UNIVERZITET SINGIDUNUM
Fakultet za informatiku i računarstvo
MASTER STUDIJE
Savremene Informacione Tehnologije

Master rad

DIGITALNA FORENZIKA DISTRIBUIRANOG INTERNET RAČUNARSTVA

MENTOR:
Docent, dr Gojko Grubor

KANDIDAT:
Vesko Mimović
Br.ind.: 410297/10

Beograd, jun 2011

DIGITALNA FORENZIKA OKRUŽENJA DISTRIBUIRANOG INTERNET RAČUNARSTVA

Sažetak

Razvojem računarske tehnologije poslednjih godina broj korisnika računara i računarskih mreža, kao i dostupnih sistema i usluga raste vrtoglavom brzinom. Trend razvoja savremenih računarskih sistema je doveo do nastanka *Distribuiranog Internet računarstva,* kompjuterskog sistema u kome kompanija koja je zainteresovana za usluge savremenog kompjuterskog okruženja za svoje potrebe iznajmljuje kompjuterski prostor u informatičkom centru druge kompanije. Rad u ovakvom okruženju pruža mnoge prednosti, ali i omogućuje pojavu raznih oblika zloupotrebe podataka koji se nalaze i razmenjuju u sistemu, odnosno do nastanka kompjuterskog kriminala. Glavni cilj istrage kompjuterskog kriminala je obezbeđenje digitalnih dokaza, upotrebom digitalne forenzike, a uz nezaobilaznu pomoć širokog spektra forenzičkih alata.

Ključne reči

Distribuirano Internet računarstvo, virtuelizacija, kompjuterski kriminal, digitalna forenzika, forenzički alat, proces odgovora na incident, paketsko njuškalo.

FORENSIC IN THE CLOUD COMPUTING ENVIRONMENT

Abstract

Development of the computer technology, in the last few years, has swiftly increased the number of computer, computer and network users, and available IT systems and services. Trend called *Cloud Computing*, computer system in which a company or a single user, interested for modern computer services, uses the information center and computer storage space of other larger company. Using other company services provides great benefit but can also cause some problems like information security and genesis of the computer crime. Main goal of forensics is to provide relevant digital evidence using wide range of forensic tools.

Key words

Cloud Computing, virtualization, computer criminal, digital forensic, forensic tool, incident response process, pocket sniffer.

SPISAK SLIKA

Slika 1. Konceptualni dijagram Distribuiranog kompjuterskog računarstva 16
Slika 2. Arhitektura prirodne virtuelizacije 18
Slika 3. Vizuelni prikaz Distribuiranog Internet računarstva 21
Slika 4. Prikaz *Mklink-a* 29
Slika 5. Proces odgovora na incident …….. 38
Slika 6. Osnovni Wireshark meni 44
Slika 7. Wireshark Capture meni 45
Slika 8. Izbor Wireshark opcija 46
Slika 9. Prikaz procesa hvatanja podataka 47
Slika 10. Prikaz progresa hvatanja podataka 47
Slika 11. Glavni prozor Wireshark-a 48
Slika 12. Wireshark upit za zatvaranje hvatanja podataka 49
Slika 13. Wireshark opcije otkrivanja i sakupljanja 50
Slika 14. Wireshark opcije definisanja imena uređaja 51
Slika 15. Otkrivanje i sakupljanje jpeg fajla u realnom vremenu 51
Slika 16. Prikaz otkrivenog jpeg fajla u realnom vremenu 53
Slika 17. Prikaz filtriranja prikazivanja otkrivenih i sakupljenih paketa 54
Slika 18. Izdvojeni i zapamćeni JPG fajl 55
Slika 19. Wireshark *Start meny* 56
Slika 20. Prikaz odabranog interfejsa 56
Slika 21. Prikaz opcija otkrivanja i sakupljanja u korporativnoj mreži 57
Slika 22. Otkrivanje i sakupljanje jpeg fajla na ispitivanom računaru 58
Slika 23. Otkriveni i uhvaćeni JPG fajl 59

SPISAK TABELA

Tabela 1. Mogućnosti *libpcap* interfejsa 61

S A D R Ž A J

DIGITALNA FORENZIKA OKRUŽENJA DISTRIBUIRANOG INTERNET RAČUNARSTVA …….. 3
Sažetak ……..……. 3
Ključne reči ..…….. 3

FORENSIC IN THE CLOUD COMPUTING ENVIRONMENT …….. 3
Abstract ……..... 3
Key words …… 3

SPISAK SLIKA ……... 4

SPISAK TABELA ……... 4

1. METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA 7

1.1. Uvodne napomene i obrazloženje rada 7
1.2. Predmet istraživanja 9
1.3. Ciljevi i zadaci istraživanja 10
1.4. Hipotetički okvir istraživačkog rada 11
1.5. Metode, tehnike i tok istraživačkog procesa 13

2. DIGITALNA FORENZIKA OKRUŽENJA DISTRIBUIRANOG INTERNET RAČUNARSTVA 16

2.1. Distribuirano Internet računarstvo (Cloud Computing) 16
2.1.1. Uvod u Distribuirano Internet računarstvo..... 16
2.1.2. Virtuelizacija u okruženju Distribuiranog Internet računarstva ... 17
2.1.3. Karakteristike Distribuiranog Internet računarstva 19
2.1.4. Digitalna forenzika u okruženju Distribuiranog Internet računarstva 21
2.1.5. Istraživačka i forenzička metodologija 27
2.1.6. Mesto i uloga forenzike u Digitalnom Internet računarstvu 30

2.2. Odgovor na incident u Distribuiranom Internet računarstvu 32
2.2.1. Značaj integracije mrežne i forenzike domaćina 32
2.2.2. Odgovor na incident koji koristi mrežu kao izvor 33
2.2.3. Odgovor na incident koji koristi domaćina kao izvor 34
2.2.4. Integracija tehnika odgovora na incident 34
2.2.5. Integracija alata 35
2.2.6. Proces odgovora na incident u Distribuiranom Internet računarstvu 36

2.3. Otkrivanje i sakupljanje podataka u mrežnom saobraćaju u realnom vremenu 42

2.3.1. Uvod 42
2.3.2 Primena Wireshark-a 43
2.3.3. Otkrivanje i hvatanje tekućih forenzičkih podataka upotrebom Wireshark-a 49
2.3.4. Otkrivanje i hvatanje tekućih forenzičkih podataka upotrebom Wireshark-a u korporativnoj mreži 55
2.3.5. Ograničenja Wireshark-a 59
2.3.6. Usluge Wireshark-a 62

3. ZAKLJUČAK 66

4. SPISAK LITERATURE 68

1. METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA

1.1. Uvodne napomene i obrazloženje rada

Naglim razvojem računarske tehnologije poslednjih godina (povećanje performansi tehnologije koju prati pad cena na tržištu) i sa pravom eksplozijom Interneta, broj korisnika računara i računarskih mreža raste vrtoglavom brzinom. Sa sve moćnijom računarskom opremom svakodnevno se uvode novi servisi, a istovremeno se u umrežavanju postavljaju viši standardi. Vremenom su se mrežni sistemi razvijali da bi danas dostigli nivo praktičnog efikasnog okruženja za razmenu podataka.

Dostupnost i fleksibilnost tehnologija današnjih savremenih računarskih mreža omogućava da se sa bilo koje tačke na planeti može povezati na mrežu i doći do željenih informacija. U poređenju sa nekadašnjom cenom korišćenja servisa mreža, cena eksploatisanja današnjih mreža je sve niža. Računarske mreže su danas nezamenjivi deo poslovne infrastrukture kako malih, tako i velikih organizacija. Poznavanje tehnologije i korišćenje mreža nije samo stvar opšte kulture. U mnogim segmentima poslovanja primena računarskih mreža obezbeđuje prednost organizacijama na tržištu (npr. elektronska trgovina omogućava i malim firmama konkurentnost na tržištu).

Tendencija razvoja savremenih računarskih sistema se pomera od u prošlosti aktuelnog lokalnog centra sa pojedinačnim ulaznim i izlaznim tačkama ka savremenim globalnim mrežama koje uključuju mnoštvo informacionih centara i stotine ulaznih i izlaznih tačaka. Kompjuterski sistem ili okruženje u kome kompanija koja je zainteresovana za usluge savremenog kompjuterskog okruženja za svoje potrebe iznajmljuje kompjuterski prostor u informatičkom centru druge kompanije, koja se bavi pružanjem usluga se naziva *Distribuirano kompjutersko računarstvo - CC(Cloud Computing)*[1].

Rad u okruženju ovakvog kompjuterskog sistema pruža mnoge prednosti, olakšava rad, kako manjim institucijama i kompanijama, tako i velikim kompanijama i poslovnim i administrativnim sistemima. Međutim, uporedo sa upotrebom sistema u cilju olakšavanja funkcionisanja poslovnog okruženja, javljaju se razni oblici zloupotreba podataka koji se nalaze i razmenjuju u sistemu. Ovakvi oblici zloupotrebe predstavljaju kompjuterski kriminalne radnje i mogu biti: protivpravno korišćenje usluga, neovlašćeno pribavljanje informacija, kompjuterske krađe, kompjuterske prevare, kompjuterske sabotaže, kompjuterski terorizam i kriminal vezan za kompjuterske mreže.

[1] Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, James "Jim" Steele, *Digital forensics for network, Internet, and cloud computing*, Syngress 2010, str. 12

Razlozi za pojavu ovih zloupotreba su različiti. Najčešći razlozi su sticanje finansijske dobiti, izazov, znatiželja, samopotrvđivanje, krađa informacija, mada su, u poslednjih nekoliko godina sve više prisutni i drugi motivi, kao što su špijunaža i kompjuterski terorizam. ''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.''[2] 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.

Forenzika igra značajnu ulogu u ovom sistemu, ali sa ograničenjima koja vežu forenzičara duboko za mrežnu i kompjutersku forenziku. Forenzika ovakvog sistema je najbolje primenjena tamo gde je mreža u vlasništvu kompanije, odnosno na granicama sistema i na desktopu ili sistemima koji imaju pristup resursima sistema. Forenzičari rade u CC okruženju u trenutku kada kompanije upućuju mnoga ograničenja forenzici, odnosno u trenutku kada mnoge kompanije još uvek izgrađuju sopstvenu infrastrukturu.

Forenzika upakovana u CC okruženje mora postaviti upit kada informacija bude poslata ka bilo kojoj granici između unutrašnjih i spoljašnjih procesa, što je jako teško pratiti tradicionalnom mrežnom forenzikom. Jednom kada informacija bude poslana u okruženje, forenzičar postaje deo kompjuterske i mrežne forenzike sa ciljem da odredi koji sistem je bio povezan sa kojim i u koje vreme. Forenzičar može imati kritičnu ulogu u izolovanju unutrašnjeg sistema od incidenata, odlučujući koji nivo kompromitovanja je došao iznutra a koji spolja.

Forenzičar može ostvariti uticaj na rezultat istrage o incidentu onoliko dugo koliko je potrebno da se podaci sakupe u kompjuteru na ulaznim i izlaznim tačkama kompanijske mreže. Upotreba osnovnih logova mrežne barijere, sistemskih logova i ostalih logova može ukazati na vreme pristupa, mesto i IP adrese koje mogu pomoći pri određivanju kako se incident širio kroz mrežu i koji bi se koraci morali preduzeti da bi se minimizirao bio kakav budući događaji, obezbeđivanjem solidnih podataka o nastalom događaju.

Veliki deo forenzike predstavlja sposobnost nadzora nad mrežnim saobraćajem koja ima za cilj izolovanje određenog broja servera koje treba istražiti tradicionalnim forenzičkim procesom.

Forenzički alati koji se koriste u ovom okruženju ukazuju na to da nadzor mreže dobija na značaju. Što više alata za vizuelizaciju podataka i alata za kontrolu protoka može biti napravljeno da radi u CC okruženju nezavisno od ograničenja operativnog sistema ili hipervizorovih ograničenja bilo kog virtuelnog sistema, forenzika će biti efektivnija i

[2] Milosavljević M.,Grubor G., *Digitalna forenzika*, Univerzitet Singidunum, Beograd 2008, str. 12

sposobnija. Premda, forenzika sada predstavlja proces nadzora nad osnovnim sistemom koji može biti skuplji, vezano za angažovanje radne snage i upravljanje logovima, bez upotrebe istih sredstava CC okruženja da pomogne da se otarasi nekih od pretraživačkih i istraživačkih procesa u značenju podataka log fajlova.

Sa ograničenjima kompleta alata, kao najbolji alati su se pokazali oni najjednostavniji, pre svih *Wireshark* i *Snort* za Windows i *Linux* i *WinPcap* za Windows, kao i osnovne mrežne barijere za oba operativna sistema.

U prvom delu rada dati su osnovni podaci o CC sistemu, njegovim karakteristikama, kao i specifičnostima koje uslovljavaju uspešnost forenzičkih metodologija, postupaka i tehnika. Takođe, predstavljene su forenzičke metodologije kao i mesto i uloga digitalne forenzike u ovom sistemu. Jasno je naznačeno koliko je poznavanje elemenata ovog sistema bitno za uspešan rad forenzičara.

U drugom delu je opisan proces odgovora na incident koji je nastao u CC sistemu, kao i njegovi osnovni elementi. Dat je i kratak osvrt na tradicionalni proces odgovora na nastali incident, kao i komparativna analiza ova dva procesa. U ovom delu se eksplicitno pokazuje koliko je poznavanje elemenata ovog procesa bitno za uspešan rad forenzičara, kao i koliko CC sistem sa svojim specifičnostima utiče na modifikaciju tradicionalnog procesa odgovora na incident.

U trećem delu rada će biti objašnjen postupak otkrivanja i sakupljanja tekućih ("živih") mrežnih forenzičkih podataka, odnosno podataka koji se prenose putem mrežnog saobraćaja u realnom vremenu. Poseban akcenat će bit stavljen na analizu rada Wireshark forenzičkog alata, alata koji predstavlja protokol za analizu mreže koji se koristi za otkrivanje i sakupljanje podataka sa mreže i prikazivanje uhvaćenih paketa podataka.

1.2. Predmet istraživanja

U ovom radu predmet istraživanja je mesto i uloga digitalne forenzike u CC okruženju, kao i upotreba softverskih forenzičkih alata u procesu odgovora na incident u cilju predstavljanja značaja digitalne forenzike za dobru korporacijsku istragu.

U prvom delu rada dati su osnovni podaci o CC sistemu i njegovim karakteristikama, kao i uticaju procesa virtuelizacije na proces digitalne forenzike. Na kraju prvog dela će biti dat osvrt na istraživačku i forenzičku metodologiju, karakterističnu za ovakvo okruženje.

U drugom delu je detaljno opisan proces odgovora na nastali incident u ovakvom okruženju, prateći njegov proces tokom svih njegovih faza, kao i specifičnosti procesa odgovora na nastali incident u odnosu na okruženje, kao okruženje u kojem je incident nastao.

U trećem delu rada predmet istraživanja je postupak otkrivanja i sakupljanja tekućih ("živih") mrežnih forenzičkih podataka, odnosno podataka koji se prenose putem

mrežnog saobraćaja u realnom vremenu. Poseban akcenat će bit stavljen na analizu rada Wireshark forenzičkog alata, kao i na analizu uhvaćenih podataka u JPEG formatu. Na kraju drugog dela će biti prezentovana ograničenja Wiresharka, kao i mogućnosti njegovih usluga, poput *TShark, RawShark, Dumpcap, Mergecap, Editcap, Text2pcap.*

1.3. Ciljevi i zadaci istraživanja

Glavni cilj ovog rada je da se prikaže značaj digitalne forenzike za korporacijsku istragu u CC okruženju, sa posebnim akcentom na značaj poznavanja načina sakupljanja i hvatanja potencijalnih digitalnih dokaza u mrežnom saobraćaju u realnom vremenu i forenzičkih alata za interpretaciju digitalnih podataka na različitim apstraktnim nivoima računarskog sistema.

1. Poseban cilj je da se izvrši analiza mesta i uloge digitalne forenzike u CC okruženju. Proces virtuelizacije, kao značajna karakteristika i preduslov postojanja ovakvog okruženja definiše određene specifičnosti digitalne forenzike koji se permanentno moraju analizirati i unapređivati, a rezultati analiza jasno prikazivati.

Karakteristike ovog okruženja poput usluge po zahtevu, širokog mrežnog pristupa, udruživanja izvora, brze elastičnosti i merljivosti usluge, modeli njegovih usluga poput Softvera kao usluge (SaaS), Platforme kao usluge (PaaS) i Infrastrukture kao usluge (IaaS) i modeli razvoja, kao što su Privatni sistem, Zajednički sistem, Javni sistem i Hibridni sistem otežavaju i komplikuju funkcionisanje digitalne forenzike, kao i primenu softverskih forenzičkih alata. Okruženje CC sistema može takođe da frustrira forenzičara u ovakvom okruženju zbog nedostatka direktnog pristupa osumnjičenim mrežnim uređajima.

2. Poseban cilj je da se utvrdi primenljivost tradicionalnog odgovora na nastali incident u CC sistemu, kao i zahteva za njegovu modifikaciju radi kvalitetne primene u novom sistemu. Tradicionalni proces odgovora na nastali incident se pre razvoja CC sistema odvijao na dva odvojena koloseka, odnosno bio je podeljen na dva nezavisna procesa i to proces u kome se kao izvor koristi mreža i proces u kome se kao izvor koristi domaćin. Kako su ova dva procesa bila odvojena i nezavisna u slučaju jednog incidenta, ovakav pristup nije bio adekvatan za primenu u novonastalom sistemu, već je postojeći proces odgovora na incident modifikovan kako bi bio uspešno primenjen u ovom sistemu.

3. Poseban cilj je izvršiti analizu osnovnih funkcionalnosti softverskog forenzičkog alata, verifikovati i vrednovani deklarisane prednosti i nedostatke sa aspekta forenzičke prakse. Značaj softverskih alata posebno je naglašen kada imamo u vidu da je zbog karakteristika, modela i razvoja CC okruženja forenzičaru onemogućen direktan pristup osumnjičenim mrežnim uređajima.

Na tržištu postoji veliki izbor komercijalno dostupnih digitalnih forenzičkih alata sa brojnim opcijama rešenja za različite forenzičke zadatke. Ovi alati često mogu zbuniti digitalnog forenzičara, pri izboru pravog alata za konkretni slučaj. Forenzička praksa

podjednako zahteva da forenzičar raspolaže sa setom raznovrsnih alata za određene namene, ali i specifičnim namenskim alatima koji su generalno bolji za rešavanje namenskih zadataka. Glavni zadaci su, da se definišu i verifikuju ključne funkcionalnosti alata i procene upotrebne vrednosti.

1.4. Hipotetički okvir istraživačkog rada

S obzirom na temu rada, moraju se postaviti dve opšte hipoteze sa radnim hipotezama.

Opšta hipoteza 1:

Moderno kompjutersko okruženje se pomerilo od, u prošlosti aktuelnog lokalnog centra sa pojedinačnim ulaznim i izlaznim tačkama ka savremenim globalnim mrežama koje uključuju mnoštvo informacionih centara i stotine ulaznih i izlaznih tačaka. Ova seoba poslova i usluga ka udaljenim centrima informacija, na kojima su smešteni računarski i skladišni kapaciteti, koji su iznajmljeni od velikih kompanija se naziva Distribuirano Internet računarstvo (*Cloud Computing*).

Kompanije i pojedinci su uvideli velike prednosti poslovanja u CC okruženju, ne samo u pogledu produktivnosti, već i pristupu veoma brzim sistemima koji upravljaju velikom količinama podataka, kao i udaljenim računarskim i skladišnim kapacitetima, transakcionim procesnim sistema i softverskim paketima koji su iznajmljeni i mogu biti bilo gde u svetu.

Međutim, ova migracija informacionih centara izaziva brojne bezbednosne komplikacije, bilo da se radi o proceduralno ili pravnim bezbednosnim komplikacijama. Tipični informacioni centar, lokalni ili na bliskoj udaljenosti, koji ima sistem fizičkog pristupa ubrzo postaje stvar prošlosti, tako da ta promena predstavlja stalni izazov bezbednosnoj industriji. Kompjuterski sistemi i mrežna forenzika se nalaze pred izazovom koji proističe iz transfera lokalnog informatičkog centra u udaljeni informatički centar kod kojeg fizički pristup nije moguć.

Radna hipoteza 1.1:

Koncept mrežne forenzike u ovakvom okruženju zahteva novi aspekt sagledavanja problema bezbednosti jer nekada neki podaci neće biti dostupni, neki podaci će biti osumnjičeni, neki podaci će biti spremni za sud i mogu se uklopiti u tradicionalni mrežni forenzički model. Izazov za svakog forenzičkog istraživača je da shvati koji set podataka spada u koju kategoriju i to dostupne, sumnjive i spremne za sud.

Opšti problem je što se principi tradicionalne digitalne forenzike ne mogu u potpunosti primeniti u CC okruženju. Otuda je digitalna forenzika u ovakvom okruženja veoma složen i vremenski zahtevan posao, koji zahteva specifične alate za analizu i posebne veštine forenzičara.

Radna hipoteza 1.2:

Koncept mrežne forenzike u ovakvom okruženju pored specifičnosti koje se ogledaju u tome da nekada neki podaci neće biti dostupni ili nedovoljno "čvrsti" da bi se prezentovali na sudu, mora da prihvati i neophodnost izmene tradicionalnog forenzičkog modela, odnosno tradicionalnog procesa odgovora na incident.

Problem koji nastaje prilikom primene tradicionalnog procesa odgovora na nastali incident u CC sistemu se nalazi u njegovoj karakteristici da se realizuje kroz dva nezavisna procesa, proces u kome se kao izvor koristi mreža i proces u kome se kao izvor koristi domaćin, što onemogućuje kvalitetnu forenzičku analizu incidenta. Prevazilaženje ovog problema leži u modifikaciji tradicionalnog procesa odgovora na incident u skladu sa specifičnostima CC sistema.

Opšta hipoteza 2:

Digitalna forenzika u CC okruženju ima za cilj da otkrije i sakupi informacije o tome kako je napadač dobio pristup računarskoj mreži i računarskom sistemu. Analiziraju se log fajlovi da se odredi kada se korisnik ulogovao ili poslednji put koristio svoj lični identifikator (ID) za logovanje. Digitalni forenzičar nastoji da odredi kojim URL je korisnik pristupio, kako se ulogovao na računarsku mrežu i sa koje lokacije.

Uspešan rad forenzičaru CC sistema može da oteža nedostatak direktnog pristupa osumnjičenim mrežnim uređajima. Od izuzetne važnosti, za sprovođenje postupka forenzičke analize predstavlja postupak otkrivanja i sakupljanja tekućih ("živih") mrežnih forenzičkih podataka, odnosno podataka koji se prenose putem mrežnog saobraćaja u realnom vremenu.

Veoma je značajno za uspešnu za forenzičku istragu odabrati softverski forenzički alat za analizu mreže koji se može koristiti i za otkrivanje i sakupljanje podataka sa mreže i prikazivanje uhvaćenih paketa podataka u realnom vremenu, što može da omogući da korisnik stekne uvid u stanje protoka podataka i da reaguje odmah po nastanku incidenta.

Radna hipoteza 2.1:

Softverski digitalni forenzički alati se mogu podeliti na više načina, zavisno od kriterijuma klasifikacije.

U odnosu na tip interfejsa softverski forenzički alati se dele na:

- digitalne forenzičke alate komandne linije i

- digitalne forenzičke alate sa GUI (*Grafical User Interface*) interfejsom.

U odnosu na programski kod, softverski digitalni forenzički alati se dele na:

- digitalne forenzičke alate zatvorenog koda i
- digitalne forenzičke alati otvorenog koda.

