Primena virtualizacije u digitalnoj forenzičkoj istrazi

Igor Franc, Aleksandar Jevremović, Mladen Veinović

Sadržaj — **U radu je predstavljen osnovni koncept virtualnih mašina, strutkura jedne virtualne mašine, opis svih fajlova od kojih se sastoji. Prikazan je način prikupljanja relevantnih podataka za forenzičku analizu i predstavljen je drugačiji koncept gde se virtualna mašina može koristiti kao forenzički alat. Identifikovana su ograničenja zbog kojih se virtualna mašina ne može koristiti kao zamena za konvencionalne tehnike i metode digitlne forenzičke istrage.Na kraju prikazano je kako se virtualna mašina može koristiti kao anti-forenzički alat.**

Ključne reči — **Anti-forenzički alat, digitalna forenzika, virtualna mašina, , VMWare, wmdk fajlovi.**

I. Uvod

U ovom radu bice obradjena uloga WMVare virtualizacije u toku digitalne forenzičke istrage. Prvo će biti objasnjen sam pojam "Virtualna Mašina" (VM) a zatim će biti prikazano kako se sve VM moze koristiti u toku digitalne forenzičke istrage. Takodje će biti reči i o tome kako se VM može koristiti kao dokaz i biće predstavljen predlog gde se VM koristi zajedno sa standardnim konvencionalnim (DD) prikupljenim digitalnim dokazom da bi se rešio slučaj potencijalnog kompjuterskog incidenta.

Dalje u radu biće reči i o tome kako se VM može koristiti i kao moćan forenzički alat uz pomoć koga možemo prikupiti podatke koji su neophodni u toku digitalne forenzičke istrage. U poslednjem delu rada biće prikazano i kako se VM može koristiti kao anti-forenzički alat kojim se mogu prikriti tragovi koji su neophodni za dalju forenzičku istragu i samim tim sprečiti normalan tok digitalne forenzičke istrage.

II. VIRTUALNA MAŠINA - VIRTUALIZACIJA

Virtualna mašina (VM) je softver koji omogućava korisniku da na jednom računaru kreira više nezavisnih i izolovanih operativnih sistema sa različitim podešavanjima samog hardvera (CPU, hard disk, memorija, mrežne kartice, i ostale komponente) i sa različitom vrstom operativnog sistema (OS) koji će se izvršavati na njima. Korisnik može da konroliše svaki sistem posebno i može ih koristiti izolovano ili povezati u računarsku mrežu.

Ovakav pristup je vrlo moćan i fleksibilan i štedi resurse jer nije potrebno više fizičkih računara već se hardver jedne mašina (host-a) deli između više VM. To funkcioniše na sledeći način, računar na kome se koristi VM zove se *Host* dok se sama VM koja je instalirana zove *Guest*. Jedan Host računar može imati veći broj Guest VM-ova koji će svi koristi fizičke resurse Host računara istovremeno kada je VM aktivna. Najjednostavnije se ovaj koncept može opisati kao pokretanje više virtualnih kompjutera na jednom fizičkom kompjuteru.

Virtualizacija nije nov koncept, prvi put je predstavljen 1960 godine na mainframe računarima. Na persolanim računarima je predstavljena 1990 godine posle čega se pojavilo više različitih softverskih paketa za ovu namenu od kojih su najpoznatiji: VMWare, Microsoft Virtual PC, Microsoft Hyper-V, Oracle VirtualBox, XEN, QEMU, KVM i ostali. Pošto je najpopularniji i najčešće korišćen VMWare on je u fokusu ovog rada i biće detaljno prikazan.

A. VMWARE

Postoje tri različita VMWare proizvoda (Workstation, Server i Player) koji se mogu koristiti za pokretanje i podešavanje virtualnih mašina.

VMWare Workstation se najčešće koristi od svih i nije besplatan (osim što se može koristiti 30 dana dok traje *trial* period).

VMWare Server ima nešto manje mogućnosti u odnosu na Workstation ali je zato besplatan i može se potpuno besplatno instalirati i koristiti.

