INTEGRISANI MODEL PROCESA DIGITALNE FORENZIČKE ISTRAGE

Autor: Uglješa Georgijević, Gradski sudija za prekršaje

Rezime: *U ovom radu, je definisan model procesa za digitalnu (forenzičku istragu kompjuterskog incidenta) koristeći teorije i tehnike iz istrage fizičkog sveta. Dok su digitalne istrage tek skoro postale uobičajene, fizičke istrage su postojale hiljadama godina i iskustvo iz njih može se primeniti na digitalni svet. Ovaj rad predstavlja ideju digitalne scene zločina sa njenim svedocima, dokazima, i događajima koji mogu biti istraženi koristeći isti model kao i kod fizičke scene zločina. Ovaj model integriše istragu fizičke scene zločina sa istragom digitalne scene zločina da bi se identifikovala osoba koja je odgovorna za digitalnu aktivnost. Model je primenljiv i na zvaničnu i na korporacijsku istragu.*

Ključne reči: *Fizički dokaz, Digitalni dokaz, Fizička scena zločina, Digitalna scena zločina, Forenzički digitalni dokaz.*

THE MODEL OF INTEGRATED DIGITAL INVESTIGATION PROCESS

Abstract: *In this paper, a process model for digital (computer incident forensic) investigations is defined using the theories and techniques from the physical investigation world. While digital investigations have recently become more common, physical investigations have existed for thousands of years and the experience from them can be applied to the digital world. This paper introduces the notion of a digital crime scene with its own witnesses, evidence, and events that can be investigated using the same model as a physical crime scene. The proposed model integrates the physical crime scene investigation with the digital crime scene investigation to identify a person who is responsible for the digital activity. The proposed model applies to both law enforcement and corporate investigations.*

UVOD

Razvoj informaciono-komunikacionih tehnologija (IKT) otvara prostor i za razne vrste zloupotreba kao i načine njihovog suzbijanja. Zloupotrebe mogu biti nenamerne i namerne. Nenamerne su posledica neadekvatnog tj. nestručnog rukovanja sistemom, dok su namerne pokušaji hakera da iskoriste mogućnosti IKT-a radi pribavljanja koristi, 9.

Upravo zbog toga pojavljuje se potreba da država u svoj pravni sistem uvedu i odgovarajuću zakonsku regulativu koja će krivično sankcionisati i samim tim zaštititi prava oštećenih. Ukazuje se potreba normativnog regulisanja uslova načina i postupaka kako kolektivno organizovanih stručnih lica tako i pojedinaca tj. sudskih veštaka, koji bi ispunjavali profesionalne, etičke i legalne uslove radi istrage, otkrivanja, dokazivanja , i razrešavanja činjenica. Često pravosudni organi ne raspolažu stručnim licima koja bi posedovala znanja vezana za IKT tehnologiju, zbog toga je neophodno veštačenje, tj. izvođenje dokaza od strane stručnih lica. Da bi dokazi bili važeći tj. priznati na sudu potrebno je ustanoviti i standardizovati proces istrage i sve njegove faze.

Procesni model koji je opisan u ovom radu nije jedini procesni model pogodan za digitalnu analizu. U prošlosti predloženo je i korišteno u organizovanju nekoliko drugih procedura istrage kompjuterskog incidenta (kriminala), [9].

Brojne istrage kriminala uključuju kompjutere u nekoj tački slučaja. Osumnjičenima za ubistva i silovanja mogu se preko naloga za pretres, analizirati njihove e-*mail* i Internet aktivnosti, da bi se našli dokazi o njihovim motivima ili skrovištima. Korporacije istražuju kompjutere kada je zaposleni osumnjičen za neautorizovane postupke. U istragama prevara skupljaju se istorijski dokazi sa servera. Zbog toga je važno da postoji model procesa za digitalnu istragu koji lako uspostavlja vezu sa fizičkom istragom za koju postoje bogata iskustva. Predstavljeni procesni model postupka digitalne istrage zadovoljava ovaj i sledeće zahteve:

- zasnova se na postojećoj teoriji fizičke istrage scene zloočina,
- praktičan je i sprovodi iste korake koje sledi realni proces istrage,
- dovoljno je generički (opšti) i nezavisn od tekuće tehnologije,
- dovoljno je specifičan da se za svaku fazu mogu razviti opšti zahtevi,
- dovoljno je apstraktan i primenljiv za zvaničnu istragu, korporacijsku istragu i primarnu reakciju na kompjuterski incident.