Pored velikog izbora digitalnih forenzičkih alata, ne može se govoriti o najboljem digitalnom forenzičkom alatu. Specijalizovani forenzički alati koriste se za samo određenu vrstu fajlova ili obavljaju samo jedan zadatak digitalne forenzičke istrage. Ovi alati su namenski i pouzdaniji te mnogo efikasnije obavljaju specifičan zadatak nego neki univerzalni alati.

Sa druge strane, sa adekvatnim skupom raznovrsnih digitalnih forenzičkih alata, forenzičar može brže i konfornije završiti više različitih zadataka digitalne forenzičke istrage.

Najbolje je rešenje da digitalni forenzičar sam, na bazi predistražnih podataka i informacija o slučaju, izvrši izbor adekvatnih alata za konkretan slučaj, uključujući skup alata za izvršenje što više digitalnih forenzičkih zadataka na terenu kao i specijalizovane alate za detaljno i precizno izvršavanje karakterističnog forenzičkog zadatka.

1.5. Metode, 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 prema prirodi istraživanja na - teorijska i empirijska, prema cilju istraživanja na - fundamentalna i primenjena i prema funkciji istraživanja na - eksplorativna i usmerena na proveravanje hipoteza, u ovom istraživačkom radu primenjena su uglavnom *fundamentalna* i *primenjena* istraživanja. Fundamentalna istraživanja 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 istraživanja, definisan kao kompjuterski incident u CC okruženju, opisan u drugom delu, a zatim praktično prikazan u trećem delu kroz postupak otkrivanja i hvatanja paketa podataka u mrežnom saobraćaju u realnom vremenu. Takođe, definisan je cilj istraživanja, kao verifikacija dela teorije korporativne digitalne forenzičke istrage. Istraživanje je izvršeno kroz faze pripreme, uglavnom teorijskog karaktera, prikupljanja i obrade podataka, izvođenja eksperimentalne verifikacije, interpretacija rezultata i izvođenje zaključaka.

U ovom istraživačkom radu korišćene su različite metode istraživanja i verifikacije procesa korporativne digitalne forenzičke istrage da bi se došlo do određenih saznanja, otkrili i izložili naučni principi, koja se primenjuje 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 i digitalnoj forenzičkoj istrazi, zatim istraživanje literaturnih podataka i materijala preuzetih iz raznih izvora, kroz faze otkrivanja, opisivanja i objašnjavanja određenih faza digitalne forenzičke istrage. Rad je struktuiran u određene celine i svaka od njih konkretno objašnjava glavne faze i procese korporativne digitalne forenzičke istrage.

U prvom delu rada dati su osnovni podaci o CC sistemu, njegovim karakteristikama, kao i specifičnostima, a pre svih procesa virtuelizacije, koje uslovljavaju uspešnost forenzičkih metodologija, postupaka i tehnika. Takođe, predstavljene su forenzičke metodologije kao i mesto i uloga digitalne forenzike u ovom sistemu.

U drugom delu je detaljno opisan proces odgovora na incident koji je nastao u CC sistemu, kao i njegovi osnovni elementi. Dat je i kratak osvrt na tradicionalni proces

odgovora na nastali incident, kao i komparativna analiza ova dva procesa. U ovom delu se eksplicitno pokazuje koliko je poznavanje elemenata ovog procesa bitno za uspešan rad forenzičara, kao i koliko CC sistem sa svojim specifičnostima utiče na modifikaciju tradicionalnog procesa odgovora na incident.

U trećem delu rada predmet istraživanja je postupak otkrivanja i sakupljanja tekućih ("živih") mrežnih forenzičkih podataka, odnosno podataka koji se prenose putem mrežnog saobraćaja u realnom vremenu.. Poseban akcenat će bit stavljen na analizu rada Wireshark forenzičkog alata, , kao i na analizu uhvaćenih podataka u JPEG formatu. Na kraju drugog dela će biti prezentovana ograničenja Wiresharka, kao i mogućnosti njegovih usluga, poput *TShark, RawShark, Dumpcap, Mergecap, Editcap, Text2pcap*.

2. DIGITALNA FORENZIKA OKRUŽENJA DISTRIBUIRANOG INTERNET RAČUNARSTVA

2.1. Distribuirano Internet računarstvo (Cloud Computing)

2.1.1. Uvod u Distribuirano Internet računarstvo

Postoje različite definicije ovog pojma, ali se oko nekih činjenica slažu i najsuprostavljeniji stavovi. Neki analitičari ga definišu usko, kao ažuriranu verziju kompjuterskih usluga, pogotovo zbog velikog broja virtuelnih servera koji su dostupni na Internetu. Drugi, idu u drugu suprotnost, i definišu ga kao sve ono što konzumiramo izvan mrežnih barijera, uključujući i konvencionalno angažovanje spoljnih izvora.



Slika 1. Konceptualni dijagram Distribuiranog kompjuterskog računarstva

Cloud Computing je ustvari metafora za Internet, ali pojam računarstva ga čini većim i složenijim od samog Interneta. *Cloud Computing* ili *Distribuirano kompjutersko računarstvo* se može shvatiti kao jednostavan sistem iznajmljenog kompjuterskog prostora u informatičkom centru druge kompanije[3]. To znači da kompanija koja

[3] Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, James "Jim" Steele, *Digital forensics for network, Internet, and cloud computing*, Syngress 2010, str. 14

iznajmljuje prostor ima kontrolu samo nad nekim aspektima ovog sistema zavisno koju je uslugu navedenog sistema iznajmila. CC sistem predstavlja prirodnu evoluciju i adaptaciju virtuelizacije, uslužno orjentisane arhitekture i koristi kompjutera.

Korisnici, bilo da su kompanije ili pojedinci, su uvideli velike prednosti koje proizilaze iz upotrebe CC okruženja, ne samo u pogledu produktivnosti, već i pristupu veoma brzim sistemima koji upravljaju velikim količinama podataka na način koji bi bio finansijski nemoguć za mala i srednja preduzeća ili institucije. Velika preduzeća, takođe, imaju prednosti jer jeftinom upotrebom kapaciteta ovog okruženja imaju na raspolaganju širok spektar usluga, poput udaljenih računarskih i skladišnih kapaciteta, transakcionih procesnih sistema i softverskih paketa koji su iznajmljeni i mogu biti bilo gde u svetu. Međutim, ova migracija informacionih centara izaziva brojne bezbednosne komplikacije, bilo da se radi o proceduralnim ili pravnim bezbednosnim komplikacijama.

Tipični informacioni centar, lokalni ili na bliskoj udaljenosti, koji ima sistem fizičkog pristupa ubrzo postaje stvar prošlosti, tako da ta promena predstavlja stalni izazov bezbednosnoj industriji. Kompjuterski sistemi i mrežna forenzika se nalaze pred izazovom koji proističe iz transfera lokalnog informacionog centra u udaljeni informacioni centar kod koga fizički pristup nije moguć.

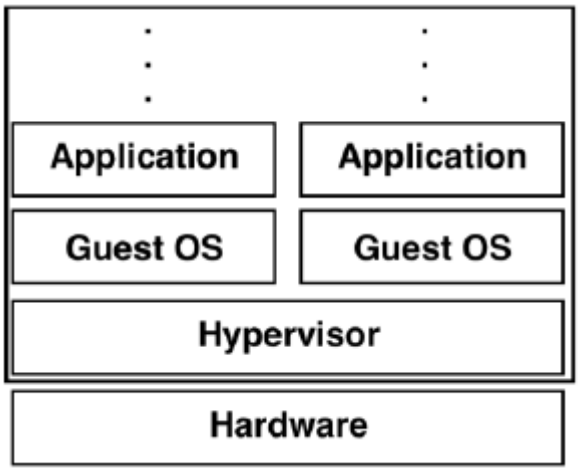
Ipak, u ovom sistemu postoji manjak potpune kontrole kompjuterskog sistema koji kompanija iznajmljuje, posebno ako se poredi sa kontrolom koju je kompanija imala koristeći tradicionalne sisteme informacionih centara.

2.1.2. Virtuelizacija u okruženju Distribuiranog Internet računarstva

Ovakav sistem zahteva neophodno menjanje načina obezbeđenja informacija koje kompanija upućuje putem bezbednosnih kontrola, politika i tehničkih rešenja, jer potpuna kontrola kompjuterskih i mrežnih usluga nije moguća u CC okruženju. Pragmatično govoreći, u ovakvom okruženju, kompanija jednostavno kupuje virtuelnu mašinu u informacionom centru druge kompanije.

Virtuelizacija je simulacija softvera i/ili hardvera na kome je drugi softver pokrenut[4]. Ovakvo, simulativno okruženje se naziva virtuelna mašina (VM). Postoje две forme virtuelizacije, prepoznate prvenstveno po računarskim arhitektonskim slojevima i to: prirodna (*native* ili *bare metal virtualization*) i domaćinova (*hosted virtualization*).

[4] Karen Scarfone, Murugiah Souppaya, Paul Hoffman, Guide to Security for Full Virtualization Technologies (Draft), Recommendations of the National Institute of Standards and Technology, Special Publication 800-125, July 2010, str. 2-1



Slika 2. Arhitektura prirodne virtuelizacije

Za izučavanje CC okruženja značajna je prirodna virtuelizacija, kod koje se hipervizor pokreće direktno na osnovnom hardveru bez OS udaljenog računara, jer se serveri mnogo češće virtuelizuju u toj formi. U ovoj formi virtuelizacije svaki gostujući OS se pojavljuje kao da ima svoj hardver, poput regularnog kompjutera, koji uključuje: CPU , memoriju, skladišni prostor (hard disk, možda flopi i CD-ROM drajv), kontrolore skladišnog prostora, Ethernet kontrolore, zvučne i displej uređaje, miša i tastaturu.

Virtuelizacija servera obezbeđuje neke bezbednosne prednosti. Pokretanje servera sa hipervizorom obezbeđuje *sandbox*, koji ograničava uticaj kompromitovanja, dok hipervizor može da obezbedi manju površinu napada nego što bi OS udaljenog kompjutera, smanjujući tako mogućnost širenja uspešnog kompromitovanja izvan udaljenog računara. Ipak virtuelizacija servera ne sprečava napadača da kompromituje server kroz ranjivosti serverskih aplikacija ili operativnog sistema *host* kompjutera, niti sprečava napadača da direktno kompromituje operativni sistem *host* kompjutera (ako postoji), kao što je napad na mrežne usluge operativnog sistema *host* kompjutera sa nekog drugog udaljenog kompjutera u istoj podmreži.

Virtuelizacija menja pristup kompjuterskoj bezbednosti i mrežnoj forenzici u CC okruženju, naročito u slučaju nastanka bezbednosnog incidenta. Virtuelizacija unosi promene u planiranje kompjuterske bezbednosti i okončavanje forenzičke istrage jer pojedini ili celokupni računarski sistemi nisu fizički dostupni. Nemoguće je misliti kako jedan uređaj fizički ima samo jedan operativni sistem koji treba istražiti.

Konkretni server može imati mnoge virtuelne servere koji su pokrenuti na konkretnom hardveru, koji ne moraju čak ni da pripadaju istoj kompaniji ili usluzi. Priroda i procesi forenzike CC okruženja mora biti usklađena sa novonastalim promenama, kao i promenama u primeni zakonskih odredbi koje regulišu pronalaženje dokaza zločina u konkretnom okruženju.

2.1.3. Karakteristike Distribuiranog Internet računarstva

Kao i drugi kompjuterski sistemi, i CC sistem se odlikuje svojim specifičnostima koje se ogledaju kroz pet osnovnih karakteristika, tri modela usluga i četiri modela razvoja[5].

Osnovne karaktristike su:

- ***Usluga po zahtevu (On-demand self-service)***
  Korisnik može jednostrano obezbediti računarske mogućnosti, kao što su vreme servera i mrežno skladištenje podataka, po potrebi, automatski bez zahteva za ljudskom interakcijom sa bilo kim uslužnim provajderom.

- ***Široki mrežni pristup (Broad network access)***
  Mogućnosti su dostupne kroz mrežu i pristup standardnim mehanizmima koji unapređuju upotrebu uskih ili prostranih klijentske platforme (poput mobilnih telefona i laptopova)

- ***Udruživanje izvora (Resource pooling)***
  Provajderovi računarski resursi su udruženi da bi služili višestrukim korisnicima upotrebom modela više zakupaca, sa različitim fizičkim i virtuelnim izvorima dinamično dodeljenim na osnovu zahteva korisnika. Pozicija izvora je nezavisna, tako a korisnik nema kontrolu nad njim, niti znanja o tačnoj lokaciji obezbeđenih izvora.

- ***Brza elastičnost (Rapid elasticity)***
  Mogućnosti mogu biti brzo i elastično obezbeđene, u neki slučajevima i automatski. Za korisnika, mogućnost je dostupna i obezbeđeno je da se često pojavljuje kao neograničena i može biti dobivena u bilo kojoj meri i u bilo koje vreme.

- ***Merljivost usluge (Measured Service)***
  CC okruženje automatski kontroliše i optimizuje upotrebu izvora rukovanjem merljivim mogućnostima na nekom nivou koji odgovara vrsti usluge. Upotreba izvora može biti nadgledana, kontrolisana i o njoj se može izveštavati obezbeđujući transparentnost kako za provajdera tako i za korisnika usluge.

Modeli usluge su:

- ***Softver kao usluga (Cloud Software as a Service-SaaS)***
  Mogućnosti obezbeđene korisniku su provajderove aplikacije pokrenute u infrastrukturi ovog kompjuterskog sistema. Aplikacije se pristupa sa različitih klijentskih uređaja kroz uzan klijentski interfejs kao što su web pretraživači (npr.

[5] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009., str. 15

web-based e-mail). Korisnik ne upravlja niti kontroliše osnovni sloj infrastrukture uključujući mrežu, servere, operativne sisteme, skladišta ili čak individualne aplikativne mogućnosti, sa posebnim izuzetkom ograničene korisnički određene aplikacije za konfiguracijska podešavanja.

- ***Platforma kao usluga (Cloud Platform as a Service -PaaS).***
  Mogućnosti koje su obezbeđene korisniku su razvijene kroz infrastrukturu kompjuterskog sistema ili stečene aplikacije kreirane upotrebom programskih jezika i alata podržanih od strane provajdera. Korisnik ne upravlja niti kontroliše osnovnu strukturu sistema uključujuću mrežu, servere, operativne sisteme, skladišta ali ima kontrolu na razvijenim aplikacijama i mogućim aplikacijama konfiguracije *host* okruženja.

- ***Infrastruktura kao usluga (Cloud Infrastructure as a Service-IaaS).***
  Mogućnosti koje su obezbeđene korisniku su obezbeđeni procesori, skladišta, mreže i ostali fundamentalni računarski izvori gde je korisnik sposoban da razvije i pokrene proizvoljan softver, koji može da uključi operativni sisteme i aplikacije. Korisnik ne upravlja niti kontroliše osnovnu strukturu sistema ali ima kontrolu nada operativnim sistemima, skladištima, razvijenim aplikacijama i moguće ograničeno kontroliše odabrane mrežne komponente (npr. *host* mrežne barijere).

Modeli razvoja su:

- ***Privatni system (Private cloud)***
  Infrastrukturom sistema se upravlja potpuno za jednu organizaciju. Može biti upravljano iz organizacije ili od strane trećeg lica.

- ***Zajednički system (Community cloud)***
  Infrastruktura sistema je deljena od strane više organizacija i podržava određenu zajednicu koja deli interes. Može biti upravljano iz organizacije ili od strane trećeg lica.

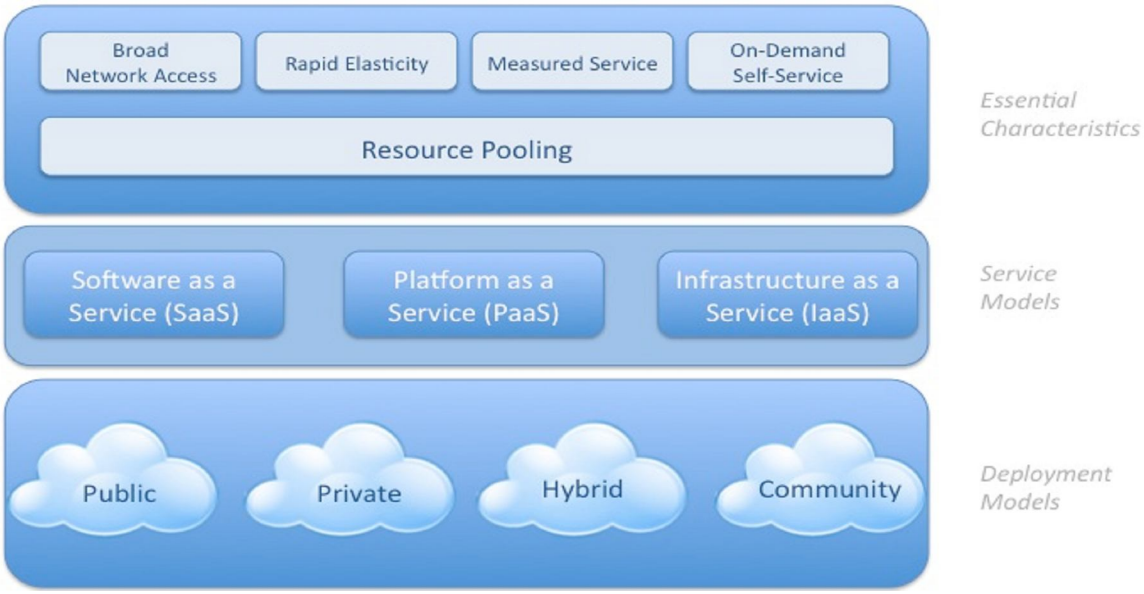
- ***Javni sistem (Public cloud)***
  Infrastruktura sistema je napravljena da bude dostupna javnosti ili velikim industrijskim grupama i u vlasništvu je organizacija koje prodaju usluge sistema.

- ***Hibridni system (Hybrid cloud)***
  Infrastruktura sistema je kompozicija od dva ili više sistema (privatni, zajednički ili javni) koji ostaju jedinstveni entiteti ali su ograničeni zajedno standardima ili privatnom tehnologijom koja obezbeđuje prenosivost podataka i aplikacija (npr. Otvaranje sistema radi uravnoteženja između dva sistema).

Softver ovog sistema uzima punu prednost sistemske paradigme jer je uslužno orjentisan sa fokusom na neograničenost državnim granicama, modularnosti i semantičkom interoperabilnosti.

Provajder usluga CC okruženja ima komplet prednosti i slabosti koje dolaze sa dizajnerskom filozofijom koju je posedovao provajder prilikom dizajniranja sistema. Ovakav dizajn i arhitektonska rešenja sistema provajdera usluga ograničavaju ono šta se može a šta se ne može uraditi forenzičkom analizom nekog događaja, kojom je kompanija otkloni problem u slučaju da smatra da je došlo do gubljenja informacija ili je sistem postao kompromitovan.

Veoma je važno da mrežni forenzičari ili bilo koje lice koje se bavi zaštitom informacija u ovakvom okruženju poznaje rešenja koja proizilaze iz ovakve arhitekture sistema provajdera usluga.



Slika 3. Vizuelni prikaz Distribuiranog Internet računarstva

Najpoznatiji provajderi poput Amazon, Salesforce, Rackspace, Microsoft Azure i Google imaju značajno različitu dizajnersku filozofiju koja proizilazi iz načina na koji oni obezbeđuju CC okruženje i iz koga proizilazi i sva složenost procesa mrežne forenzike koji je iniciran od strane zainteresovane kompanije, koja smatra da je sistem kompromitovan.

2.1.4. Digitalna forenzika u okruženju Distribuiranog Internet računarstva

U okruženjima koja su prethodila CC okruženju bezbedno okruženje[6] je bilo bilo koje mesto ili bilo koji uređaj sa koga korisnici pristupaju mreži i sistemskom uslugama, a koje je kompanija koja pruža usluge obezbedila. Kod CC okruženja fleksibilnost je

[6] C. Perrin, *There is no perimeter*, TechRepublic, 2008., str. 455

postala naslednik bezbednog okruženja, kojoj se mogu pridružiti mnogobrojni načini konzumacije informacija na različitim uređajima širom sveta. U svetu mrežnih usluga i sistema konzumacija informacija će se odvijati putem Interneta koji će zakomplikovati svaku bezbednosnu istragu kompjutera.

CC okruženje sa osobinama poput iznajmljenog sajber prostora sa svojim uslugama, Web ili nekim drugim, pristupom putem pretraživača (*browser*) ili prilagodljivom aplikacijom mora biti dobro obezbeđen i zaštićen protiv zloupotrebe ili prevare. Takođe, postoje i zahtevi pravne prirode kojih se mora pridržavati vezano za upućivanje podataka i sistema podataka koji se sve više udaljavaju od lokalnog centra ka udaljenom, fizički nedostupnom iznajmljenom prostoru.

Računarske mreže koje se zasnivaju na korišćenju CC okruženja zahtevaju promene u korporativnoj i bezbednosnoj politici imajući u vidu udaljeni pristup, pristup informacijama putem pretraživača, poresku politiku, politiku zaštite privatnosti, sisteme upravljanja i izveštavanja koji kontrolišu kako je informacija obezbeđena u ovom okruženju i koja može biti bilo gde u svetu. Ovo je potpuni kontekst CC okruženja koje kompanije koriste, a koji zahteva kompleksno i izazovno bezbednosno okruženje, što sačinjava moderno bezbednosno okruženje.

Moderno bezbednosno okruženje se sada mora sagledavati kako kao kompleks sistema (paket hardvera i operativnog sistema u virtuelnom okruženju), informacija, pristupnih pravila i politika koje upravljaju protokom informacija i pristupima, tako i kao odgovor na incident čiji nastanak ima za posledicu usložavanje arhitekture CC okruženja i procesa podrške. Ova "Deperiferizacija"[7] zahteva potpuno novi pristup i to ne samo činjenici kako je sistem programiran, već i kako se upravlja sa bezbednošću informacijama. Ove promene se moraju još uvek usavršavati kroz praktičnu proveru, mada se veći sistemi već pripremaju za susret sa zahtevima industrije. U budućem periodu, ovo će obuhvatati zahteve kako kompanije zaista mogu upućivati mrežne i kompjuterske forenzičare u CC sisteme.

Mrežni forenzičari u ovakvom okruženju moraju biti fokusirani samo na podatke koji dolaze sa ili odlaze ka sistemu kojem kompanija ima pristup, iako će ovakvo fokusiranje uzrokovati nedostatak ostatka stvarne slike sistema. Mrežna forenzika mora biti deo zajedničkog angažovanja svih komponenti koje se ujedinjuju u kompjuterski sistem. Bez mrežnog forenzičkog istraživanja, prilikom razumevanja arhitekture CC okruženja, i mogućih kompromisa će doći do previda ili propusta. Mrežni forenzički istraživač takođe mora da razume ovaj kompjuterski sistem kao sistem u kome jedna kompanija iznajmljuje od druge prostor za rad.

Iznajmljeni prostor u ovakvom sistemu može biti globalni pristupni informacioni centar povezan sa mnogim drugim kompanijama gde se korisnička mrežna pristupna tačka može nalaziti na bilo kom mestu na Internetu. Podaci u ovakvom okruženju mogu biti kopirani u bilo kom informacionom centru svetu i oni su u vlasništvu i upotrebi provajdera usluga

[7] W. Pieters, A. van Cleef, *The precautionary principle in a world of digital dependencies*, 2009., str. 50–56

CC sistema. Provajder ovakvog sistema ima svoje sopstvene politike, bezbednosne sisteme, hardverske i softverske pakete koji su nezavisni od toga šta koja kompanija radi u okruženju. Korisnici usluga ovakvog sistema mogu ali i ne moraju imati dozvoljen pristup podacima kojima se raspolaže u sistemu ukoliko je kompjuter sa kojeg se pristupa mreži osumnjičen da je žrtva malicioznih programa ili hakera, ili da su podaci ukradeni od strane insajdera ili autsajdera.

