle nekog vremenskog perioda provedenog na tom Internet lokaciji, napravljena je prava slika stanja. Slika koja sledi pokazuje primenu forenzičkog alata *X-Ways Forensics* koji ima ulogu i da izvuče informacije iz RAM memorije.



Slika45. Delovanje forenzičkim alatom X-Ways Forensics na virtuelnu mašinu

Sa slike, Slika45, može se videti da je korisnik delovao na nekom određenom Web sajtu što je u sredini radnog prostora forenzičkog alata *X-Ways Forensics*. Može se primetiti da je status istrage u procesu *Running* – radnom, a može se reći da se radi o živoj forenzici. Sa slike se može videti još i da se proces istrage žive forenzike odvija nad folderom Temp. Tu se čuvaju sve informacije o procesima i operacijama koje korisnik vrši nad operativnim sistemom i o tome kako ga koristi. U ovom slučaju, reč je o operativnom sistemu Microsoft Windows 7 koji je instaliran na virtuelnoj mašini, a ona se nalazi kao *child*, u okviru domena. Domen je instaliran i konfigurisan na hardverskom *host-u*, koga pokreće operativni sistem Microsoft Windows 2008. Bitna informacija za tok događaja je da je slika koja je uzeta sa virtuelna mašine preko naredbe *PrtScBreak* na tastaturi i potom obrađena u Paint aplikaciji koja je sastavni deo operativnog

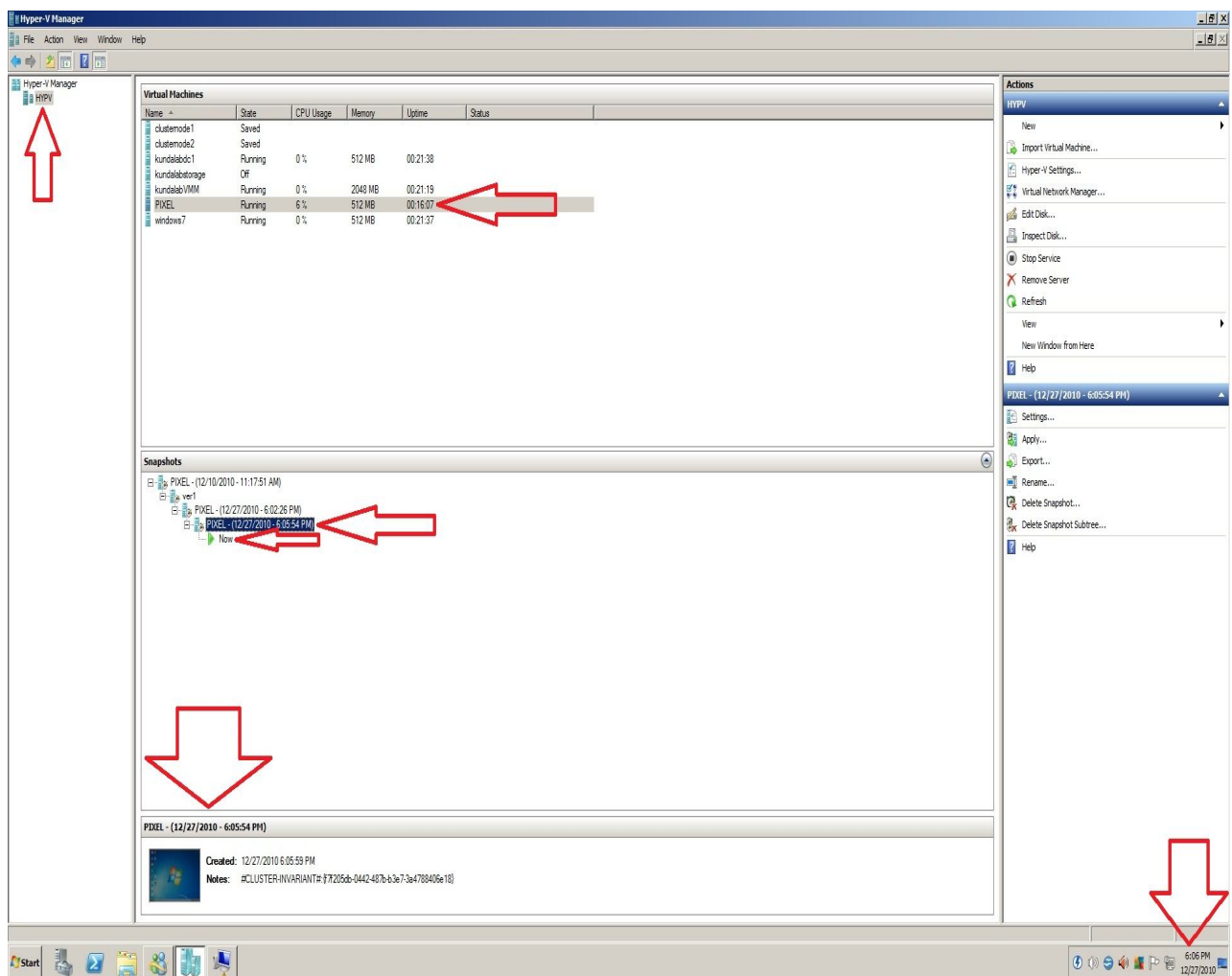
sistema Windows 7, je datum, vreme, dan i mesec. Pošto je virtuelna mašina radila u režimu pristupa na *Web* stranici i potom je uzet prvi *snapshot* iliti slika stanja, sledeća slika to prikazuje.



Slika46. Prva slika stanja virtuelne mašine

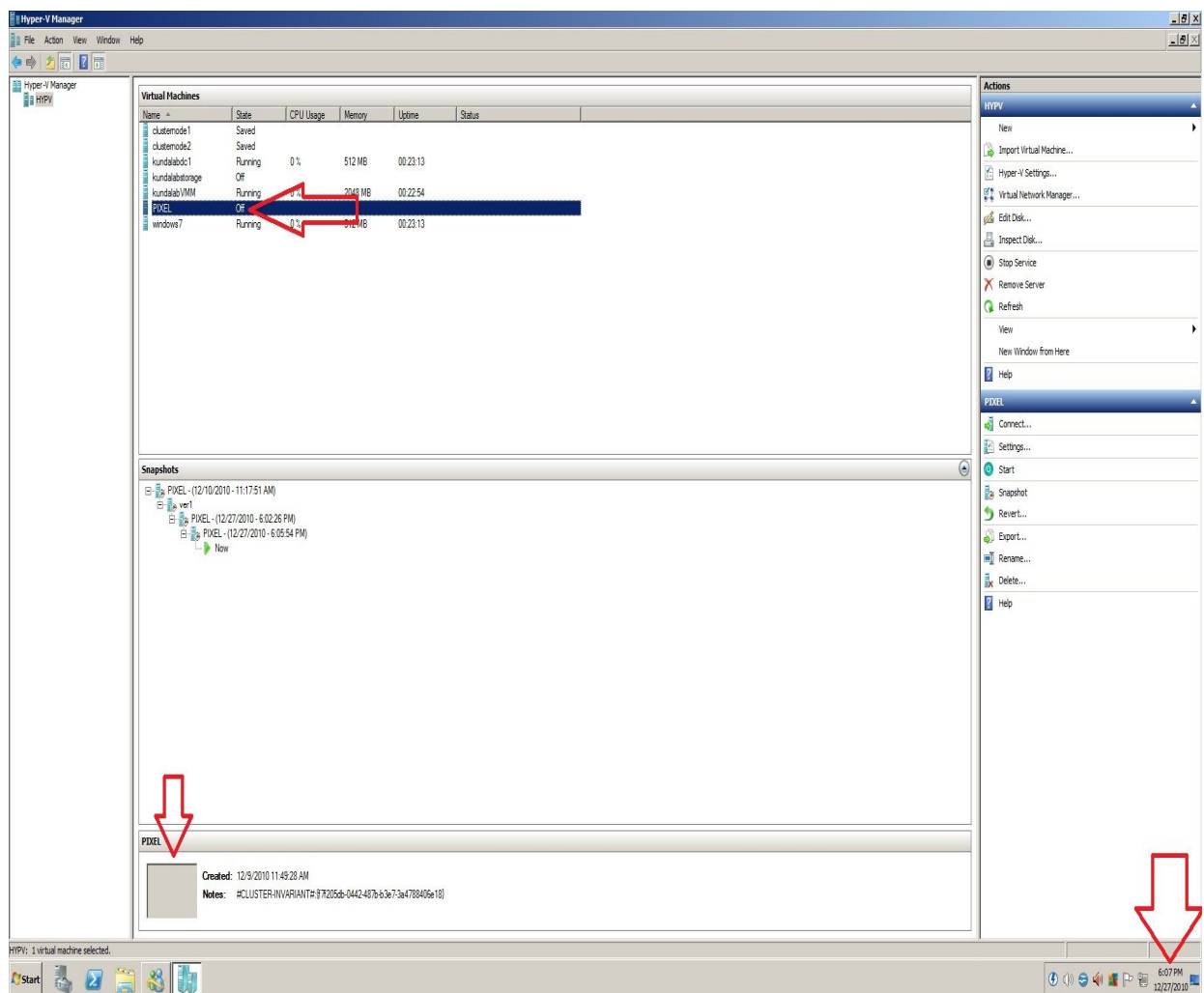
Sa slike, Slika46, može se videti da se operacija okidanja slike stanja odvija u konzoli *Hyper-V Manager*. Sledeća informacija govori o imenu *host-a* koji se u ovom slučaju zove HyperV, a virtuelna mašina koja se koristi u opitu zove se Pixel. U prozoru *Virtual Machines* se vidi da virtuelna mašina Pixel radi, tj. da je u stanju rada, koliko virtuelna RAM memorije poseduje i koliko je vremenski bila uključena. Informacija na satu operativnog sistema *host-a* u donjem desnom uglu, pokazuje datum i vreme koje govori da je od pristupa sa forenzičkim alatom na virtuelnu mašinu prošlo oko dva minuta, kada je napravljena prva slika stanja virtuelne mašine Pixel. Prozor *Snapshots* na slici, Slika46, pokazuje informacije da se slika stanja kreirala, ali i kada se kreirala i u koje vreme. Tačnije pokazuje ime virtuelne mašine, datum i vreme. I po

ovom datumu se vidi da je kreirana slika stanja posle oko dva minuta od pristupa forenzičkim alatom. A strelica ispod slike stanja pokazuje da je virtualna mašina i dalje u stanju rada, trenutno. U nastavku opita, korisnik je dobio mogućnost da sa virtualnom mašinom Pixel, pristupa određenim Web stranicama, vrši preuzimanje određenog sadržaja sa Web stranica, kreira određene fajlove i folder i da ih otvara i zatvara i šta god je želeo mogao je da uradi u određenom ili ne određenom vremenskom periodu. Bitno je bilo da digitalni forenzičar nije bio prisutan dok je korisnik radio razne operacije i radnje sa virtualnom mašinom. Potom je napravljena nova slika stanja kao što je prikazano na sledećoj slici.



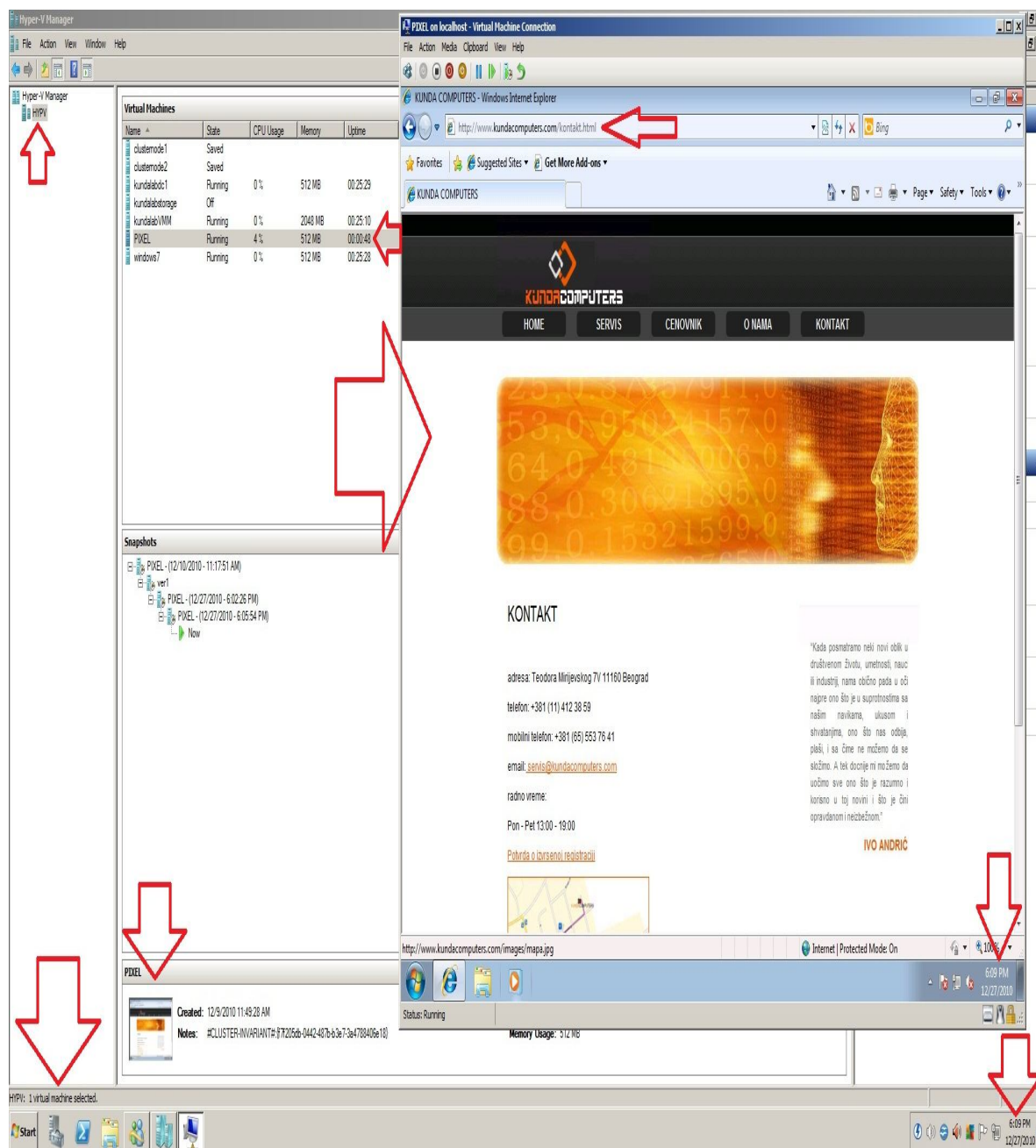
Slika47. Druga slika stanja virtualne mašine

Slika47 prikazuje da je na virtualnoj mašini Pixel izvršila još jedna slika stanja i to posle nekih tri minuta. Te informacije su vidljive na satu koji pokazuje vreme operativnog sistema *host-a*, u donjem desnom uglu. U prozoru *Virtual Machines* vidi se da je vreme rada virtualne mašine povećano, što dokazuje da nije isključivana. U prozoru *snapshots* se pojavila nova slika stanja što dokazuje da je urađena nova slika stanja posle oko tri minuta. Sada na virtualnoj mašini Pixel imaju snimljene dve slike stanja i ona nije isključivana tokom ovih operacija.



Slika48. Isključena virtuelna mašina

Sa slike, Slika48, može se videti da je virtuelna mašina isključena i u stanju je Off. Ako bi se ovo desilo kod fizičke mašine sve informacije iz RAM memorije bi bile izgubljene a one mogu nositi veliki broj dokaza o osumnjičenoj mašini. Ali i ako je virtuelna mašina isključena i to je urađeno sa namerom, treba se vratiti u prethodno stanje, tačnije pokrenuti poslednju sliku stanja, na primer, i videti šta je od informacija u RAM memoriji ostalo. Slika stanja se lako pokreće, tako što dvoklikom miša na odabranu virtuelnu mašinu pokrenuta je virtuelna mašina i otvoriće se prozor u kome će biti slika operativnog sistema te odabrane virtuelne mašine. Ako je virtuelna mašina bila isključena, moraće da se prvo podigne operativni sistem, pa potom da se unesu korisničko ime i lozinka, a tek onda da se pristupi operativnom sistemu i okruženju. Ali kada se slika stanja startuje, tada će se virtuelna mašina pokrenuti u onom trenutku kada je slika stanja i urađena. Tako da postoji mogućnost da se odmah nađete u okruženju operativnog sistema, bez logovanja i ako je posle slike stanja virtuelna mašina isključena.

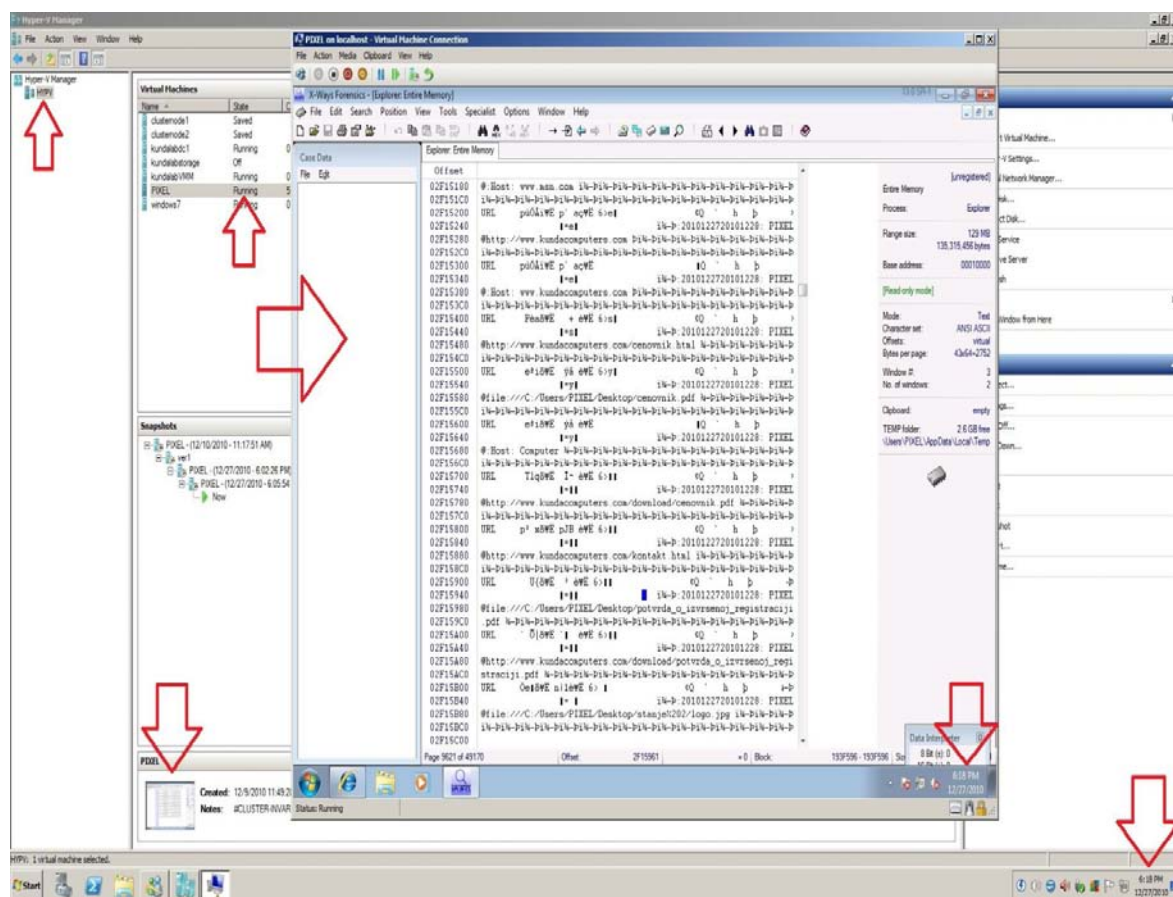


Slika49. Pokrenuta slika stanja

Slika49 prikazuje da se virtuelna mašina uključila, i da radi samo četrdeset osam sekundi. Sa slike se može videti i da je stanje startovane slike stanja u procesu rada, ali i prozor koji pokazuje da je virtuelna mašina u trenutku slikanja slike stanja bila u stanju rada i da je Web stranica bila maksimizirana. U donjem desnom delu slike, Slike49, vide se satovi i vremena kao i datumi kako na *host-u* tako i na *child-u*. Ono što je zanimljivo je da su posao čuvanja informacija odradili fajlovi .bin, .vsv, .xml i .avhd. Ovi fajlovi daju mogućnost virtuelnim mašinama da i ako se one

isključke, kao i kod fizičkih mašina, sve informacije iz RAM memorije nestanu i izgube se. Postoji mogućnost da se vrate u prethodno stanje. Sve informaciju podešavanja konfiguracije mašine, sačuvanih promena na *hard disc-u* pa i sačuvanih informacija u RAM memoriji pružaju dobijanje mogućnosti da se korisnik oseti kao da i nije isključio virtuelnu mašinu. Sve ovo može biti korišćeno u istrazi protiv osumnjičene virtuelne mašine, pa zato svaki digitalni forenzičar mora imati u vidu da se zbog toga otvara mogućnost da osumnjičeni deluje na ove dokaze, tačnije na slike stanja, anti forenzički, kako bi uklonio dokaze. Ali ako se dobije mogućnost i osumnjičeni ostavi slike stanja, trebaju se kopirati u dve kopije, jednu čuvati kao nepromenjeni dokaz a drugu uvesti na radnu stanicu i ispitati je, jer u sebi nose veliki broj informacija koje su korisne za istragu.