Za rad je korištena literatura koja definiše procedure za istragu fizičke forenzičke scene sa ciljem pronalženja modela koji bi se mogli primeniti za digitalnu forenzičku istragu.

U tom smislu, umesto da se kompjuter koji se nalazi na sceni na kojoj se odigrao zločin, tretira kao neki predmet, smatraće se kao ***sekundarna scenu zločina***. Tako če se koristiti isti principi istrage, kao kad se ispituje soba u kojoj se dogodio neki zločin, iako su različite specifične metode i tehnologija za digitalnu forenzičku istragu.

Drugi autori koriste termine tipa "*digitalna scena zločina*" ili "*kompjuterska scena zločina*" za bilo koju scenu zločina u kojoj se nalazi neki kompjuter. U ovom radu termin "*digitalna scena zločina*" koristi se za digitalno okruženje, koje se nalazi u hardveru i softveru. Postoje radovi koje koriste termin *digitalna scena zločina* na isti način kao u ovom radu, ali oni ne primenjuju procedure fizičke forenzičke istrage.

Digitalna forenzička istraga kompjutera ili nekog drugog digitalnog uređaja ima sličnosti sa istragom fizičke scene zločina zbog količine potencijalnih dokaza. Kao što fizička scena može biti obrađena za identifikaciju velikog broja dokaza, na isti način i kompjuter, iako je samo jedan fizički predmet, može biti obrađen za identifikaciju mnoštva dokaza kao što su identitet počinioca, vlasništvo podataka, vreme i pozicija događaja. Digitalni podaci mogu biti analizirani na isti način kao i fizički dokazi.

U radu su predstavljena dva modela, za: korporacijsku forenzičku istragu i zvanični proces istrage.

1. MODELI ZA FORENZIČKU ISTRAGU

1.1 Korporacijski model istrage

Funkcionalni korporacijski model istražnog postupka može se opisati sledećim fazama, [5]:

- **Priprema za incident**: sa odgovarajućom obukom i infrastrukturom;
- **Detekcija incidenta**: identifikovati sumnjivi incident;
- **Prva reakcija**: prepoznati i potvrditi da se incident dogodio, sakupiti preliminarne, nestabilne i posredne dokaze (koji se vremenom degradiraju);
- **Formulisanje strategije reakcije**: na bazi poznatih infdikatora;
- **Dupliranje**: napraviti fizičku *miror* sliku kompromitovanog sistema;
- **Istraga**: ispitati sistem radi identifikacije ***ko***, ***šta*** i ***kako*** je izvršio napad;
- **Implementacija mera zaštite**: izolovati kompromitovan sistem pre nego što je vraćen u normalni režim rada;
- **Nadzor mreže**: posmatrati mrežu radi identifikacije novih (ponovljenih) napada;
- **Oporavak**: vratiti sistem u originalno stanje sa dodatnim merama zaštite;
- **Izveštavanje**: dokumentovati reakciju na incident (kriminal) i izvestiti;
- **Završna faza**: revidirati saniranje incidenta i eventualno poboljšati proces.

1.2 Zvanični model istrage

U SAD "*Department of Justice*" objavio je model procesa istrage u "*Vodiču za istragu elektronske scene zločina*", 9. Vodič odgovara fizičkoj sceni zločina, tako da je akcenat stavljen na te zahteve, a malo pažnje obraća na forenzičku analizu digitalnih sistema. Faze modela su sledeće:

- **Priprema**: pripremiti opremu i alat potreban za istragu**;**
- **Sakupljanje**: naći i sakupiti elektronske (digitalne) dokaze;
  - **Osigurati i proceniti scenu**: obezbediti scenu radi bezbednosti lica i integriteta podatka i identifikovati potencijalne dokaze;
  - **Dokumentovanje scene**: dokumentovati fizički opis scene uključujući fotografije računarskog sistema;
  - **Sakupljanje dokaza**: (forenzička akvizicija) zapleniti fizički računarski sistem, ili napraviti fizičku (*miror*) kopiju podataka na forenzičkom računarskom sistemu;
- **Pregled**: tehnički pregled i ispitivanje sistema radi nalaženja potencijalnih dokaza;
- **Analiza**: (digitalna forenzička analiza) istražni tim pregleda rezultate tehničkog pregleda radi procene njihove važnosti za slučaj;
- **Izveštaj**: izveštaj se pravi posle svakog slučaja kompjuterskog (incidenta) kriminala.

Ovaj model je baziran na standardnoj istrazi fizičke scene zločina i kao i prethodni model, ne obraća mnogo pažnje na proces forenzičke analize digitalne scene zločina i ne ispunjava zahteve modela za proces istrage digitalnih dokaza.