Ova kompleksna serija veza između provajdera i korisnika usluga u ovakvom sistemu obezbeđuje plodno tlo za hakere i kriminalce koji žele da provale u sistem zbog njihovih ličnih interesa. Ovakav sistem, takođe, prestavlja plodno tlo i za insajdera, pre svega zbog jeftine cene podešavanja za rad u ovakvom sistemu. Za otprilike $40 mesečno može se izvršiti potpuno podešavanje servera za bilo kakvu upotrebu ili bilo kojeg korisnika koji ima kreditnu karticu. Jednostavni programi poput WinSCP se mogu koristiti za pristup kompjuteru koji funkcioniše u ovom sistemu, ili ako se valjano konfiguriše može jednostavno biti kao bilo koji drugi FTP server (*File Transfer Protocol*) na Internetu što znači da bilo koji FTP klijent uključujući i Windows mounting process može biti korišten za ostavljanje podataka na server.

Neke kompanije poput Drop box i Mozy nude ove usluge besplatno do 2 GB informacija po korisniku e-mail adrese. Cena nerazumevanja mrežne forenzike u ovakvom kompjuterskom sistemu može biti pogubna za bilo koju kompaniju, ako se desi da su njeni podaci izgubljeni ili možda ukradeni od strane nekog zaposlenog.

Ovakav kompjuterski sistem sa svim svojim prednostima i ograničenjima, može takođe biti veoma komplikovano okruženje za tradicionalno obučenog profesionalca da razume samo kako su mreža i sistem u ovakvom kompjuterskom sistemu porozni i kako tradicionalna forenzika ne može da se u potpunosti uklopi u CC sistem.

Sa Amazon Web servisom (Amazon Web Services, AWS) kupuje se lik Amazon mašine (Amazon Machine Image, AMI) kako za Linux tako i za Windows. Sa ovakvim servisima se mogu pokrenuti virtuelne mašine i raditi sve stvari koje podržava operativni sistem. Ovim servisima se ne stiče vlasništvo nad mrežnom arhitekturom, mrežnim barijerama informacionog centra, niti nad hardverom koji podržava instalirani softver. Ipak, korisnik usluga poseduje svoju celokupnu virtuelnu mašinu, bilo Linux ili Windows i sa njom može da radi šta god hoće, u okviru granica virtuelnog sistema.

Ovo je skoro identičan način podešavanja virtuelnog sistema kao i onaj na koji su kompanije podešavale svoje interne virtuelne sisteme u okviru svojih kompanijski kontrolisanih informacionih centara. Ovo uzrokuje migracije alata i aplikacija u odnosu na alate i aplikacije koje su se koristili u tradicionalnim kompjuterskim sistemima a kojima je bilo neophodno da naprave promene u registrima kompjuterskog sistema koji je u funkciji. Ključna stvar kod Amazona je ta što kada jednom virtuelni server bude ugašen, lik biva izgubljen i nemoguće ga je povratiti, zato je veoma važno da se nikada ne zatvara lik koji se istražuje, sve dok forenzičko istraživanje ne bude kompletirano od strane forenzičara ili forenzičkog tima.

Kod Microsoft Azure, korisnik poseduje sve iznad operativnog sistema i ne može menjati ništa u operativnom sistemu, uključujući i registre. Bilo koji sistem koji je instaliran u sistemu može biti instaliran kao XCopy[8], i u tom slučaju softver ne može praviti nikakve promene u registrima kompjutera ili zahteva dublju integraciju u operativni sistem kao što većina softvera koji su bazirani na Windows čine. Kod ovog programa ne može se otkloniti neispravnost aplikacija u okviru programa da bi se videlo da li se nešto dešava u mreži[9].

Ovaj program je uokviren kao podrška Web servisima i zahteva novi pristup razmišljanja o programu posebno u odnosu na tradicionalni softver, uključujući otkaze i iznenadna gubljenja kompjuterskih sistema. Upotreba ovog programa će ubrzati operacije za transakcionalne i merljive sisteme, ali nalik Amazonu, jednom izgubljeni lik nije više dostupan analizama i istraživanju.

Rackspace sledi isti dizajn kao i Amazon, ali je prilagođeniji Linuxu nego mešavini više operativnih sistema. Nalik Amazonu, data je jednostavna virtuelna mašina koja može da radi šta god je potrebno. Rackspace je fleksibilniji sa dinamičnim redimenzionisanjem i procesiranjem sistema koji je kompanija iznajmila, ali zbog upotrebe jednog operativnog sistema tipično mešovito okruženje u većim kompanijama ne postoji. Kao i kod drugih osnovnih provajdera CC sistema kada se virtuelna mašina ugasi nemoguće je oporaviti ili povratiti podatke jer su oni zauvek izgubljeni.

Platforma i usluge koje kompanija kupuje su osnovne tačke za mrežnu forenziku. Kada se donosi odluka koji će se provajder koristiti veoma je važno znati kako ovakav sistem funkcioniše, kada šta i sa čim može biti učinjeno i šta i sa čime ne može biti učinjeno. Neki procesi su veoma dobri u ovakvom okruženju poput transakcionih procesa, merljivih Web servera i usluga. Ovo okruženje je takođe veoma snažno u slučaju izvršenja velikog broja zadatih operacija i zadataka ili u slučaju obrade podataka iz ogromnih baza podataka (kapaciteta reda veličina terabyte) ili za bezbednosnu pretragu log fajlova.

Kompaktna ograničenja ovakvog okruženja se moraju poznavati ako se želi uspešno realizovati mrežna i kompjuterska forenzika. Odluka o upotrebi provajdera u ovakvom okruženju mora biti razmotrena ne samo zbog usluga koje provajder nudi, već i zbog toga kako kompanija koja ih kupuje ima nameru da ih koristi. Odluka ima direktnu implikaciju na to kako će se upravljati kompjuterskom i mrežnom forenzikom. Veoma je važno da odeljenje za bezbednost kompanije ima ravnopravan glas u kompanije prilikom izbora provajdera i na pravo nadzora nad uslugama izabranog provajdera.

Postoje mnoge zajedničke osobine svih provajdera u ovakvom sistemu koje odeljenja za bezbednosti i forenzičari mogu slediti uprkos različitim provajderima i uslugama koje su obezbeđene u ovakvom sistemu. U nekim slučajevima, uprkos namerama provajdera, virtuelno okruženje će komplikovati, a u nekim smanjivati efektivnost mrežne forenzike.

---

[8] D. Chappell, *Window Azure and ISVs: A guide for decision makers*, Microsoft Corporation, 2009., str. 2

[9] D. Chappell, *Introducing the Windows Azure platform*, Microsoft Corporation, 2009., str. 17

Zajedničke osobine provajdera ovog sistema su sledeće[10]:

- Onemogućen je pristup mrežnim ruterima i ostalim komponentama mrežne arhitekture.

- Onemogućen je pristup velikim instalacijama mrežnih barijera, najbliža mrežna barijera je ona koja se nalazi u operativnom sistemu.

- Ne postoji mogućnost dizajniranja mrežne mape poznatih skokova sa jedne tačke na drugu koja će ostati statična ili konzistentna duž ruterske šeme sistema.

- Sistem se podrazumeva kao robni sistem koji se dizajnira da može biti podignut i ugašen prema korisnikovoj želji. Kada je virtuelna mašina ugašena ne postoje fizički podaci tog lika i on je jednostavno izgubljen. Ako je virtuelna mašina bila spuštena onda je ceo sistem, uključujući i log fajlove uništen i neće moći biti oporavljen.

- Virtuelna mašina može biti podignuta i ugašena po želji bilo kog broja administratora u kompaniji i to na osnovu jedne *on-demand* usluge. Kompanija mora da napravi novi komplet bezbednosnih politika i planova da bi radila sa sumnjivim kompromitovanim serverima i uslugama.

- Moguće je napraviti bistrim (*bitstream*) lik virtuelne mašine ali samo u skladu sa standardom ISO (*International Organization for Standardization*) koji se može istraživati *offline*. Ipak, ISO lik se može pohraniti i u okviru sistema Distribuiranog Internet računarstva radi deljenja sa licima koja sprovode zakon ili pravnim savetnicima.

- Koje su usluge u ovakvom okruženju obezbeđene, poput Softvera kao usluge (*SaaS*) ili Platforma kao usluga (*PaaS*) ili Infrastruktura kao usluga (*IaaS*), proizvodi razlike u tome kakve će bezbednosne saglasnosti, kontrole, politike i istraživačke standarde kompanija implementirani[11].

- Pretnje po izložene usluge u CC sistemu su iste kao i po bilo koje druge izložene usluge koje kompanija nudi bilo kome drugom na Internetu.

- Mrežni forenzičar je ograničen na alat na ograničenom prostoru pre nego na celokupnoj mreži jer istraživač ne može koristiti dostupan alat u celoj mreži.

---

[10] Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, James "Jim" Steele, *Digital forensics for network, Internet, and cloud computing*, Syngress 2010, str. 8

[11] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, April 2009, str. 20

Koncept mrežne forenzike u ovakvom sistemu zahteva novi aspekt sagledavanja problema bezbednosti jer nekada neki podaci neće biti dostupni, neki podaci će biti sumnjivi, neki podaci će biti spremni za sud i mogu se uklopiti u tradicionalni mrežni forenzički model. Izazov za svakog forenzičkog istraživača je da shvati koji komplet podataka spada u koju kategoriju i to dostupne, sumnjive ili spremne za sud.

Rad sa kompanijskim pravnim savetnicima i ekspertima u ovakvom kompjuterskom sistemu će biti potreban sve dok se udruženja za opštu bezbednost podataka ne uhvate u koštac sa promenama koje donosi ovakav kompjuterski sistem po bezbednost informacija uopšte.

Model ovakvog kompjuterskog sistema može biti veoma koristan za forenzičare jer dozvoljava skladištenje veoma velikih log fajlova na skladišnim mestima ili veoma velikih baza podataka za jednostavno povlačenje podataka i otkrivanje. Neki od novijih alata za vizuelizaciju omogućavaju odličnu forenziku i predstavljaju odlične alate za rano upozoravanje inžinjera i istraživača bezbednosti. Neki alati za vizuelizaciju podataka rade zapravo isto kao i tradicionalni alati poput NetFlow, ali oni nisu imali nikada nameru da budu mrežni forenzički alati.

Od inžinjera bezbednosti i IT stručnjaka se zahteva da budu kreativni sa svojim postojećim alatima, kao i da ih učine funkcionalnim u postojećem kompjuterskom sistemu. Dodatni problem čini pitanje kako mrežna forenzička istraga može biti uspešna u ovakvom kompjuterskom okruženju ukoliko je ono nepoznato inžinjerima bezbednosti. Odeljenje bezbednosti trebalo bi biti deo celokupnog procesa donošenja odluke počevši od izbora arhitekture, usluga i sistema koji će biti stavljen u provajderov informacioni centar.

Ukoliko je odeljenje bezbednosti informacija uključeno u proces od samog početka i ako se desi neki bezbednosni incident, stručnjaci za bezbednost će biti potpuno upoznati sa logičnom konstrukcijom kompjuterskog sistema. Odelenje bezbednosti mora znati u kakvom su međusobnom odnosu kompjuterski sistem i usluge, odnosno kako je arhitektura konstruisana da omogući deobu podataka kroz mnogostruke granice sistema i kompjuterske slojeve. CC okruženje dolazi sa svojim kompletom standarda, terminologije i najbolje prakse što može biti jako teško za upravljanje u okviru tradicionalnog bezbednosnog konteksta.

Takođe je veoma teško, sada, znati šta se događa sa sistemom u ovakvom okruženju zbog nedostatka dobro razvijenih alata ili standarda bezbednosti informacija i prakse. Postoje veoma dobri pokušaji u razvoju standarda i prakse bezbednosti informacija, ali oni još uvek nisu univerzalno adaptirani i prilagođeni za sada veoma dinamičnom i promenljivom okruženju. Adaptacija i prihvatanje ovakvog sistema u kompanijama je takođe zakomplikovana sa tolerancijom rizika koje kompanije imaju i koliko dobro su razvijene definisane potrebe za kompjuterskim sistemom u okviru sveukupnog poslovnog modela kompanije.

Ni jedna diskusija o ovakvom kompjuterskom sistemu se ne može kompletirati bez razumevanja pretpostavke rizika koji se može dogoditi prilikom premeštanja podataka i usluga u informacioni centar neke druge kompanije. Neke kompanije imaju regulatorne i pravne zahteve koji moraju biti upućeni u ovakvom kompjuterskom sistemu. Nedavno, provajderi ovakvih sistema su takođe upućivali ovakve zahteve, poput skoro kompletiranog SAS 70 sertifikata u AWS centru podataka (*Amazon Web Services, 2010*). Procena rizika za ovakvo okruženje treba da prati standardni proces procene rizika, ali mora inkorporirati činjenicu da kompanija ne poseduje hardver niti mrežnu infrastrukturu.

Tehnički, mrežni provajderi u ovakvom kompjuterskom sistemu imaju pristup svim podacima duž celog sistema u sopstvenim informacionim centrima. Kompanija koja traži usluge ovakvog kompjuterskog sistema mora da balansira rizik i mogućnost nastanka incidenta (štete) na podacima kojima se pristupa, koji se menjaju ili koji se odbijaju u sistemu.

Sa stanovišta bezbednosti mreže svi podaci koji se preusmeravaju kroz sistem su vidljivi i može im se pristupiti sa strane mrežnog provajdera. Ipak, svi podaci nisu vidljivi kompaniji koja je kupila usluge sistema zbog snažnih ograničenja u virtuelnom okruženju koja koriste provajderi ovih sistema.

2.1.5. Istraživačka i forenzička metodologija

Istraživačke i forenzičke metode u CC sistemu su drugačije u odnosu na tradicionalne kompjuterske sisteme. Ove metode predstavljaju dodatak standardno dobro razumljivom forenzičkom procesu u kojem se mrežni uređaji i dodeljene mreže mogu fizički dostići i pregledati. CC sistem postavlja dodatne izazove pred forenzičara kojem nije bliska istraga virtuelnog lika udaljenog sistema koji nije fizički dostupan ili koji ne raspolaže odgovarajućim alatom za efikasnu istragu u ovakvom okruženju.

Virtuelizacija operativnog sistema dozvoljava implementaciju mnogih različitih operativnih sistema koji dele istu, osnovnu platformu izvora. Operativni sistem i bezbednosni softver operativnog sistema dele isti hardver i mnogo drugih (N + 1) "servera" na fizički istom hardveru. Hipervizor je *host* operativni sistem koji realizuje dodeljivanje resursa, kao što su RAM, CPU i disk I/O, između svih operativnih sistema koji su pokrenuti kao " gostujući operativni sistemi".

Kao što je ranije rečeno, dok je pokrenut *host* operativni sistem, hipervizor, kao softver koji usmerava saobraćaj, čini mrežnu karticu beskorisnom za forenzičara iako je mrežna kartica podešena za rad u slobodnom modu. Hipervizor, takođe, dinamično kontroliše upotrebljene RAM i CPU, čineći nadzor RAM sumnjivim kao informaciju spremnu za sud. Dinamični proces duž celog hipervizora i upotreba virtuelnih prostora dramatično limitira aktivnosti forenzičara. Jako je mala ili nikakva mogućnost zamrzavanja upotrebljenog RAM ili šta je u L1 i L2 keš memoriji ili šta je na mrežnoj kartici šta bi se od navedenog moglo povezati sa forenzikom u ovakvom kompjuterskom okruženju.

Realno, metodologije koje se upotrebljavaju moraju se menjati da bi se prilagodile dinamičnom i tekućem kompjuterskom okruženju u kojem se mrežni protok može pojednostavljeno predstaviti kao uređaj koja radi onlajn i čiji rad je narušen. Ovo nije samo podrška kompanijama da upravljanju svojim poslovima, već i podršku softveru koji se koristi za posao. Ovo će frustrirati standardne forenzičke alate, jer su ograničeni na virtuelne mašine sve dok mrežne barijere i mrežni interfejsi nisu dostupni.

Dobra strana CC sistema je ta što nisu svi svesni njegovog potencijala niti rizika koji proizilaze iz rada u takvom okruženju. Što se više pristupa podacima i što se više podataka deli između sistema, to je više tragova o pristupu i deljenju jer obično korisnički interfejs skladišti podatke uključene u proces negde u softveru. Uskladišteni podaci su prednost za istragu, dozvoljavaju forenzičaru da izvrši nesmetano proces. Ali, to takođe znači da bilo ko ko ima pristup uređaju u kontekstu korisnika može da ima pristup bilo kom sistemu koji ima uskladištene podatke. Ovo obezbeđuje plodan izvor informacija i pomoćnih sistema koji mogu biti deo istrage.

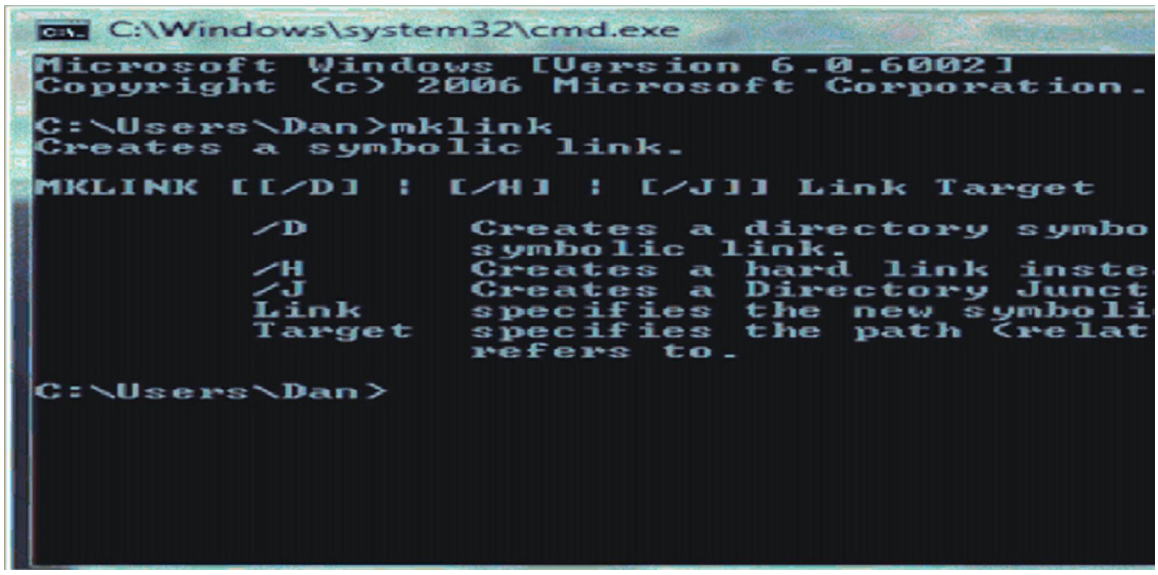
Ljudi su, povrh svega, stvorenja sa navikama i loše navike udružene sa skrivenim dokumentima, kao što su neočišćena skladišta pretraživača i fragmenti fajlova mogu ukazati na materijal koristan za istraživanje. Često se ovi podaci nalaze na korisničkim sistema poput laptopova, desktopova i mobilnih telefona. Sistemi servera ne bi trebao da imaju softvere kojima se može upasti u privatne *drop box* u ovom okruženju, ali ako postoje onda dodatno usmeravaju forenzičku istragu.

Drop box je Web bazirana fajl *host* usluga koja se upotrebljava u ovom okruženju radi omogućavanja korisnicima skladištenje i deljenje fajlova i foldera sa drugima u Internetu upotrebom fajl sinhronizacije.

Sistemi u kojima se može upadati u *drop box* imaju privatna skladišta na korisnikovom kompjuteru koji obezbeđuju bogatstvo informacija kao što je skladišni trodnevni ciklus, što znači da je sve ono što je izbrisano sa kompjutera u zadnjih tri dana ostalo uskladišteno, sve do sledećeg ciklusa brisanja lokalnog skladišta. Ova rezervna kopija na lokalnom kompjuteru može omogućiti forenzičaru da ima najmanje trodnevni pregled o tome šta se dešavalo na kompjuteru ili mreži jednog korisnika. Sistemi kojima se može upadati u *drop box* kroz Web interfejse imaju takođe opciju *Recent* koja se može koristiti samo onda kada je forenzičaru omogućen legalan pristup sistemu da odredi ko je nedavno pregledavao i skidao fajlove.

Mnogi dodaci funkcionisanju operativnih sistema, sa dodacima novih kompleta komandi u operativnim sistemima na koje možda forenzičar nije svestan su samo neki od stvari koje komplikuju posao forenzičke analize. CC okruženje zahteva da je forenzičar svestan mnogih načina na koje podaci mogu da iscure sa jednog sistema na drugi. Bilo koji uređaj povezan u mrežu može pristupiti podacima poslanim *drop box* samo ako je i on na *drop box*, čineći opciju *Recent* važnim dodatkom za prikupljanje podataka u mrežnoj forenzici.

Ako forenzičar sumnja da je kompromitovani kompjuter bio korišten za skladištenje podataka na *drop box* ili nekom njegovom ekvivalentu, korisno je pogledati simboličnu vezu između lokalnih foldera i *online* drajv sistema. *Mklink* je linijski komandni alat kod Windows 7 i Vista koji omogućava da se napravi simbolična veza koju su napravili drajv sistemi ovog okruženja da bi uskladištili podatke ili izvršili transfer fajlova. Pregled kompjuterske hijerarhije fajlova radi potrage za simboličnom vezom koja upućuje na drajvere CC okruženja je brz i jednostavan put ka postavljanju *off-site* sistema i brzog napuštanja detekcije tako da izgleda kao normalan mrežni saobraćaj kroz *Hypertext Transfer Protocol* (HTTP).



Slika 4. Prikaz *Mklink-a*

Dobra strane ove funkcije za svakog forenzičara je simbolična veza, koja daje i informaciju kada je napravljena. Standardno, jedina lica sa administrativnim pristupom mogu napraviti simbolične veze, ali softverska instalacija takođe, može da ovo izvede ako je pokrenuta kao administratorska. Važno je u CC okruženju potražiti povezane fajlove i foldere kada se istražuje sistem i onda, ukoliko je moguće, povući logove lokalnih mrežnih barijera da bi se videlo koliko često se ovim vezama pristupalo kako od strane lica koji koriste sistem tako i od malicioznih programa. Ova činjenica usložava forenzičku istragu, ali može i da ukaže na ostale izvore informacija koji možda nisu odmah bili vidljivi na kompromitovanom sistemu.

Aplikativni softver koji je direktno dodat mrežnoj podeli će pokazati pravila mrežnih barijera na lokalnom uređaju koji obezbeđuje dodatne informacije mrežnom forenzičaru, poput čitanja log fajlova lokalnih mrežnih barijera. Ovi log fajlovi su odlučujući elementi u određivanju vremena i mesta veze koja je učinjena mrežnim drajverima u CC okruženju. Razvijeni lokalni uređaji za nadzor mreže mogu pomoći rešavanju odlazeće mrežne podele i aktivnosti upotrebom *drop box* ili *Mozy* ili čak posebno napravljenom mrežnom podelom u ovom okruženju za neku kompaniju.

Ograničenja u ovome procesu proističu iz toga da mrežni nadzor može biti realizovan samo na aktuelnoj mreži koju poseduje kompanija dok je jedina aktivnost za vreme za koje se logovalo na sistem bola pristup log fajlovima i logovima mrežnih barijera CC sistema. U sistemu koji obezbeđuje Softver kao uslugu, ovo postaje približno nemoguć zadatak bez boljeg razvoja forenzičkih alata.