Ako se deluje sa forenzičkim alatom na pokrenutu virtuelnu mašinu iz slike stanja, može se videti šta je korisnik radio i koje operacije je izvodio dok digitalni forenzičar, kako je prethodno rečeno nije bio prisutan u periodu od oko tri minuta.



Slika50. Delovanje forenzičkim alatom na startovanu virtuelnu mašinu

Slika50 prikazuje da posle pokretanja virtuelne mašine iz slike stanja može da se deluje forenzičkim alatom i da se pristupi vađenju bitnih informacija o prethodnom radu korisnika na toj virtuelnoj mašini.

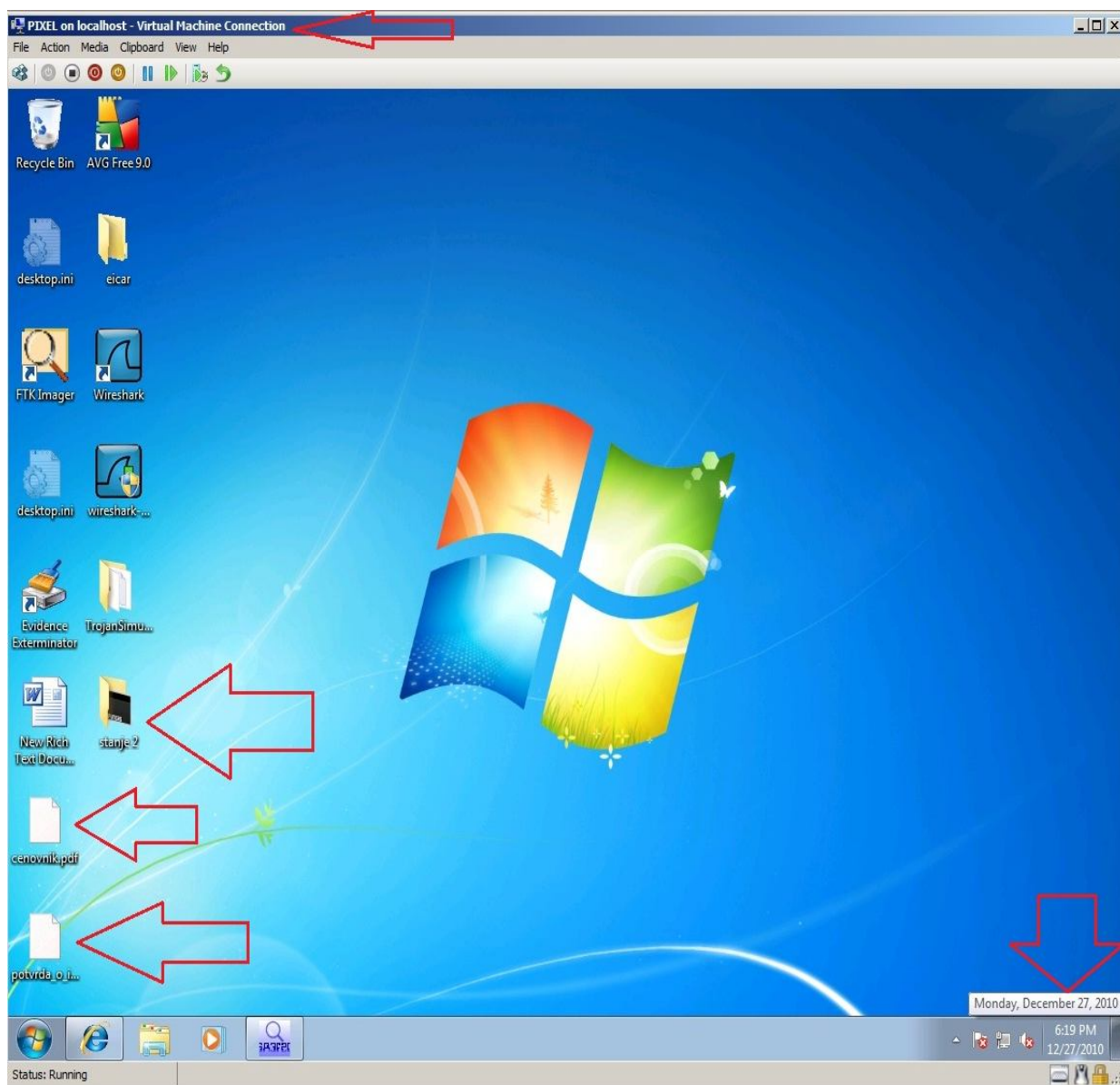
Explorer: Entire Memory	
Offset	
02F15180	@:Host: www.msn.com i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F151C0	i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15200	URL púÓÄi%È p' aq%È 6>e €Q ` h b `
02F15240	I=e i%-p:2010122720101228: PIXEL
02F15280	@http://www.kundacomputers.com p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F152C0	i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15300	URL púÓÄi%È p' aq%È IQ ` h b `
02F15340	I=e i%-p:2010122720101228: PIXEL
02F15380	@:Host: www.kundacomputers.com p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F153C0	i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15400	URL Pèaö%È + è%È 6>s €Q ` h b `
02F15440	I=s i%-p:2010122720101228: PIXEL
02F15480	@http://www.kundacomputers.com/cenovnik.html %-p%-p%-p%-p%-p%-b
02F154C0	i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15500	URL e%iö%È ýâ è%È 6>y €Q ` h b `
02F15540	I=y i%-p:2010122720101228: PIXEL
02F15580	@file:///C:/Users/PIXEL/Desktop/cenovnik.pdf %-p%-p%-p%-p%-p%-b
02F155C0	i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15600	URL e%iö%È ýâ è%È IQ ` h b `
02F15640	I=y i%-p:2010122720101228: PIXEL
02F15680	@:Host: Computer %-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F156C0	i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15700	URL Tlqö%È î- è%È 6> €Q ` h b `
02F15740	I= i%-p:2010122720101228: PIXEL
02F15780	@http://www.kundacomputers.com/download/cenovnik.pdf %-p%-p%-p%-b
02F157C0	i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15800	URL p² xö%È pJB è%È 6> €Q ` h b `
02F15840	I= i%-p:2010122720101228: PIXEL
02F15880	@http://www.kundacomputers.com/kontakt.html i%-p%-p%-p%-p%-p%-b
02F158C0	i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15900	URL U{ö%È ² è%È 6> €Q ` h b -b
02F15940	I= i%-p:2010122720101228: PIXEL
02F15980	@file:///C:/Users/PIXEL/Desktop/potvrda_o_izvršennoj_registraciji
02F159C0	.pdf %-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15A00	URL ` Ö ö%È ` î è%È 6> €Q ` h b `
02F15A40	I= i%-p:2010122720101228: PIXEL
02F15A80	@http://www.kundacomputers.com/download/potvrda_o_izvršennoj_regi
02F15AC0	straciji.pdf %-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15B00	URL Öe ö%È nilè%È 6> €Q ` h b 4-b
02F15B40	I= i%-p:2010122720101228: PIXEL
02F15B80	@file:///C:/Users/PIXEL/Desktop/stanje%202/logo.jpg i%-p%-p%-p%-b
02F15BC0	i%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-p%-b
02F15C00	

Slika51. Radni prostor forenzičkog alata X-Ways Forensics

Slika51 je izvađena iz prethodne slike, Slika50. To je urađeno da bi se videle jasno sve informacije koje su izvađene iz virtuelne RAM memorije virtuelne mašine Pixel u vremenskom periodu kada digitalni forenzičar nije bio prisutan u prostoriji a korisnik je vršio određene radnje sa virtuelnom mašinom. Taj vremenski period je trajao oko tri minuta. Radi ovog opita je uzeto

namerno kraće vreme koje treba proveriti, ali to nije obavezno. Može se uzeti duži vremenski period istrage ili manipulacije sa virtuelnom mašinom, samo bi tada lista dokaza bila duža, a to opet zavisi sa frekvencijom korišćenja virtuelne mašine od strane korisnika. Kako je prikazano na slici, Slika51, vidi se redosled kojim je korisnik pristupao *Web* lokacijama sa datumom i tačnom *URL* lokacijom. Potom se vidi da je pristupao određenoj stranici koja mu je omogućila da preuzme fajl sa ekstenzijom .pdf koji je daljom istragom pronađen na *hard disc-u* virtuelne mašine. Korisnik je mogao i da uradi jednu anti forenzičku aktivnost, a to je da promeni ekstenziju fajla kojeg je preuzeo. To se lako može otkriti delovanjem sa forenzičkim alatom i preuzimanjem slike *hard disc-a*, potom pronaći određene sumnjive fajlove i sa potpisom bita videti o kojim fajlovima je reč. Jer operativni sistem uvek potpisuje ekstenzije fajlova kako je predefinisano od konstruktora i programera operativnog sistema. Tako da se lako može saznati da li je promenjena ekstenzija i uočiti o kojim fajlovima je reč. Ove manipulacije i prevare uglavnom koriste osumnjičene osobe koje se bave razmenom slika dečije pornografije. Ovakve prevare i anti forenzičke aktivnosti su česte ali ih lako možete uočiti i otkriti.

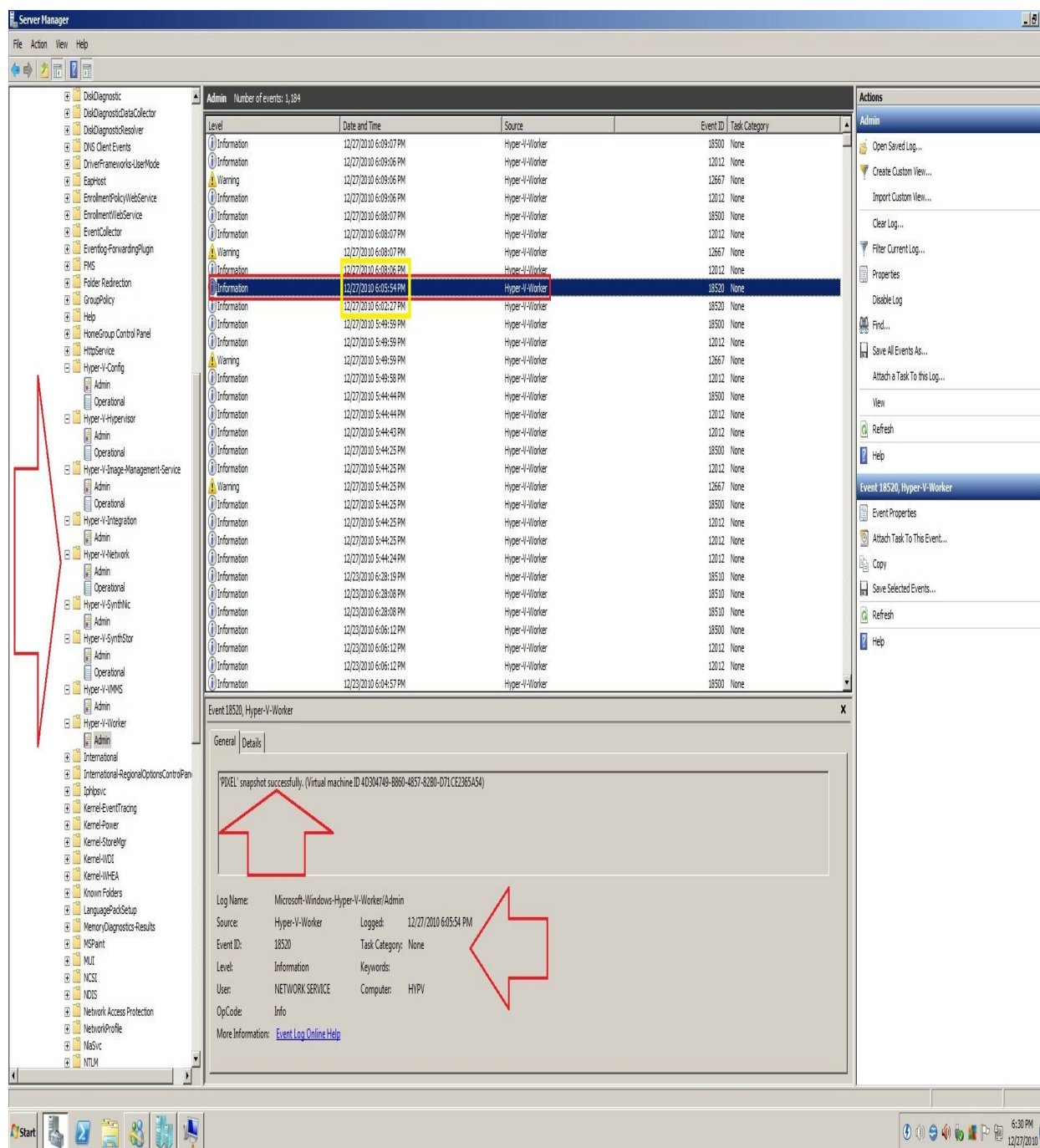
Sledeća bitna informacija sa slike, Slika51, je da je korisnik izvršio preuzimanje fajla .jpg i prebacio ga na *hard disc* svoje virtuelne mašine. Ono što je bitno, a to je da se vide tačne lokacije do fajlova koji su smešteni na neki *hard disc* ili neki prenosni uređaj i da je onda i lako naći te fajlove koji su preuzimani sa *Web* stanica. Isto tako predhodno je napomenuto i da se vide i celokupne *URL* lokacije i da onda digitalni forenzičar ima mogućnost da sa svoje radne stranice pristupi tim *Web* stranicama u cilju prikupljanja većeg broja dokaza. Pristup se vrši sa radne stanice a nikako ne sme da vrši bilo kakav pristup sa osumnjičene mašine, jer tada osumnjičeni ima puno pravo da kaže da nikada nije pristupao i da je digitalni forenzičar ta osoba koja je vršila pristup. Time se dokaz vezan za pristup određenim *Web* stranicama obara pred sudom i više nije merodavan. Zato svako delovanje u istrazi digitalni forenzičar mora vršiti sa svoje radne stanice i na kopijama koje su namenjene za istragu. Jer postoji mogućnost da digitalni forenzičar ako pokvari mesto krivičnog dela osumnjičene virtuelne mašine izvrši anti forenzičku aktivnost sam protiv sebe. Sve predhodne informacije mogu biti korišćene kao dokaz ako za to postoji potvrda na osumnjičenoj virtuelnoj mašini. A te informacije su predstavljene na sledećoj slici.



Slika52. Dokazi na virtuelnoj mašini

Sa slike, Slika52, može se videti vreme i datum kada je istraga vođena, ali i ime virtuelne mašine na kojoj se istraga u ovom opitu sprovodi. Tri strelice sa leve strane slike pokazuju na fajlove koji su u istrazi uz pomoć forenzičkog alata otkriveni. Ali to nije dovoljno u nekim slučajevima da bude čvrst dokaz. Potrebno je uporediti i kopiju bit po bit kada se preuzme slika *hard disc-a* sa preuzetim fajlovima i ako je potpisano istim bitovima može se smatarati odgovarajućim dokazom. Ali ako korisnik izmeni sadržinu fajla a ako se o takvom fajlu i radi i ako se za taj fajl istraga vezuje, može se desiti da korisnik želi da primeni određenu anti forenzičku aktivnost. Tada se mora pristupiti određenoj metodi u zavisnosti toka nastavka istrage. Ono što je bitno, a vezano je za manipulisanje slikama stanja o kojima je i reč u ovom poglavlju, a to je da se bitna informacija može naći u log fajlovima *host-a*. Jer ako korisnik i izvrši

određenu anti forenzičku radnju nad slikama stanja i ako ih premesti na drugu lokaciju, na *host-u* će ostati zabeleženo da je slika stanja bila izvršena i to nad određenom virtuelnom mašinom. A sledeća slika to i prikazuje.



Slika53. Log fajl host-a

Slika53. prikazuje log fajlove na *host-u* u kojima je zabeleženo da se odvijala operacija pravljenja slike stanja na virtuelnoj mašini kao *child-u* a to je Pixel. Zabeležen je i datum kao i vreme kada se ta operacija i dogodila. Vidi se na hijerarhijskom stablu koji su to log fajlovi ali i u centralnom prozoru. Ove informacije je bitno da ima digitalni forenzičar kako bi mogao da ima dokaz da se na tom serveru iliti *host-u* zaista odvijala operacija slikanja slike stanja virtuelne mašine koja je *child* tog *host-a*. Ove informacije, na primer, sprečavaju manipulaciju i anti forenzičke aktivnosti, jer osumnjičeni ne može da kaže da je ta virtuelna mašina migrirala u to virtuelno okruženje.

Sve su ovo informacije koje mogu da daju jednu sliku događaja o aktivnostima korisnika na virtuelnoj mašini, na primer, Pixel u trajanju od tri minuta, kao što je izvedeno u opitu. Ovim se dokazuje i delovanje korisnika na virtuelnu mašinu i ako nije ili čak jeste imao određene ne zakonite ili zakonite radnje.

3.2. Studija slučaja 2: zombiranje

Zombiranje virtuelnih mašina koriste uglavnom lica koja žele da nanose štetu korisniku čija je virtuelna mašina i da svojim delovanjem vrše radnje koje se kose sa zakonskim odredbama.

3.2.1. Zombirana virtuelna mašina u *hyper-V* okruženju

Kada se spomene izraz, zombirana mašina, misli se na računar koga poseduje vlasnik ali ga koristi treće lice koje vlasniku računara nije poznato. Sa zombiranim računarom se rade određene ne zakonite radnje i postupci za koje vlasnik ne zna i često se vlasnik zombiranog računara stavlja pred lice pravde a da i sam nije svestan da je učinio to ne zakonito delo, što i jeste istina. Ovakve operacije hakera i lica sumnjivih pravdi su česta pojava u celom svetu. Ponekad su zloupotrebljeni ili iskorišćeni pojedinci a često i neke organizacije koje u svom posedu imaju veći ili veliki broj računara. Kako tehnologija napreduje tako se i anti forenzičke radnje sve više i više koriste za raznorazne prevare i ucene. Ovakve ne korektne radnje po zakonu zemlje u kojoj se odvijaju mogu naneti velike štete društvu ali i pojedincu. U Republici Srbiji nisu česte ovakve pojave zombiranja kompjutera ali u zemljama zapada i istoka su ovakve pojave postale svakodnevnica. A kada dođe do određene zloupotrebe postavlja se velika obaveza pred digitalnog forenzičara ili celokupan tim forenzičara, kao i pred istražne organe da dokažu ko je zapravo učinio ne zakonitu radnju. Pošto dokaz mora biti upotrebljen pred sudom i pred porotom, a svi digitalni dokazi su jedna apstrakciona pojava za ljude iz sfere pravde, postoji velika zebnja da se neki slučajevi ne mogu rešiti.

Kako tehnologija korača sve većim i većim koracima kroz vreme, tako i pokušava da se prilagodi kako ljudima pa i okruženju gde se tehnologija i primenjuje. Zato se i događa da se novi operativni sistemi kao i virtuelno okruženje o kome se govori u ovom radu, dosta često prilagodi kako pozitivnoj strani zakona pa tako i onoj drugoj koja koristi sve mogućnosti da obmane i sakrije dokaze. Suština je u tome da samo virtuelno okruženje, korišćenje virtuelnih mašina, pa i hardvera koji može biti fizički ali i virtuelni, dovodi do većeg broja mogućnosti obmane

istražitelja. Sve ove informacije se mogu brzo i jednostavno uz nekoliko klikova na tastaturu i miša ukloniti i ostaviti računar bez dokaza. Ali ipak ovde nije kraj celokupnog istraživanja digitalnih dokaza u virtuelnom sistemu jer kako i u realnom životu ne postoji savršen zločin koji uvek ostavi neki trag, tako i u virtuelnom okruženju uvek imaju tragovi koji se mogu prikupiti. Bitno je samo kako voditi istragu, kako prići problemu i kako ga sprovesti bez odstupanja da ne bi došlo do greške. Pošto se u ovom poglavlju razrađuje tema o zombiranim virtuelnim mašinama i ako ta pojava nije postala standardna u svetu kriminala ali se ipak koristi u zemljama zapada i istoka, sama virtuelizacija nije uzela još maha na svetskom tržištu. Predviđanja ljudi iz korporacija koje se bave i prave virtuelno okruženje, a koje je budućnost ali i počinje da biva sadašnjost Globalnog okruženja, je da tek u periodu od narednih deset do dvanaest godina treba da zaživi u celom svetu.

Borba protiv anti forenzičkih delovanja zahteva da se uspostavi dobra komunikacija između provajdera koji će nuditi usluge virtuelizacije, da se centralizuje celokupan sistem i da se klijentima odrede odgovarajuće mere kako zaštite pa tako i prava za pristupe ali i za korišćenje odgovarajućih resursa, ma šta to bilo, da li hardver ili softver. Celokupan sistem potrebno je pratiti i ako postoji odgovarajuća pretnja moguće je filtrirati saobraćaj za praćenje onih grupa paketa koji se smatraju sumnjivim. Postoje forenzički alati koji omogućavaju praćenje paketa i njihovu filtraciju. Filtracija paketa je veoma bitna jer ako se prati celokupan saobraćaj dokumenata na mreži bilo bi potrebno da imate veliki broj ljudi da sve informacije o podacima isprate. Jer primera radi, sama autentifikacija i pristup resursima jednog računara drugom, daće na desetine informacija.