VMWare Player je takodje potpuno besplatan proizvod ali ne poseduje mogućnost podešavanja VM-a što je neophodno za digitalnu forenziču istragu i samim tim se ne može koristiti za ovu namenu.

Virtualna mašina predstavlja grupu fajlova i evo spiska svih fajlova od kojih se sastoji jedna VMWare virtualna mašina. Prisustvo bilo kog od ovih fajlova na hard disku može biti dokaz da se na tom računaru trenutno nalazi ili se nekada nalazila neka VMWare virtualna mašina.

.Log – Predstavlja jednostavnu log datoteku aktivnosti VM,

.VMDK– Ovo je zapravo sam hard disk sa virtualnim Guest operativnim sistemom, može biti fixed veličine (ne menja veličinu tokom rada VM) ili dynamic (počinje sa minimalnom veličinom i uvećava se u toku rada VM po

Igor Franc, Univerzitet Singidunum, Danijelova 29/32, 11000 Beograd, Srbija (telefon: 381-64-3579397, e-mail: ifranc@singidunum.ac.rs)
Aleksandar Jevremović, Univerzitet Singidunum, Danijelova 29/32, 11000 Beograd, Srbija (telefon: 381-64-1327119, e-mail: ajevremovic@singudnum.ac.rs)
Mladen Veinović, Univerzitet Singidunum, Danijelova 29/32, 11000 Beograd, Srbija (telefon: 381-63-1013391, e-mail: mveinovic@singidunum.ac.rs)

potrebi do određene predefinisane veličine koja predstavlja maksimum,

.VMEM – je backup virtualne mašine(paging fajl VM-a),

.VMSN – je VMware snapshot fajl, kreira se kada je sačuvano stanje VM-a i ime dobija po imenu stanja koje je zadato prilikom čuvanja stanja,

.VMSD–ovaj fajl sadrži meta podatke o snapshot-u i kreira se prilikom pravljenja slike stanja VM,

.NVRAM– fajl koji sadrži BIOS virtualne mašine,

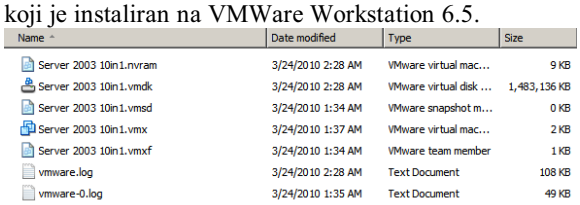
.VMX– predstavlja konfiguracioni fajl virtualne mašine, u zavisnosti od operativnog sistema sadrži različite podake.Ovo je jednostavan tekstualni fajl koji se lako može menjati uz pomoć bilo kog tekst editora (Notepad),

.VMSS-predstavlja 'suspended state' fajl, u njemu se čuvaju stanje VM kada je u suspend stanju,

.VMTM-ovo je konfiguracioni fajl koji sadrži podatke o grupi u kojoj se VM nalazi,

.**VMXF**-kreira se ako se VM ukloni iz grupe i čuva podatke koji su neophodni da bi se VM mogla vratiti ponovo u grupu.

Na sledećoj slici možete videti primer fajlova jedne VMWare virtualne mašine. Konkretno ovde se radi o Microsoft Windows 2003 Server R2 operativnom sistemu koji je instaliran na VMWare Workstation 6.5.



Name	Date modified	Type	Size
Server 2003 10in1.nvram	3/24/2010 2:28 AM	VMware virtual mac...	9 KB
Server 2003 10in1.vmdk	3/24/2010 2:28 AM	VMware virtual disk ...	1,483,136 KB
Server 2003 10in1.vmsd	3/24/2010 1:34 AM	VMware snapshot m...	0 KB
Server 2003 10in1.vmx	3/24/2010 1:37 AM	VMware virtual mac...	2 KB
Server 2003 10in1.vmxf	3/24/2010 1:34 AM	VMware team member	1 KB
vmware.log	3/24/2010 2:28 AM	Text Document	108 KB
vmware-0.log	3/24/2010 1:35 AM	Text Document	49 KB