2.1.6. Mesto i uloga forenzike u Digitalnom Internet računarstvu

Forenzika igra značajnu ulogu u CC okruženju, ali sa ograničenjima koja vežu forenzičara duboko za mrežnu i kompjutersku forenziku. Forenzika ovakvog okruženja je najbolje primenjena tamo gde je mreža u vlasništvu kompanije, odnosno na granicama sistema i na desktopu ili sistemima koji imaju pristup resursima okruženja. Forenzičari rade u ovom okruženju u trenutku kada kompanije upućuju mnoga ograničenja forenzici, odnosno u trenutku kada mnoge kompanije još uvek izgrađuju sopstvenu infrastrukturu ovakvog okruženja. Moguće je vratiti se i ponovo podesiti osnovnu forenzičku sposobnost, što treba uraditi ako sposobnost upravljanja forenzikom nije deo originalnog biznis plana pomeranja informacija i sistema u CC okruženju.

Forenzika upakovana u ovo okruženje mora postaviti upit kada informacija bude poslata ka bilo kojoj granici između unutrašnjih i spoljašnjih procesa, što je jako teško pratiti tradicionalnom mrežnom forenzikom. Jednom kada informacija bude poslana u okruženje, forenzičar postaje deo kompjuterske i mrežne forenzike sa ciljem da odredi koji sistem je bio povezan sa kojim i u koje vreme. Forenzičar može imati kritičnu ulogu u izolovanju unutrašnjeg sistema od incidenata, odlučujući koji nivo kompromitovanja je došao iznutra a koji spolja.

Forenzičar može ostvariti uticaj na rezultat istrage o incidentu onoliko dugo koliko je potrebno da se podaci sakupe u kompjuteru na ulaznim i izlaznim tačkama kompanijske mreže. Upotreba osnovnih logova mrežne barijere, sistemskih logova i ostalih logova može ukazati na vreme pristupa, mesto i IP adrese koje mogu pomoći pri određivanju kako se incident širio kroz mrežu i koji bi se koraci morali preduzeti da bi se minimizirao bio kakav budući događaji, obezbeđivanjem solidnih podataka o nastalom događaju. Veliki deo forenzike predstavlja sposobnost nadzora nad mrežnim saobraćajem koja ima za cilj izolovanje određenog broja servera koje treba istražiti tradicionalnim forenzičkim procesom.

U ovom stadijumu, proces postaje problematičan jer su granice kompromitovanog sistema sa bilo kojim sistemom sa kojim ima pristup porozne. Forenzika može biti proređena sa dubljom kompleksnom inspekcijom paketa zaglavlja i šifrovanog sadržaja, kao i sa potpunom statusnom inspekcijom. Ovo je mnogo sličnije bilo kom dobrom sistemu detekcije upada (IDS) ili sistemu zaštite od upada (IPS). Problem je što je u informacionom centru CC okruženja forenzičar ograničen na podatke koji se mogu oporaviti na serveru. Saobraćaj koji je na matičnoj ploči mreže neće biti dostupan zbog načina na koji sistem virtuelizacije funkcioniše.

Mrežni forenzičar mora da zapamti da je saobraćaj usmeren ka serveru koji se istražuje jedini saobraćaj koji je vidljiv bilo kojim forenzičkim alatom koji je pokrenut na nivou servera. Nemoguće je izolovati seriju kompromitovanih kompjutera i nemoguće je "njuškati kroz lokalnu mrežu" u ovom okruženju zbog načina na koji sistem hipervizora i virtuelizacije funkcionišu.

Sa ograničenjima kompleta alata, kao najbolji alati su se pokazali oni najjednostavniji, pre svih *Wireshark* i *Snort* za Windows i Linux i *WinPcap* za Windows, kao i osnovne mrežne barijere za oba operativna sistema. Forenzički alati koji se koriste u ovom okruženju ukazuju na to da nadzor mreže dobija na značaju. Što više alata za vizuelizaciju podataka i alata za kontrolu protoka može biti napravljena da radi u CC okruženju nezavisno od ograničenja operativnog sistema ili hipervizorovih ograničenja bilo kog virtuelnog sistema, forenzika će biti efektivnija i sposobnija. Premda, forenzika sada predstavlja proces nadzora nad osnovnim sistemom koji može biti skuplji, vezano za angažovanje radne snage i upravljanje logovima, bez upotrebe istih sredstava okruženja da pomogne da se otarasi nekih od pretraživačkih i istraživačkih procesa u značenju podataka log fajlova.

2.2. Odgovor na incident u Distribuiranom Internet računarstvu

2.2.1. Značaj integracije mrežne i forenzike domaćina

Istorijski, odgovori na incidente u mreži i na domaćinu su bili odvojeni, sa odvojenim područjima operacija sa malom ili nikakvom saradnjom između onih koji su se specijalizovali za bilo koju od ove dve oblasti[12]. Jaz između ove dve tehnike se pripisuje brojnim razlozima, uključujući i poznavanje različitih tehničkih zahteva, različitih procedura i procesa, administrativnih i političkih realnosti sa kojima se susreće svaka organizacija i na kraju uključenih setova alata.

Ovaj nesrećni disparitet za rezultat ima pojavu i postojanje neefikasnih tehnika kojima organizacije obezbeđuju svoje mreže. Razvojem *sajber* napada i obaveštajnih struktura, unapređenjem obrazovanja kriminalaca kao i povećanjem broja sofisticiranih eksploatacija ovaj problem će se samo uvećavati ako se ne preduzmu neki konkretni koraci na povećanju bezbednosti mreža. Nedostatak sposobnosti odgovora je duboko ukorenjen problem koji mora biti razumljiv i mora biti upućen na adrese korporacija i vlada.

Da bi došli do željenog cilja, moramo znati gde se trenutno nalazimo. Trenutno stanje možemo pokazati analizom tradicionalnog procesa odgovora na nastali incident.

U tradicionalnoj metodologiji jedan incident može biti identifikovan upotrebom različitih sredstava i tehnika[13], poput:

- Antivirus upozorenja (AV)
- Sistemi za detekciju napada (IDS) i Sistemi za prevenciju napada (IPS)
- Mrežne barijere (FW) i/ili Sistem upravljanja bezbednosti informacija (SIMS)
- Kartoni problema (sporih ili nestalnih performansi)
- Neobjašnjive i neautorizovane modifikacije naloga
- Odbijanje Izveštaja korisnika usluga (DoS)

[12] AccessData Corporation, *The importance of Integrating Host and Network Forensics*, USA 2005., str. 1
[13] AccessData Corporation, *The importance of Integrating Host and Network Forensics*, USA 2005., str. 1

Kratak pregled ove liste otkriva da ovi izvori mogu da budu podeljeni u dve široke kategorije i to one koje se bazirane na mrežnoj forenzici i one koje se baziraju na forenzici domaćina. AV, IPS, Kartoni problema, Modifikacija naloga i DoS koriste domaćina kao izvor, dok IDS i SIMS koriste mrežu kao izvor podataka. U razumevanju ovakve podele leži problem odgovora na nastali incident.

Za istraživanje mreže kao izvora se formira poseban tim koji odgovara na incident i istražuje ga, dok se identična procedura sprovodi kada za izvor imamo domaćina. Ukrštanje rada ova dva, nezavisna i odvojena tima se retko dešava.

Nedostatak integracije za posledicu ima neuspešno upravljanja većinom procesa odgovora. Često nedostatci nastaju u međuprostoru rada dva tima. Ovaj nedostatak je neizbežan u slučaju primene tradicionalne forenzičke metodologije jednostavno zbog toga što i mrežna i forenzika domaćina imaju svoje slabosti i nedostatke.

2.2.2. Odgovor na incident koji koristi mrežu kao izvor

Odgovor na incident koji se bazira na mreži kao izvoru podataka ima svoje prednosti i slabosti.

Sofisticirani izvršilac napada je jako svestan da postoje predmeti koji su rezultati eksploatacije na nivou domaćina. Ovi predmeti se mogu naći u memoriji (promenljivi podaci), fajlovima, razmenjenim fajlovima, hard diskovima, USB drajvovima, CD/DVD i ostalim statičkim medijima. Kako se ovi predmeti lako mogu detektovati, tako mogu i da se učine nejasnim, odnosno potpuno da se izbrišu i na taj način učine potpuno beskorisni.

Tehnika je veoma poznata, bilo koja prosta Google pretraga za „anti-forensics“ doneće pregršt pronađenih, jednostavno primenjivih, skripti i tehnika koje se mogu realizovati uz minimalan napor. Čak i najnespremniji napadač može pronaći i iskoristiti ovakve predmete. Napadačima je neophodno samo da „poseduju“ domaćina da bi razvili i upotrebili ove metode.

Upotreba ovih metoda ustvari predstavlja prednost procesa odgovora na nastali incident koji se bazira na mreži kao izvoru[14]. Napadač nikada precizno ne može da zna gde se podaci sakupljaju na mreži niti gde se skladište (pogotovo u CC sistemu), što u praksi znači da napadač nije sposoban da koristi ovakve podatke koji ostaju netaknuti.

Postoje dve slabost odgovora na nastali incident koja se bazira na mreži kao izvoru. Prva slabost je ta što je jako lako nekoga „nasamariti“, odnosno učiniti da se pojavi nešto što ustvari ne postoji ili nije u stvarnosti kao u prikazanom stanju. Ukoliko ne postoji veoma striktan izvor paketa tekućih podataka nemoguće je sa sigurnošću tvrditi odakle je i kada je nešto stiglo.

[14] AccessData Corporation, *The importance of Integrating Host and Network Forensics*, USA 2005., str. 2

Druga slabost predstavlja skretanje delova podataka koji se upućuju. Velike količine paketa se preusmeravaju tokom protoka čak i u najprostijim mrežama. U cilju nadzora ovih podataka često je obavezno implementiranje neke vrste podešavanja ili filtriranja ogromnih količina podataka. Upotreba podešavanja i filtriranja podataka izaziva određene probleme, poput onih kada se vrši precizno podešavanje i na taj način se gube određeni delovi ili celi podaci, odnosno kada se vrši grubo podešavanje i filtriranje koje rezultira ogromnim količinama podataka koji se moraju prilagođavati.

2.2.3. Odgovor na incident koji koristi domaćina kao izvor

Proces odgovora na incident koji se bazira na domaćinu kao izvoru je veoma solidan jer obezbeđuje postojanost podataka[15]. Tehnologija je veoma razvijena i u literaturi dobro objašnjena, tako da je poznat postupak odgovora kada dođe do pronalaska, filtriranja, izolovanja i izveštavanja o izbrisanim fajlovima, razmenjenim prostorima, izlistanim predmetima i drugačije korumpiranim ili zamenjenim fajlovima. Velika količina spakovanih „digitalnih otisaka" je izdana da bi obezbedila neoborive dokaze da je to taj fajl. Mala je šansa da dođe do prevare da li je to fajl koji je interesantan za proces odgovora na incident.

Proces odgovora na incident koji se bazira na domaćinu kao izvoru veoma brzo sazreva u okruženju analize memorije (*resident memory analysis*). Procesi koji su sakriveni u memoriji, uhvaćeni ili ubačeni *dlls* se takođe lako detektuju. Istraživanje domaćinove memorije lako otkriva skrivene procese.

Ponekad je korumpirani predmet kompletno očišćen. Proces čišćenja može biti prost kao i proces defragmentacije diska, mada retko potpuno efektan ili kompleksan poput višestrukog prepisivanja površine diska u skladu sa Federalnim standardom obrade informacija FIPS.

Inkriminisani predmeti takođe mogu biti zaštićeni šifrom. Postupak kodiranja je izuzetno usavršen, tako da često predstavlja nepremostiv problem jer možemo posedovati podatke koji su šifrovani tako da su potpuno beskoristni za istragu.

2.2.4. Integracija tehnika odgovora na incident

Kao i kod kombinovane vojne taktike, gde pojedine specijalnosti pokrivaju slabosti drugih specijalnosti, odnosno druge specijalnosti obezbeđuju sopstvene slabosti, i kod procesa odgovora na incident možemo koristiti integraciju dveju tehnika da bi napravili jedan komplementaran i kompaktan proces i obezbedili da slabosti jedne tehnike budu

[15] AccessData Corporation, *The importance of Integrating Host and Network Forensics*, USA 2005., str. 2

nadoknađene prednostima druge. Integracija tehnika odgovora na incident se najbolje može prikazati na primeru jedne od najopasnijih tehnika mrežne eksploatacije *EPROM rootkit*.

Rootkit predstavlja specifičnu vrstu malicioznog softvera koji se sakriva odmah po instaliranju, a zatim otvara procese i specifične sektore hard diska, a takođe ostvaruje i mrežne kontakte za zadnja vrata na mreži. U slučaju *EPROM rootkit*, ovaj maliciozni softver se instalira na EPROM (Erasable Programmable Read-Only Memory) nekog perifernog uređaja ciljanog računara. Ovaj periferni uređaj je najčešće mrežna kartica ili zvučna kartica. *EPROM rootkit* se takođe može naći instaliran i na memoriji video kartice.

Ono što čini *rootkit* tako opasnim jeste njegova sposobnost da preživljava reinstalaciju inficiranog uređaja. Od trenutka kada se njegov kod nastanio u memoriji perifernog uređaja brisanje operativnog sistema je neefikasno za oporavak sistema. Čim se novi operativni sistem instalira on poziva drajvere perifernih uređaja, EPROM šalje *rootkit* u RAM memoriju i opaki, skriveni proces je ponovo aktivan i otvara skrivene konekcije izvan mreže. Njegove aktivnosti u memoriji na inficiranom uređaju je izuzetno teško detektovati. Kako on ne vrši eksploataciju domaćina on zahteva napadački vektor kako bi ga inficirao. Ova činjenica predstavlja jedinstvenu priliku za prvo detektovanje njegovih aktivnosti.

U slučaju odgovora na incident kombinovanim tehnikama, tim za odgovor na incident koji koristi mrežu kao izvor, odnosno IDS bi trebao da detektuje *rootkit* napadački vektor.

U nekim slučajevima se može desiti da IDS nema poslednje ažurirane signature malicioznih softvera ili da ih uopšte ne poseduje, odnosno može se dogoditi da je IDS isključen i da signatura nije aktivna. Međutim, čak i u ovakvim slučajevima se mora obezbediti da se celokupan mrežni saobraćaj snima i skladišti za buduće preglede bez obzira da li znamo da je on maliciozan ili ne u određenom trenutku.

U ovom trenutku se uključuje tim za odgovor na incident koji koristi domaćina kao izvor. Ovaj tim istražuje ciljanog domaćina upotrebom različitih alata. On može upotrebiti *rootkit* detektore otvorenih izvora, binarne *boot* diskove ili standardne alate operativnih sistema za izvođenje svojih ispitivanja. Ukoliko ne upotrebimo tehnologije *rootkit* detekcije ili istraživanja promenljive memorije pre isključivanja računara propustićemo zapažanje infekcije. Ukoliko je *rootkit* „okačio“ svoja zadnja vrata na neki od postojećih portova, kao što je *http*, čak ni skeniranje mobilnih portova neće ga detektovati.

2.2.5. Integracija alata

Ako izaberemo set alata koji obezbeđuje kompletnu integraciju tehnika odgovora na incident (upotrebu mreže i domaćina kao izvora) eliminisaćemo sve tačke slabosti koje su se pojavljivale odvojenom upotrebom pojedinačnih tehnika, naročito onih koje su

nastajale u međuprostorima delovanja dva odvojena tima. Takođe, primenom ovakvih alata eliminišemo latentnost koja se može pojaviti prilikom razmene podataka između dva tima. Sprovodeći oporavak upotrebom integrisanih alata dozvoljavamo više neposrednih oporavaka od infekcije. Upotrebom integrisanih alata može se sažeti obuka i na taj način redukovati troškovi.

Ovakav pristup procesu odgovora na nastali incident je jedina uspešna strategija u borbi protiv incidenta. Da bi se realizovala ovakva strategija neophodno je da setovi integrisanih alata ispune određene zahteve[16], i to:

- Obavezno snimanje celokupnog mrežnog saobraćaja.
- Saobraćaj mora biti sposoban za ponovnu reprodukciju.
- Sadržaj mrežnog saobraćaja mora bit izdvojen u prirodnom formatu.
- Izdvojeni mrežni sadržaj mora biti integrisan u alat za ispitivanje na nivou domaćina.
- Matični fajlovi moraju biti sposobni za brisanje jer proces uklanjanja uništava inficirane fajlove.
- Svi dokazni predmeti moraju biti pripremljeni za dalju upotrebu u skladu sa zahtevima forenzičara i institucija koje sprovode zakon, kompletne i nepromenjene, i deljive sa ostalim alatima.

Istraživači i forenzičari sada imaju veće mogućnosti da iskoriste ove alate i da se uhvate u koštac sa kompleksnijim izazovima odgovor na incident. Integrisani procesi omogućavaju organizacijama da integrišu njihove forenzičke procese radi uobličavanja njihovih istraga i značajnog smanjenja vremena za proces odgovora i oporavak sistema. Upotrebom čak i pojedinačnih istraživačkih rešenja dozvoliće organizacijama da konsoliduju njihove zahteve za obukom i postizanjem veće efikasnosti bez angažovanja dodatnih izvora. Na kraju, integracija mrežne i forenzike domaćina će sačuvati organizacijama vreme i novac i značajno smanjiti rizik narušavanja sistema.

2.2.6. Proces odgovora na incident u Distribuiranom Internet računarstvu

Proces odgovora na incident predstavlja proces koji se preduzima nakon nastanka događaja koji predstavlja kriminalnu radnju ili indicija da neki događaj predstavlja kriminalnu radnju[17]. Proces je dobro poznat i veoma razumljiv društvu informatičkih forenzičara. Sastoji se od nekoliko važnih koraka koji slede ponovljivu i zajedničku

---

[16] AccessData Corporation, The importance of Integrating Host and Network Forensics, USA 2005., str. 4

[17] Tim Grance, Suzanne Chevalier, Karen Kent, Hung Dang, *Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response (Draft)*, Recommendations of the National Institute of Standards and Technology, Special Publication 800-86, August 2005., str. 3-1

praksu koristeći lanac nadležnosti koji vodi do pravne valjanosti[18]. Ovi koraci forenzičkog procesa su zajednički i tradicionalnoj i mrežnoj forenzici i veoma važno je razumeti ih.

Definisana su četiri primarna koraka u forenzičkom procesu, i to:

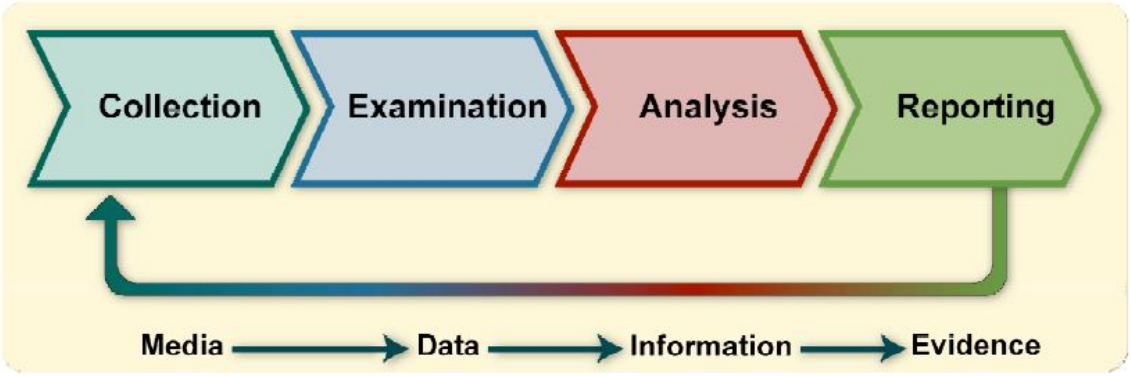
- ***Prikupljanje (Colection) podataka***
  U ovoj fazi forenzičkog procesa identifikuju se izvori podataka i prikupljaju se podaci. Tokom prikupljanja podataka istraživač pravi kopije log fajlova, diskova, izveštaja i pristupnih logova koji su neophodni da potvrde ili pobiju pretpostavljenu kriminalnu aktivnost, kao i da obezbede autentične kopije sa potpunim logovima, u skladu sa zahtevima pravnog postupka koji se sprovodi tokom istrage i procesiranja incidenta. Podaci prikupljeni u ovoj fazi su veoma su važni za istragu i predstavljaju deo kompromitovanog sistema ili kriminalne aktivnosti.

- ***Ispitivanje (Examination) podataka***
  Nakon što su podaci prikupljeni, sledi njihovo ispitivanje, što znači njihovu identifikaciju i organizuju u smisaone celine. U ovoj fazi se mogu prespojiti operativni system ili aplikacije kod kojih su nejasni datum i kod, kao i kompresija podataka, kodiranje i mehanizmi kontrole pristupa. U ovoj fazi se takođe vrši i filtriranje korisnih podataka, što je veoma značajno imajući u vidu izuzetno obimnu količinu prikupljenih podataka.

- ***Analiza (Analysis) podataka***
  U ovoj fazi procesa podaci koje smo dobili u prethodnoj fazi se analiziraju i pripremaju za prezentaciju. Priprema i analiza imaju za cilj da se definišu i odrede da li je zločin počinjen i da li ima dovoljno vidljivih dokaza sa kojima se može izaći pred sud u skladu sa važećim zakonskim propisima. Takođe, u ovoj fazi se vrši konačan izbor valjanih dokaza, vrše se dodatna objašnjenja, kao i eventualan povratak na fazu prikupljanja podataka za novo pronađene podatke.

- ***Izveštavanje (Reporting)***
  U ovoj fazi forenzičkog procesa dokazi i zaključci do kojih se došlo tokom prethodnih faza se mogu prezentovati menadžmentu ili sudu bez straha da će biti odbačeni kao neosnovani ili nepravilno prikupljeni i obrazloženi.Ova faza obuhvata kontinuirani pregled i recenziju procesa istrage tekućeg zadatka, a ima za cilj da pomogne politici da identifikuje mane, proceduralne greške i ostala zapažanja do kojih se došlo tokom prethodnih faza.

[18] Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, James “Jim” Steele, Digital forensics for network, Internet, and cloud computing, Syngress 2010. , str. 10



Slika 5. Proces odgovora na incident

Da bi se izbegle greške koje mogu da dovedu u pitanje celokupan proces forenzičke istrage incidenta, mnoge institucije i kompanije definišu i izdaju priručnike kojima se definišu postupci aktivnosti u pojedinim fazama procesa. Jedan od vodećih priručnika je priručnik koji je definisao Nacionalni Institut za standarde i tehnologiju, Specijalna publikacija 800-86 (Tim Grance, Suzanne Chevalier, Karen Kent, Hung Dang, August 2005, *Guide to Integrating Forensic Techniques into Incident Response*).

Ovaj priručnik obezbeđuje dobru osnovu za forenzičare digitalnih incidenata. Međutim, koliko god ovaj priručnik bio kvalitetna osnova, kompanije je moraju prilagoditi specifičnostima svoga delokruga poslovanja, tako da se obično uz njega publikuju dodatna uputstva koja definišu specifične bezbednosne politike, kao i pravne odredbe koje regulišu oblast zaštite podataka i istrage digitalnih incidenata.

Forenzičari CC sistema moraju poštovati i pratiti odredbe standarda propisanih priručnicima i uputstvima digitalne forenzike. Međutim, neophodno je uočiti razlike koje se pojavljuju ispred forenzičara kada istražuju incident u ovakvom kompjuterskom sistemu[19]. Navedene razlike se ogledaju u sledećem:

- Istraga je ograničena na lika uređaja umesto na celokupni uređaj. Umesto celog diska, mrežni istraživači su ograničeni na rad sa likom diska. Ovo znači da se isključuje pristup naslovima na RAM-u ili drugim komponentama koji spadaju u standardan spektar osumnjičenih medijuma u tradicionalnoj digitalnoj forenzici.

- U liku uređaja se mogu naći sve standardne informacije koje se nalaze na serverima informacionih centara ako je sakupljen odgovarajući ISO lik uređaja.