Ulaz hakera ili lica koje želi da iskoristi tuđi računar, nije baš jednostavno, ali nije ni ne izvodljivo. Koriste se odgovarajući operativni sistemi kao što su *Linux* i određeni alati, od kojih se uglavnom koriste trojanski konji. O trojanskim konjima i još o virusima i crvima biće reči u sledećem poglavlju.

Urađen je opit praćenja jednog klijenta koji pokušava da prebaci trojanskog konja na računar koji želi da preuzme u svoje rukovanje i da uz pomoć tog računara nanese štetu korisniku, čiji je računar zapravo. Pošto korisnik koristi internet konekciju, preko kabla ili bežične konekcije, osoba koja želi da nanese štetu, otvaranjem određenog porta izvršiće napad. Napad će početi preko aktiviranja nekog servisa koji ima za zadatak da otvori određeni port i omogući korisniku da preko alata i uz pomoć operativnog sistema na primer *Linux* preuzme kontrolu nad virtuelnom mašinom koju napada. Taj servis može biti preuzet sa nekog *Web* sajta ili poslat na e-mail adresu žrtve. Postoje različite aktivnosti lica koja nisu na strani pravde, ali pošto se u ovom radu opisuju anti forenzička delovanja i aktivnosti, nije objašnjeno u detalje kako se napada i zauzima virtuelna mašina. Kada se otvori port i haker preuzme kontrolu nad virtuelnom mašinom, tada ima mogućnost i korišćenja slike ekrana sa udaljenog pristupa ako želi. Pošto se haker pribojava da korisnik primeti njegovo delovanje, mora koristiti odgovarajuće alate, ili aplikacije da neometano iskoristi virtuelnu mašinu. Spominje se virtuelna mašina, jer je ona predmet ovog istraživačkog rada, ali ovakav upad se može odvijati i na fizičkim mašinama, kao i na mobilnim telefonima ali i na svim uređajima koji nisu dobro zaštićeni a koriste Globalnu mrežu. Trojanski konji imaju ulogu da se kopiraju na virtuelnu mašinu koja je napadnuta i da otvore zadnja vrata kako se to u svetu informatike zove. Postoje aplikacije koje pokreću procese, a oni simuliraju zadanja vrata na operativnim sistemima koja su legalno postavljena i to u instalacijama. Te procese koriste službe kompanija da na jednostavniji način ispravljaju greške u operativnom sistemu, ali i bezbednosne službe zemalja u kojima te korporacije funkcionišu. Zadnja vrata hakeri ostavljaju da se mogu lakše vratiti na virtuelnu mašinu koju su već napali i da ne bi morali

Pošto je u opitu izvršen napad na jednu virtuelnu mašinu, a praćenjem mrežnog saobraćaj zabeleženo je, pomoću forenzičkog alata, da se sa jedne lokacije na drugu kopira određeni sadržaj. Tačnije, jedan klijent kopira na drugog klijenta fajl koji simulira virus u ovom slučaju, a može biti i trojanski konj, ta aktivnost je zabeležena i praćenje je počelo.

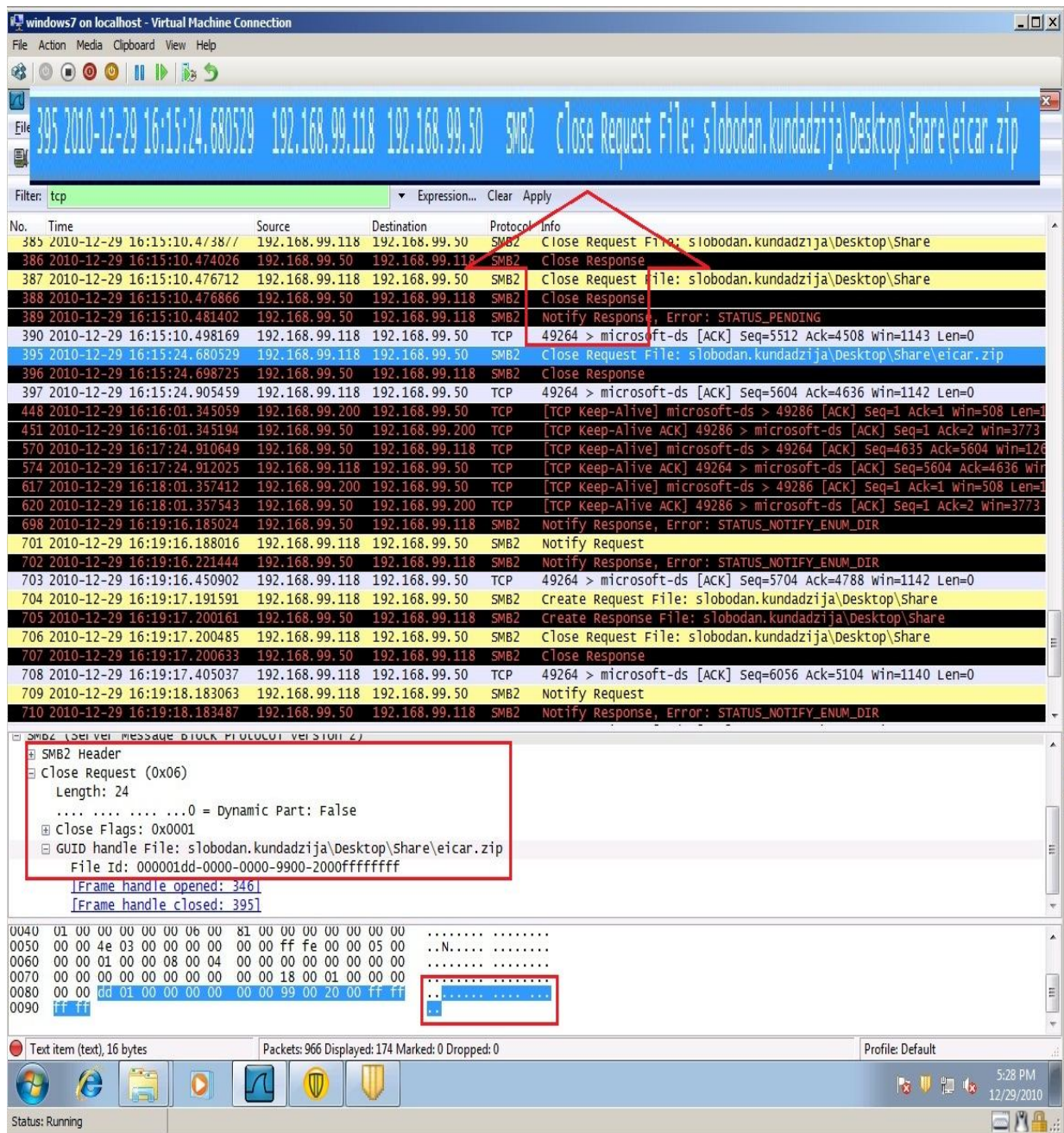


Kada je forenzički alat, kao što se može videti sa slike, Slika54, zabeležen je fajl eicar.zip i tada se krenulo u proces praćenja komunikacije korisnika dve mašine. Fajl *eicar* je vrsta kontrolnog virusa koji je korišćen za opit i koji treba da alarmira antivirusni softver. Koristi se da proveriti koji je stepen sigurnosti operativnog sistema i ne nanosi nikakvu štetu operativnom sistemu. Sa slike se vidi da je kreiran zahtev za kopiranje fajla, tačnije korisnik koji se sada sumnjiči za napad je na IP adresi 192.168.99.118 jer je lociran od strane forenzičkog alata da je izvor ove komunikacije koja sledi. Dok je mašina koja se prati i koja prima ovaj fajl, je destinaciona mašina i ima IP adresu 192.168.99.50. Iz ovih informacija se može videti da su na istom opsegu mreže ali i da su u nekoj od internih mreža. Sa slike se vidi i vreme kada je izvorni računar pokrenuo zahtev za kopiranje. Sve ove informacije su bitne jer kada digitalni forenzičar pristupi istrazi na računaru koji je slao kao i na računaru koji je prima poruku mora imati u vidu u kom smeru da pokrene istragu i da se drži vremena koja su zabeležena i koja govore kada se neka od ne zakonitih aktivnosti desila. Na slici se može videti celokupna komunikacija kada je zahtev za kopiranje izdat od strane izvora ka strani destinacije mašine. Ono što digitalni forenzičar može da iskoristi od informacija je i binarni zapis fajla eicar.zip i kada bude uzimao sliku *hard disc-a* osumnjičenog može uporediti i izneti kao jedan od dokaza pred organe pravde. Sa slike, Slika54, može se videti i putanja do fajla na računaru, tačnije gde će biti kopiran. To može biti bitna informacija kako bi smanjila vreme delovanja digitalnog forenzičara u istrazi i onemogućila osumnjičenog da manipuliše ili primeni anti forenzičku aktivnost nad dokazom koji ga sumnjiči. Slika takođe pokazuje da je forenzički alat *Wireshark* zabeležio i o kojem protokolu se radi, a postoji mogućnost da se izvrši filtriranje celokupnog saobraćaja i na primer izdvoji se samo TCP komunikacija.

Transmission Control Protocol (TCP) je jedan od osnovnih Internet protokola. Sastoji se od dve komponente pa onda ceo paket ima naziv TCP/IP. TCP pruža usluge direktnog razmenjivanja fajlova između dva *host-a* na istoj mreži kao što je i slučaj u ovom opitu. A dok IP upravlja adresama i rutama između različitih mreža. Na TCP protokol se oslanjaju glavne Internet aplikacije kao što su *World Wide Web*, *e-mail* i *file transfer*. Aplikacije koje ne zahtevaju pouzdan protokol kao što je TCP mogu koristiti UDP protokol. Na slici, Slika54, može se primetiti i pojava još jednog protokola a to je SMB2 protokol.

Server Message Block (SMB) Version 2 je protokol koji se koristi kod Microsoft operativnih sistema i poboljšana je verzija prethodnika koji se zvao SMB. Zadatak SMB2 protokola je da omogućiti klijentu koji je izdao zahtev za kopiranje određenog sadržaja kroz mrežu ka drugom klijentu, tačnije sa računara na računar. Osnove transporta SMB2 protokola koriste TCP protokol. Ove informacije su bitne jer mogu dati digitalnom forenzičaru dokaz da je klijent koji je u ovom slučaju izvor sa IP adresom 192.168.99.118 stvarno zatražio da premesti, tačnije kopira fajl eicar.zip na klijentsku mašinu koja je destinacija.

Sledeća slika pokazuje da se konekcija kopiranja fajla završila u određeno vreme i da su protokoli zatvorili zahtev koji je bio predhodno otvoren.

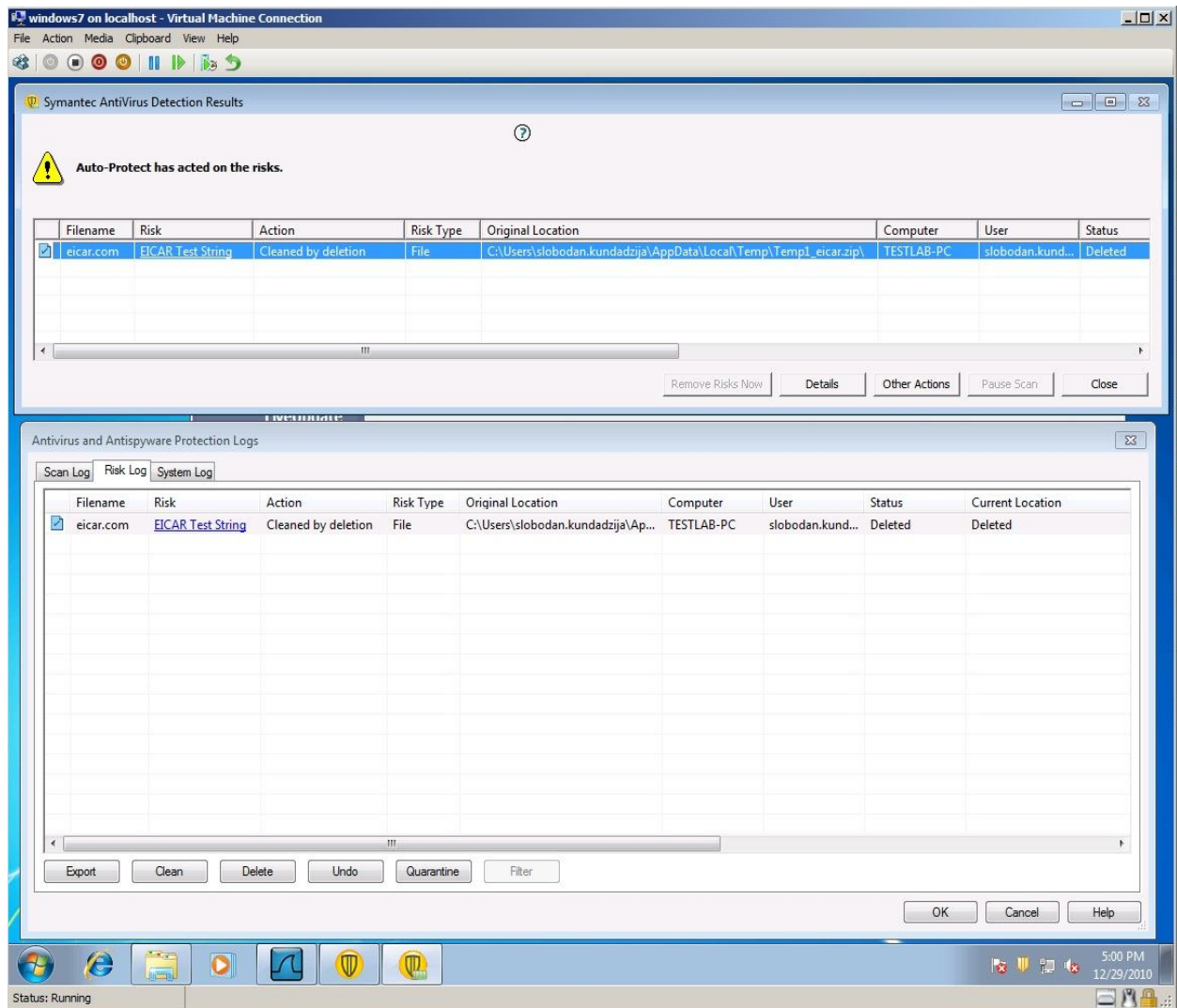


Slika55. Kraj kopiranja fajla eicar.zip

Na slici, Slika55, jasno se vidi kada se transfer fajla završio i ako se uporedi sa prethodnom slikom, Slika54, može se zaključiti da je trajao svega 14 mili sekundi, što je kratak vremenski period. Ostale informacije sa slike govore da se protokol SMB2 zatvorio jer je zahtev za kraj korišćenja protokola urađen. Može se videti jasna lokacija gde je fajl smešten i putanja na *hard disc-u* destilacione mašine. Vidi se još i binarni zapis koji govori o kraju kopiranja fajla u trenutku kada se celokupan fajl kopirao sa izvora ka odredištu i kada je prestao da se koristi za tu svrhu kopiranja protokol SMB2. U nastavku prikupljenih informacija uz pomoć forenzičkog alata Wireshark može se videti da korisnik koji je kopirao fajl nastavio da koristi folder u kome

je fajl kopiran. To se može protumačiti i da je njegova konekcija prema folderu na tuđoj mašini ostala i dalje aktivna što pokazuje Slika55.

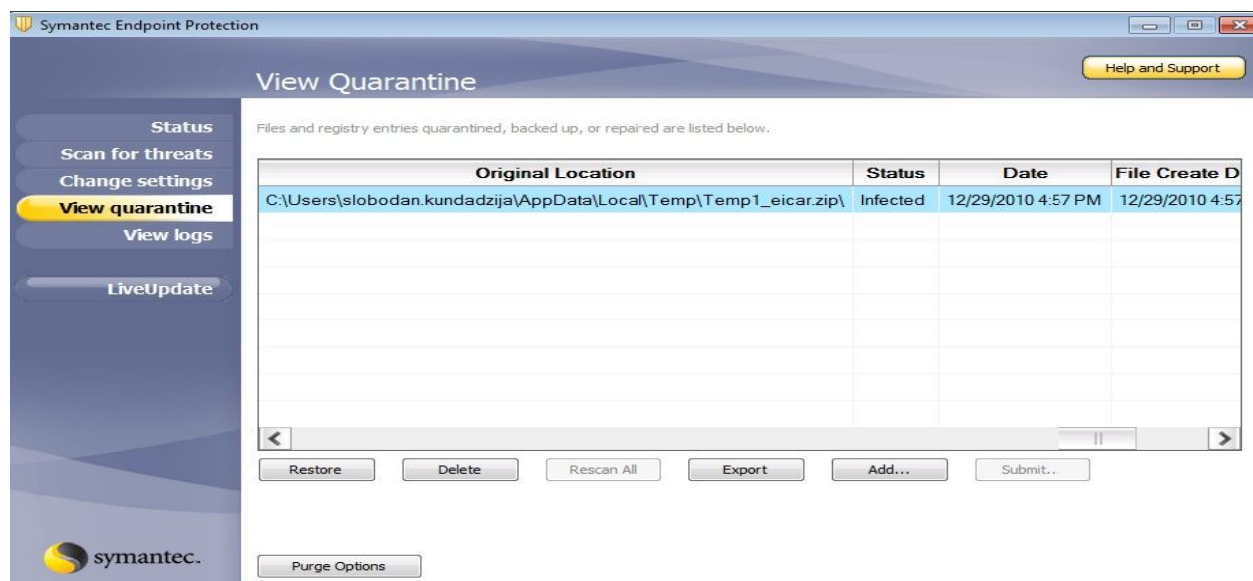
Pošto se opit bavi mogućim zombiranjem virtuelne mašine, dalje se opisuje pristup virtuelnoj mašini koja je zombirana i pokušaj dokazivanja da je koristilo treće lice preko određenih dokaza. Na virtuelnoj mašini koja je destinacija kopiranog fajla, korišćen je anti virusni softver *Symantec*, koji nudi dobru zaštitu od mogućih napada. Kada se pristupilo virtuelnoj mašini sa IP adresom 192.168.99.50 koja je okarakterisana kao zombirana mašina, dobile su se sledeće informacije.



Slika56. Symantec zabeležio napad virusa

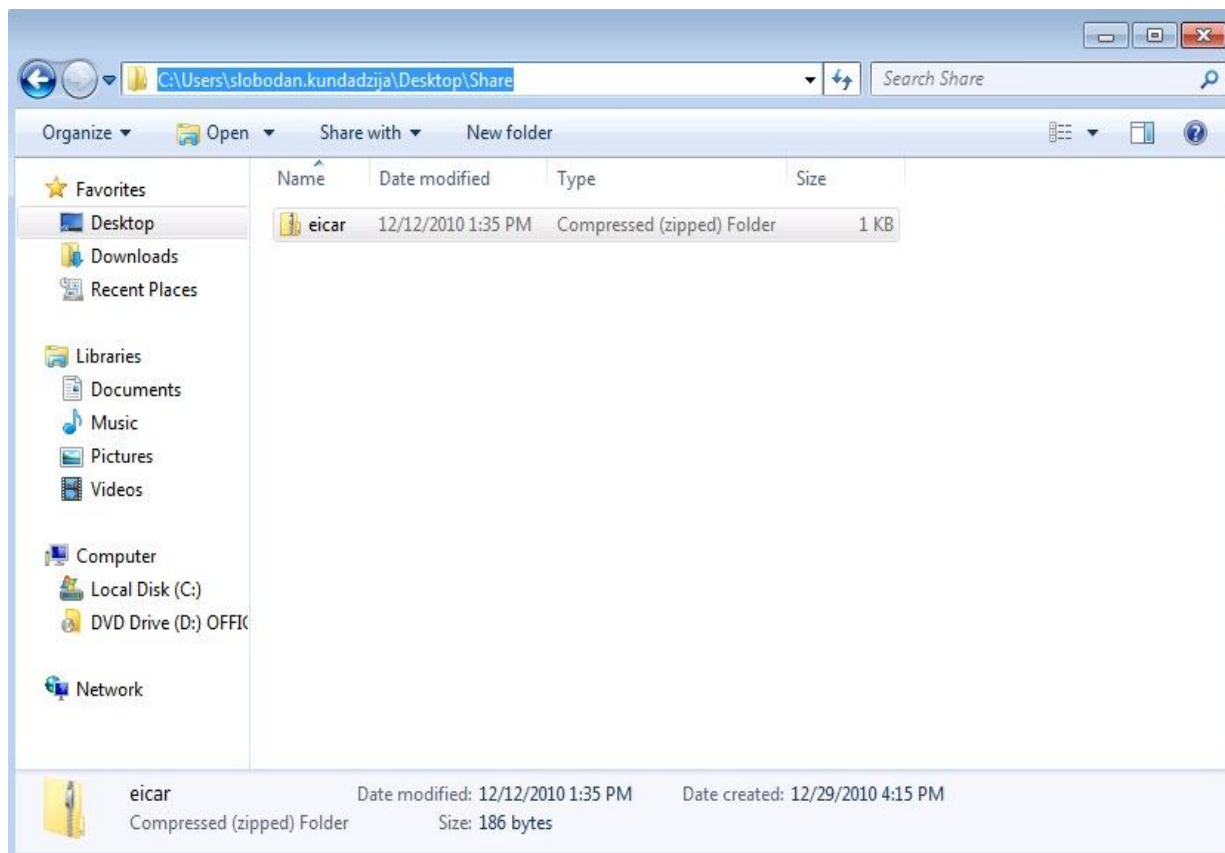
Sa slike, Slika56, antivirusni softver zabeležio prisustvo virusa *eicar* i locirao ga, a potom ga je i izbrisao. Te informacije se mogu videti u gornjem delu slike, dok u donjem delu slike, postoje zabeležene informacije o delovanju fajla u operativnom sistemu, ali i delovanju anti virusa *Symantec* na isti fajl i vide se da je obrisan. Mogu se videti lokacija, ime računara, korisnik

operativnog sistema, delovanje na fajl. Ono što je bitno za digitalnog forenzičara, jeste da je zabeleženo postojanje određenog fajla koji je u operativnom sistemu i koji je korišćen na istom sistemu jer je anti virusni softver delovao na taj fajl i obrisao ga. Pozitivno je to što je fajl uklonjen u karantin antivirusnog softvera, ali ako su sa te virtuelne mašine rađene određene ne zakonite aktivnosti i da pre toga praćenje nije izvršeno, dobile bi se loše ocene o mogućem osumnjičenom i tada bi bio procesuiran pogrešni korisnik. Zbog toga su bitne informacije koje su sprovedene praćenjem mrežnog saobraćaja, kao i informacije koje govore koji je od računara pokrenuo zahtev za kopiranje fajla, a koji je računar taj fajl i primio.