1.3 Model istrage fizičke scene zločina

Sa aspekta teorije istrage, konsultovana je brojna literatura za fizičke istragu, [5], [9], [9, 9, 9. Faze fizičke istrage scene zločina su:

- **Očuvanje, fiksiranje scene zločina:** prvi korak je da se pomogne povređenima, zatim sledi potraga za osumnjičenima i hapšenje osumnjičenih i zadržavanje svih svedoka. Fizička scena zločina mora biti osigurana, a pristup sceni zločina omogućen samo ovlašćenim licima, istražnim organima, (kriminalistički inspektor, detektiv, forenzičar sudske medicine i.t.d.).
- **Pregled scene zločina:** istražni organ pažljivo pretražuje scenu zločina da bi identifikovao očigledne delove dokaza i kratkotrajne dokaze (krv, sluz, sperma, pljuvačka i.t.d.). Početna opažanja tipa ***ko, šta, gde, kada, kako*** dokumentuju se i kreira se početna teorija (***hipoteza slučaja***).
- **Dokumentovanje scene zločina:** scena zločina se dokumentuje fotografisanjem, skiciranjem i snimanjem digitalnog video snimka. Dokaze treba jednoznačno označiti, dokumentovati jasno, potpuno i sakupljati ih za analizu.
- **Pretraga scene zločina:** brojni obrasci istrage koriste se da bi se identifikovali dodatni dokazi koji nisu otkriveni u predistažnom postupku (pregledu). Teorija razvijena u pretrazi koristi se za pretragu specifičnih dokaza koji nedostaju (npr., oružje kojim je počinjeno ubistvo).
- **Rekonstrukcija scene zločina:** događaji koji su se dogodili na mestu zločina određuju se na osnovu izgleda scene zločina, mesta i pozicije fizičkih dokaza, analiziranih rezultata iz forenzičke laboratorije i naučnih metoda primenjenih u istrazi i analizi dokaza.

Ovaj model omogućava kompletnu dokumentaciju mesta zločina i koristi *detektivsko* iskustvo (iskustvo istražnog organa) da bi se došlo do korisnih dokaza. Svi fizički predmeti ne mogu da se uzmu sa mesta zločina, tako da *Faza Pretrage scene zločina* mora biti potpuna da bi se sakupili potrebni dokazi, ali ne sme se preoptereti laboratorija sa predmetima koji nemaju veze sa slučajem.

2. MODEL INTEGRISANIH PROCESA DIGITALNE FORENZIČKE ISTRAGE

Ovaj model istrage koristi mnoge faze koje su opisane u poglavljima 0, 0 i 1.3, ali prilazi problemu sa druge tačke gledišta. Model koristi pretpostavku da je kompjuter sam po sebi mesto zločina, nazvan ***digitalna scena zločina*** i primenjuje tehnike istrage fizičke scene zločina. Istraga fizičke scene zločina koristi zakone prirode i bogata iskustva, da bi otkrila fizičke dokaze, a istraga digitalne scene zločina koristi kôd da bi otkrila digitalne dokaze, [5].

U istrazi fizičke scene zločina, najpoznatija primenjena teorija je *Lokardov zakon razmene,* [18]*:* "Kada dva objekta dođu u kontakt, doći će do razmene materije između njih". Na primer, dlake i vlakna sa zločinca često se zadržavaju na fizičkoj sceni zločina. Sličan efekat se dešava u digitalnoj sceni zločina. Privremene datoteke, sadržaj memorije koji je snimljen na disku i izbrisani delovi datoteka, mogu ostati zbog delovanja softvera (alata, OS) koji je osumnjičeni koristio i izvršavao u toku napada. Podatak ulazi i ostaje u digitalnoj sceni zločina, ostavljajući tragove digitalnog dokaza iza sebe na raznim mestima u memorijskim elementima računarskog sistema (hard disku, memoriji, pokretnim memorijskim elementima i.t.d.). Rad ***digitalnog forenzičara*** u potpunosti zavisi od rada operativnog sistema i aplikativnih programa, zato što oni nezavisno od korisnika kontrolišu koji dokaz je napisan i u kojem delu memorijskih lokacija.

Koristeći koncept da je kompjuter sam za sebe scena zločina, može se teorija istrage fizičke scene zločina primeniti na digitalnu forenzičku istragu. Rezultirajući model procesa opisan je u sledećem poglavlju, uključujući kratak opis akcija koje treba preduzeti. Forenzička istraga digitalne scene zločina integrisana je sa istragom fizičke scene zločina tako da fizički dokazi mogu biti sakupljeni i povezani sa digitalnom aktiv-

nošću napadača (X). Digitalna scena (X) osumnjičenog kompjuterskog kriminala može se smatrati za sekundarnu scenu zločina, u odnosu na fizičku scenu zločina.