[19] Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, James “Jim” Steele, Digital forensics for network, Internet, and cloud computing, Syngress 2010. , str. 11

- Ako je disk šifrovan a ključ je izgubljen, postoje softveri koji će dozvoliti licu da angažuje mnoge instance u CC sistemu da pomognu u razbijanju šifre hard diska.

- Veoma će biti teško dobiti bilo kakvu formu informacije koja je preusmerena ako nije već u mrežnom uređaju.

- Slobodan (*Promiscuous mode*) mod neće raditi u CC sistemu, mrežna interfejs kartica (NIC) može biti smeštena u slobodan mod, ali će samo moći da čita podatke koji su poslani ka nekom posebnom računaru zbog načina na koji Xen hipervizor (*Xen hypervisor*) funkcioniše i usmerava saobraćaj. Nema mogućnosti da se pročita nešto što je prošlo kroz ram hipervizora ka drugim sistemima.

- Postoji mogućnost realizacije dubljeg logovanja u ovakvom okruženju kroz velike baze podataka (*big table*) jer kompanije funkcionišu u komercijalnom kompjuterskom sistemu. Logovanje svega na mrežu, pa nakon toga izgradnja logičnih logova čine prednost ovog okruženja za istraživanje od strane forenzičara.

- Lik uređaja (*ISO lik*) može biti pohranjen u sigurnom okruženju sistema kao deo virtuelnog privatnog CC sistema bez uticaja lokalnog informacionog centra ili da budu pohranjeni lokalno na disk inžinjera zaduženog za bezbednost. Ova mogućnost obezbeđuje mnogo užu listu ljudi koji imaju dozvoljen pristup likovima uređaja i obezbeđuje bolji lanac nadležnosti nego kod pohranjivanja i zaključavanja diska u kartoteku fajlova na duži vremenski period iz kojih postoji realna mogućnost da mogu biti ukradeni ili izgubljeni.

- Upotreba mera dvostruke autentifikacije logovanja obezbeđuje viši nivo bezbednosti podataka i usluga u ovakvom kompjuterskom sistemu, i mogu se upotrebljavati za pohranjivanje logova, koji su ograničeni na manje grupe ljudi koji mogu pristupiti bazi na regularnoj osnovi. Na primer, AWS koristi infrastrukturu javih ključeva radi autentifikacije. Različite grupe ljudi mogu dobiti različite PKI ključeve koji im dozvoljavaju pristup manjim kompjuterskim podsistemima sa jednostavnijim menadžmentom PKI nego što je obično dato tekućim bezbednosnim autentifikacionim merama.

- Postoji potencijal za potpunu sposobnost C2 nivoa logovanja na server baze podataka i individualnih sistema bez napuštanja prostora ili računarske sposobnosti u delu kompanije. Logovi su ogromni i mogu brzi i jednostavno da nadvladati mogućnost kompanije da uskladišti informacije. Premda su alati za vizuelizaciju i analizu podataka za bezbednost informacija i analizu logova ovog okruženja trenutno na relativno primitivnom nivou, postoji niz kompanija koje su uključene u izgradnju mernih alata koji će eventualno biti sposobni da prate mogućnosti CC okruženja. Jednom kada alati budu dovoljno zreli, forenzičari koji rade u ovom okruženju će moći jednostavno da pritisnu dugme i izvrše istragu duž celog sistema. Već sada se uočavaju trendovi u ovom smeru, čiji su predvodnici kompanije koje barataju alatima za bezbednost sistema.

- Antivirus i antispam u ovom okruženju, kao i ostali alati za identifikaciju malicioznih programa takođe postaju deo iskustva ovakvog kompjuterskog okruženja. Ovakav kompjuterski sistem, ako je pravilno konfigurisan može brzo identifikovati maliciozne programe (*malware, spyware, i spam softvere*) jer je moć kompjutera sa desktopa premeštena u udaljene centre. Ovo komplikuje postupak forenzičke istrage ako se kopiraju kritične usluge kompjutera koji se istražuje.

Sve ove karakteristike mogu se upakovati u proces odgovora na nastali incident, obezbeđujući merljivu i bezbednu forenzičku sposobnost za kompaniju koja može takođe biti deljena sa spoljnim ekspertima zavisno od slučaja i to angažovanjem specifičnih delova sistema za specifične funkcije deljenja forenzičkih podataka. Pošto CC okruženje može da asistira brojnim procesima u koje se uključuje forenzika sistema on se koristi za brzu identifikaciju osnovnih snaga i slabosti u podršci forenzičke istrage.

Dodatne komplikacije mrežnom forenzičkom istraživaču predstavljaće i upotreba kriptozaštite između sistema u ovakvom okruženju, kao i način na koji je kriptozaštita implementirana kroz različite sisteme ovog okruženja. U nekim slučajevima, upotrebom sistema dvostrukih mera autentifikacije (poput upotrebe PKI u AWS) da bi se ograničio pristup sistemu izdavanjem specijalnih kompleta ključeva, sužava se lista osumnjičenih.

Gubitak ovih ključeva može omogućiti bilo kome da izvrši upad u sistem, zloupotrebu podataka i izmenu strukture sistema, tako da je zaštita upotrebe PKI sistema kod AWS veoma važna, i zbog toga se ključevi nikada ne daju bilo kojem administratoru sistema. Specijalni serveri mogu biti posebno podešeni za obezbeđivanje podataka sa različitim kompletima ključeva tako da se može obezbediti potpuna bezbednost podataka i samo razmena ključeva između malog i ograničenog broja ljudi u kompaniji dozvoljava pristup sistemu bez uznemiravanja administratora sistema.

Mogućnost animiranja zajednice zainteresovane za ovaj sistem može, takođe, biti od pomoći u otkrivanju i razvoju pravnih regulativa i drugih procesa poput analize log fajlova, ISO lika, skladišnog prostora i pristupa, sa ciljem izgradnje jednog veoma jednostavnog i za merenje i montažu prostog sistema koji je otvoren svakom ko je zainteresovan za njega.

Rad u CC okruženju može takođe da frustrira forenzičara u ovakvom okruženju zbog nedostatka direktnog pristupa osumnjičenim mrežnim uređajima. Podešavanja ovog sistema na *host* infrastrukturi takođe frustrira forenzičare. Dostupni dokazi mogu biti ograničeni na virtuelnu mašinu ili sistem a ne na trag koji vodi kroz sistem, od jednog do drugog kraja sistema. Ovakvi sistemi su samo logične hijerarhije u istrazi pre nego su sposobne da direktno nadgledaju podatke sa nekog od namenskih uređaja (poput SPAN porta ili mrežnog tap-a).

Mrežne barijere su ograničene na mrežne barijere uređaja i ne mogu da obezbede dovoljno informacija forenzičaru u cilju kvalitetnog sprovođenja istrage. Dodatno, forenzičari moraju investirati u nove veštine i nove alate za efektivniji rad u ovakvom okruženju. Komplikovanje procesa je izazov koji izlazi pred aktuelne veštine i alate, koji

se moraju permanentno razvijati. Ovo znači da su aktuelne veštine i alati u CC okruženju nezreli kada se govori o veštinama i alatima koji su dostupni kada su sistem i mreža u potpunosti u posedu kompanije.

Softver kao usluga unosi dodatne komplikacije jer kompanija ne poseduje kompjutere u kojima su uskladišteni podaci ili softvere koji su pridruženi podržavajućim sistemima koji omogućavaju rad softverima. Na primer, mnoge kompanije koriste Salesforce.com koji se nalazi u kompletu SaaS usluge i koristi za upravljanje korisničkim servisom. Jedini podaci koje vlasnik poseduje su njegovi podaci. Jedino mesto za snimanje mrežnog saobraćaja se nalazi na granicama kompanijskih mreža, bilo gde da se granice pojavljuju na Internetu.

Tradicionalna mrežna forenzika je efektivno zaustavljena na granicama kompanijine mreže i ne može se pristupiti niti istražiti uređaj ili saobraćaj na Salesforce.com. Sve veze podataka između Salesforce.com i ostalih pretraživača su šifrovani u SSL-u (*Secure Sockets Layer*) i on radi na mobilnim uređajima što komplikuje bilo koji pokušaj istrage. Ako pojedinac u organizaciji pristupa Salesforce.com sa ukradenog iPhona sa koga nije promenjena obavezna SSH (*Secure Shell*) šifra, svi podaci koji se nalaze u okviru naloga mogu biti ukradeni bez ikakvog obaveštenja ili mogućnosti praćenja i ulaska u trag kroz mrežu šta se tačno desilo ili kako su podaci ukradeni. Bilo koji sistem praćenja ne funkcioniše u CC okruženju, ostavljajući forenzičara vezanih ruku, jer se celokupan događaj desio van korporativne mreže na nečijem tuđem sistemu, upotrebom tuđeg softvera.

2.3. Otkrivanje i sakupljanje podataka u mrežnom saobraćaju u realnom vremenu

2.3.1. Uvod

Postupak otkrivanja i sakupljanja tekućih ("živih") podataka u CC sistemu u realnom vremenu, odnosno u trenutku odvijanja mrežnog saobraćaja je od izuzetnog značaja za sprovođenje forenzičke analize[20]. Promene u mrežnoj tehnologiji su ozbiljno ograničile korisnu upotrebu aplikacija za otkrivanje i sakupljanje podataka u mrežnom saobraćaju u realnom vremenu.

Na primer, aktiviranje *host* snifera u okruženju svičeva ili bežičnoj mreži će omogućiti vidljivost samo saobraćaja upućenog ka sebi i sopstvenog emitovanog saobraćaja čak i ako je snifer podešen za rad u slobodnom modu. U ovakvom okruženju snifer zahteva specijalne, skupe drajvere ili se moraju koristiti neka druga hardverska ili softverska rešenja, poput *network tap* i *spanning* port.

Kako su ovi podaci dinamični, njihovi delovi se moraju konvertovati u statičke fajlove i proračunati njihova povezanost. Da li podatke skladištimo lokalno i prosleđujemo kao pakete ili samo pratimo tok podataka u mrežnom saobraćaju?

Ovaj izbor obezbeđuje različite mogućnosti za narušavanje i modifikovanje mrežnih logova. Na primer, ako su logovi tekući onda se mogu videti znaci upada na mestu gde je napadač preuzeo kontrolu nad senzorom. Sa tehnologijom skladištenja i prosleđivanja, napadač ima mogućnost da izbriše dokaze upada pre nego što će oni biti upućeni sistemu koji napadač ne kontroliše.

U sistemu tekućih podataka nemamo mogućnost da kreiramo kriptografske kontrolne pakete ukoliko mehanizam protoka podataka to ne obezbeđuje. Obično, u funkciji je korisnički protokol UDP (*User Datagram Protocol*) koji ne dozvoljava povezivanje i integraciju sistema za proveru ispravnosti paketa podataka. Ipak, kada tražimo aplikacije logova u sistemu tekućih podataka trebali bi pokušati pronaći onaj koji se odlikuje obezbeđenjem integriteta prosleđenih podataka.

[20] Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, James “Jim” Steele, Digital forensics for network, Internet, and cloud computing, Syngress 2010. , str. 23

2.3.2. Primena Wireshark-a

Wireshark je softverski protokol analizator ili aplikacijsko "paketsko njuškalo" koje se koristi za rešavanje problema na mreži, za analizu mrežnog saobraćaja, razvoj softvera i protokola i obrazovanje[21].

Paketsko njuškalo (poznato i kao mrežni analizator ili protokol analizator) je kompjuterski softver koji može presresti i uhvatiti bilo koje podatke koji se prenose u CC okruženju[22]. Kako podaci protiču u oba pravca duž sistema, Wireshark sakuplja sve jedinice podataka protokola PDU (*protocol data unit*) i dekodira i analizira njihov sadržaj u skladu sa odgovarajućim RFC ili drugim specifikacijama.

Wireshark je programiran da prepozna strukturu različitih mrežnih protokola. Ovo svojstvo mu omogućava prikazivanje sažetih i pojedinačnih polja PDU i interpretira njihovo značenje.

On prestavlja koristan alat za bilo koga ko ima kontakta sa mrežom a može se koristiti i u laboratorijama i tokom realizacije kurseva analize podataka i otklanjanja problema.

U skladu sa Wireshark FAQ "*Wireshark* je najpopularniji protokol za analizu mreže. On poseduje bogate i snažne karakteristike i aktivan je na većini kompjuterskih platformi uključujući Windows, OS X, Linux i UNIX. Mrežni profesionalci, bezbednosni eksperti, eksperti za razvoj i edukaciju ga koriste regularno širom sveta. On je slobodno dostupan kao otvoren izvor i izdat pod GNU (*General Public License*) verzija 2." Uputstvo za upotrebu Wireshark-a kaže da je Wireshark protokol za analizu mreže koji se može koristiti za otkrivanje i sakupljanje podataka sa mreže i prikazivanje paketa podataka.

Do juna 2006. Godine Wireshark je bio poznat kao Ethereal koji je Gerald Combs izneo u središte pažnje javnosti 1998. godine. U to vreme je Ethereal je bilo mrežno njuškalo sa upotrebom grafičkog interfejsa GUI (*Graphical User Interface*). Nakon što je prešao iz NIS-a (*Network Integration Services*) u CACE Technologies promenio je ime Ethereal u Wireshark. Svi razvojni programi protokola nakon 2006. godine su izvedeni pod imenom Wireshark.

Wireshark može biti upotrebljen za otklanjanje problema u mreži, ispitivanje bezbednosnih problema, deblokiranje problema implementacije protokola, izučavanje unutrašnjosti protokola i mnogo toga više. Na www.wireshark.org se može dobiti binarni kod ili izvor za Wireshark. Pošto se uputstva za instalaciju mogu menjati sa svakom verzijom programa najbolje se obratiti Wireshark Web sajtu za detaljne instrukcije.

---

[21] Cisco Certified Network Associate (CCNA), *Exploration 4.0. Network Fundamentals, Lab 2.6.2: Using Wireshark™ to View Protocol Data Units*

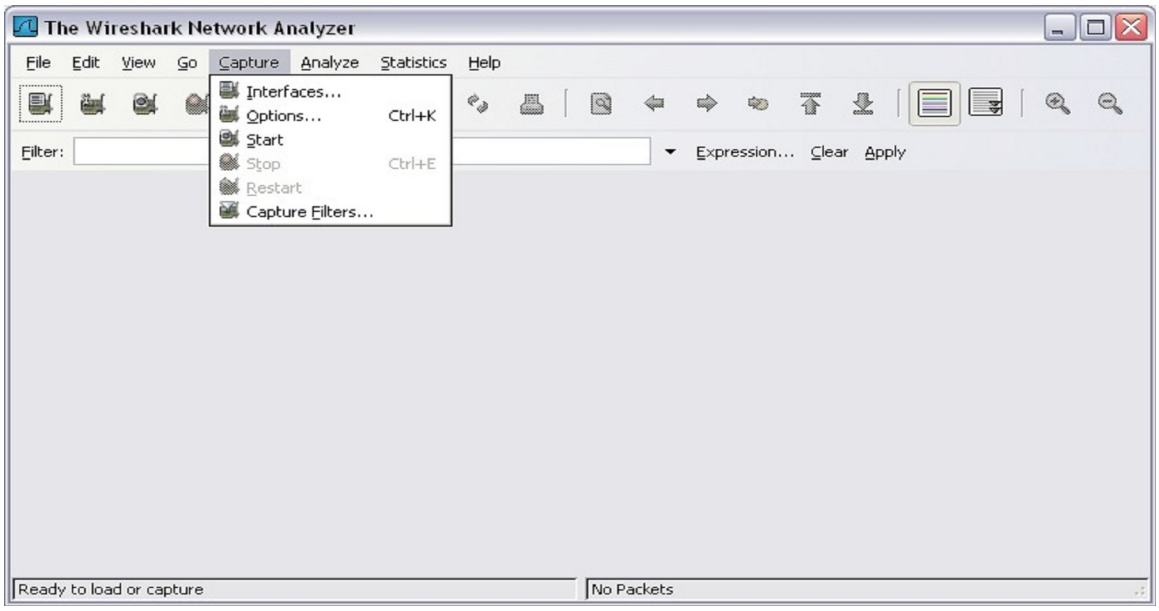
[22] Ulf Lamping, Richard Sharpe, Ed Warnicke, *Wireshark Developer's Guide for Wireshark 1.5*, 2004-2011. str. 1

Poslednje verzije će detektovati prisustvo ili odsustvo WinPcap, ukloniće prethodno instalirane verzije i instalirati najnovije drajvere. Instalaciju treba pokrenuti kao administrator. Suprotno opštem mišljenju, Wireshark aplikacija ne zahteva administratorski pristup da bi se pokrenuo. Samo NPF (*Netgroup Packet Filter*) drajveri zahtevaju pokretanje kao administrator.

Kako se radi o GUI aplikaciji u realnom vremenu, Wireshark daje mnoge mogućnosti osnovnom konceptu *tcpdump*, pa je korisnik u stanju da vidi rezultat i reaguje na njega u realnom vremenu.

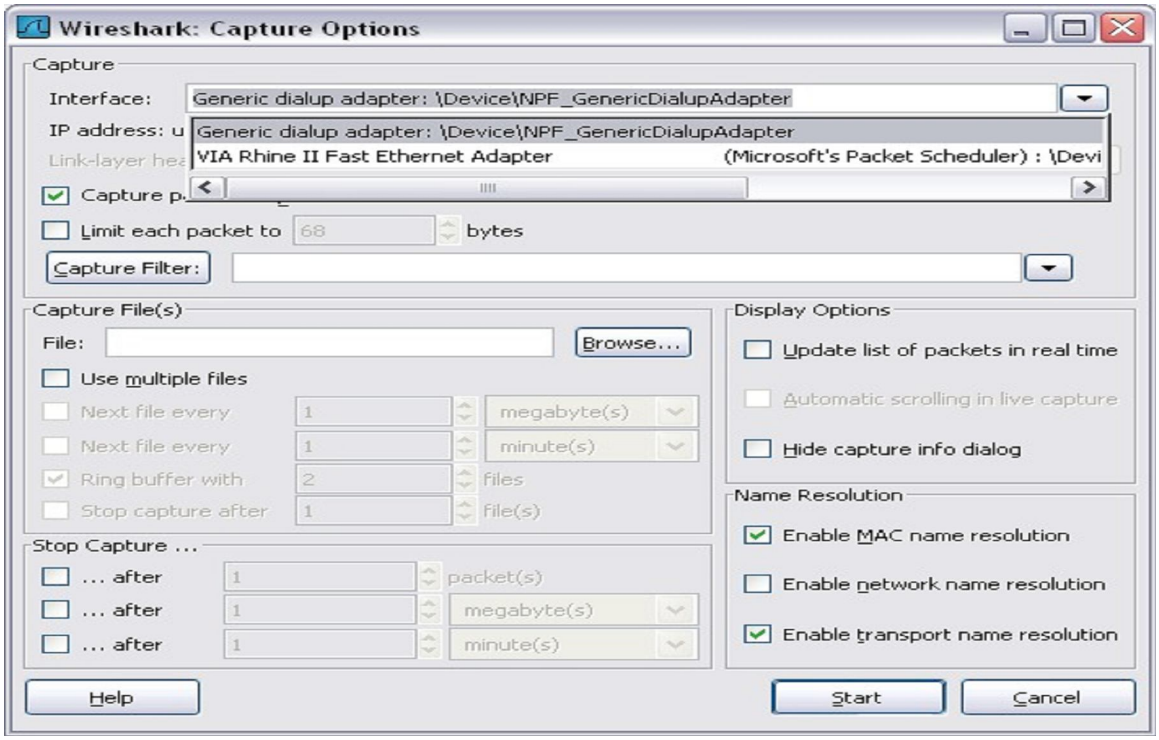
Da bi se izvršilo hvatanje PDU na kompjuteru na kojem je instaliran Wireshark, neophodno je da postoji mrežna konekcija i da je Wireshark pokrenut pre bilo kog pokušaja hvatanja podataka.

Nakon pokretanja Wireshark-a na ekranu će se prikazati prozor kao na slici 6.



Slika 6. Osnovni Wireshark meni

Da bi započeli hvatanje podataka izabraćemo opciju **Capture** i u padajućem meniju odaberemo **Option**. **Option** dijalog obezbeđuje opseg podešavanja i filtera koji određuju kada i koliko podataka iz mreže će biti uhvaćeno.



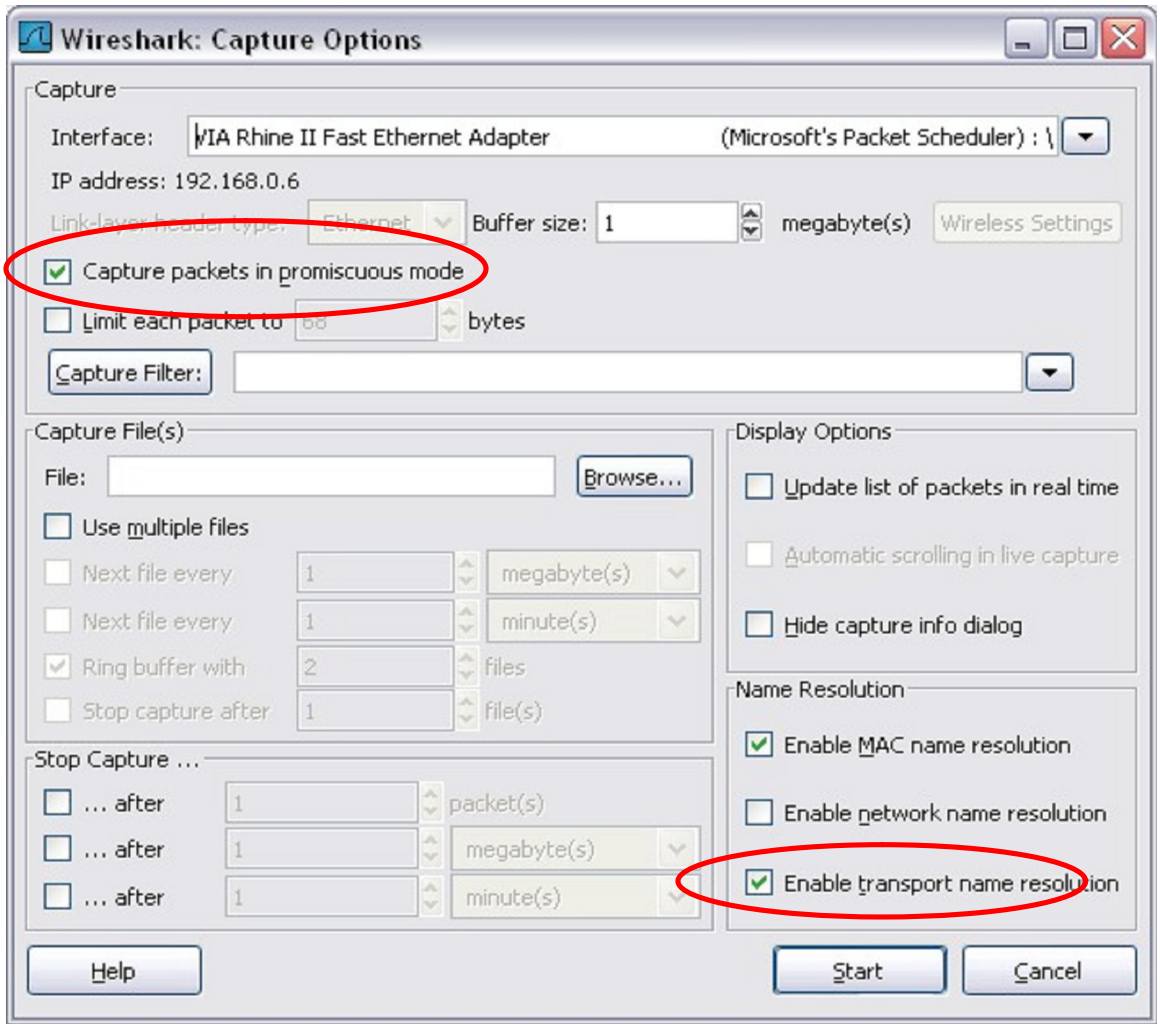
Slika 7. Wireshark **Capture** meni

Izuzetno je važno da se na početku uverimo da je Wireshark podešen za nadzor odgovarajućeg interfejsa. U padajućem meniju sa **Interface** liste odabraćemo mrežni adapter koji je u upotrebi. Tek nakon izbora interfejsa ostale opcije mogu biti podešene. Među nekoliko dostupnih opcija u meniju **Capture Options** dve naznačene opcije su vredne dodatnog objašnjenja.