Slika57. Symantec karantin

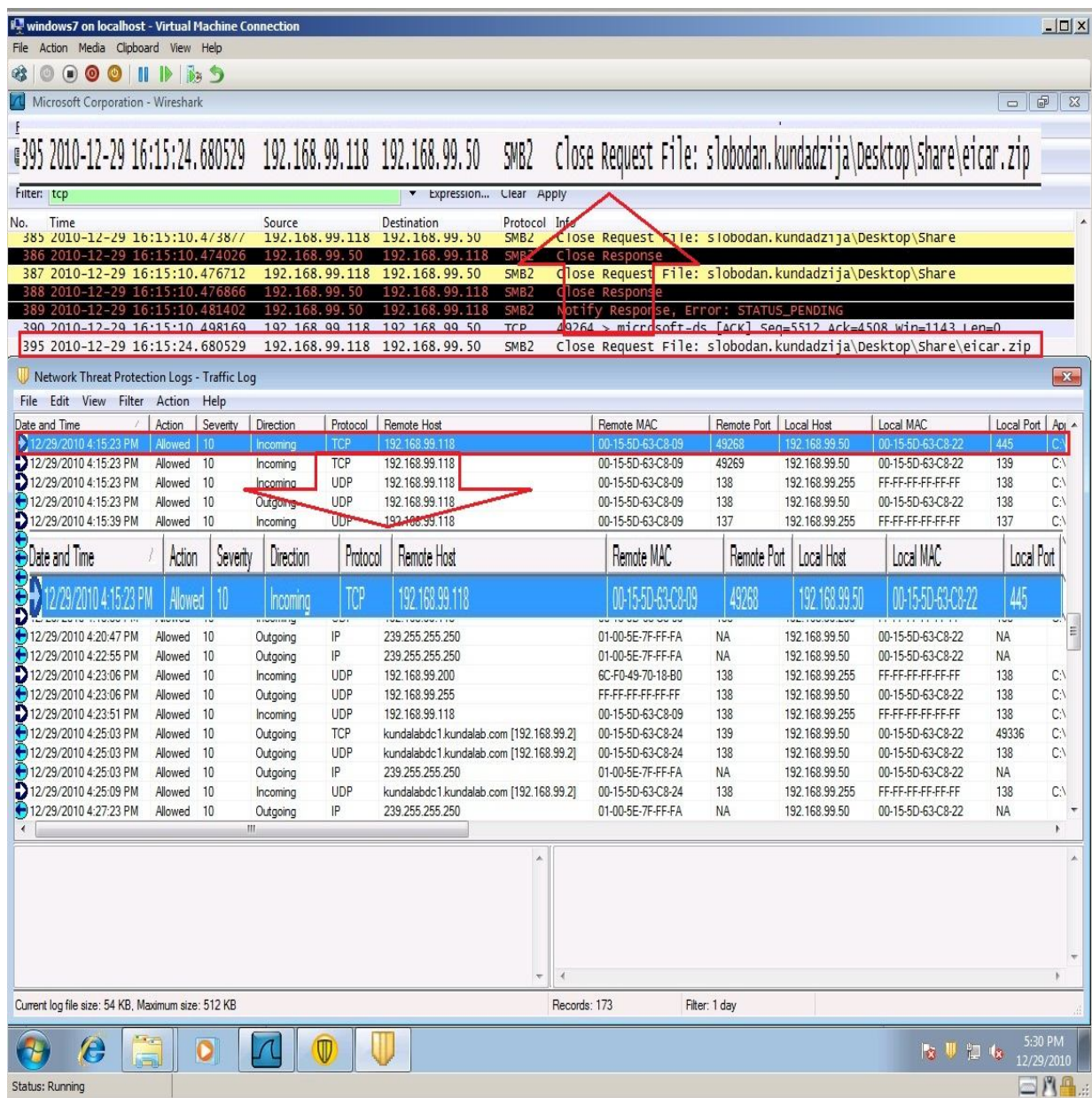
Slika57 pokazuje koja je bila originalna lokacija fajla eicar.zip i koji mu je bio status kada je aktiviran antivirusni softver koji je fajl smestio u karantin. Može se videti i informacija kada je kreiran fajl na korisnikovom računaru. Digitalni forenzičar mora imati dobra pred istražna saznanja o mogućem ili incidentu koji se dogodio kako bi imao pravu sliku ko je pravi osumnjičeni, jer sve informacije govore da je osumnjičeni korisnik koji se postao zombiran računar, da nema pred istražnog rada. Ovo je jedan od mogućih delovanja anti forenzičkih aktivnosti. Jer kako izraz, anti forenzičke aktivnosti, mnogima deluje i šalje sliku o određenim softverima, alatima za uklanjanje dokaza kao i raznoraznim postupcima brisanja fajlova, nije samo vezano za anti forenziku, ovaj primer zombiranja računara, kao što je u ovom opitu zombirana virtuelna mašina, vrši obmanu ne samo korisnika čiji je računar zombiran nego i obmanu digitalnog forenzičara.



Slika58. Putanja do fajla eicar.zip

Slika58 prikazuje celu putanju do fajla eicar.zip kao i vreme kada je fajl kreiran na destinacionom računaru. Vidi se informacija da je fajl kompresovan i da nije bilo uticaja na promenu potpisa ekstenzije tog fajla. U ovom slučaju deluje jednostavna putanja jer je folder u kome je fajl eicar.zip na desktopu operativnog sistema Microsoft Windows 7 koji je destinacioni računar, ali zbog opita zombiranja virtuelnog računara nije bila bitna nota zavlačenja fajla i menjanja potpisa ekstenzije jer to nije poenta, već da se vide vremena kreiranja i uporedi sa podatkom iz pred istrage, kako bi se tretirao onaj koji je fajl kopirao na destinacionu virtuelnu mašinu sa IP adresom 192.168.99.50.

Na sledećoj slici izvršiće se upoređivanje pred istražnih radnji i praćenja mrežne komunikacije između dva računara i dokazi koji su zabeležili delovanje anti virusnog softvera *Symantec*.

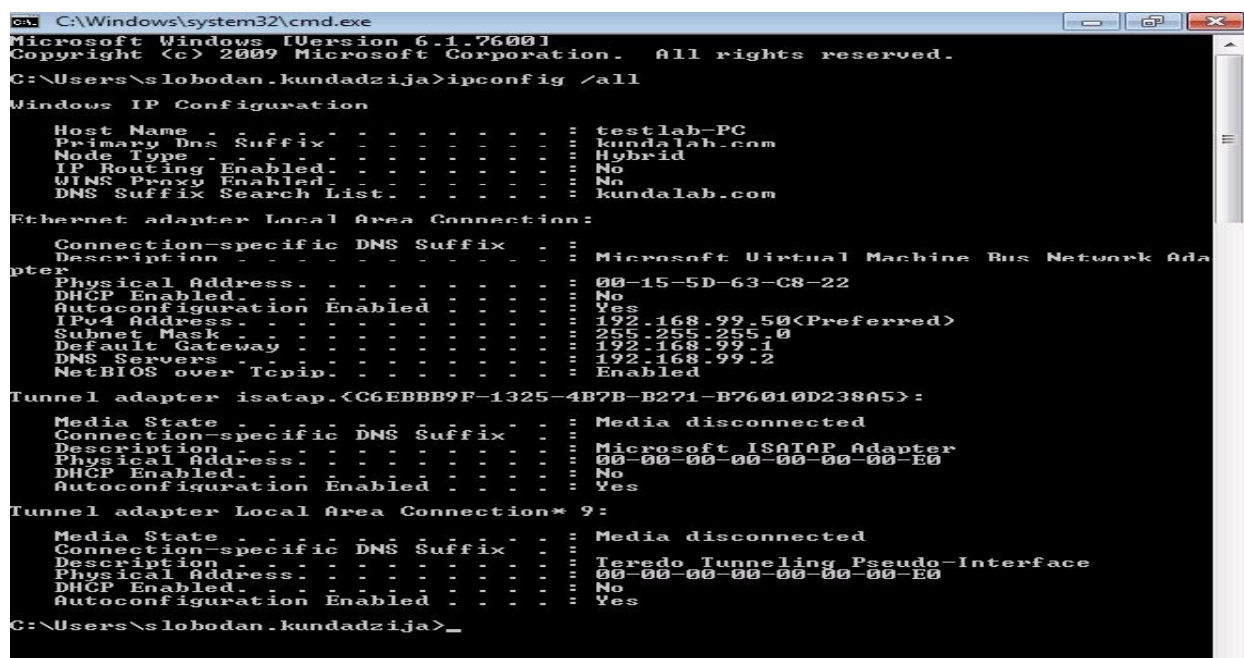


Slika59. Zabeleženo zatvaranje zahteva kopiranja fajla eicar.zip

Slika59 prikazuje da se pred istražne radnje praćenja komunikacije između dva računara poklapaju sa izvršenim incidentom kopiranja fajla eicar.zip. Dobijene su informacije kada se konekcija i korišćenje protokola između dva računara završilo i upoređene sa delovanjem antivirusnog softvera na destinacionoj virtuelnoj mašini koja je napadnuta od strane izvora sa IP adresom 192.168.99.118, što se može i videti na slici. Prozor koji je u donjem uglu slike, Slika59, je deo anti virusnog softvera Symantec, a on prikazuje da ovaj anti virusni softver može da izvrši i ulogu fajervola. Informaciju koju nudi, treba iskoristiti, jer ta informacija govori da korisnik koji je izvorni računar, ima jedinstvenu MAC adresu po kojoj može biti praćen i dalje.

Vidi se i protokol preko koga se kopiranje fajla eicar.zip ostvarilo sa izvornog na destinacioni računar.

Media Access Control address (MAC address) je adresa koja ima ulogu da bude jedinstveni identifikator za određeni mrežni adapter. Može se koristiti u brojnim mrežnim tehnologijama, a najčešće se koristi u tehnologiji IEEE 802. Inženjeri instituta IEEE određuju pravila o dodeli karaktera za MAC adrese. Pravila mogu biti MAC-48, EUI-48 i EUI-64. MAC adrese se uglavnom dodeljuju od strane proizvođača koji ih hardverski upisuju u mrežni adapter. Kada ih dodeli proizvođač dužan je da čuva informacije o njima i moguće je kontaktirati ga radi dobijanja tih informacija. Ali pošto se tehnologija razvija brzo ali i korporacijske procene za jeftinom radnom snagom i slabijim kvalitetom robe koju proizvode, uticalo je i na segment pravljenja mrežnih adaptera. Tako da je sada zbog masovne proizvodnje moguće kupiti adapter za manje od dolara i sa softverske strane dodeliti mu i MAC adresu. To otvara novu mogućnost anti forenzičkog delovanja i dozvoljava osumnjičenom da menja adresu i informacije. Što opet može dovesti u zabludu digitalnog forenzičara ako predhodno nije prikupio informacije o incidentu koji istražuje. Isto važi i za virtuelne mrežne adaptore kojima se mogu menjati softverskim putem MAC adrese. Ovo je još jedna od mogućih zloupotreba i obmanama od strane lica koji su okrenuti protiv lica pravde.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\slobodan.kundadzija>ipconfig /all

Windows IP Configuration

Host Name . . . . . : testlab-PC
Primary Dns Suffix . . . . . : kundalab.com
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : kundalab.com

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Virtual Machine Bus Network Adapter
Physical Address. . . . . : 00-15-5D-63-C8-22
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.99.50(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.99.1
DNS Servers . . . . . : 192.168.99.2
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{C6EBBB9F-1325-4B7B-B271-B76010D238A5}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Local Area Connection* 9:

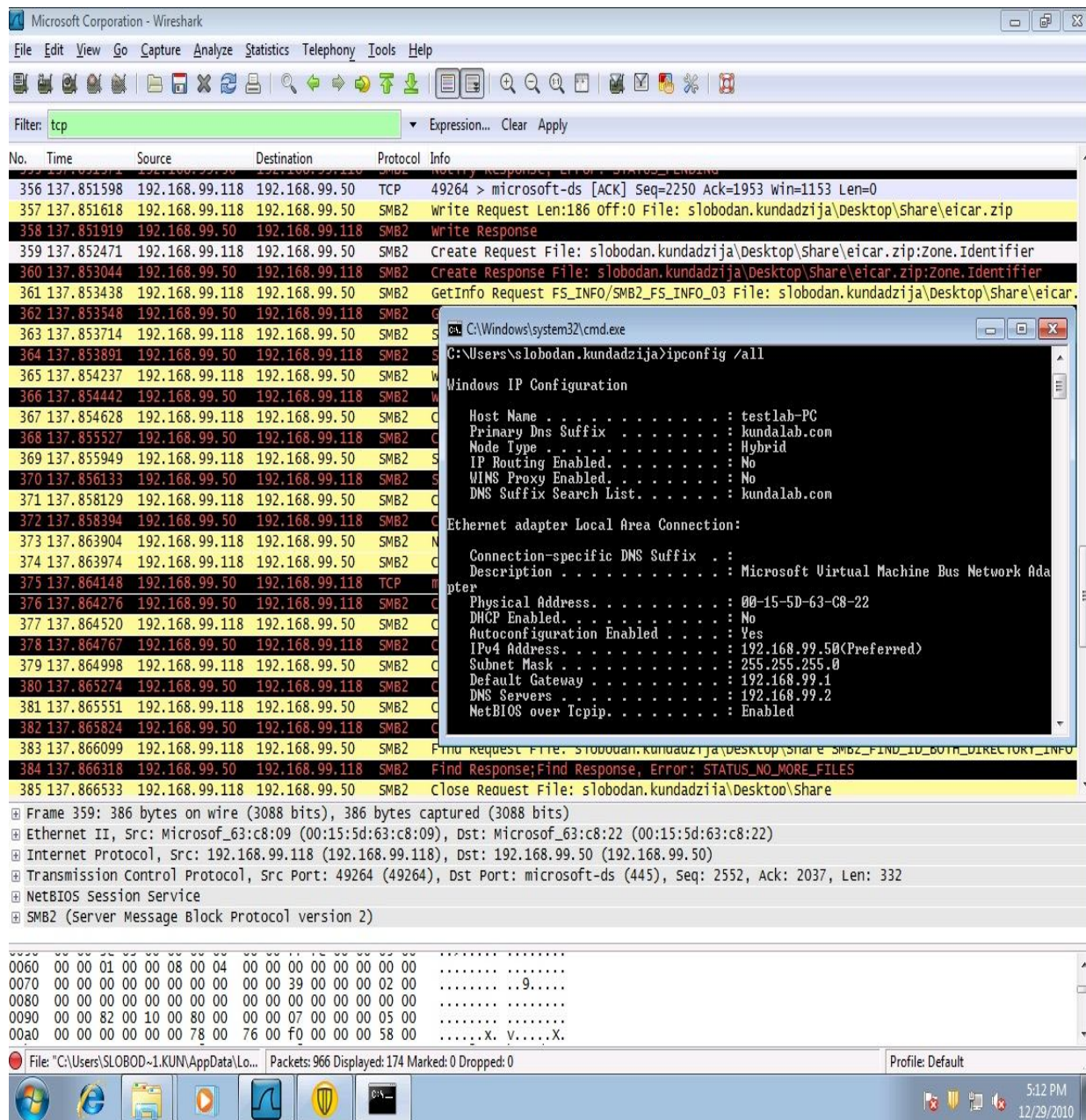
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes

C:\Users\slobodan.kundadzija>
```

Slika60. Komandna linija

Sa slike, Slika60, mogu se videti sledeće informacije koje su vezane za korisnika koji je u ovom opitu žrtva iliti destinacioni virtuelni računar. Do informacija iz komandne linije se dolazi kada u Start meniju unesemo naredbu cmd i tada će se otvoriti komandna linija. Potom se unosi naredba *ipconfig/all* i dobiće se listing informacija kao na slici. Od informacija na raspolaganju su imenu računara, kome DNS-u pripada, o kojem mrežnom adapteru je reč. Vidi se da se radi o virtuelnom mrežnom adapteru. Dalje se mogu videti MAC adresa i uporediti je sa pred istražnim

radnjama sa forenzičkim alatom *Wireshark* kao jedan od dokaza. Mogu se još videti informacije o IP adresi, difoltnom gejtvju.

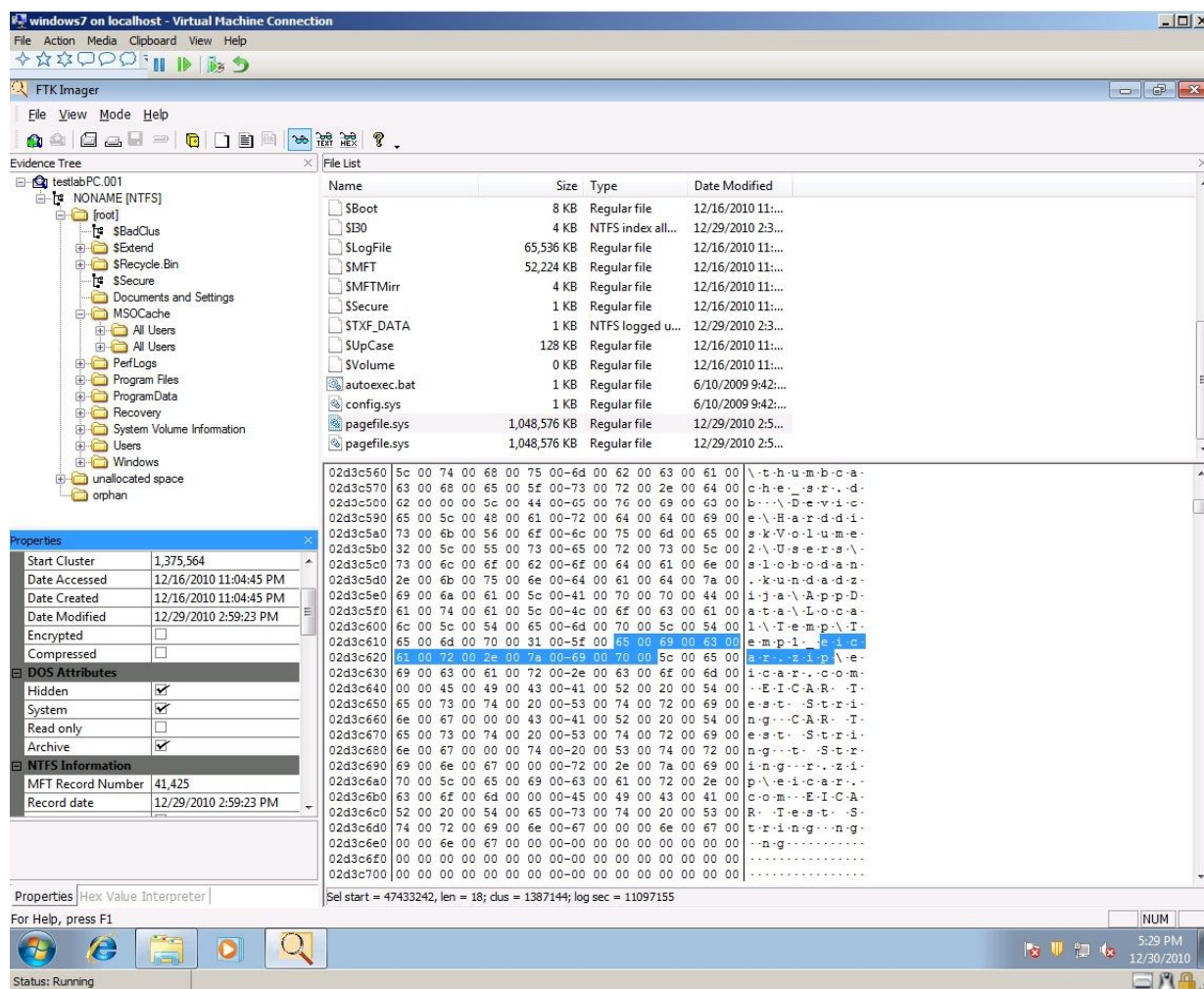


Slika61. Poređenje IP i MAC adresa izvornog i destinacionog računara

Na slici, Slika61, vide se informacije o IP i MAC adresama izvornog i destinacionog računara koji su imali uspostavljenu konekciju za kopiranje fajla eicar.zip. Komandna linija pokazuje informacije o računaru na koji je fajl eicar.zip kopiran i koji je zloupotrebljen, kao i MAC adresu u poređenju sa forenzičkim alatom *Wireshark*. U donjem delu slike moguće je videti MAC

adresu računara koji je izvorni i koji je zahtevao prvi konekciju preko protokola za kopiranje fajla, ali i IP adresu što se može uporediti sa slikom, Slika59, gde je fajervol od antivirusnog softvera Symantec uhvatio i zabeležio MAC adresu izvornog računara i uporediti je kao dokazni materijal. Ali uz oprez, da ne dođe do anti forenzičkog delovanja na virtuelni adapter i promenu MAC adrese.

Kako bi slučaj imao još jedan čvrsti dokaz da je destinaciona virtuelna mašina zloupotrebljena od strane trećeg lica, primenjen je forenzički alat za pravljenje slike *hard disc-a*. Bitno je napraviti sliku *hard disc-a* bit po bit kako bi pred sudskim organom dokaz bio ne oboriv. Sledeća slika pokazuje delovanje forenzičkog alata i uzimanje slike *hard disc-a*.



Slika62. Forenzički alat FTKImager

Slika62 prikazuje delovanje forenzičkim alatom na destinacionu virtuelnu mašinu radi skupljanja informacija sa *hard disc-a* bit po bit kako bi pred organima suda digitalni forenzičar imao čvrst dokaz. Ako se uporedi dokaz bita sa slike, Slika62, sa slikom, Slika54, i vidi se bitski raspored potpisanog fajla eicar.zip, može se dokazati da je na računaru sada stvarno fajl koji je uhvaćen u procesu kopiranja. Proces kopiranja je počeo od izvorišnog računara IP adrese 192.168.99.118 na

destinacioni virtuelni računar 192.168.99.50, sa tačnom lokacijom i vremenom, kao i sa vremenskim periodom i završetkom konekcije. Uporedi će se pred istražna aktivnost digitalnog forenzičara uz pomoć forenzičkog alata *Wireshark* i aktivnost na računaru koji je prvobitno moglo se reći bio osumnjičen a potom se dokazalo da je ipak zombiran. Istraga se dalje prenosi na sada osumnjičeni računar koji je u prethodnom tekstu nazvan kao izvorni.

Sve informacije treba prikupiti, zabeležiti i voditi istragu veoma pažljivo sa ocenom ko je sumnjiv za incident koji se dogodio. Jer digitalni forenzičar ako nastavi istragu na sledeći računar, niko mu ne garantuje da i taj računar nije zombiran i da se sa njim vrše određene ne zakonite radnje. Tako da se može reći da nekada i jaka mašta kao i određena vizija mogu da pomognu u pravcu delovanja istrage, ali ne uvek. Mora se delovati brzo ali i pravično kako se ne bi desilo da hakeri ili ljudi sa druge strane pravde ne uklone dokaze koje im omogućava sam operativni sistem čak bez delovanja anti forenzičkih alata.

3.3. Studija slučaja 3: kloniranje

Kloniranje operativnog sistema omogućava korisniku da vrati svoj operativni sistem na stanje početka, tačnije u onoj trenutak kada je klon operativnog sistema i napravljen. Ova aktivnost može pozitivno uticati na legalan rad korisnika u virtuelnom ili klasičnom mrežnom okruženju ili samo na mašini koju korisnik koristi, ali isto tako može imati ulogu uklanjanje dokaza sa mašine. Inače svako kloniranje se odvija na način kopiranja bit po bit i takvo se čuva na nekom *hard disc-u* ili DVD-u.

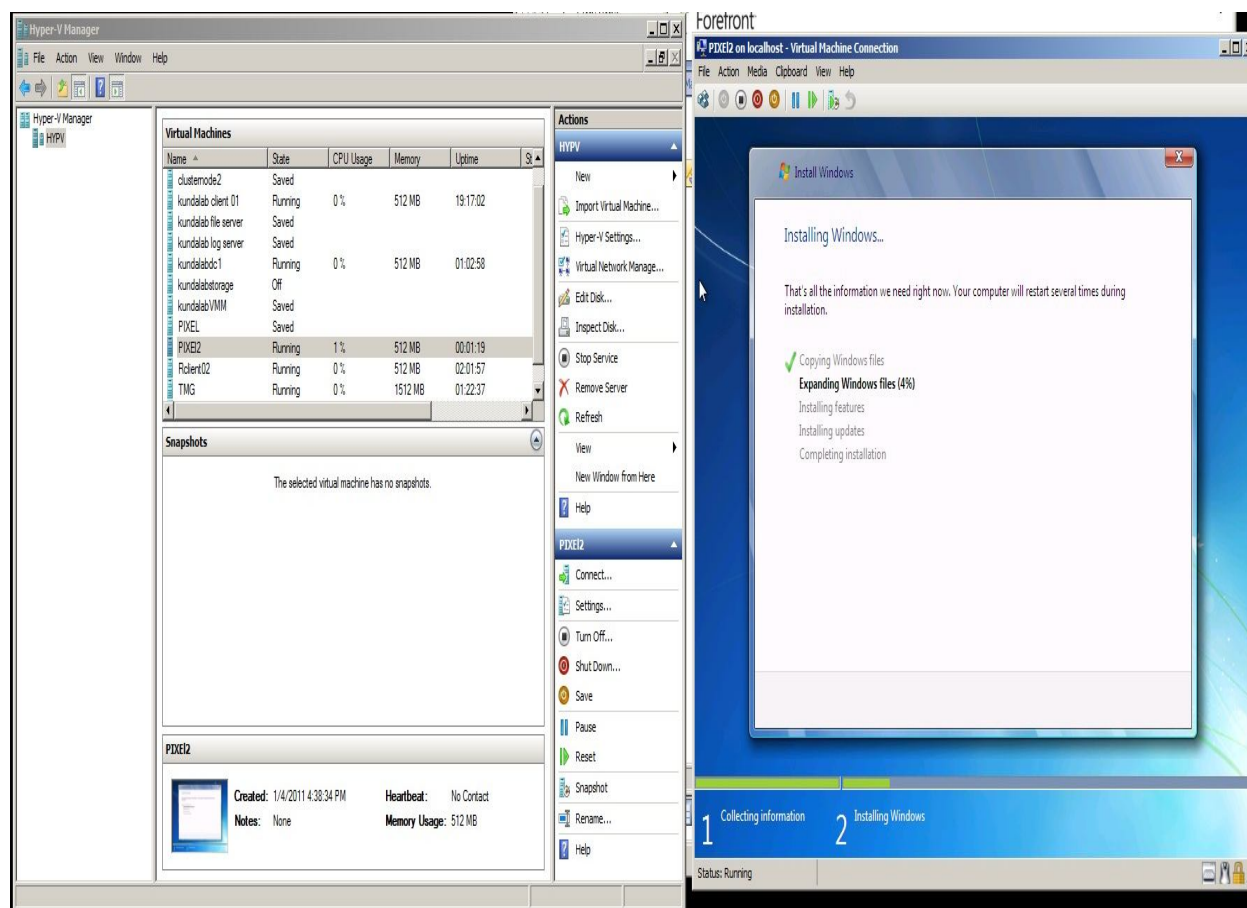
3.3.1. Anti forenzičko delovanje kloniranja operativnog sistema

Kao što je u prethodnim poglavljima ovoga rada rečeno, anti forenzičke aktivnosti mogu da se sprovedu i preko korišćenja mogućnosti koje se dobijaju od procesa koji su legalni i stvoreni da pomognu lakše operisanje i manipulisanje sa fajlovima, folderima a nekada i sa celokupnim operativnim sistemom. Jedna od mogućnosti je i kloniranje operativnog sistema. Kloniranje operativnog sistema nudi opciju koja omogućava korisniku ili administratoru da kada jednom instalira na *host* ili *child* operativni sistem i prateće drajvere kao i programe i aplikacije koji obezbeđuju korektan rad mašine, smesti kopiju takvog operativnog sistema na određenu lokaciju koja može biti neki prenosni *hard disc* ili *DVD disc*, i kao takvog ga čuva. Kada dođe do problema u operisanju operativnog sistema, postoji mogućnost vraćanja originalne iliti prve dobre verzije, koja je sačuvana kako je pomenuto malo pre, i to u veoma kratkom vremenskom periodu od par minuta. Kaže se kratkog vremenskom periodu, jer određeni alati za brisanje i uklanjanje podataka ili dokaza, nekada moraju da rade na živom operativnom sistemu i do deset, dvadeset a nekada čak i do trideset minuta, a da pri tom obrišu samo određene zapise koji se mogu smatrati dokazima, ali ne i sve fajlove i dokumenta. Zato se u ovom radu obrađuje i ova oblast kloniranja operativnog sistema, koji se može vratiti na isti računar za svega nekoliko minuta. Ovo je jedna od mogućih anti forenzičkih dejstvovanja na uklanjanje dokaza koji mogu biti usmereni protiv osumnjičenog lica a koji želi da te dokaze i ukloni. Ono što je bolje od anti forenzičkih alata, kod kloniranja operativnog sistema i njegovog vraćanja na mašinu, je

moгуćnost da klonirani operativni sistem koji se vraća na mašinu a koji je u obliku imidža, vrši kopiranje originalne verzije bit po bit i takvu je i vraća na mašinu. Iz ovog ugla deluje da ako osumnjičeni uradi ovakvu operaciju vraćanja klona operativnog sistema na mašinu, celokupna particija sa dokazima na kojoj je bio sistem biće prepisana originalnom verzijom i tada će sve stare informacije biti izbrisane, a postavljene nove sa originalnog operativnog sistema. Ako se ovako sagledaju stvari deluje logično da se radi o odličnoj anti forenzičkoj zamci za digitalnog forenzičara. Ali pošto savršeni zločin ne postoji i uvek se nađe bar i najmanji trag koji može da otkrije određenu ne zakonitu radnju od strane osumnjičenog, tako i ovaj slučaj kloniranja operativnog sistema na virtuelnu mašinu za sobom ostavlja određene dokaze, repove incidenta koji se dogodio.

Sproveden je još jedan opit u ovom radu, koji pokazuje takve tvrdnje, da ostaju dokazi i ako se kopiranje izvrši bit po bit.

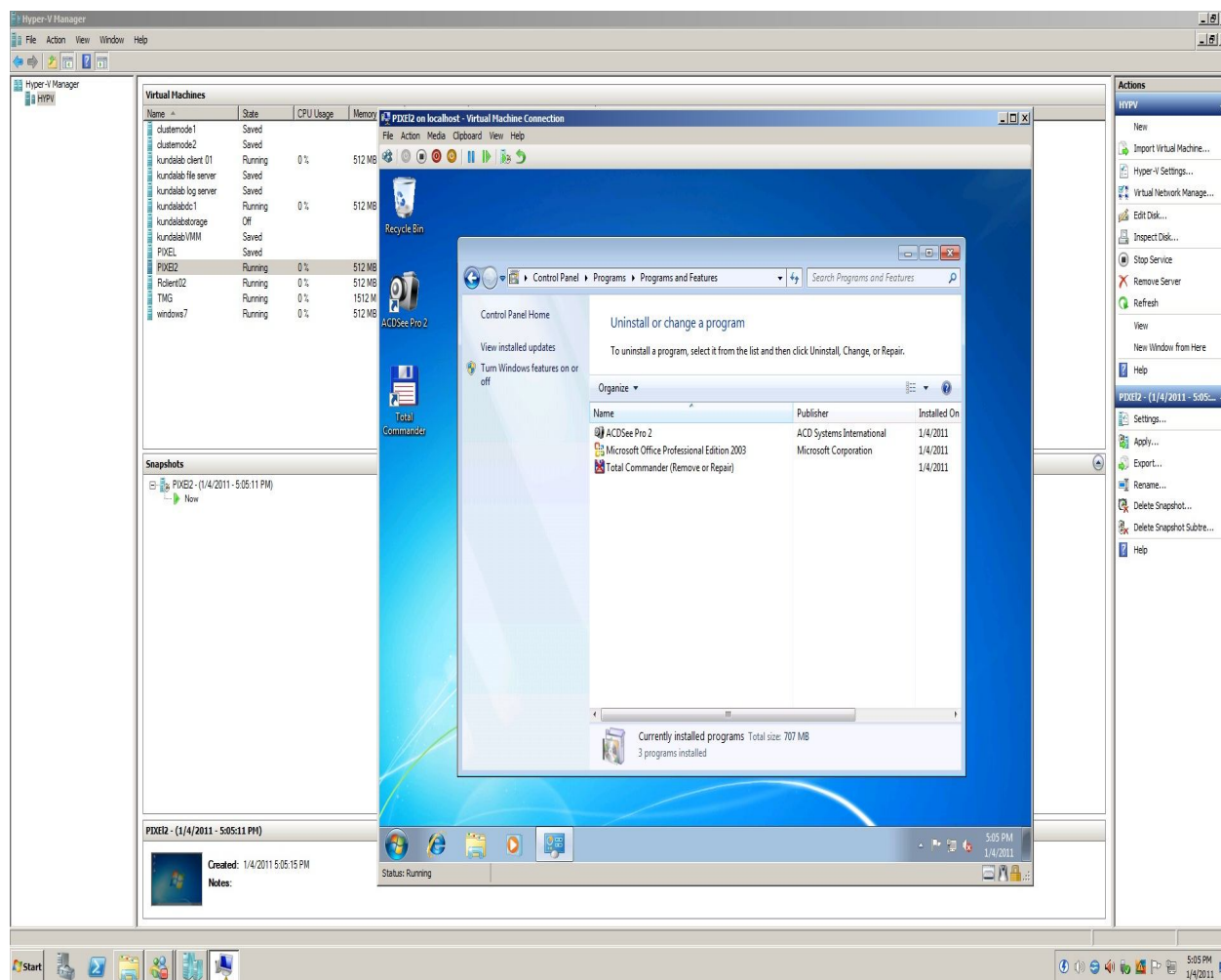
Prvo se stupilo u pravljenje virtuelne mašine, tako što je izabran odgovarajući hardver. Pošto je ubačen instalacioni disc operativnog sistema Microsoft Windows 7 i krenulo u proces instaliranja. Kao što se može videti na sledećoj slici.



Slika63. Proces instalacije operativnog sistema na virtuelnu mašinu

Slika63 prikazuje proces instalacije operativnog sistema Microsoft Windows 7, na virtuelnu mašinu, koja koristi 512Mb RAM memorije sa *host-a* i koja je u procesu rada tek nekih minut

vremena. Vidi se i informacija koje je ime virtuelne mašine, a ime joj je Pixel2. Sa desne strane slike, Slika63, vidi se proces instaliranja operativnog sistema, tačnije kopiranje fajlova operativnog sistema na *hard disc* virtuelne mašine. Ono što se ne vidi na slici, a podešeno je u konfigurisanju hardvera virtuelne mašine Pixel2 je da je veličina VHD-a 15GB. Bitno je napomenuti da se operativni sistema prvi put instalira na virtuelnu mašinu Pixel2 čiji je VHD prvi put kreiran. Znači, pre nije postojala niti je bila kreirana ni virtuelna mašina, niti VHD.

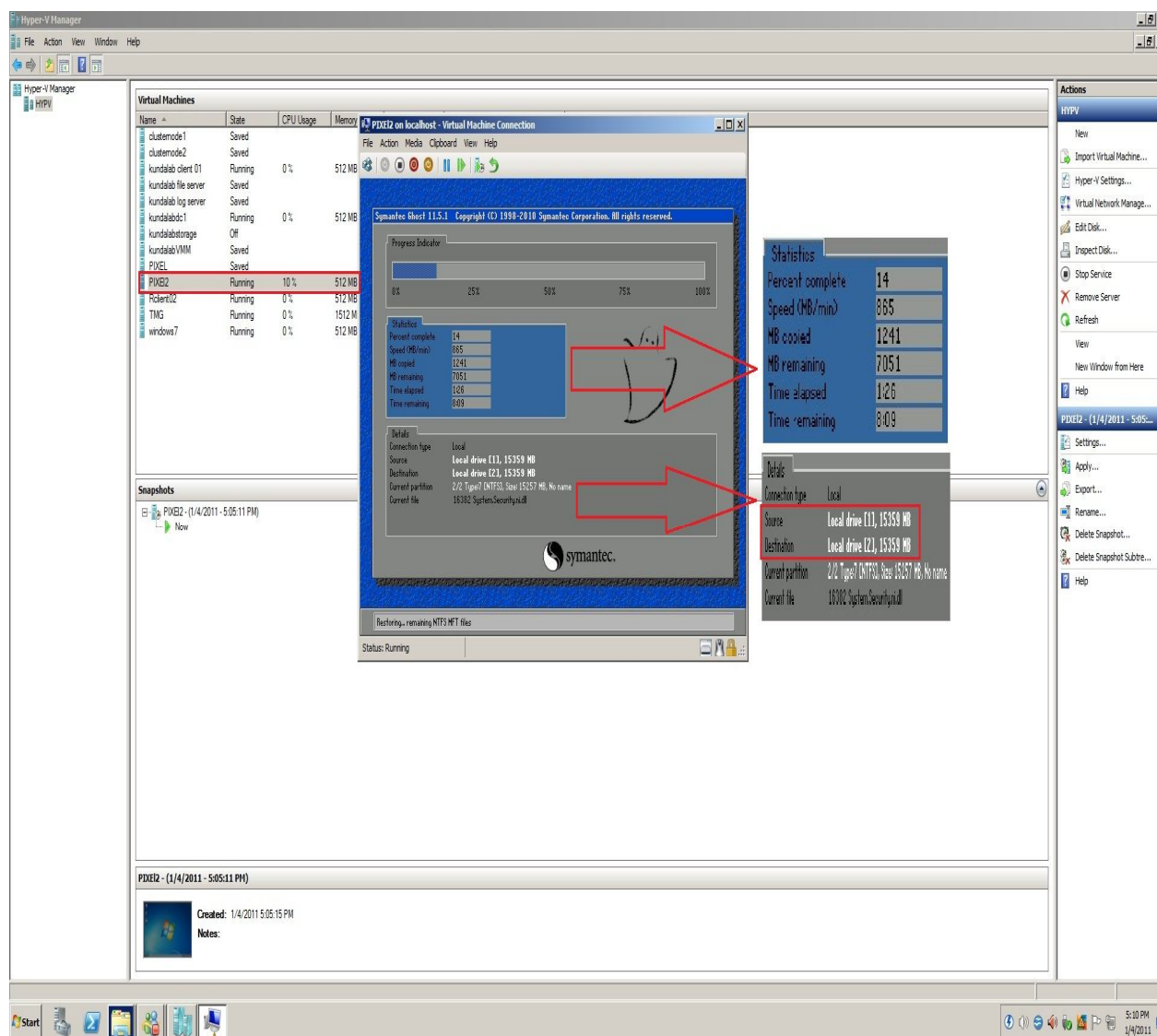


Slika64. Instalirane aplikacije na virtuelnoj mašini Pixel2

Kada se instalacija operativnog sistema završila, pristupilo se instaliranju odgovarajućih aplikacija koje su potrebne za svakodnevno korišćenje virtuelne mašine. Te aplikacije se mogu videti na slici, Slika64, a to su *Microsoft Office 2003* paket, jer korisnik ima potrebe da koristi *Outlook 2003* zbog *e-mail* pošte, *Word* i *Excel* za unos podataka u dokumente i određene obračune. Instalirane su još i aplikacije za manipulaciju sa slikama, kao i aplikacija za jednostavno nadgledanje i operisanje sa fajlovima i folderima. Smatrano je da su ove osnovne aplikacije dovoljne za korektan rad, a po potrebi uvek se može instalirati i veći broj aplikacija ako je korisniku potrebno. Podešeni su i provereni sve drajveri pre instaliranja aplikacija, i stanje

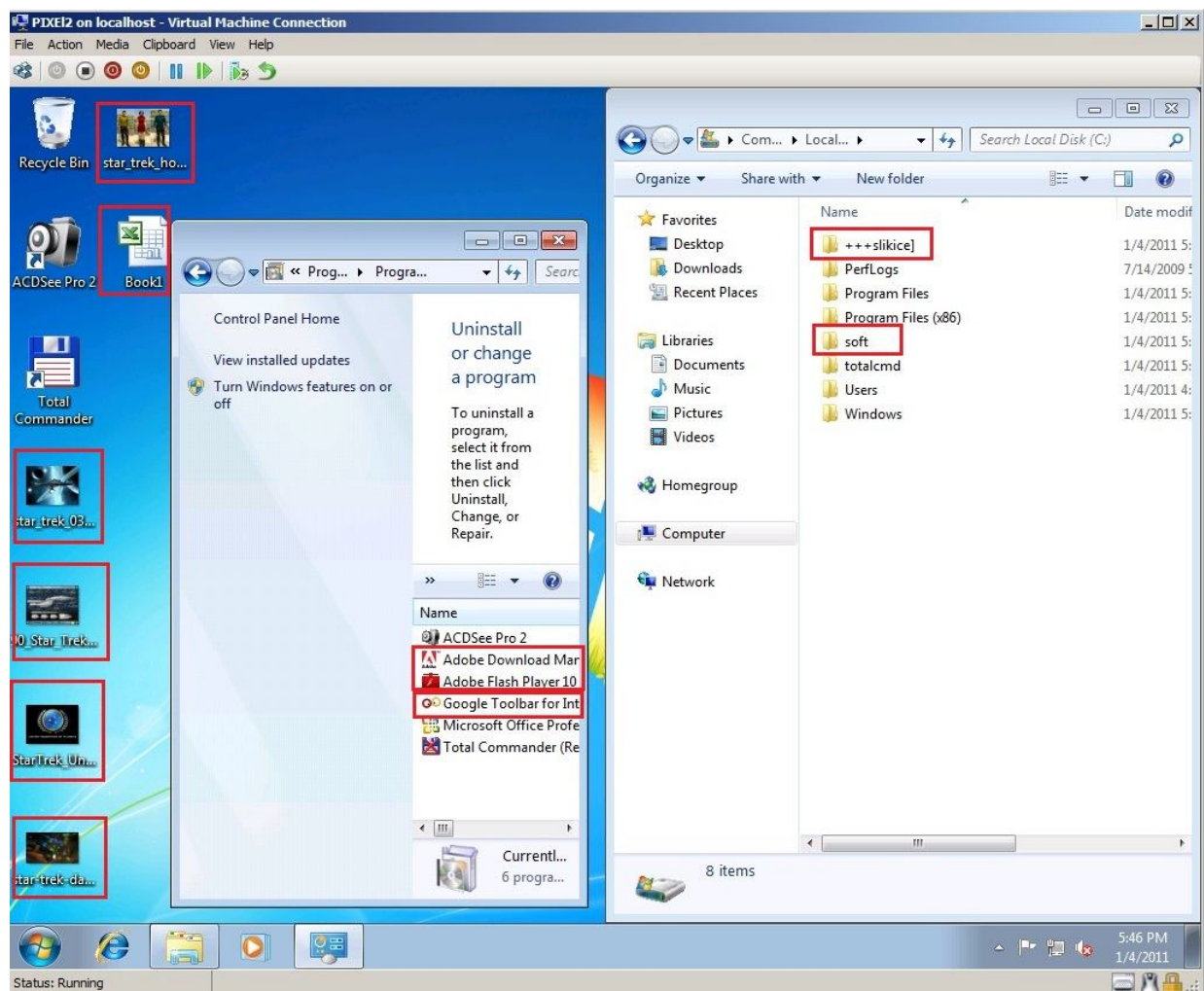
je bilo korektno. Podešena je i internet konekcija, kao i sva setovanja tokom instalacije koja su vezana za region i jezik u kome se virtuelna mašina koristi.

Ovakav operativni sistem može se smatrati korektnim i može se upotrebiti i kopirati kao klon. Jer ako dođe do određenih problema u daljem radu operativnog sistema na virtuelnoj mašini Pixel2, a da se ne bi radila celokupna ponovna instalacija ili popravka operativnog sistema, a te su opcije ponuđene kod pokretanja instalacionog diska, pravi se klon. Instalacija i popravka operativnog sistema trajaće nekada i do dvadeset i pet minuta, a nekada manje, mada češće i duže u zavisnosti o kakvoj konfiguraciji hardvera virtuelne mašine je reč. Zato pravljenje klona ovog operativnog sistema može da obezbedi brže osposobljavanje virtuelne mašine za rad sa povratkom napravljenog klona.



Slika65. Pravljenje klona operativnog sistema

Slika65 prikazuje alat za pravljenje klona operativnog sistema na virtuelnoj mašini, koji kopira bit po bit operativnog sistema na određenu lokaciju koja može biti neki prenosni *hard disc*. Taj *hard disc* koji prima imidž klona na sebi mora imati dovoljnu veličinu da celokupan imidž smesti na sebe. Sa slike se može uočiti i da se procesorsko zauzeće povećalo tokom operacija pravljenja klona. Mogu se videti još i informacije o brzini prepisivanja klona, kao i o lokaciji sa koje se prepisuje, tačnije izvorna lokacija i lokacija koja će biti destinaciona. Mogu se videti i veličine klona koji se kopira sa izvora i kolika će veličina klona biti na destinaciji. Isto su pokazana i vremena koja objašnjavaju koliko je prošlo od početka operacije, i koliko je ostalo do kraja operacije kloniranja operativnog sistema.