Sl. 1. Spisak fajlova MS Windows 2003 Server VM

III. VIRTUALNA MAŠINA KAO DOKAZ

Pre procesa analize u toku digitalne forenzičke istrage potrebno je prvo pronaći lokaciju VM. Često je to vrlo jednostavan zadatak jer korisnici u velikom broju slučajeva na menjaju podrazumevanu lokaciju za čuvanje VM-a koja je u slučaju VMWare folder pod imenom "My Virtual Machines" a koji se nalazi u folderu koji se kreira za svakog korisnika na datom računaru i može se desiti da je za pristup ovom folderu potrebna lokalna administratorska šifra jer korisnici imaju pravo da zaštite svoje fajlove od ostalih korisnika na sistemu.

Ukoliko se fajlovi ne nalaze na podrazumevanoj lokaciji potrebno je traziti lokaciju fajlova koji se nekada mogu nalaziti i na nekom eksternom medijumu ili se čak može desiti i da su fajlovi obrisani sa hard diska (ovde je potrebno imati u vidu da se **vmdk** fajlovi nece slati u Recycle Bin prilikom brisanja zbog svoje veličine već se direktno brisu). Ukoliko se sumnja da je na računaru nekada postojala VM a ne mogu se pronaci fajovi onda je potrebno proveriti da li se može negde na hard disku pronaći "My Virtual Machines" folder i da li postoji bilo koji VM fajl koji može da ukaže na postojanje VM na tom računaru, kao i to da li možda postoje podaci o uklonjenoj VMWare aplikaciji na samom sistemu.

Evo kratkog prikaza šta se sve može naći na hard disku kao potencijalni pokazatelj da je tu nekada bila instalirana VM:

- **Program icon** – ukoliko je VM aplikacija uklonjena ili obrisan folder saVM aplikacijom može se desiti da se na hard disku i dalje negde nalazi ikonica samog programa,
- **Dll fajlovi** – može se desiti da se u windows system folderu još uvek nalazi neki od dll fajlova koji nije obrisan tokom uklanjanja aplikacije,
- **Temp folder** – posle uklanjanja VM aplikacije moguce je da se nesto od fajlova jos uvek nalazi u Temp folderu OS,
- **Lnk fajlovi, prefetch fajlovi i MRU** – potrebno je proveriti da li postoje tragovi u navedenim fajlovima
- **Regystri** – često u registar bazi OS ostanu tragovi o nekim instaliranim programima pa samim tim i VM aplikacijama,
- **File associations** – moguće je videti da je za otvaranje odredjene vrste fajlova podešana neka VM aplikacija u samom OS,

Virtual adapters- prilikom instalacije odredjenog VM softvera često se kreiraju i neki virtualni adapteri, na primer kod VMWare se uvek kreira "VMware Network Adaptor" koji može biti siguran pokazatelj da je na tom računaru bila instalirana ova aplikacija.

A. PRIKUPLJANJE I OPORAVAK OBRISANIH ILI ŠIFROVANIH VIRTUALNIH MAŠINA

Osnovna stvar kod vraćanja obrisanih fajlova jeste prvo proveriti da li se oni nalaze u Recycle Bin-u. Kod VM fajlova to nije slučaj jer su ovi fajlovi mnogo veće veličine i zbog limita se ne salju u Racycle Bin već se brisu direktno ali postoji način da se oni povrate za dalju digitalnu forenzicku analizu. Pošto je fajl dosta veliki (veličine i do nekoliko GB) neki put je moguće vratiti ga u potpunosti a u nekim slučajevima moguće je povratiti samo delove VM (fragmente) koji se mogu koristiti u daljoj digitalnoj forenzičkoj istrazi.