Podešavanje Wiresharka za hvatanje podataka u slobodnom modu (*promiscuous mode*) je veoma značajno. Ukoliko ova opcija nije čekirana, biće moguće uhvatiti samo PDU koji je upućen ka ispitivanom računaru. Ukoliko je ova opcija čekirana, biće moguće uhvatiti PDU upućen ka ispitivanom kompjuteru, kao i celokupan PDU koji je detektovan sa ispitivanog kompjutera na nekom mrežnom segmentu. Važno je napomenuti da ovako hvatanje PDU zavisi od karakteristika uređaja pomoću kojeg se ispitivani kompjuter povezuje na mrežu. Kako se često koriste različiti uređaji za povezivanje kompjutera na mrežu (habovi, svičevi, ruteri) različiti će biti i rezultati Wireshark pretrage.

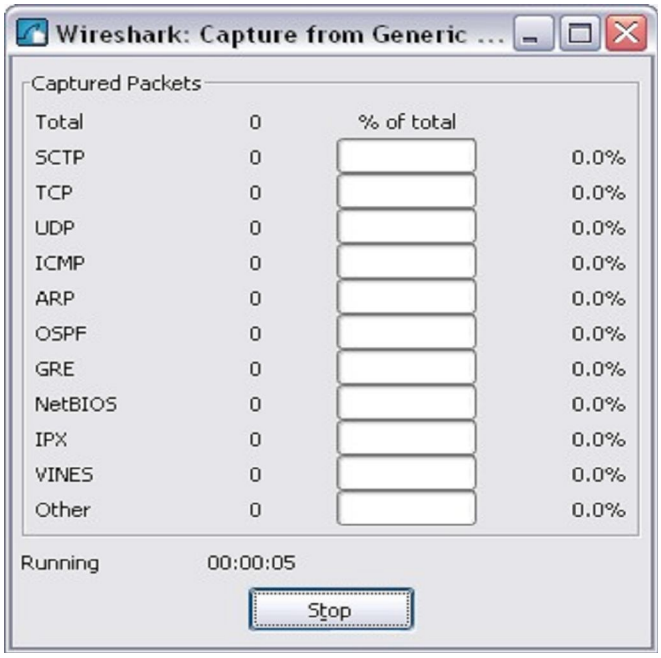
Čekiranjem opcije Wiresharka za određivanje imena mreže (*network name resolution*) dozvoljava se kontrolisanje da li će ili ne Wireshark prevoditi mrežne adrese koje su otkrivene u PDU u imena. Premda je ova opcija korisna, proces određivanja imena adrese može uhvatiti dodatne PDU i tako možda ugroziti analizu.

Pored navedenih postoji još dostupnih opcija filtriranja i sakupljanja podataka, kao i ostalih podešavanja.



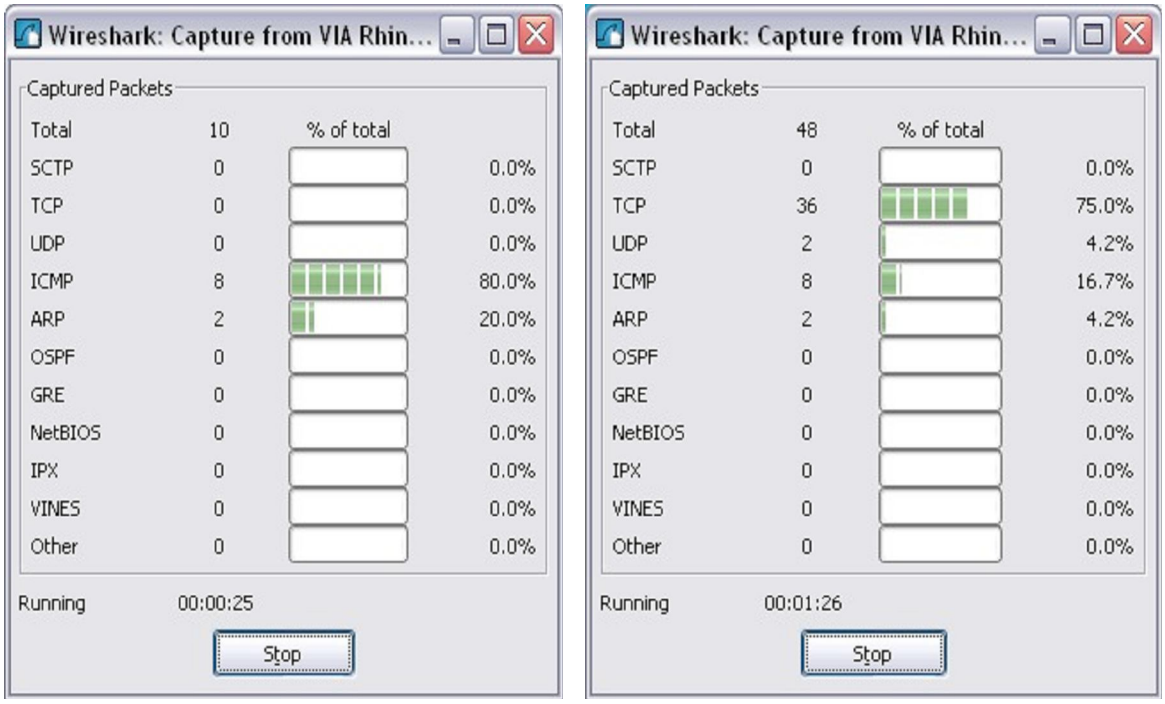
Slika 8. Izbor Wireshark opcija

Aktiviranjem opcije **Start** započinje proces hvatanja podataka, čiji se progres može pratiti u posebnom prozoru.



Slika 9. Prikaz procesa hvatanja podataka

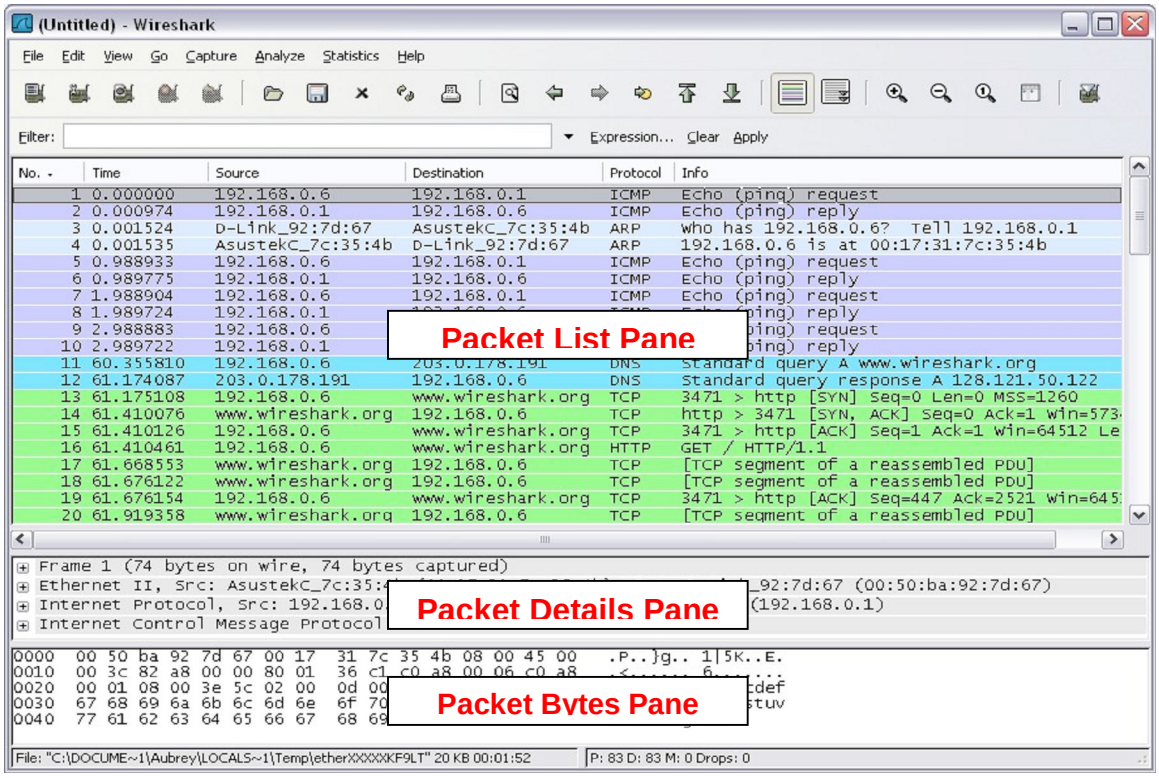
Kako se PDU sakupljaju, u prozoru koji prikazuje progres hvatanja se prikazuju vrste i broj sakupljenih PDU.



Slika 10. Prikaz progresa hvatanja podataka

Na primeru je prikazano sakupljanje ping procesa i nakon toga pristup web strani. Kada se klikne na **Stop** opciju, proces sakupljanja se zaustavlja i prikazuje se glavni ekran.

Glavni prozor Wiresharka ima tri okvira:



Slika 11. Glavni prozor Wireshark-a

PDU lista ili Okvir liste paketa (*Packet List Pane*) se nalazi na vrhu prozora i prikazuje pregled uhvaćenih paketa. Klikom na paket u ovom okviru, kontrolišemo šta će biti prikazano u druga dva okvira.

PDU detalji ili Okvir detalja paketa se nalazi u sredini prozora i detaljnije prikazuje pakete odabrane u Okviru liste paketa.

PDU bajt ili Okvir bajta paketa se nalazi na dnu prozora i prikazuje aktuelne podatke odabrane u Okviru liste paketa. Prikazani podaci su u heksadecimalnoj formi i predstavljaju aktuelne binarne podatke, a takođe se odnose na polja koja su odabrana u Okviru detalja paketa.

Primer iznad prikazuje uhvaćeni PDU kada je pristupao www.Wireshark.org. Označen je paket broj 1. U okviru detalja je su prokazani detalji odabranog paketa i to protokoli i polja protokola. Protokoli i polja se prikazuju u obliku stabla podataka koje se može širiti i skupljati. U okviru bajta paketa prikazuju se podaci u heksadecimalnom zapisu. Ovi podaci su izuzetno važni, posebno kada se rade detaljne pretrage paketa podataka.

Podaci uhvaćeni PDU mogu biti sačuvani u fajlu. Ovaj fajl može biti otvoren pomoću Wiresharka radi ponovnih i dodatnih analiza u nekom budućem vremenu bez potrebe za ponovnim hvatanjem podataka u saobraćaju.

Informacije o uhvaćenim podacima u fajlu su iste kada se fajl otvori posle nekog vremena kao i onda kada su uhvaćene. Kada se zatvara fajl sa uhvaćenim podacima Wireshark će postaviti pitanje da li će biti zapamćeni uhvaćeni PDU.



Slika 12. Wireshark upit za zatvaranje hvatanja podataka

Izborom **Continue without Saving** zatvaramo fajl i napuštamo Wireshark bez pamćenja prikazanih uhvaćenih podataka.

2.3.3. Otkrivanje i hvatanje tekućih forenzičkih podataka upotrebom Wireshark-a

Nakon pokretanja i izbora interfejsa na kojem će se izvršiti otkrivanje i hvatanje forenzičkih mrežnih podataka u realnom vremenu može se preći na posao upotrebom – l parametra u cilju određivanja interfejsa koji će se hvatati i – k parametrom kojim će se reći Wireshark-u da startuje odmah sa otkrivanjem i sakupljanjem.

Wireshark –i *interface-name* –k

U cilju određivanja imena interfejsa, treba startovati Wireshark, otvoriti meni za otkrivanje i sakupljanje, odabrati opciju (slika 13.) i označiti interfejs koji bi želeli da koristimo.

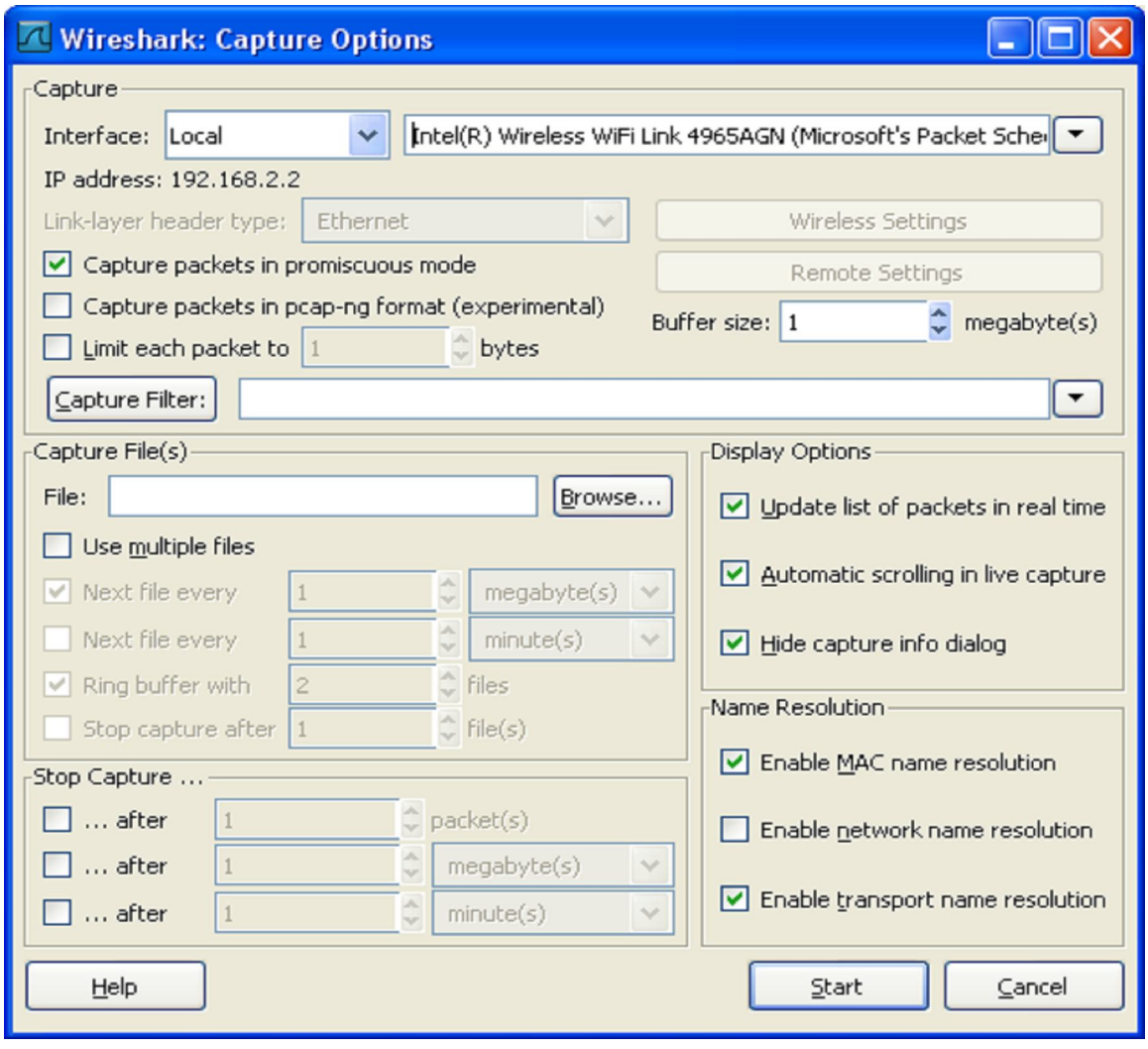
Kada se pritisne **End** ključ, pomeriće se kursor u desnu stranu prozora. Za vreme pomeranje sa desna na levo, označiti od kraja linije do "\Device". Na slici 13. ime uređaja bi bilo "\Device\ NPF_{5DCA03D5-BC20-4A6A-B7EB-B2E48577F39B}". Ovo treba koristiti kao – I parametar na prečici Wireshark-a.

Prečica će prizvati Wireshark kao što je pokazano u sledećem primeru:

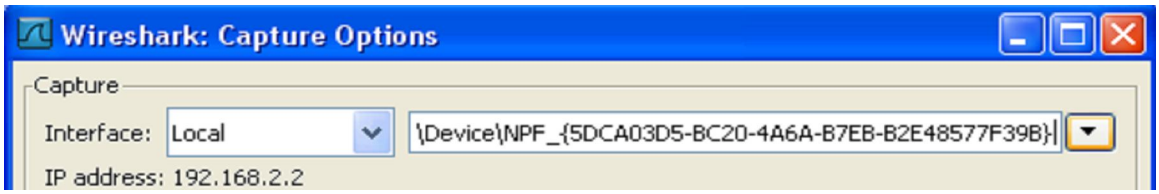
Wireshark –i \Device\NPF_{5DCA03D5-BC20-4A6A-B7EB-B2E48577F39B}-k

Može se čak odrediti i filter za otkrivanje i hvatanje upotrebom –f parametara sledeći uhvaćeni izraz filtra koji se želi koristiti. Sve aplikacije njuškala o kojima se raspravljalo imaju dva glavna moda operacija: otkrivanje i sakupljanje i prikazivanje. Uopšteno, ako želimo otkriti i sakupiti sve željene informacije onda koristimo filtere prikazivanja da bi smanjili obim otkrivenih i sakupljenih informacija i prikazali čistu sliku nekih aspekata mrežnog saobraćaja. Da bi se pomoglo pomenutim naporima, Wireshark ima razumljive argumente za prikazivanje parametara filtera. Na www.wireshark.org/docs/dfref/ se mogu naći detaljnija ponuda referenci filtera za prikazivanje.

Wireshark GUI je organizovan slično kao i *tcpdump* i ostali komandno linijski alati za prisluškivanje. GUI dozvoljava korisniku da deluje po podacima koje je pronašao na displeju.



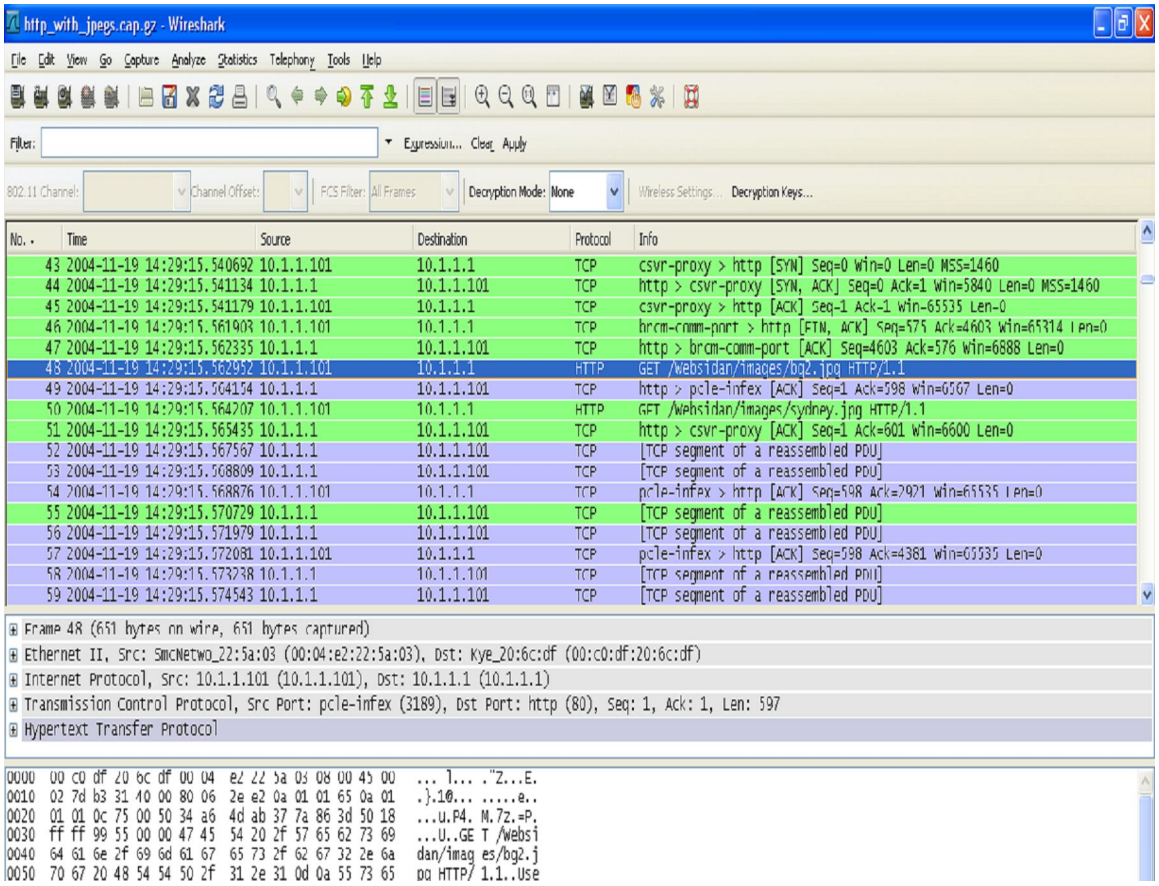
Slika 13. Wireshark opcije otkrivanja i sakupljanja



Slika 14. Wireshark opcije definisanja imena uredjaja

Na sajtu http://wiki.wireshark.org/SampleCaptures je obezbeđena biblioteka primera otkrivenog i sakupljenog saobraćaja. Na nesreću, u današnje vreme Web sajtovi ne dozvoljavaju skidanje primera zbog tehničkih zahteva.

Mogućnosti Wiresharka ćemo ilustrovati kroz prikaz otkrivanja i sakupljanja fajlova jpeg formata. Za vreme posmatranja otkrivanja i sakupljanja u realnom vremenu ili ponovnom postupku možemo zatražiti od Wireshark-a da sledi TCP tok. Wireshark pokazuje samo poslane i primljene pakete između dva *hosta* izlistane u tekućem označenom paketu. Na slici 15. je pokazano da GET (*vrsta HTTP zahteva*) metod sadrži u okviru saobraćaja HTTP, uhvaćene pakete poslate od *hosta* 10.1.1.101 ka *hostu* 10.1.1.1.



Slika 15. Otkrivanje i sakupljanje jpeg fajla u realnom vremenu

Potražimo sliku koja je bila otkrivena i skinuta sa osumnjičenog uređaja. Pregledom HTTP saobraćaja pronaći ćemo paket sa slikom. Slika koja je pronađena se nalazi u paketu 48. Kada ga označimo i kliknemo desnim klikom pokazaće se meni kao na slici 16.