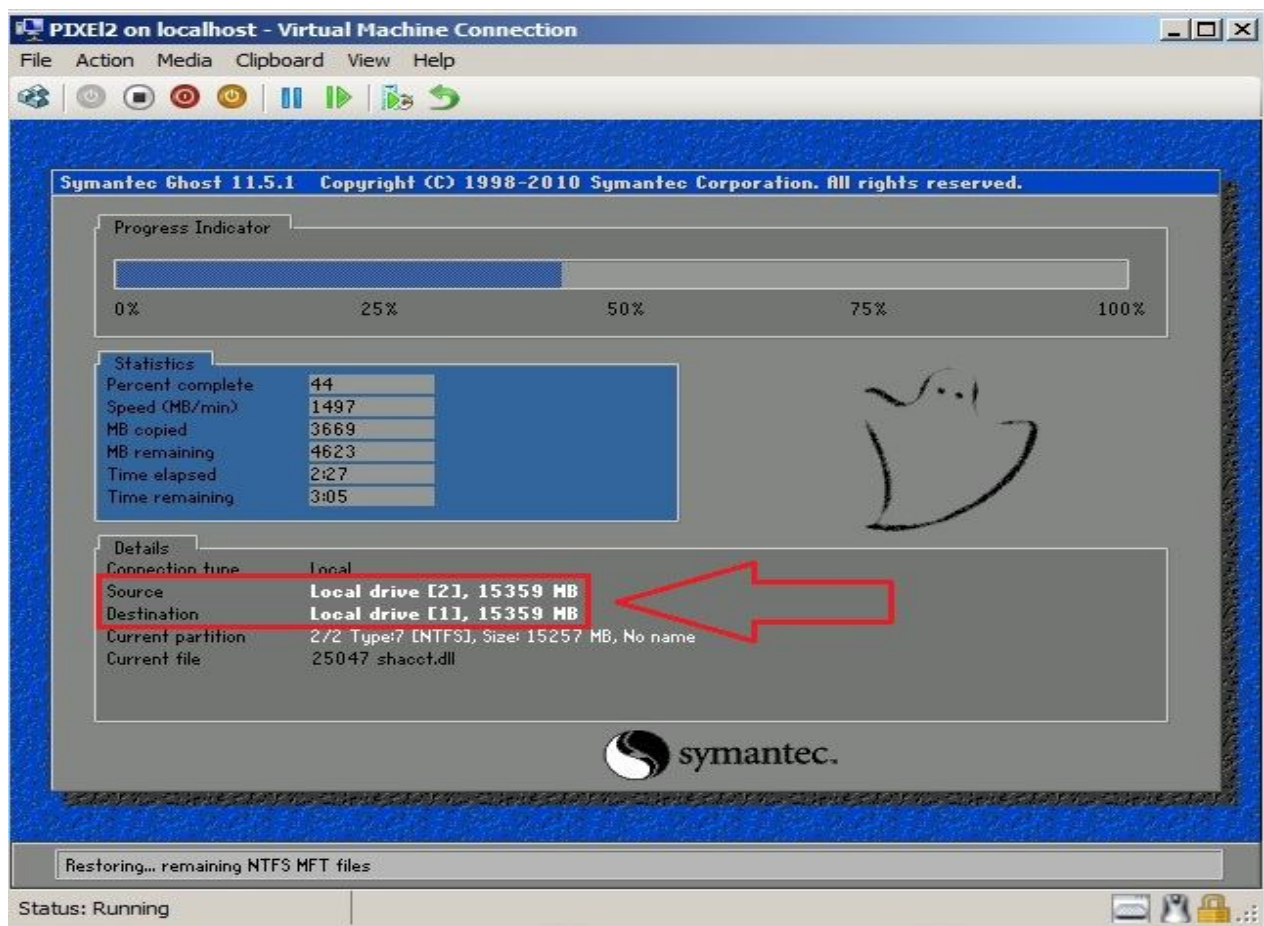


Slika66. Preuzeta dokumenta kao i instalirane aplikacije sa Interneta

Posle određenog vremena od završetka kloniranja operativnog sistema Microsoft Windows 7 na virtuelnu mašinu Pixel2, korisnik je mašinu startovao i sa njom vršio određene operacije instaliranja, surfovanja na Internetu, preuzimanja sadržaja sa Web stranica. Sve te informacije prikazane su na slici, Slika66. Vidi se da je korisnik preuzeo određene slike i stavio ih na desktop operativnog sistema, da je instalirao još tri aplikacije, kao i da je kreirao dva foldera u *root-u* C

particije operativnog sistema i u njih smestio određena dokumenta. Sada se može pretpostaviti da je korisnik Pixel2 virtuelne mašine osumnjičena osoba koja je uradila određene ne zakonite radnje. Preuzimala je sadržaj sa Web stranica koji nije zakonit, instalirala određene aplikacije koje mogu biti primera radi, aplikacije za napad kroz mrežu ili neki anti forenzički alati. Kreirao je foldere i u njih smeštao određen sadržaj na primer slika dečije pornografije.

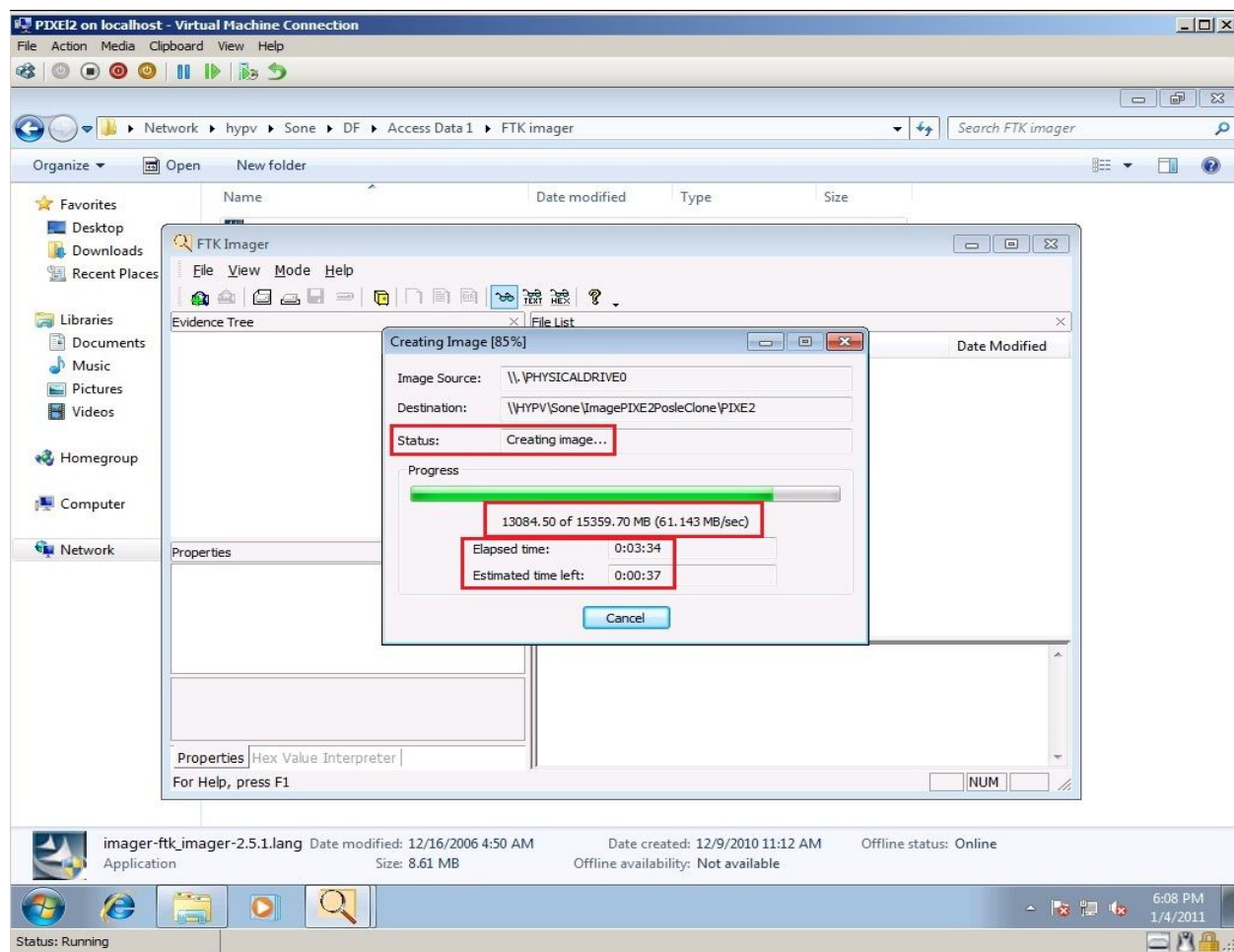
I sada ako bi se osumnjičeni korisnik osetio da je praćen od strane istražnih organa i pretpostavio mogućnost upada na njegovu lokaciju i istragu virtuelne mašine ili čak celokupnog *host-a*, morao bi da sprovede određene anti forenzičke radnje. Ali ako pokrene neki anti forenzički alat, sa operativnog sistema bi mu bilo izbrisano skoro sve vezano za njegovo poslednje delovanje na operativni sistem, kao i njegovo delovanje na Internet i konekcije, ali ostale bi slike, folderi i dokumenta koje je kreirao. Ako obriše i foldere, slike i dokumenta, a ako je dovoljno edukovan pretpostaviće da mu je najbolje rešenje da umesto starog i korišćenog operativnog sistema prepíše novi čiju je kopiju napravio pre nekog vremena, tačnije upotrebiće klon. Jer klon prepisuje celokupnu particiju starog sistema bit po bit sa novim sistemom, a pošto se uglavnom sve bitne stvari vezane za čuvanje podataka o delovanju korisnika čuvaju na particiji operativnog sistema, pokrenuće klon koji je napravio i prepisati sve dokaze novim operativnim sistemom.



Slika67. Vraćanje klona na virtuelnu mašinu Pixel2

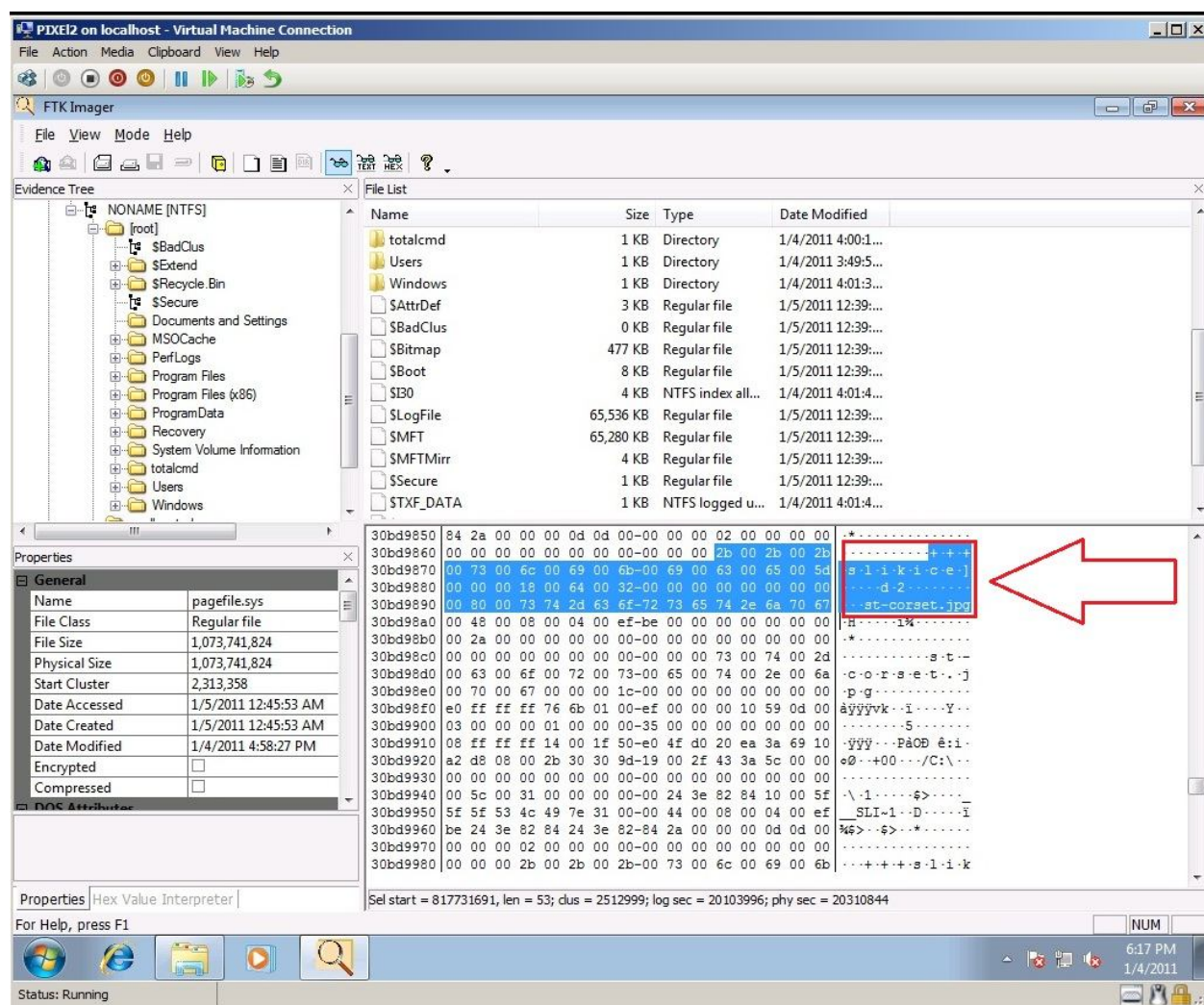
Slika67 pokazuje da je osumnjičeni korisnik pribegao uklanjanju dokaza, vraćanjem originalnog operativnog sistema koji je klon, misleći da će klon prepisati bit po bit celokupan operativni sistem koji je okarakterisan kao osumnjičeni i tako ukloniti dokaze. Vidi se sa slike da se sada klon vraća sa *hard disc-a* 2 koji je sada izvor a kada je pravljen bio je odredište, na *hard disc* 1. Na slici se može videti procenat operacije prepisivanja klona na virtuelnu mašinu, kao i tekući fajl koji se prepisuje. Sa slike se još vidi da celokupni vremenski period prepisivanja klona neće trati duže od pet do šest minuta. To vreme je trenutno najbrže uklanjanje dokaza sa operativnog sistema i particije na kojem je operativni sistem. Zato se može smatrati jednim od anti forenzičkih delovanja osumnjičenih lica.

Kada se proces vraćanja klona na virtuelnu mašinu završio, a virtuelna mašina je i nekoliko puta restartovana i osumnjičeni korisnik pomislio da se iz virtuelne RAM memorije uklonili svi dokazi koji mogu da ga terete, tada je nastupio digitalni forenzičar sa forenzičkim alatom *FTKImager*.



Slika68. Delovanje na osumnjičenu virtuelnu mašinu sa forenzičkim alatom

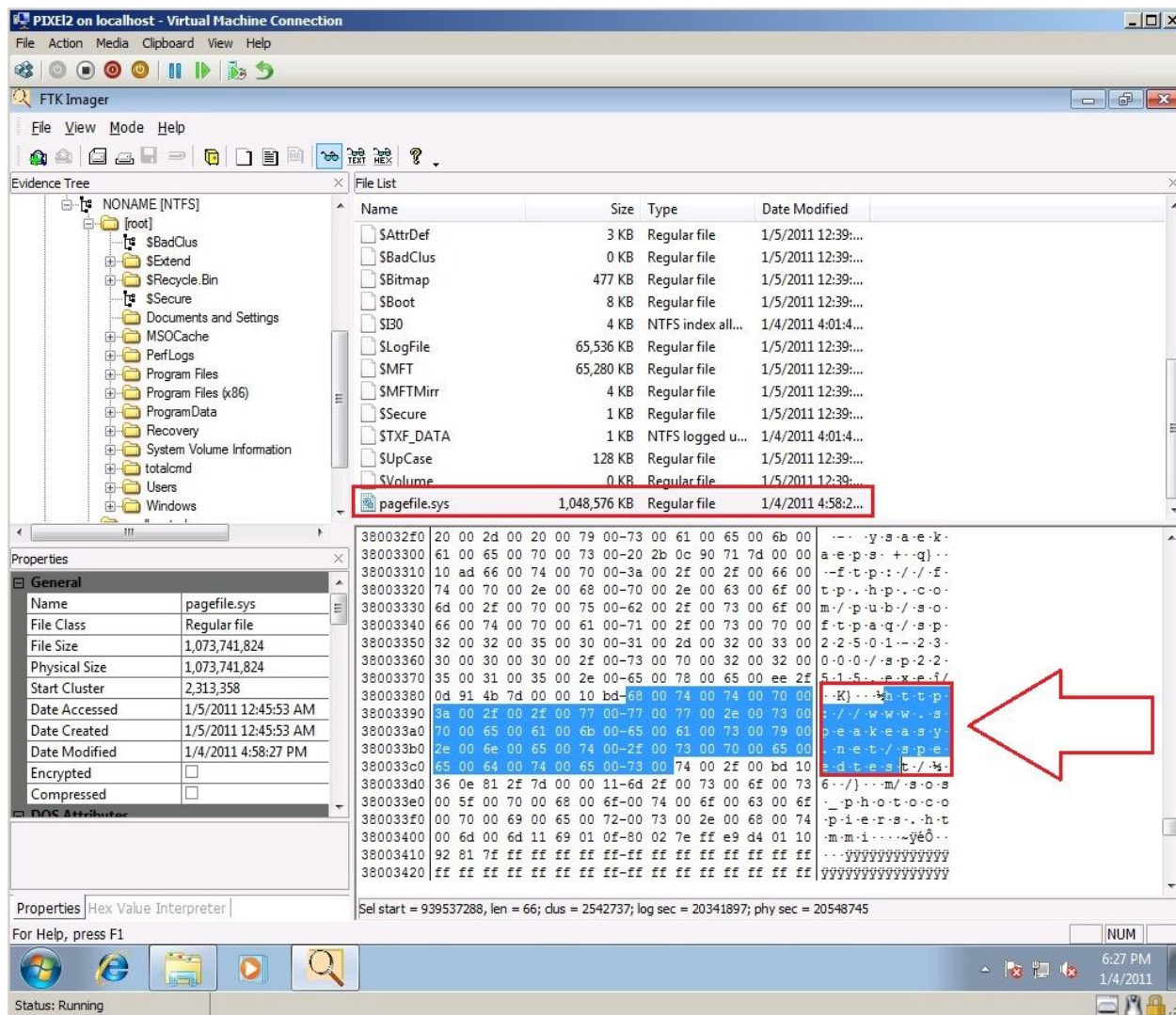
Digitalni forenzičar pokrenuo je istragu sa forenzičkim alatom *FTKImager* i napravio sliku *hard disc-a* osumnjičene virtualne mašine Pixel2, kao što se može videti sa slike, Slika68. Sa slike se vidi status rada forenzičkog alata nad živom virtualnom mašinom koja je predhodno uključena od strane osumnjičenog. Naravno, završen je i klon operativnog sistema. Sadašnje stanje virtualne mašine Pixel2 je isto ono stanje sa početka poglavlja, tačnije opita kada je klon i napravljen. Tako mišljenje ima i osumnjičeni koji je ovu operaciju sproveo zbog anti forenzičkog delovanja na uklanjanje dokaza sa svoje osumnjičene virtualne mašine. Slika pokazuje i veličinu *hard disc-a* virtualne mašine, ali i vreme za koje će se slika *hard disc-a* napraviti na forenzičkoj radnoj stanici, na kojoj će digitalni forenzičar dalje sprovoditi istragu.



Slika69. Istraga digitalnog forenzičara nad virtualnom mašinom Pixel2

Kada se preuzimanje slike *hard disc-a* završilo sa forenzičkim alatom i kada je taj imidž učitao u forenzički alat *FTKImager*, što se može videti sa slike, Slika69, posle pretrage po *root-u* C particije osumnjičene virtualne mašine, dobili su se podaci za koje je osumnjičeni bio siguran da su izbrisani. Ako uporedimo sliku, Slika66 i vidimo da je osumnjičeni kreirao folder pod

imenom, +++slikice], i to pre celokupnog procesa prepisivanja klona koji je predhodno objašnjen, posle nekoliko restartovanja virtualne mašine, forenzički alat je izvukao ovu informaciju iz fajla, pagefile.sys, kao što se vidi na slici, Slika69. Ova informacija može da potvrdi delovanje osumnjičenog da je kreirao taj folder pre anti forenzičke radnje brisanja starog operativnog sistema i prepisivanja novog operativnog sistema uz pomoć klona. Sledeća slika daje još bitnih informacija izvučenih iz virtualne RAM memorije i fajla pagefile.sys.



Slika70. Forenzički alat FTKImager

Slika70 prikazuje informacije i daje tačnu URL adresu kojoj je osumnjičeni korisnik pristupao pre nego što je izvršio kloniranje operativnog sistema. URL lokacija pokazuje da je posećivao određeni sadržaj Web stranice kojoj digitalni forenzičar može da pride sa svoje radne stanice i proveriti o kakvom se sadržaju radi.

Postoje sve informacije kojima je osumnjičeni korisnik pristupao sa virtualnom mašinom Pixel2 pre operacija kloniranja operativnog sistema i vraćanja virtualne mašine u prvobitno

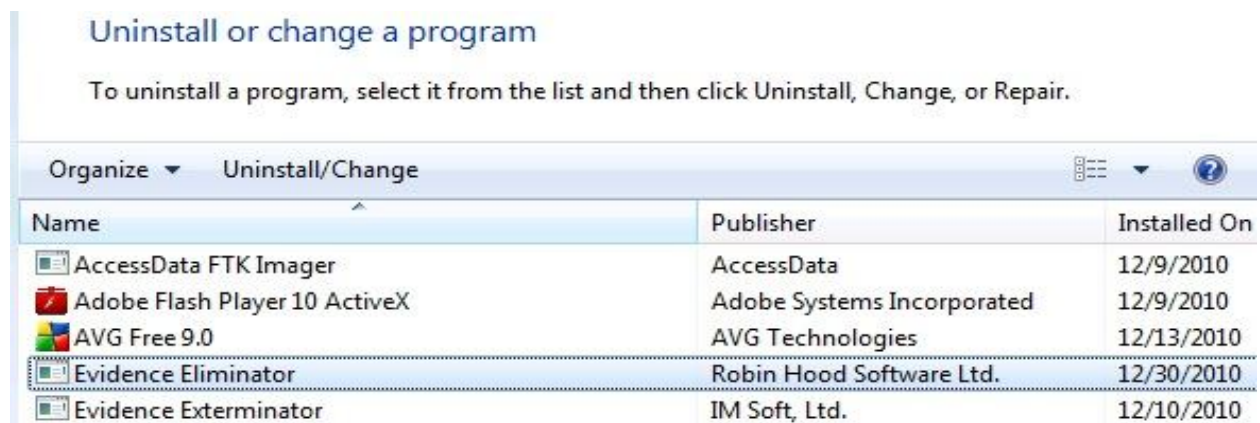
podešavanje. Informacije su pronađene i zna se da je osumnjičeni posećivao određene sadržaje Web stranica, preuzimao slike i dokumenta, kreirao .xml dokument i .doc dokument. Preuzimao je sadržaje sa Web stranica, kao i surfovao po Internetu. Tako da je pokušaj klona prepisivanje bit po bit sakrio i prepisao sve stare informacije novi. Nisu pronađeni ni folderi ni slike, kao i dokumenta na novom operativnom sistemu na virtuelnoj mašini, jer je operacija klon učinila svoje, ali dokazi o delovanju korisnika su ostali u pagefile.sys fajlu i pomogli digitalnom forenzičaru u rasvetljavanju incidenta jedne virtuelne mašine, kao i pokušaja delovanja uklanjanja dokaza.

3.4. Studija slučaja 4: *Evidence Eliminator*

Program *Evidence Eliminator* je antiforenzički alat koji ima ulogu da ukloni dokaze o konekcijama ka Internetu i određenih ali ne i svih radnji korisnika a koje bi mogle biti okarakterisane kao ne zakonite. Program se može preuzeti sa **Web** stranice i može se preuzeti u dve verzije od dva izdavača. Postoji i besplatan program koji ima smanjeni broj opcija u setovanjima samog programa i takav je korišćen u obe verzije od dva izdavača u ovoj studiji slučaja.

3.4.1. Antiforenzičko delovanje na digitalne dokaze sa alatom *Evidence Eliminator*

Program za uklanjanje dokaza, kojeg preporučuje mnogi ljudi iz sveta informatike, a može se lako preuzeti sa Interneta je anti forenzički alat *Evidence Eliminator*. Pošto se ovaj rad bavi mogućim anti forenzički delovanjem u virtuelnom okruženju kojeg pokreće *hyper-V*, a instaliran je na *host-u* čiji je operativni sistem *Microsoft Windows 2008* i klijenti koji su deo *host-a* su virtuelne mašine sa operativnim sistemom *Microsoft Windows 7*, isproban je i ovaj anti forenzički alat.

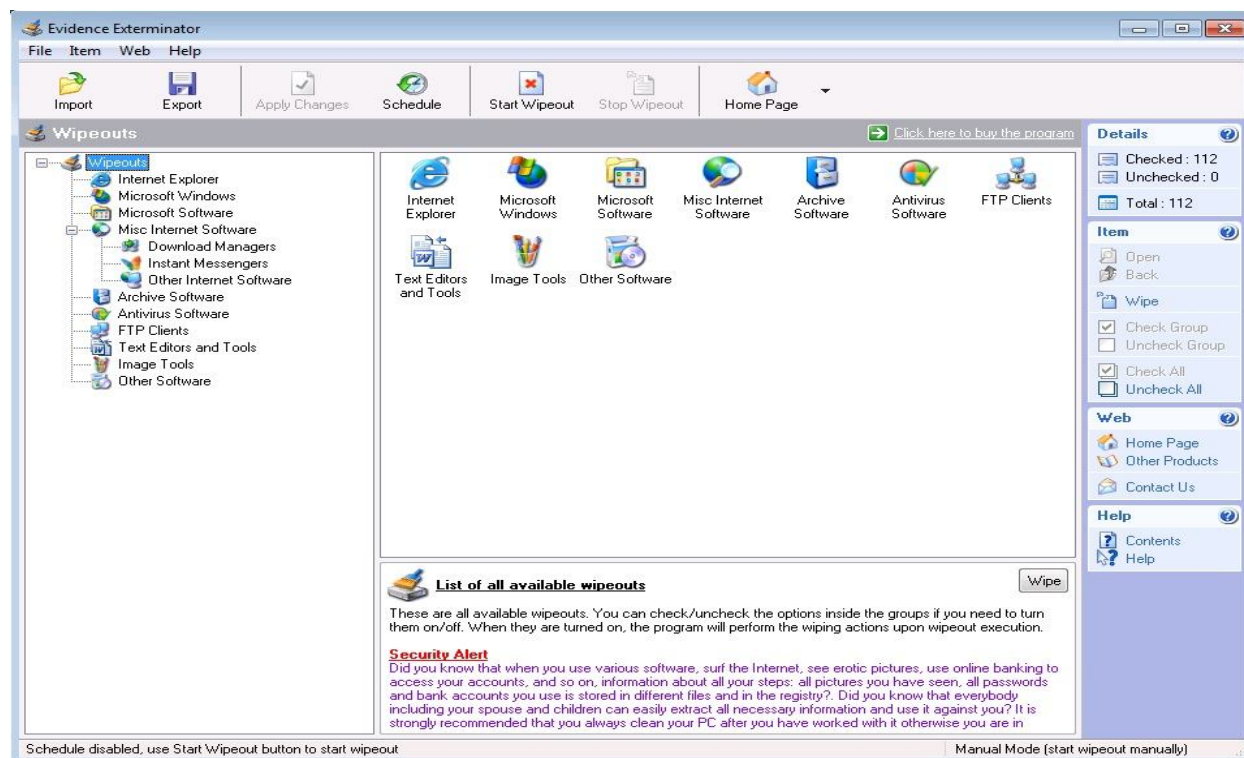


To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.		
Organize ▾ Uninstall/Change		
Name	Publisher	Installed On
 AccessData FTK Imager	AccessData	12/9/2010
 Adobe Flash Player 10 ActiveX	Adobe Systems Incorporated	12/9/2010
 AVG Free 9.0	AVG Technologies	12/13/2010
 Evidence Eliminator	Robin Hood Software Ltd.	12/30/2010
 Evidence Extreminator	IM Soft, Ltd.	12/10/2010

Slika71. Instalirani anti forenzički alat *Evidence Eliminator* na virtuelnoj mašini

Program kada se preuzme sa *Web* stranice i kada se instalira nudi veliki broj informacija koje može da ukloni, a koji mogu biti dokazi i koji mogu da sumnjiče pojedinca ako se pronađu na njegovom računaru. Takvi dokazi se mogu upotrebiti pred sudom i porotom i napraviti problem pojedincu. Zato, mnogi koji se bave ne zakonitim radnjama promenjuju alate koji imaju cilj anti forenzičkog delovanja na svoj računar. Program postoji u dve verzije od dva izdavača a to su *Robin Hood Software Ltd* i *IM Soft Ltd*, kao što je predstavljeno na slici, Slika71. U ovom radu biće opisan alat od IM Soft Ltd izdavača jer slikovitije nudi informacije koje uklanja sa računara korisnika, kada ga ovaj pokrene. Mala je razlika u delovanju druge verzije alata *Evidence Eliminator* od drugog izdavača, a razlika je u tome što briše skoro iste informacije, samo proces brisanja traje pre restartovanja računara dosta duže, nekada može da traje i preko trideset minuta u zavisnosti kolika je sistemska particija i koliko su brzi *hard disc*-ovi na kojima se operacija uklanjanja dokaza sprovodi. Isto je to što da bi uklonili dokaze iz temporari foldera i pagefile.sys koji su vezani za RAM memoriju računara, obe verzije alata zahtevaju od korisnika da restartuje računar. Postoje propusti ako se na lice incidenta dođe pre nego što korisnik restartuje računar i tada će dobar broj dokaza biti spašen, tačnije ovaj anti forenzički alat ih neće ukloniti. To može napraviti problem osumnjičenom, a pomoći digitalnom forenzičaru. U korišćenju oba alata, propust je bila kanta za otpatke koja nije bila obrisana i ako piše na stranici izdavača da je i ona uključena sa ostalim opcijama uklanjanja dokaza. Na kantu za đubre namerno nije delovano sa pražnjenjem od strane korisnika u sprovođenju opita, da se vidi da li će to alat uraditi umesto korisnika ali se to nije desilo.

Slika koja sledi pokazuje broj mogućih informacija koje anti forenzički alat *Evidence Eliminator* treba da ukloni.



Slika72. Evidence Eliminator posle instalacije

Kao što slika, Slika72, pokazuje, vidi se stablo hijerarhije koje ima određene grupacije i podele vezane za operativni sistem Microsoft Windows. Broj dokaza koji treba da se uklone je veoma veliki, bar kako proizvođač kaže. Taj broj se može videti sa slike i nalazi se sa desne gornje strane i iznosi čak 112 izabranih dokumenata. Može se izvršiti izbor svih kao što je na slici i prikazano, ili da se neki dokumenti ne brišu a određeni koje korisnik izabere, brišu. Zanimljivost je da proizvođač govori o uklanjanju dokaza vezanim najviše za Internet Explorer, jer je tome data najveća pažnja zato što se Internet koristi od strane korisnika najviše. Naravno, na Internetu se dešavaju razna dela i ne dela koja mogu da sumnjiče korisnike i odvedu ih pred lice pravde. Zato se ovaj alat nudi na Internetu kako bi se dokazi uklonili.