Šifrovanje VM je vrlo složen proces i može se vršiti kroz nekoliko različitih slojeva (layer-a). Sam folder u kome se nalazi VM moguće je šifrovati određenim osnovnim Windows algoritmom za tu namenu FDE (Full Disk Encryption) kao što je na primer softver BitLocker ili neki od programa za tu namenu. Dodatno i sam virtualni operativni sistem može biti šifrovan. Pristup sifrovanim fajlovima i pristup šifrovanom hard disku izlazi van okvira ovog rada tako da ovde nece biti objasnjen.

B. *Različiti pristupi pravljenja kopije VM*

Standardno pravljanje imidža u forenzičkoj istrazi radi se na jedan od dva načina. Prvi način je tako što se hard disk priključi na neku vrstu uređaja koji onemogućuju upisivanje sadržaja odnosno koji garantuju da se sadržaj hard diska nece promeniti (hardware write blockers), drugi način je tako što se računar podiže sa nekog live diska (Helix, Knopix STD) i tada se moze koristiti i softverski način blokiranja upisa (software write blockers). Tek posle ovog kada je osigurano da neće doći bi promene podataka na hard disku moguće je nekim programom za tu namenu napraviti imidž diska (FTKImager).

Sl. 2. Helix 3 live OS startovan na WMVare Workstation 6.5

Što se VM tiče tu je stvar potpuno drugačija jer VM predstavlja skup fajlova koje je potrebno kopirati, ali to nije dovoljno jer se moze desiti da se na hard disku nalaze jos neki povezani fajlovi koji će kasnije biti neophodni u toku digitalne forenzicke istrage. Takođe se moze javiti problem sa MACE podacima koji se mogu izmeniti u odnosu na Host mašinu koja se koristi i samim tim uništiti dalji tog digitalne forenzičke istrage. Zbog svega navedenog kopiranje fajlova se ne smatra dobrom metodom za ovu namenu već je potrebno prvo na standardan način izvršiti forenzicku akviziciju podataka pa tek onda iz nje ekstraktovati VM fajlove i analizirati ih.

Jos jedan od čestih situacija jeste da se na računaru Host-u nalazi folder koji sluzi za razmenu podataka sa VM (shared folder) i ukoliko bi se podaci prikupljali samo prostim kopiranjem fajlova do tih podataka više ne bi mogli doći osim ako bi i dalje imali pristup datom računaru, što je u nekim slučajevima potpuno nemoguće. Ovde je bitno naglasiti da se VMmože montirati i kao fizički uređaj uz pomoć raznih softverskih aplikacija i onda vršiti analiza podataka.

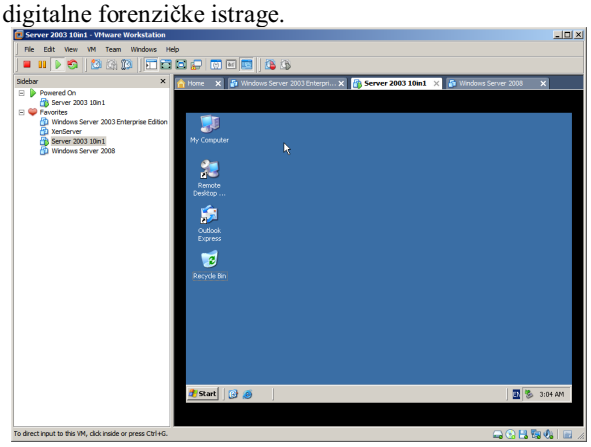
C. *Istraga VM*

Istraga VM je skoro ista kao i standardno prikupljenog forenzičkog imidža. VM se može istrazivati na standardan način kao imidž koji je napravljen od strane forenzičara klasičnom metodom. Međutim VM sadrži i meta podatke koji mogu biti vrlo korisni jer daju razne dodatne informacije o VM i Host računaru na kome se izvršavala koji mogu biti vrlo korisni forenzičarima u toku digitalne forenzičke istrage. Primer takvih podataka su MACE podaci koji mogu dati uvid u to koji korisnički nalog se koristio na host računaru kada se pristupano VM, tu mozemo videti i dodatne informacije o samom korisniku računara ili u najgorem slučaju samo korisnički nalog koji je bio u upotrebi.