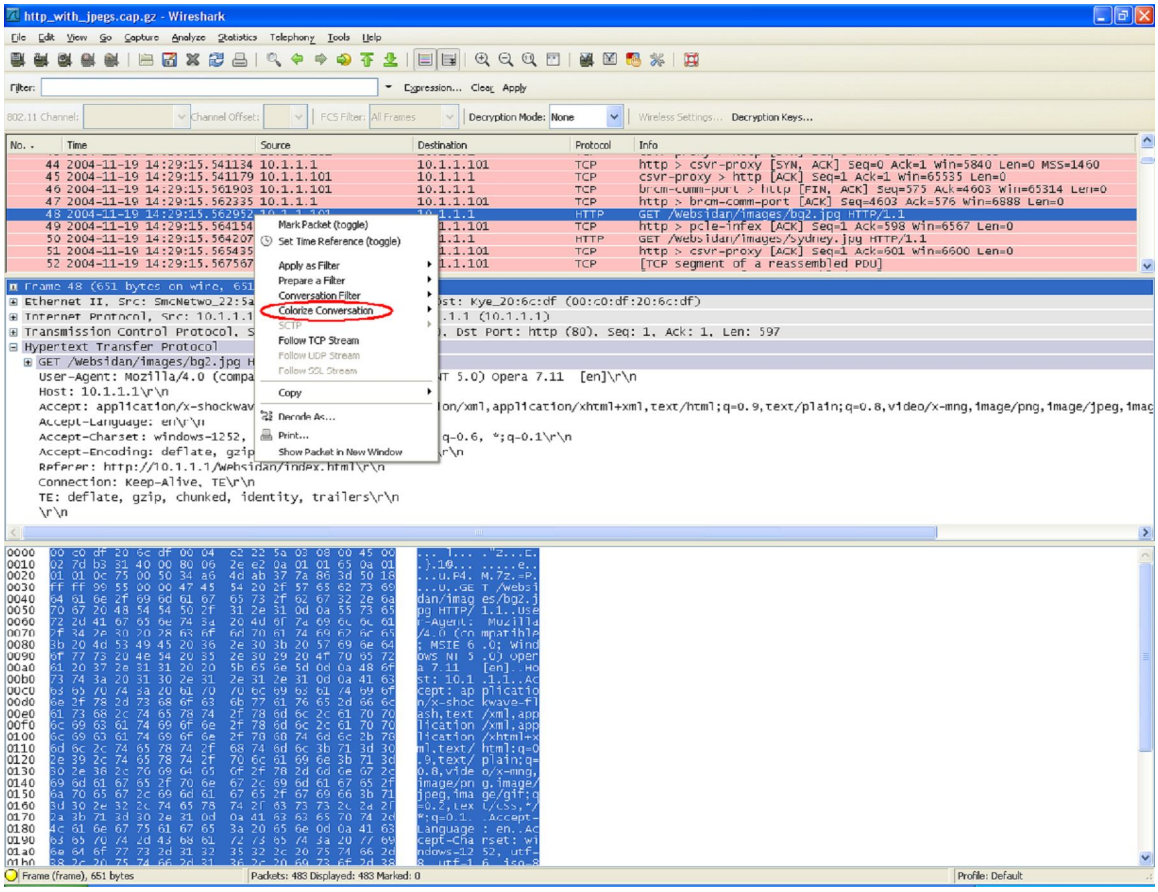
Klikom na opciju **Colorize Conversation** u prikazanom meniju, Wireshark će ponuditi paletu boja za označavanje konverzacije između 10.1.1.101 i 10.1.1.1. Jednom kada je označimo, konverzacija za koju smo zainteresovani će bit izdvojena od svih ostalih koje su otkrivene i sakupljene, kao što je pokazano na slici 16.

Da bi se filtriralo prikazivanje svih konverzacija izuzev odabrane izabraćemo opciju **Follow TCP Stream** na istom meniju kao što je prikazano na slici 17.

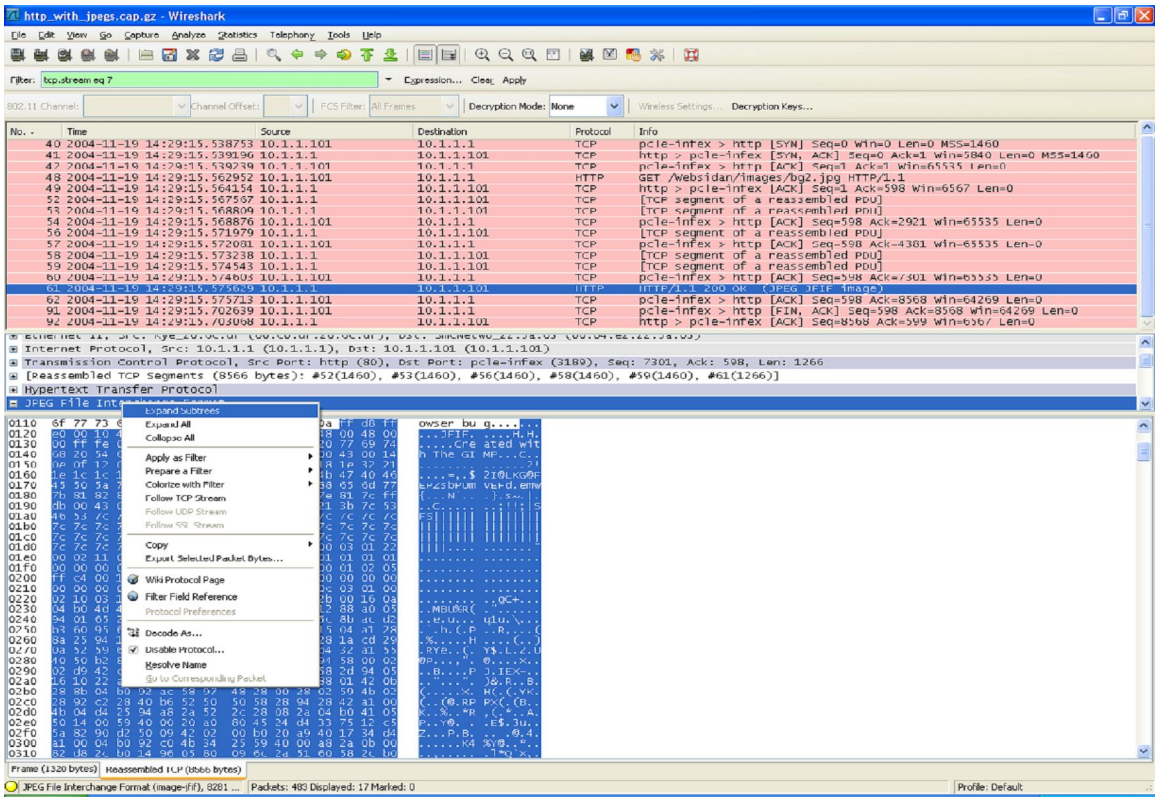
Posle sleđenja TCP toka, Wireshark može da kreira i izda tekst fajl u ASCII formatu podataka koji se nalaze u aplikativnom sloju OSI referentnog modela, po sledećem:

```
GET /Websidan/images/bg2.jpg HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
NT 5.0) Opera 7.11 [en]
Host: 10.1.1.1
Accept: application/x-shockwave-flash,text/
xml,application/xml,application/xhtml+xml,text/
html;q=0.9,text/plain;q=0.8,video/x-mng,image/
png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1
Accept-Language: en
Accept-Charset: windows-1252, utf-8, utf-16, iso-8859-
1;q=0.6, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Referer: http://10.1.1.1/Websidan/index.html
Connection: Keep-Alive, TE
TE: deflate, gzip, chunked, identity, trailers
HTTP/1.1 200 OK
Date: Sat, 20 Nov 2004 10:21:07 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Fri, 12 Jan 2001 05:00:00 GMT
ETag: "46a4f-2059-5e467400"
Accept-Ranges: bytes
Content-Length: 8281
Connection: close
Content-Type: image/jpeg
X-Pad: avoid browser bug
......JFIF.....H.H......Created with The GIMP...C......
..........2!....=,.$2I@LKG@FEPZsbPUmVEFd.emw{...N`...}.s~.
|...C.......;!!;|SFS|||||||||||||||||||||||||||||||||
|||||||||||||||.....".....................
.....................................gC+..
```

..MBU%R(."........e.u...q1u.\....`.h.(.P..R,...
(.%.....H....(..)
RYe..(.Y$.L.2.U@P...,".@..
.X....B....PJ.IEX-...."...".)&.R..B.(.....X.H(.(.YK.
(..(@.RPPX(.(B..K..%..*R,(.*..A.P..Y@. ..



Slika 16. Prikaz otkrivenog jpeg fajla u realnom vremenu



Slika 17. Prikaz filtriranja prikazivanja otkrivenih i sakupljenih paketa

U blizini početka fajla možemo videti reči JPEG File Interchange Format (JFIF), za kojima sledi "Created with the GIMP". JFIF ukazuje da poruka sadrži JFIF fajl. GIMP je GNU program za manipulaciju sa slikama (*GNU Image Manipulation Program*), koji se aktivira u Windows okruženju. Ako je za istragu značajno dokazivanje koji kompjuter proizvodi sliku, mora se istražiti i dokazati činjenica da kompjuter koji proizvodi slike morao imati aktivan GIMP u nekom vremenu. Iz ugla forenzike, ovo je bitna karakteristika koja sužava opseg svih mogućih osumnjičenih kompjutera na samo onaj kompjuter koji je imao aktiviran GIMP u nekom slučaju.

Vratimo se nazad na analizu, u listi okvira paketa, u paketu 61, videćemo polje informacija koje ovaj paket sadrži kao JPEG zahtev. Označimo paket sa levim klikom. Panel detalja paketa sadrži sedam linija sa plusem ispred njih. Oni uključuju okvir, Ethernet, IP, TCP, ponovo sakupljene TCP segmente, HTTP i JFIF. Ako kliknemo desnim klikom na JPEG liniju videćemo meni koji se pojavljuje na slici 17.

U ponudjenom meniju odaberimo opciju **Export Selected Packet Bytes**. Dijalog box će ponuditi izbor za pamćenje odabranog teksta u BIN, DAT ili RAW formatu. Kako znamo da se ovde ustvari radi o aktuelnom JFIF fajlu, možemo ignorisati preporuke i umesto toga zapamtiti ove podatke kao JPG fajl, kao što je prikazano na slici 18.



Slika 18. Izdvojeni i zapamćeni JPG fajl

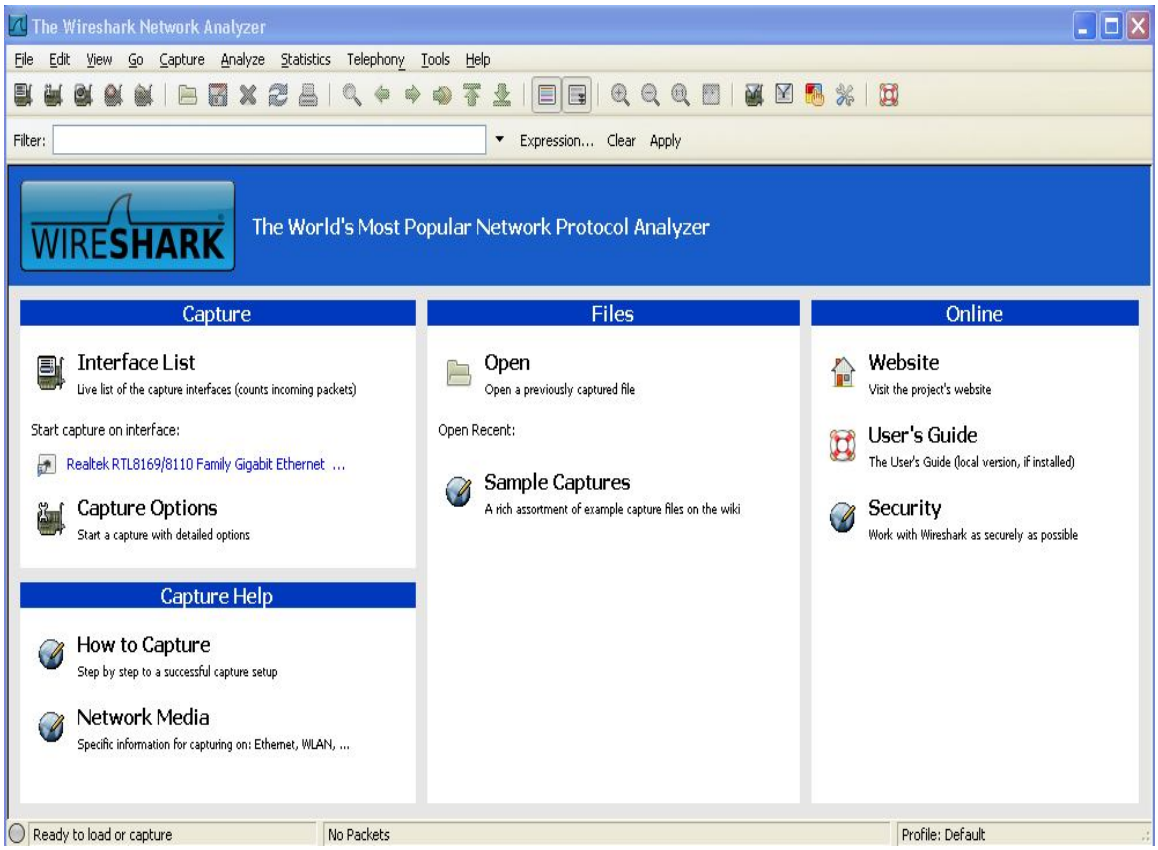
2.3.4. Otkrivanje i hvatanje tekućih forenzičkih podataka upotrebom Wireshark-a u korporativnoj mreži

Prikaz postupka otkrivanja i hvatanja tekućih podataka upotrebom Wiresharka-a se najefikasnije može prikazati kroz stvaran postupak otkrivanja, hvatanja i prikazivanja tekućih podataka u zatvorenoj korporativnoj mreži.

Instalacija Wiresharka-a na korisničkom računaru u mreži se odvija u skladu sa korisničkim uputstvom[23], kao što je već ranije pomenuto, samostalno, bez obzira na odsustvo statusa administratora. Nažalost, bezbednosna politika upravljanja datom mrežom, što nije redak slučaj u praksi, ne dozvoljava testiranje Wireshark-a sa računara koji imaju status administratora.

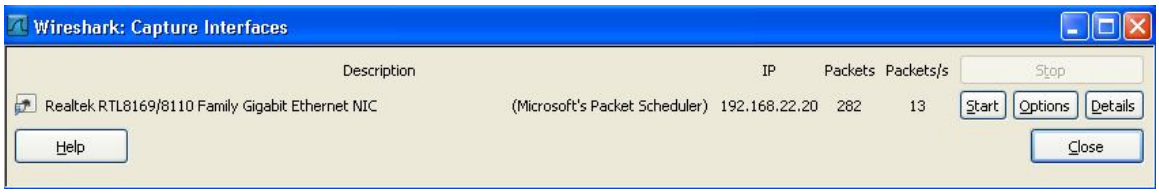
Nakon pokretanja programa na ekranu će se prikazati prepoznatljivi Wireshark *Start meny*, koji dozvoljava korisniku da bira opcije otkrivanja, hvatanja i prikazivanja, kao i da upravlja podacima.

[23] Ulf Lamping, Richard Sharpe, Ed Warnicke, *Wireshark Developer's Guide for Wireshark 1.5*, 2004-2011.



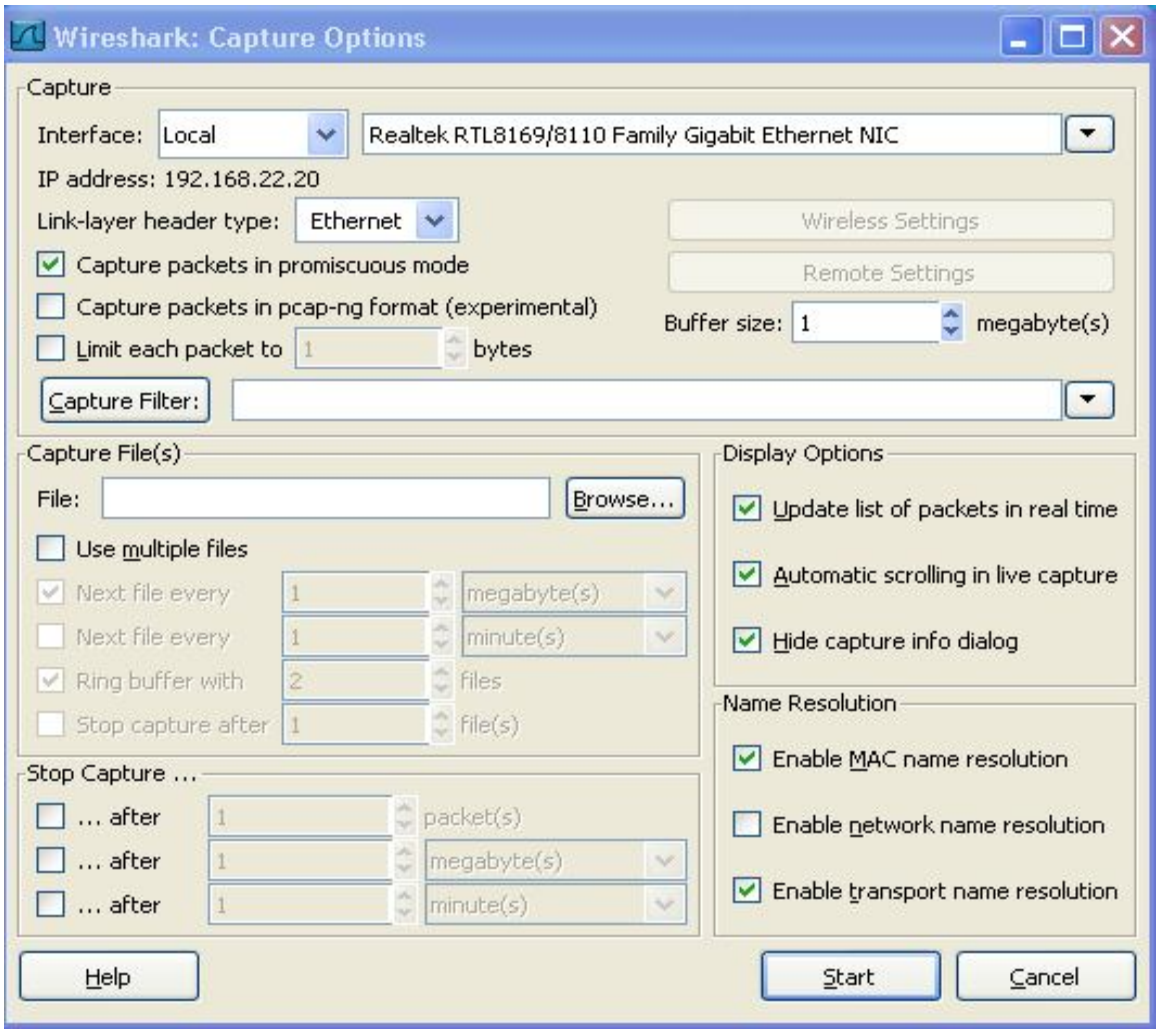
Slika 19. Wireshark *Start meny*

Izborom opcije **Interface List** stičemo uvid u odabrani interfejs na kome se vrši postupak otkrivanja i hvatanja podataka, IP adresu korisnika, kao i broj paketa podataka koji su trenutno otkriveni i dostupni za hvatanje.



Slika 20. Prikaz odabranog interfejsa

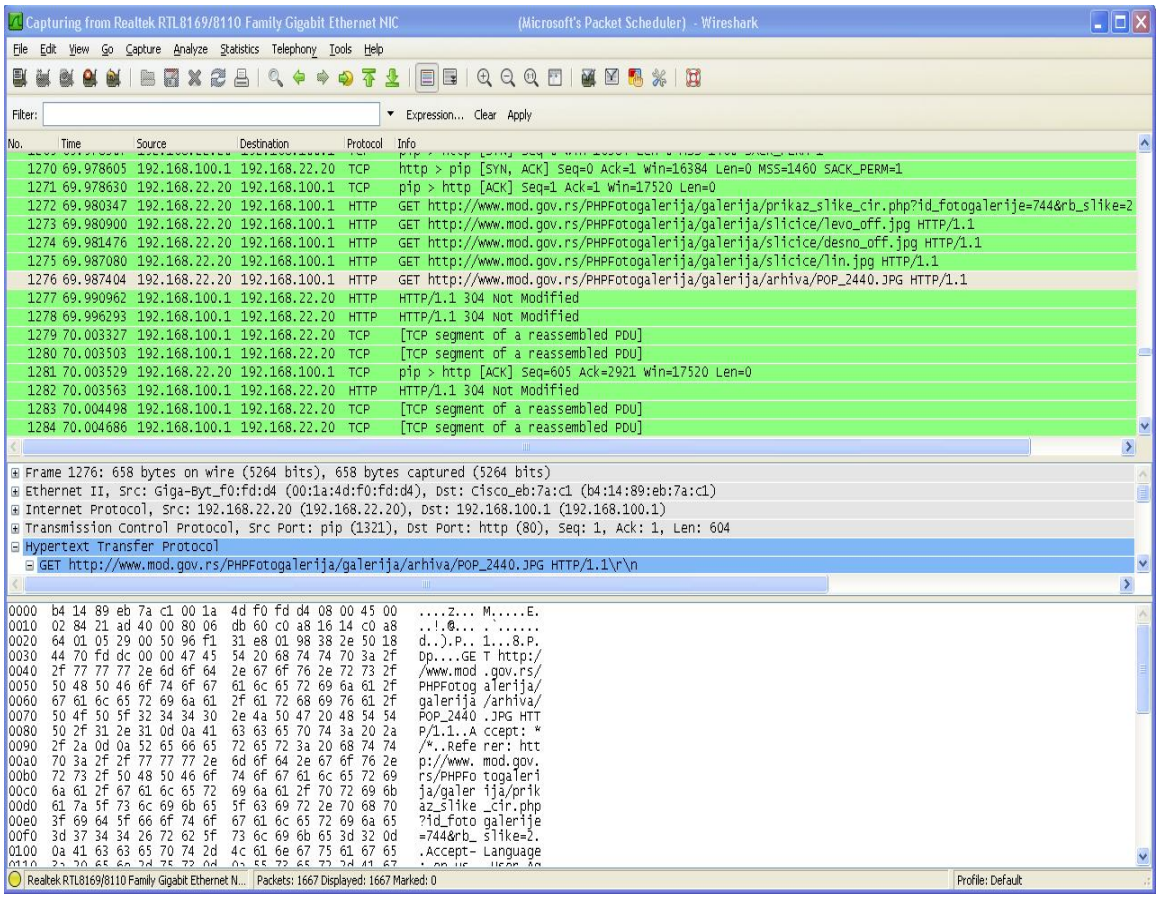
Izborom opcije **Capture Options** u *Start meny* prozoru, odnosno opcije **Options** u prikazu odabranog interfejsa, na raspolaganju nam je prozor **Capture Options**. Izborom ponuđenih opcija upravljamo procesom otkrivanja, hvatanja i prikazivanja tekućih podataka.



Slika 21. Prikaz opcija otkrivanja i sakupljanja u korporativnoj mreži

O meniju Wireshark opcija hvatanja je već bilo reči, ali je veoma važno napomenuti da rad u režimu slobodnog (*Promiscuous mode*) moda neće biti moguć u ovoj mreži sa računara sa korisničkim statusom, iako je ova opcija čekirana. To znači da neće biti moguće uhvatiti celokupan PDU koji je detektovan sa ispitivanog kompjutera na nekom mrežnom segmentu, već samo PDU upućen ka ispitivanom kompjuteru.

Hvatanje PDU upotrebom Wireshark-a u slobodnom modu je nemoguće zbog načina na koji Xen hipervizor (*Xen hypervisor*) funkcioniše i usmerava saobraćaj. Stepen privilegije ispitivanog računara (koji ima status korisnička) pristupu hipervizoru (*virtual machine manager*) je na najnižem nivou, odnosno nema odobren status koji bi mu omogućio direktan pristup fizičkim hardverima, tako da ne postoji mogućnost da se pročita nešto što je prošlo kroz ram hipervizora ka drugim sistemima.



Slika 22. Otkrivanje i sakupljanje jpeg fajla na ispitivanom računaru

Ispitivanje mrežnog saobraćaja Wireshark-om ćemo ilustrovati kroz prikaz otkrivanja i hvatanja fajlova jpeg formata. Wireshark pokazuje samo poslane i primljene pakete između dva *hosta* izlistane u tekućem označenom paketu. Na slici 22. je pokazano da GET (*vrsta HTTP zahteva*) metod sadrži u okviru saobraćaja HTTP, uhvaćene pakete poslate od *hosta* 192.168.100.1 ka *hostu* 192.168.22.20.