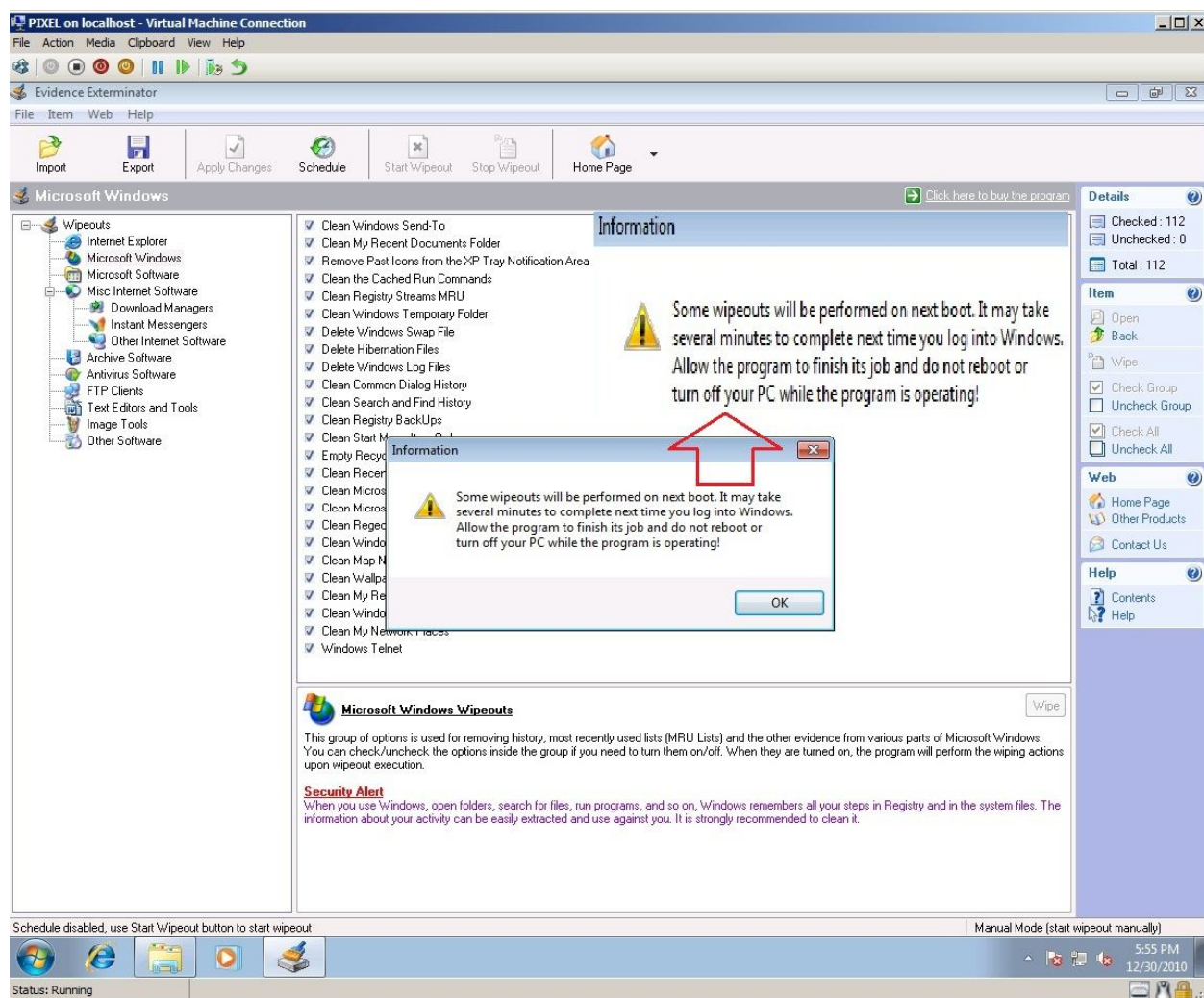
Features

- Windows SWAP file
- Windows Application logs
- Windows Temporary Files
- Windows Recycle Bin
- Windows Registry Backups
- Windows Clipboard Data
- Start Menu Recent Documents history
- Start Menu Run history
- Start Menu Find Files History
- Start Menu Find Computer History
- Start Menu Order Data
- Start Menu Click History
- Microsoft Internet Explorer temporary typed URLs, index files, cache and history
- Microsoft Internet Explorer AutoComplete memory of form posts and passwords
- Microsoft Internet Explorer Cookies (Selective cookie keeping for versions 5 and above)
- Microsoft Internet Explorer Internet components (Selective keeping of components)
- Microsoft Internet Explorer Download Folder memory
- Microsoft Internet Explorer Favorites List
- Microsoft Outlook Express v5+ database of (Selective keeping of mail and news groups)
- Windows Media Player History
- Windows Media Player PlayLists in Media Library
- America OnLine Instant Messenger contacts
- Netscape Navigator temporary typed URLs, files, cache and history
- Netscape Navigator Cookies (Selective cookie keeping for versions 4 and above)
- Netscape Mail v4+ sent and deleted e-mails
- Netscape Mail hidden files
- Customizable lists of files and folders, with or without their contents
- Customizable scan lists of file types in specific folders
- Customizable scan lists of file types on all drives
- Deleted filenames, sizes and attributes from drive directory structures
- Free cluster space ("Slack") from all file tips
- Magnetic remnants from underneath existing files/folders
- All free unallocated space on all hard drives
- Evidence of activity in many other programs, using Plug-In modules
- Slack space and deleted entries in the Windows registry
- Created and modified dates and times on all files and folders
- Windows Registry Streams

Slika73. Karakteristike anti forenzičkog alata Evidence Eliminator

Slika73 pokazuje čak trideset sedam karakteristika operativnog sistema na koje će delovati antiforenzički alat, *Evidence Eliminator*, posle pokretanja. Spisak je dosta veliki ali kroz ispitivanje se došlo do podataka da se kanta za otpatke nije ispraznila posle restarta. History iz Internet Explorera nije obrisan pre restartovanja virtuelne mašine kada je to bilo zahtevano od strane anti forenzičkog alata, kao ni favoriti. Izbrisani su kuki-i i temporari folder ali je ostao funkcionalan pagefile.sys. Tako da ako bi digitalni forenzičar izvršio upad i pokrenuo istragu pre restartovanja virtuelne mašine, mogao bi da prikupi ipak nekoliko dokaza bitnih i čak i iz RAM memorije koje bi bile dovoljne za incident koji se dogodio. Anti forenzički alat se ne bavi fajlovima, dokumentima, folderima, aplikacijama koje se nalaze na virtuelnoj mašini osumnjičenog korisnika, a koji mogu biti dovoljni kao dokazi da se osumnjičeni izvede pred lice pravde.

Slika koja sledi opisuje da korisnik mora da sačeka nekoliko minuta da alat odradi svoje operacije.



Slika74. Informacija o restartovanju mašine posle dela rada alata

Slika74 pokazuje informaciju o kojoj je predhodno bilo reči da korisnik mora da zna da će alat odraditi podešavanja posle sledećeg restartovanja operativnog sistema, da ta podešavanja mogu da traju i do nekoliko minuta, a kako bi se završila pre pojavljivanja prozora za logovanje korisnika na operativni sistem. I da bi bilo omogućeno da alat završi svoj posao uklanjanja dokaza, korisnik se obaveštava da ne isključuje niti da restartuje svoju mašinu dok alat ne završi svoj posao.

3.5. Studija slučaja 5: *Malveri*

Ova studija slučaja opisace programe čija je uloga da utiču negativno na rad korisnika na virtuelnoj ili fizičkoj mašini u nekom mrežnom okruženju, pritom da neki od njih imaju ulogu humanih virusa samo u virtuelnom svetu ali i ulogu da se pojave pred korisnikom kao legalni programi a da posle instalacije na korisnikovu mašinu krenu da ruše operativni sistem.

3.5.1. Virusi, trojanski konji i crvi

Pošto se ovaj rad bavi istragom anti forenzičkog delovanja od strane lica koje rade ne zakonite radnje i koji žele da uklone dokaze ali i oni koji su u prethodnim poglavljima pominjani kako koriste tuđe računare napadajući ih raznim programima i alatima kao bi zloupotreba prošla razarajuće ali i ne opaženo od strane korisnika koje postaju žrtve. Za te aktivnosti koriste se i na raspolaganju su protivnici anti virusnih programa a oni su virusi, trojanski konji ili kako ih još zovu skraćeno trojanci i crvi.

Mnogi ljudi svrstavaju ove tri grupe u jednu nazivajući ih virusima i prave grešku ne znajući da postoje velike razlike kako uticaja na računarski sistema pa tako i borbe kao i odbrane od njih. Reči trojanac, crv i virus se često koriste za istu konstataciju kada se računar počne ponašati onako kako korisnik ne želi, ali oni nisu isti. Isto je to što su virusi, trojanci i crvi maliciozni programi koji mogu da nanesu štetu mašini, ali kako je malo pre napomenuto da postoje razlike među njima, to je bitna informacija u vezi zaštite mašine od njihovog delovanja.

Virusi:

- Dolaze na mašinu pričvršćeni uz program ili fajl tako da se mogu lako prenositi sa jednog *host-a* na drugi ili u kombinaciji sa *child-om*.
- Ostavljaju inficirane fajlove dok putuju kroz mrežu isto kao i virusi koji napadaju ljude.
- Virusi mogu varirati u obliku ali i težini nanete štete mašini koju su napali, neki mogu biti uzročnici blagih i dosadnih efekata, dok drugi mogu oštetiti i hardver mašine kao i softver ali i fajlove.
- Gotovo svi virusi su vezani za izvršni fajl, što znači da virus može postojati na mašini ali ne mora i da znači da će mašina biti zaražena ako se nije pokrenuo ili otvorio zlonamerni fajl.
- Virus se neće širiti bez delovanja ljudskog faktora ako ga ne inicira, tačnije ako ne manipuliše sa zlonamernim fajlom virus će mirovati.

- Zato se mora voditi računa da se ne inicira širenje virusa jer ljudski faktor najčešće ne svesno inicira širenje tako što deli zaraženi fajl ili šalje je putem e-mail.

Crv:

- Prva konstatacija vezana za crva je da je sličan svojim dizajnom kao virus, jer se i smatra pod klasom virusa.
- Crv se širi od mašine do mašine, ali u odnosu od virusa ima sposobnost da putuje bez iniciranja ljudskog faktora.
- Najveća snaga crva ali i opasnost za mašinu je što ima sposobnost sa se kopira na mašini pa umesto jednog kada se prebacuje sa mašine na mašinu, prebaciće se na stotine ili hiljade crva što može izazvati veoma razorne efekte za mašinu
- Opasnost postoji ako se crv primeni u *e-mail* adresaru, jer to može izazvati da se svakom prijatelju iz adresara uputi na *e-mail* na stotine crva, i onda se širenje nastavlja na adresarima prijatelja i tako redom.
- Snaga crva i primena je da se troše veliki hardverski resursi *host-a* i *child-a* i pretnja postoji da se i fizički ili virtuelni *host* obori, tačnije onemogućiti prilaz jer se u svakom trenutku bombarduje mrežni adapter *host-a* sa crvima.

Trojanski konji:

- Ima snagu obmane, jer je pun trikova, pa je i ime dobio po mitskom Trojanskom konju. Na prvi pogled može da izgleda kao koristan softver, ali će napraviti štetu kada se jednom instalira i pokrene na mašini.
- Osobe koje ih programiraju nastoje da ih predstavljaju kao legalan i legitiman softver kojeg korisnik treba da instalira na svojoj mašini.
- Trojanci su poznati i za stvaranje *backdoor* – zadnjih vrata na mašini. Tada osobe koje se bave ne zakonitim radnjama pristupaju mašini a da korisnici za to nisu ni svesni. Tada mašina postaje zombirana i osobe koje zloupotrebu vrše mogu da rade sa mašinom koja je zombirana šta god žele, da brišu fajlove, vrše pretragu, zloupotrebljavaju informacije i još dosta ne zakonitih radnji.
- Ono što trojance razlikuje od virusa i crva je to da se ne kopiraju sami i da ne vrše zarazu drugih fajlova, već to radi osoba koja ih je napravila i zaposela mašinu.

Spyware Adware:

- Služe da prikupe informacije o mašini i korisniku a da korisnik na to nije pristao niti da je obavešten
- Mogu se instalirati na mašinu na nekoliko načina, prvi način je putem virusa na primer. Drugi način je da se kao i trojanac instalira putem legalnog softvera na mašinu i pokrene ne znajući da je štetan.

Ove informacije o malicioznim fajlovima digitalni forenzičar mora da zna i da njima barata ali i da je informisan o njihovim novim verzijama, jer su one oružje sumnjivih osoba koje se bave ne zakonitim radnjama na Internetu pa i u virtuelnom okruženju. Ta vrsta oružja može da ima ulogu nanošenja štete kompaniji pa i pojedincu ali isto tako može se koristiti i u anti forenzičkom delovanju uklanjanja dokaza o incidentu koji se dogodio.

4. Diskusija

1. Razlike u pristupu digitalnog forenzičara na fizičku i virtuelnu mašinu

Tokom ispitivanja koja su predhodno urađena i opisana u ovom master radu došlo se do saznanja da razlike postoje. Jer ako pogledamo fizičku mašinu kojoj pristupa digitalni forenzičar u toku određene istrage, tada je potrebno da se fizička mašina ili nasilno isključi ili joj se pristupi u forenzičkoj istrazi na živo, tačnije kada je fizička mašina uključena. Uzimanje *image-a hard disc-a* i potom oduzimanja fizičke mašine ako je to moguće omogućuje digitalnom forenzičaru da prikupi i skladišti dokaze koji terete osumnjičenog. Sve predhodne aktivnosti nastupaju onda kada se fizička mašina locira i onda joj se pristupi. Mogu se prikupiti mnogobrojni i čvrsti dokazi, ali se mora voditi računa da ih predhodno osumnjičeni ne ukloni. Razlika se javlja kod virtuelnih mašina, jer se pristup vrši na *host* koji pokreće virtuelne mašine. Tek tada je moguće pokrenuti istragu jer virtuelnom mašinom moguće je upravljati sa udaljenih lokacija. Bitna stvar je u tome da je virtuelna mašina na *host-u* predstavljena kao nekoliko fajlova koji se mogu lako kontrolisati što od strane digitalnog forenzičara, tako i od strane osumnjičenog. Mogućnosti vraćanja slika stanja u predhodna imaju bitnu ulogu u istrazi digitalnog forenzičara. Kada je potrebno da se uzmu informacije sa virtuelne mašine tada se mogu preuzeti i svi fajlovi koji tu virtuelnu mašinu i opisuju hardverski, ali i virtuelni *hard disc-ovi* u kojima je zabeleženo sve kao i kod fizičkih *hard disc-ova*. Tako preuzeti fajlovi mogu se na jednostavan način uvesti na radnu stanicu digitalnog forenzičara i potom se može izvršiti istraga.