IV. VIRTUALNA MAŠINA KAO FORENZIČKI ALAT

Ne tako davno podizanje forenzičkog imidža je trajalo nekoliko sati pa i čitav dan i sastojalo se u tome da se hard disk sa imidžom ubaciovao fizički u kompjuter i tako podizao. To je često zahtevalo pravilno konfigurisanje sistema da prepozna različit hardver koji se nalazi na fizičkom računaru a koji se nije nalazio na originalnom računaru odakle je napravljen imidž.

Kod VM procedura se drastično promenila i to vreme je redukovano, potrebno je nekoliko klikova misem da bi se podigao sistem i to bez ikakvih hardverskih radova (ubacivanja hard diska u računar). Hardver je standardizovan tako da se automatski podesava bez potrebe za dodatnim drajverima. Na ovaj način štedi se vreme forenzičara i samim tim ubrzava čitav proces digitalne forenzičke istrage.



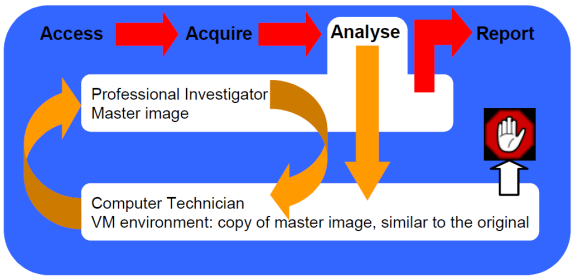
Sl. 3. Startovan MS Windows 2003 Server R2 na VMWare Workstation 6.5

Ovakav sistem se može koristiti da bi se u toku forenzičke istrage ili prilikom veštačenja na sudu mogli grafički predstaviti određeni elementi sistema koji se koristio za napad ili koji je meta napada. Na primer moguće je prikazati kreirane fajlove i foldere zajedno sa datumima kreiranja, na ovaj način moguće je i prikazati prisustvo određenih vrsta malicionznih programa kao što su virusi, crvi ili trojanci.

A. *Dvostruki pristup*

Ono što se ovde javlja kao problem jeste to što prilikom podizanja sistema u virtualnom okruženju neizbezno je da ce doci do određenih promena na samom imidžu tako da on više neće biti identičan onom koji je uzet sa originalne

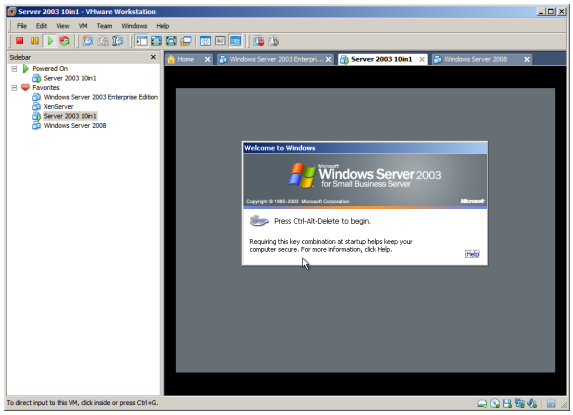
mašine (Hash vrednost). Samim tim ovakav dokaz nije validan pred sudom i iz tog razloga se predlaze primena dvostrukog pristupa po kome bi se original čuvao dok bi se njegova kopija podizala preko VM i na njemu bi se vršila razna ispitivanja dok bi original ostao netaknut i na taj način bi se mogao bez problema koristiti kao validan dokaz na sudu. Kao što je poznato prikom uzimanja imidža pravi se jedinstvena hash vrednost koja garantuje da nije doslo do bilo kakvih promena na imidžu tokom forenzicke istrage tako da pošto se sva istrazivanja sprovode na kopiji koja ja podignuta na VM-u ta vrednost će ostati očuvana.