Potražimo sliku koja je bila otkrivena i skinuta sa osumnjičenog uređaja. Pregledom HTTP saobraćaja pronaći ćemo paket sa slikom. Slika koja je pronađena se nalazi u paketu 1276. Kada ga označimo i kliknemo desnim klikom pokazaće se meni sa svim raspoloživim informacijama u druga dva panoa prikazanog prozora, kao što je u prethodnom primeru objašnjeno. Uhvaćeni fajl je prikazan na slici 23.



Slika 23. Otkriveni i uhvaćeni JPG fajl

2.3.5. Ograničenja Wireshark-a

Izučavanjem i praktičnom primenom Wiresharka prepoznati su neki, veoma značajni bezbednosni zahtevi. Mnogi korisnici pokreću Wireshark kao administratora, što je podesnije, ali ako neko uzrokuje prekomerno angažovanje *buffer-a* ili ga neko drugi eksploatiše, onda aplikacija može pasti i ostaviti napadača kao administratora. Wireshark je implementiran kao ANSI C kod, koji predstavlja standard Američkog Instituta za standarde (American National Standards Institute) za C programske jezike, radi šire kompatibilnosti nasuprot bezbednijim jezicima poput Java ili C#. ANSI C je ranjiviji na bezbednosne probleme poput prekomernog angažovanja *buffer-a* nego jezici sa mnogim ograničenjima.

Da bi se ispunili postavljeni bezbednosni zahtevi Wireshark je tokom poslednjih nekoliko godina razvijan tako da danas ima više od milion kodnih linija, od kojih je većina nastala kao doprinos rada širokog kruga eksperta za razvoj sa širokim spektrom stručnih ekspertiza.

Da bi se ograničili efekti bilo kakvih bezbednosnih izazova, PC treba konfigursati da automatski startuje WinPcap NPF nakon startovanja PC-ija, a zatim pokrenuti Wireshark kao normalni korisnik. Wireshark startuje NPF kao standardan sistem.

Ako se NPF ne pokreće kao sistem, kao administrator, drajveri se mogu startovati na četiri načina:

- Pokrenuti kompjutersku upravljačku aplikaciju sa komandne linije, tako da će biti pokrenut kao administrator.

  runas /u:domain\admin-acct "C:\WINDOWS\system32\devmgmt.msc"

- U meniju **Device Manager**, izabrati **View** | **Show hidden devices**, otvoriti **Non-Plug and Play Drivers** i desnim klikom kliknuti na **NetGroup Packet Filter Driver**. U podešavanjima drajvera može se podesiti startovanje kao automatsko. Ukoliko je ovakvo podešavanje već podignuto, moraćemo zaustaviti drajvere i promeniti podešavanje.

- Možemo pokrenuti aplikaciiju uslužne kontrole (kao administratora) radi konfigurisanja NPF za automatski start.

  runas /u:domain\admin-acct "sc config npf start= auto"

- U registrima (ponovo kao administrator) možemo promeniti:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
  NPF\Start from 0x3 (SERVICE_DEMAND_START) to 0x2
  (SERVICE_AUTO_START) or 0x1 (SERVICE_SYSTEM_START).

Najbezbednije rešenje je pokretanje drajvera pre startovanja Wiresharka, kao i njihovo zaustavljanje nakon svake sesije. Zapamtićemo niz fajlova kao wireshark.bat radi upotrebe za startovanje NPF i pokretanja Wireshark-a, kao i za zaustavljanje NPF drajvera na kraju. Za realizaciju startovanja i zaustavljanja drajvera neophodna je upotreba administratorske lozinke. Wireshark.bat fajl bi izgledao ovako:

```
echo    off
echo    "First stop the netgroup packet filter driver in case it's already running"
runas   /u:psu\craigs-high "net stop npf";net
echo    "Next start the npf with admin privileges. Wireshark will then start with normal user
        privileges."
runas   /u:psu\craigs-high "net start npf"
"c:\program files\wireshark\wireshark.exe–i \Device\NPF_{5DCA03D5-BC20-4A6A-B7EB-
B2E48577F39B} –k"
echo    "Finally stop the netgroup packet filter.
runas   /u:psu\craigs-high "net stop npf"
```

Svi sistemi za nadzor mreže koji se oslanjaju na *libpcap* imaju ista ograničenja. Ova ograničenja su rezultat razvoja metoda otvorenih izvora. Dok se neko ozbiljnije ne

zainteresuje za razvoj drajvera za fizičke i virtuelne interfejse, *libpcap* ima malo ili nimalo mogućnosti sa ovim interfejsima. Zbog toga svaka aplikacija koja se oslanja na *libpcap* neće biti sposobna da otkrije, sakupi i interpretira informacije na ovakvim interfejsima. U tabeli 1. sumirane su *libpcap* mogućnosti na koje se oslanja Wireshark.

Kao dodatak, Win32 verzija Wireshark-a ima neke probleme sa mrežnim barijerama treće strane. Do sada su poznati problemi sa *SonicWALL Global virtual private network (VPN) Client, Cisco VPN client, F-Secure Anti-Virus Client Security, Sunbelt Kerio Personal Firewall i Checkpoint VPN1 SecureClient*. Provera trenutnih bezbednosnih zahteva se može proveriti na Wireshark CaptureSetup/Interfering Software Web strani.

Table 2.2 Libpcap Interface Capabilities

	AIX	FreeBSD	HP-UX	Irix	Linux	Mac OS X	NetBSD	OpenBSD	Solaris	Tru64UNIX	Windows
Physical Interfaces											
ATM	Unknown	Unknown	Unknown	Unknown	Yes	No	Unknown	Unknown	Yes	Unknown	Unknown
Bluetooth	No	No	No	No	Yes[a]	No	No	No	No	No	No
CiscoHDLC	Unknown	Yes	Unknown	Unknown	Yes	Unknown	Yes	Yes	Unknown	Unknown	Unknown
Ethernet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FDDI	Unknown	Unknown	Unknown	Unknown	Yes	No	Unknown	Unknown	Yes	Unknown	Unknown
FrameRelay	Unknown	Unknown	No	No	Yes	No	Unknown	Unknown	No	No	No
IrDA	No	No	No	No	Yes	No	No	No	No	No	No
PPP[b]	Unknown	Unknown	Unknown	Unknown	Yes	Yes	Unknown	Unknown	No	Unknown	Yes
TokenRing	Yes	Yes	Unknown	No	Yes	No	Yes	Yes	Yes	Unknown	Yes
USB	No	No	No	No	Yes[c]	No	No	No	No	No	No
WLAN[d]	Unknown	Yes	Unknown	Unknown	Yes	Yes	Yes	Yes	Unknown	Unknown	Yes
Virtual Interfaces											
Loopback	Unknown	Yes	No	Unknown	Yes	Yes	Yes	Yes	No	Yes	N/A[e]
VLAN Tags	Yes	Yes	Yes	Unknown	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[a] Linux Affix Bluetooth stack only
[b] PPP noncontrol frames only
[c] Latest libpcap Concurrent Versions System (CVS) required (which exact version?)
[d] On some platforms: Wireless Local Area Network (WLAN) noncontrol frames only, with fake Ethernet headers, and only traffic to and from the machine doing the capturing
[e] Windows does not have a UNIX-style loopback interface

Tabela 1. Mogućnosti *libpcap* interfejsa

2.3.6. Usluge Wireshark-a

Razvijači Wireshark su u cilju proširivanja mogućnosti Wireshark-a kreirali nekoliko dodatnih usluga, i to:

- TShark
- RawShark
- Dumpcap
- Mergecap
- Editcap
- Text2pcap

TShark

TShark je protokol za analizu mreže koji dozvoljava da se otkriju i sakupe paketi podataka iz mreže u realnom vremenu ili pročita paket sa prethodno zapamćenog uhvaćenog fajla ili odštampane dekodirane forme ovih paketa sa standardnog izlaza ili pisanjem paketa u fajl. Format otkrivenog i sakupljenog fajla je *libpcap* format, koji je takođe format koji koristi *tcpdump* kao i mnogi drugi brojni alati.

Podešavanje filtera Tshark-a, koji dozvoljavaju da se odaberu paketi koji će biti dekodovani ili zapisani u fajlu, je veoma moćno. Upotrebom TShark-a, više se polja filtrira nego bilo kojim drugim protokolom za analizu, a takođe i sintaksa kojom se mogu kreirati filtri je bogatija. Razvojem TShark procesa analize mreže može se očekivati sve više polja kojima je dozvoljeno u čitanje filtrima.

Rawshark

Rawshark čita tekuće pakete fajla ili nekog drugog izvora i štampa linije objašnjavajući njegov izlaz, prateći set pronađenih polja za svaki paket na standardnom izlazu. Za razliku od Tshark-a, Rawshark ne pravi pretpostavke o sažimanju ili ulazu. Indikatori `-d` i `–r` moraju biti određeni sa ciljem da budu spremni za podizanje. Jedan ili više `-F` indikatora treba da bude određen ako želimo da izlaz bude koristan. Ostali indikatori slede pravila kao kod Wireshark-a i TShark-a.

Dumpcap

Ako želimo da izvedemo neprimetno otkrivanje i sakupljanje mrežnog saobraćaja ili pokrenutog procesa sakrivenog od prosečnog korisnika, možemo upotrebiti Dumpcap. Da

bi se izvršila bilo koja usluga komandne linije sa administratorovom privilegijom upotrebljavamo komandu *run* da bi se pokrenuli komandnu liniju za korisnika sa administratorovim privilegijama.

runas /user:domain\userid "cmd.exe"

Domain\userid je domenska i korisnička ID jednog naloga sa administratorovom privilegijom *hosta*. Radi nastavka analize upotrebom komandne linije, pokrećemo *utilityname* sa parametrima koji su zahtevani za ovo otkrivanje i sakupljanje paketa iz mreže.

Dumpcap je alat za skladištenje mrežnog saobraćaja. On dozvoljava otkrivanje i sakupljanje paketa podataka sa mreže u realnom vremenu i zapisivanje paketa u fajl. Format fajla koji je otkriven i sakupljen Dumpcap-om je *libpcap* format. Dumpcap se razlikuje od *tcpdump* i *WinDump* alata po tome jer poseduje određeni broj parametara koje daju instrukcije Dumpcap-u kada da zaustavi sakupljanje podataka. Navedimo nekoliko Dumpcap-ovih izlaznih kontrola, i to:

- - a <capture autostop condition> – Određuje kriterijume koji određuju kada će Dumpcap prekinuti zapisivanje otkrivenog i sakupljenog fajla. Kriterijum je u formi *test:*value, gde test može biti jedan od sledećih:

    - *duration:*value – Zaustavlja zapisivanje uhvaćenog fajla nakon isteka value sekundi.

    - *filesize*:value – Zaustavlja zapisivanje uhvaćenog fajla nakon dostignute value veličine kilobajta (gde je kilobajt 1024 bajta). Ako se ova opcija koristi zajedno sa -b opcijom, Dumpcap će zaustaviti zapisivanje tekućeg uhvaćenog fajla i prebacivanja na sledeći ako je veličina fajla dostignuta.

    - *files:*value – Zaustavlja zapisivanje uhvaćenog fajla nakon dostignutog value broja zapisanih fajlova.

- - b <capture ring buffer option> – Uzrokuje podizanje Dumpcap-a u modu "*multiple files*" u kojem će zapisivati nekoliko uhvaćenih fajlova. Kada se prvi uhvaćeni fajl ispiše Dumpcap će se prebaciti na ispisivanje sledećeg fajla i tako redom. Kreirano ime fajla se bazira na imenu datom –w opcijom, brojem fajla i datumom vremenom kreiranja fajla, poput
  outfile_00001_20050604120117.pcap, outfile_00001_20050604120523.pcap, …

- Sa *files* opcijom fajla moguće je oformiti "*ring buffer*". Ovako će se ispisivati novi fajlovi sve do broja fajlova koje je određen, i na kojoj tački će Dumpcap izbaciti podatke iz prvog fajla i započeti zapisivanje u sledeći i tako redom. Ako *files* opcija nije podešena novi fajl će se ispisivati sve dok se ne dostigne jedan od uslova za zaustavljanje otkrivanja i sakupljanja podataka ili se ne napuni disk, tako da se sa ovim mora postupati veoma obazrivo.

- Kriterijum forme *key*:value, gde je *key* jedan od sledećih:

  - *duration*:value – Prebacuje na sledeći fajl nakon isteka value sekundi, čak i kada tekući fajl nije potpuno ispisan.

  - *filesize*:value – Prebacuje na sledeći fajl nakon dostizanja value veličine kilobajta (gde je kilobajt 1024 bajta).

  - *files*:value – Počinje ponovi sa prvim fajlom posle value broja ispisanih fajlova (u formi ring buffer-a).

- - B <capture buffer size> – Važi samo za Win32: podešava veličinu otkrivenog i sakupljenog *buffer-a* (u megabajtima, standard je 1 MB). Ovu operaciju izvodi drajver za otkrivanje i sakupljanje paketa podataka u *buffer-u* sve dok mogu da budu ispisana na disk. Ako se susretnemo sa odbačenim paketima prilikom otkrivanja i hvatanja paketa, treba pokušati povećati veličinu diska.

- - c <capture packet count> – Podešava maksimalni broj paketa koji se čitaju tokom otkrivanja i sakupljanja podataka u realnom vremenu .

Mergecap

Mergecap je program koji kombinuje višestruko otkrivene i sakupljene zapamćene fajlove u jedinstvene izlazne fajlove određene sa - w argumentom. Mergecap zna kako da čita otkrivene i sakupljene fajlove *libpcap-om*, uključujući i one uhvaćene sa *tcpdump*, Wireshark-om i ostalim alatima koji otkrivaju i sakupljaju u ovom formatu.

Mergecap može da ispisuje fajlove u nekoliko izlaznih formata. Indikator – F može da se koristi za određivanje formata u kojem će biti ispisan uhvaćeni fajl, dok *mergecap – F* obezbeđuje listu dostupnih izlaznih formata.

Paketi ulaznih fajlova su spojeni hronološkim redom baziranim na pojedinačnim otisku vremenskog okvira sve dok je – a indikator određen. Mergecap pretpostavlja da su okviri u pojedinačnim uhvaćenim fajlovima već pohranjeni po hronološkom redu. Kada je – a indikator određen, paketi se kopiraju direktno sa svakog ulaznog fajla u izlazni fajl, nezavisno od bilo kog otiska vremenskog okvira.

Editcap

Editcap je program koji čita neke ili sve uhvaćene pakete ulazih fajlova, opcionalno on ih konvertuje na različite načine i zapisuje u uhvaćeni izlazni fajl (ili fajlove). Standardno, on čita sve pakete ulaznih fajlova i zapisuje ih u izlazni fajl u *libpcap* fajl formatu.

Lista brojeva paketa može biti određena u komandnoj liniji. Opseg brojeva paketa može biti određena kao opcija *start–end*, odnoseći se na sve pakete od početka do kraja. Selektovani paketi sa ovim brojevima neće bit zapisani u uhvaćenom fajlu. Ako je –r indikator određen, celokupan selektovani paket je okrenut. U tom slučaju samo selektovani paketi će biti zapisani u uhvaćenom fajlu.

Editcap može da zapiše fajl u nekoliko izlaznih formata. Indikator –F se koristi za određivanje formata u kojem će biti zapisan izlazni fajl, *editcap – F* obezbeđuje listu dostupnih izlaznih formata.

Text2pcap

Text2pcap je program koji čita ASCII heksadecimalne podatke i zapisuje podatke u *libpcap* uhvaćenom formatu. Text2pcap može da čita multiple pakete u heksadecimalnom obliku i da od njih izgradi uhvaćeni fajl. Takođe je sposoban da generiše maketu Ethernet, IP i UDP, TCP ili SCTP (*Stream Control Transmission Protocol*) zaglavlja sa ciljem da izgradi potpuno obradivi paket od podataka sa aplikativnog nivoa koji se nalaze u heksadecimalnom obliku.

Text2pcap razume generisanu heksadecimalnu formu dodavanjem -Ax-tx1. Drugim rečima, svaki bajt je pojedinačno prikazan i okružen prostorom. Svaka linija počinje sa opisom pomeranja pozicije u fajlu. Pomeranje je heksadecimalan broj (može takođe biti i okta ili decimalan) sastavljen od više od dva šestocifrena broja.

3. ZAKLJUČAK

Pomeranjem modernog kompjuterskog okruženja od, u prošlosti aktuelnog lokalnog centra sa pojedinačnim ulaznim i izlaznim tačkama ka savremenim globalnim mrežama koje uključuju mnoštvo informacionih centara i stotine ulaznih i izlaznih tačaka, odnosno seobom poslova i usluga ka udaljenim centrima informacija, na kojima su smešteni računarski i skladišni kapaciteti, koji su iznajmljeni od velikih kompanija, stvoreni su uslovi za unapređenje poslovanja pojedinaca i kompanija. Prednosti poslovanja u CC okruženju se ogleda kako u pogledu produktivnosti, tako i u pristupu veoma brzim sistemima koji upravljaju velikom količinama podataka, kao i udaljenim računarskim i skladišnim kapacitetima, transakcionim procesnim sistema i softverskim paketima koji su iznajmljeni i mogu biti bilo gde u svetu.

Međutim, uporedo sa brojnim prednostima rada u ovakvom okruženju susrećemo se sa brojnim bezbednosnim komplikacijama, bilo da se radi o proceduralnim ili pravnim bezbednosnim komplikacijama. Kompjuterski sistemi i mrežna forenzika se nalaze pred izazovom koji proističe iz transfera lokalnog informatičkog centra u udaljeni informatički centar kojem fizički pristup nije moguć.

Koncept mrežne forenzike u ovakvom okruženju zahteva novi aspekt sagledavanja problema bezbednosti. Opšti problem je što se principi tradicionalne digitalne forenzike ne mogu u potpunosti primeniti u CC okruženju. Otuda je digitalna forenzika CC okruženja veoma složen i vremenski zahtevan posao, koji zahteva specifične alate za analizu i posebne veštine forenzičara.

Digitalna forenzika u CC okruženju otkriva i sakuplja informacije o tome kako je napadač dobio pristup računarskoj mreži i računarskom sistemu. Analizom fajlova se određuje kada se korisnik ulogovao ili poslednji put koristio svoj lični identifikator (ID) za logovanje. Digitalni forenzičar nastoji da odredi kojim URL je korisnik pristupio, kako se ulogovao na računarsku mrežu i sa koje lokacije.

Poslovanje u CC okruženju predstavlja mnoge izazove i prilike mrežnoj i kompjuterskoj forenzici. Izazove koje ovaj sistem reflektuje na distributivni model, koji je prihvaćen i adaptiran u mnogim kompanijama kroz angažovanje sopstvenih i spoljnih izvora, mrežni i kompjuterski centri podataka odslikavaju na posao i poslovne operacije. Promene u bezbednom okruženju, deperiferizacija naših sistema i mreža zahtevaju novi pristup bezbednosti informacija kao i mrežne i kompjuterske forenzike. Ovde se nailazi na plodno tlo za hakere, što zavisi od načina na koji smo izgradili arhitekturu mreže i kako odgovaramo na rizik u ovakvom kompjuterskom sistemu.

Od izuzetne važnosti, za sprovođenje postupka forenzičke analize predstavlja postupak otkrivanja i sakupljanja tekućih ("živih") mrežnih forenzičkih podataka, odnosno podataka koji se prenose putem mrežnog saobraćaja u realnom vremenu.

Za uspešnu forenzičku istragu je veoma važno odabrati softverski forenzički alat za analizu mreže koji se može koristiti i za otkrivanje i sakupljanje podataka sa mreže i prikazivanje uhvaćenih paketa podataka u realnom vremenu, što može da omogući da korisnik stekne uvid u stanje protoka podataka i da reaguje odmah po nastanku incidenta.

Na tržištu postoji se može naći veliki broj digitalnih forenzičkih alata, ali se uprkos tome ne može se govoriti o najboljem, univerzalnom digitalnom forenzičkom alatu. Specijalizovani forenzički alati koriste se za samo određenu vrstu fajlova ili obavljaju samo jedan zadatak digitalne forenzičke istrage. Ovi alati su namenski i pouzdaniji te mnogo efikasnije obavljaju specifičan zadatak nego neki univerzalni alati. Najbolji rezultati se u forenzičkoj istrazi postižu upotrebom adekvatnog skupa raznovrsnih digitalnih forenzičkih alata, naročito kada forenzičar sam, na bazi predistražnih podataka i informacija o slučaju, izvrši izbor adekvatnih alata za konkretan slučaj, uključujući skup alata za izvršenje što više digitalnih forenzičkih zadataka na terenu kao i specijalizovane alate za detaljno i precizno izvršavanje karakterističnog forenzičkog zadatka.

Filozofije dizajna najuticajnih provajdera CC okruženja, poput Windows Azure, AWS i Rackspace se moraju uzimati u obzir kada se vrši forenzička analiza infrastrukture sistema kompanija koje njihove usluge. Proces odgovora na incident ne treba biti menjan ali način na koji se definiše upravljanje uslugama okruženja mora biti deo procesa odgovora na incident. Nedostatak alata za nadzor sistema, potreba za novim metodama programiranja radi praćenja transakcija u mreži, kao i osposobljenost lica koja se staraju o bezbednosti sistema moraju da se menjaju sa ciljem podizanja bezbednosti sistema. Prednosti forenzike ovog sistema kao što su skladištenje ISO forenzičkog lika kompjutera, mogućnost da se procesuiraju i uskladište veliki log fajlovi, mogućnost izgradnje sistema koji dozvoljavaju deljenje informacija samo među autorizovanim osobama su glavne prednosti ovog sistema. Kompanije i odeljenja kompanija za bezbednost moraju biti svesni snage i ograničenja ovog okruženja i u skladu sa tim planirati procese mrežne i kompjuterske forenzike.

4. SPISAK LITERATURE

[1] Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, James "Jim" Steele, *Digital forensics for network, Internet, and cloud computing*, Syngress 2010.

[2] Milosavljević Milan, Gojko Grubor, *Digitalna forenzika*, Beograd 2008.

[3] Tim Grance, Suzanne Chevalier, Karen Kent, Hung Dang, *Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response (Draft)*, Recommendations of the National Institute of Standards and Technology, Special Publication 800-86, August 2005.

[4] Karen Scarfone, Peter Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, Recommendations of the National Institute of Standards and Technology, Special Publication 800-94, February 2007.

[5] Karen Scarfone, Murugiah Souppaya, Paul Hoffman, *Guide to Security for Full Virtualization Technologies (Draft)*, Recommendations of the National Institute of Standards and Technology, Special Publication 800-125, July 2010.

[6] D. Chappell, *Window Azure and ISVs: A guide for decision makers*, Microsoft Corporation, 2010.

[7] D. Chappell, *Introducing the Windows Azure platform*, Microsoft Corporation, 2009.

[8] C. Perrin, *There is no perimeter*, TechRepublic, 2008.

[9] W. Pieters, A. van Cleef, *The precautionary principle in a world of digital dependencies*, 2009.

[10] AccessData Corporation, *The importance of Integrating Host and Network Forensics*, USA 2005.

[11] Chris Boyd, Pete Forster, *Time and date issues in forensic computing, case study*, National Technical Assistance Centre, UK, January 2004.

[12] Peter Mell, Tim Grance, *Definition of Cloud Computing*, National Institute of Standards and Technology, Information Technology Laboratory, Version 15, 2009.

[13] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, April 2009.

[14] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, December 2009.

[15] Ulf Lamping, Richard Sharpe, Ed Warnicke, *Wireshark Developer's Guide for Wireshark 1.5*, 2004-2011.

[16] Cisco Certified Network Associate (CCNA), Exploration 4.0. Network Fundamentals Lab 2.6.2: *Using Wireshark™ to View Protocol Data Units*