2. Specifičnosti anti forenzičkih aktivnosti u virtuelnom okruženju

Kada je reč o anti forenzičkoj aktivnosti u virtuelnom okruženju, tada se prvo mora voditi računa o edukaciji osobe koja tim virtuelnim okruženjem i upravlja. Samo virtuelno okruženje nudi veliki niz mogućnosti da se fajlovima, koji mogu biti potencijalni dokazi, upravlja i da potom budu uklonjeni sa virtuelne mašine koja je predmet istrage digitalnog forenzičara. Mogućnosti migracije virtuelne mašine mogu omogućiti da se celokupne virtuelne mašine premeste sa jednog *host-a* na drugi. Potom se prvi *host* ostavi kao potencijalni osumnjičeni bez dokaza na njemu, dok se na drugom *host-u* određena ne zakonita radnja nastavlja da se ne ometano odvija. Lako se mogu premeštati i virtuelni *hard disc-ovi* na druge *host-ove*. Virtuelne mašine, kao i njihovi konfiguracioni fajlovi sa sve fajlovima *hard disc-ova* i fajlovima slika stanja mogu se u par klikova premestiti na neki prenosivi *hard disc*. Moguća je manipulacija fajlovima koji opisuju virtuelnu mašinu tako što mogu biti premešteni na neku drugu particiju *host-a*. Fajlovima se potom promeni ime ili ekstenzija, kako bi se izvršila obmana digitalnog forenzičara. Ako je kojim slučajem digitalni forenzičar ovu mogućnost prevideo, mogao bi da izgubi veoma bitan dokaz ili celu virtuelnu mašinu koja bi mogla da tereti osumnjičenog.

3. Prednosti i nedostaci rekonstrukcije forenzičkog događaja u statičkoj i dinamičkoj forenzičkoj analizi

Kada se kaže dinamička forenzička analiza može se sprovesti kod slika stanja virtuelne mašine ili kako joj je i ime – *snapshots*, tada se misli da ova vrsta analize može biti promenljiva. Suprotno od dinamičke analize je statička analiza i ona se sprovodi kog uzimanja slike *hard disc-a* ili kako je još zovu – image *hard disc-a*. Kada se pravi slika celog *hard disc-a* i sprovodi se statička forenzička analiza tada se uzima celokupan sadržaj *hard disc-a* ili virtuelne ili fizičke mašine. Bitno je reći da se kopija diska pravi kopiranjem celokupnog sadržaja bit po bit, što može predstavljati dobar dokaz pred sudskim organima. Jer dokazi koji se poklope, a kojima su se poklopili bit po bit brojevi, postaju čvrsti dokazi. Razlika statičke u odnosu na dinamičku forenzičku analizu je u tome što slike stanja ili *snapshots* beleže samo one promene koje su nastale od poslednje sačuvane slike stanja. Ova vrsta forenzičke analize ne može imati toliko čvrstih dokaza kao što je može imati statička forenzička analiza, mada ti dokazi mogu pomoći digitalnom forenzičaru u kom pravcu da povede istragu.

4. Uticaj kloniranja virtuelne mašine na anti forenzičke aktivnosti

Kada se klonira stanje virtuelne mašine koje je korektno, tada se može uraditi klon virtuelne mašine koji se može čuvati za potrebno vraćanje kada za to dođe vreme. Sam proces kloniranja operativnog sistema virtuelne mašine ne traje dugo što se vremenskog perioda tiče. Ako se obave neke ne zakonite radnje i izvrši preuzimanje sadržaja sa *Web* stranica, a da bi se dokazi brzo uklonili, postoji mogućnost vraćanja u prvobitno stanje gde će se celokupna particija prepisati sa već napravljenim klon operativnim sistemom. Izbrisaće se sve što je predhodno bilo na particiji *hard disc-a* virtuelne mašine na kojoj se stavlja klon operativnog sistema. Kada je operacija kloniranja operativnog sistema sprovedena na fizičkoj mašini, potom restartovana fizička mašina vise puta jer je takva procedura vraćanja klona, tada se sve bitne informacije iz RAM memorije izbrisale. Ali, kada se kloniranje operativnog sistema primeni na virtuelnu mašinu ostaju informacije u virtuelnoj RAM memoriji, u fajlu .bin. Ove informacije je moguće izvući i posle nekoliko restartovanja virtuelne mašine, ali je ne moguće potkrepiti te informacije dokazima na *hard disc-u* virtuelne mašine jer su prepisivanjem klona bit po bit uklonjene. Za digitalnog forenzičara ostaju informacije da se na toj virtuelnoj mašini odvijala neka sumnjiva radnja koje mogu biti potkrepljene pod istragom, koja je obuhvatala praćenje osumnjičenog i njegovo delovanje na Internetu.

5. Zapažanja kod korišćenja anti forenzičkog softvera *Evidence Eliminator*

U master radu su primenjena dva anti forenzička alata sa istim imenom *Evidence Eliminator* ali od različitih izdavača. Preuzeta je i primenjena besplatna verzija koja se mogla preuzeti sa *Web* stranica izdavača. Sama aplikacija po sebi nudi uklanjanje velikog spektra potencijalnih dokaza, čak je to cifra od 112 potencijalnih dokaza, koja mogu teretiti osumnjičenog. Treba napomenuti da su preuzete besplatne verzije i da nisu imale potpuna podešavanja, ali sam proces uklanjanja dokaza sa *hard disc-a* mora dugo da traje. Jer se na mestima koja se uklanjaju, moraju upisati umesto do sada upisanih binarnih brojeva redovi nula ili jedinica naizmenično. Pošto *hard disc-ovi* imaju svoje brzine rada, tako je vreme ovog procesa uklanjanja dokaza varirajuće. U ispitanoj verziji anti forenzičkog softvera *Evidence Eliminator* mogu se videti brojni nedostaci koji su u predhodnim poglavljima opisani. Ali pošto je ovo bila besplatna verzija, proizvođači tvrde da se sa kompletnom verzijom mogu prekinuti svi linkovi i ukloniti svi dokazi koji sumnjiče osobu koja ovaj softver koristi.

6. Zaključak

Digitalnu forenziku mnogi smatraju mladom naukom, jer njeno postojanje je stupilo u primenu sa pojavom računara. U toku prošlog veka su po prvi put umrežena četiri računara i stvorila se vizija o razmeni fajlova na daljinu uz korišćenje mreže. Kako se svet razvijao i tehnologije koje su imale visok uspon u veoma kratkom periodu prošlog i početkom 21. veka, tako se i stvorila ali i brzo razvila Internet globalna mreža. To je donelo puno pozitivnih opcija u svetu industrije, trgovine, komunikacije i još mnoštva oblasti iz javnog ali i privatnog života ljudske populacije na planeti. Ali, kako se stvari koje su revolucionarne i koje se velikom brzinom svakodnevno razvijaju i za sobom vuku ili ih potpomažu razne informacione nauke, tako se otvara mogućnost velikih zloupotreba koje ne mogu biti uvek kontrolisane. Kada se dese, nanose velike materijalne i moralne štete pojedincu ali i društvu. Incidentnim situacijama, u virtuelnom svetu nalik na krivična dela ili čak zločine u svakodnevnom životu, u istrazi treba pristupiti drugačije nego u svetu koja ljudska čula rezonuju i osećaju. U poređenju sa dlakom od osumnjičenog ili čaure od metka, kod digitalne forenzičke istrage moraju se razumeti apstraktne pojave u računarskom okruženju. Ovde su dokazi binarni 0 i 1, kao i velika lepeza fajlova kojima funkcionalnosti mogu biti različite, informacije koje mogu biti promenjene u samo jednom deliću sekunda i sa jednim klikom na miš, tako da digitalni forenzičar jednostavno ostane bez dokaza.

Iako je tako mlada kao nauka, digitalna forenzika može da se nosi rame uz rame sa svim naukama. Razvoj i napredovanje digitalne forenzike kao nauke je u velikom usponu. Progresivno napredovanje mora da ide uvek uz korak sa novim tehnologijama. Kako se informacione tehnologije razvijaju, digitalna forenzika mora da ih prati, ali uvek da ima i rezervu. Mora uvek da ide korak ispred noviteta u tehnologijama kako bi obezbedila mogućnost istrage i prikupljanja čvrstih i neoborivih dokaza, a da pre toga osumnjičeno lice ih ne ukloni.

Kao što je u ovom radu obrađena tema pristupa digitalnog forenzičara u *Clouding Computing* okruženje, kao i moguće prednosti ali i mane virtuelnog okruženja, koje mogu biti iskorišćene za zloupotrebu i nanošenje štete celokupnom okruženju ali i pojedincima. Ovo govori u prilog tome, da svaki forenzičar mora da se svakodnevno edukuje i prati razvoj kako korisnih aplikacionih rešenja ali isto tako i da prati razvoj malicioznih aplikacija koje nanose štetu. Moraju se razvijati sistemi i aplikacije koje će omogućiti odbranu od ne zakonitih napadača. Maksimalna bezbednost u virtuelnom okruženju ne postoji, pa se onda mora voditi računa o ljudskom faktoru greške i preuzimanju softvera koji u prvi mah deluje korektno a po njegovom instaliranju se dobije trojanski konj kao u mitskom delu. Korišćenje materijala koji su dostupni u pisanoj ili video formi na Internetu može puno koristiti digitalnom forenzičaru. Bitno je da se nauka koja svakodnevnim koracima grabi sve više i više, mora razmenom iskustva i deljenjem materijala savladavati i razvijati. Otvaranjem pitanja i ulascima u diskusiju sa kolegama iz naučne oblasti digitalne forenzike, moraju se nalaziti odgovori za određene situacije. Svako novo saznanje u vezi određenog problema u sferi digitalne forenzike, može dati veliki podstrek u pozitivnom rešavanju istrage koje se otvaraju svakodnevno na globalnoj mreži i koje utiču na rad i razvoj društva u celini.

6 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. Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Second Edition, Academic Press, 2004
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., *Primena modela sazrevanja procesa zaštite informacija*, doktorski rad, Univerzitet SINGIDUNUM Beograd 2007
5. Milosavljević M., Grubor G., *Osnovi bezbednosti i zaštite informacionih sistema*, Univerzitet Singidunum, 2006.
6. Milosavljević, M., Grubor, G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Beograd, 2009.
7. Milosavljević, M., Grubor, G., *Istraga kompjuterskog kriminala*, Univerzitet Singidunum, Beograd, 2009.
8. Milosavljević, M., *Računarska inteligencija*, Skripta Elektrotehničkog fakulteta, Beograd, 2007.
9. Prof. Dr. Slobodan R. Petrović, *Kompjuterski kriminal*, II izdanje, VIZ, Beograd, 2004

Web izvori:

10. http://www.virtuatopia.com/index.php/Hyper-V_Essentials
11. <http://www.ncjrs.gov>
12. <http://www.ncjrs.gov>
13. <http://www.tcpdump.org>
14. <http://judiciary.house.gov>
15. <http://www.iacis.org>
16. http://www.forensicswiki.org/wiki/Anti-forensic_techniques
17. <http://www.forensicscience.ufl.edu>

18. <http://www.esecurityplanet.com/trends/article.php/3694711/Anti-Forensic-Methods-Used-by-Jihadist-Web-Sites.htm>
19. <http://www.avgthreatlabs.com/webthreats>
20. http://us.norton.com/security_response/threatexplorer/index.jsp
21. <http://forums.islamicawakening.com/f18/anti-forensics-32255>
22. <http://www.ieee-security.org/Cipher/PastIssues/2010/E99.Nov-2010/E99.Nov-2010.html>
23. http://www.symantec.com/security_response/writeup.jsp?docid=2005-081910-3934-99
24. http://www.symantec.com/security_response/writeup.jsp?docid=2005-081910-3934-99
25. http://us.norton.com/security_response/writeup.jsp?docid=2010-122111-5625-99