Sl. 4. Dvostruki pristup prikupljanju podataka

B. *Čist operativni system u svakom trenutku*

Jos jedna od bitnih prednosti korišćenja VM je što se vrlo lako i jednostavno u svakom trenutnku moze podici nov čist virtualni operativni sistem na kome se mogu vrsiti razlicita testiranja i mogu se u toku forenzickog procesa testirati različite vrste malicionznog koda kao i to da se moze na licu mesta u toku ekspertize a u toku procesa digitalne forenzicke istrage pred sudom demonstrirati rad određenih softvera i tako sudiji i ostalim ne tehničkim licima pokazati na lep i vizuelno prijemčiv način funkcionisanje određenog softvera.



Sl. 5. Startni ekran MS Windows 2003 Server R2 operativnog sistema

V. VIRTUALNA MAŠINA KAO ANTI-FORENZIČKI ALAT

Iako se VM-a može koristiti u toku digitalne forenzičke istrage kao značajna pomoć takođe se ona može koristiti u kao sredstvo za skrivanje tragova ili remećenje normalnog toka digitalne forenzičke istrage od strane kompjuterskih (cyber) kriminalaca. Kao što je već ranije rečeno VM predstavlja skup fajlova koji se mogu obrisati ili se mogu nalazite na nekom eksternom medijuma. Takođe je moguće da za određenu VM je dovoljno da se na računaru nalazi instaliran VMWare Player ili Server koji je zaduzen za otvaranje **vmdk** fajlova. Bitno je napomenuti da se određene VM mogu pokrenuti čak i bez programa koji je potrebno da bude instaliran na hard disk računara što još više ometa tok digitalne forenzičke istrage.

Pošto je moguće da se virtualna mašina nalazi na externom medijumu postoji opasnost da je taj medijum na neki način kriptovan da bi se sprečio pristup fajlovima neovlašćenim osobama ali o ovome je već bilo reči u radu i ovo izlazi van okvira ovog rada.

VI. ZAKLJUČAK

Tehnologija VM je danas postala često primenjena u različitim vrstama poslovnih okruženja. Samim tim neophodno je analizirati različite načine na koji je moguće prikupiti podatke koji su neophodni za digitalnu forenzičku istragu u uslovima VM okruženja. Ovde je bitno naglasiti da postoje velike razlike u prikupljanju standardnih i VM operativnih sistema i u radu je predložen dvostruki pristup koji se može koristiti za digitalnu istragu VM. U radu je objašnjeno i koliko vremena se može uštedeti korišćenjem tehnlogoije VM u digitalnoj forenzičkoj istrazi ali je prikazano i to kako se ova tehnologija može koristiti i u svrhu ometanja digitalne forenzičke istrage (kao anti-forenzički alat).

LITERATURA

[1] Brown, C. L. T. (2005). Computer Evidence: Collection & Preservation. Hingham, MA: Charles River Media.

[2] Kruse II, W. G., & Heiser, J. G. (2002). Computer Forensics: Incident Response Essentials (1st ed.): Addison Wesley Professional.

[3] Nelson, B., Phillips, A., Enfinger, F., & Steuart, C. (2006). Guide to Computer Forensics and Investigations, Second Edition (2nd ed.). Boston, MA: Thomson Course Technology.

[4] Computer Forensic Analysis in a Virtual Environment: University of Western Sydney D. Bem and E. Huebner, University of Western Sydney, 2007.

[5] www.e-fense.com/helix – HELIX LIVE CD, 2010

[6] www.accessdata.com - FTK IMAGER, 2009

[7] www.vmware.com – VMWARE SOFTWARE, 2010

ABSTRACT

The paper presents the basic concept and structure of virtual machine.Shows the way to collect relevant data for DF investigation and introduced a different concept where the virtual machine can be used as forensic tools.Identified constraints for which the virtual machine can not be used as a replacement for conventional techniques and methods for DF investigations.At the end of the paper shows how the virtual machine can be used as an anti-forensic tools.

USING VIRTUALIZATION IN DF INVESTIGATION

Igor Franc, Aleksandar Jevremović, Mladen Veinović