U ovoj oblasti, postoje brojne interpretacije i mišljenja oko ključnih reči. Da bi se sprečila konfuzija, definišimo osnovne termine procesa, tako da najtačnije odražavaju izabrani pristup problemu:

- **Fizički Dokaz:** fizički objekti koji mogu utvrditi da je kriminalni akt počinjen, i koji mogu da omoguće vezu između zločinca i žrtve, ili mogu da omoguće vezu između zločina i izvršioca zločina, 9. Kompjuter, hard disk, PDA i CD-ROM su primeri fizičkog dokaza.
- **Digitalni dokaz:** digitalni podatak koji može potvrditi da je kompjuterski kriminal počinjen i koji može da omogući vezu između kriminala i njegovog izvršitelja, 9. Podatak u memoriji, na hard disku, ili u mobilnim telefonima primeri su digitalnog dokaza.
- **Fizička scena zločina:** fizičko okruženje gde postoje fizički dokazi zločina ili incidenta. Okruženje gde se prvi kriminalni akt dogodio je ***primarna fizička scena zločina,*** a sledeće scene su ***sekundarne fizičke scene zločina***. Ova definicija je kreirana prema definiciji koju je definisao Lee, 9.
- **Digitalna scena zločina:** Virtuelno okruženje koje se sastoji od hardvera i softvera gde digitalni dokaz zločina ili incidenta postoji. Okruženje gde se prvi kriminalni akt dogodio je ***primarna digitalna scena zločina*****,** a sledeće scene se nazivaju ***sekundarnim digitalnim scenama zločina****.*

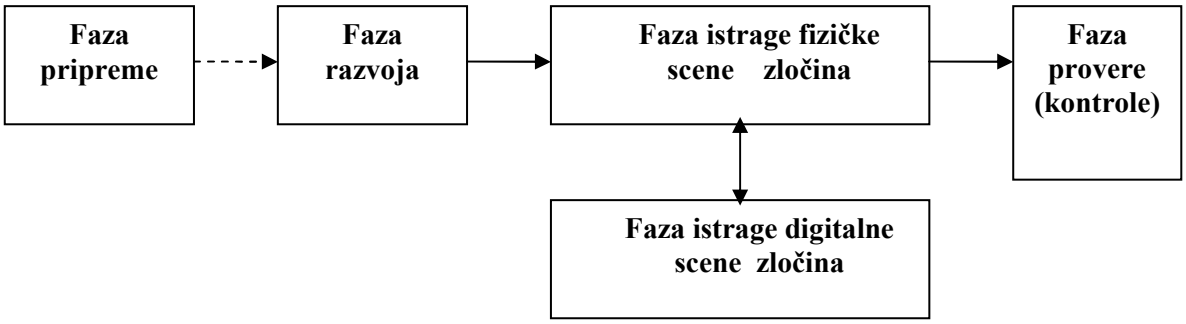
Ovaj model procesa primenljiv je na obe vrste istrage, korporacijsku i zvaničnu. Zbog toga se izrazi “scena zločina” i “incident” koriste u opštem smislu. Pod fizičkom scenom zločina podrazumeva se sto zaposlenog kojeg ispituje organa istrage, centar za obradu podataka koji sadrži server, soba za istragu dečije pornografije, ili kola u kojim je čovek ubijen i u kojima na suvozačevom sedištu stoji otvoren laptop. Incident je bilo koja serija događaja koji zahtevaju reagovanje interventnog tima za kompjuterski incident, ili forenzičkog tima za prikupljanje dokaza. Ovo uključuje upad u server, izdavanje naloga za pretres kuće osumnjičenog i reagovanje specijalne jedinice MUP-a za borbu protiv visokotehnološkog (kompjuterskog) kriminala na hitni poziv 92.

Pretpostavljamo da je veličina scene zločina inicijalno definisana prirodnim granicama oko poznatih dokaza. Na primer, ukoliko je zločin počinjen u kući, onda kuća i vlasništvo oko nje može biti inicijalna fizička scena kriminala, a veličina kasnije može biti povećana ili smanjena zavisno od novih dokaza koji se pronađu. Za kompjuter, inicijalna digitalna scena zločina je tipično virtuelno okruženje kreirano lokalnim operativnim sistemom i hardverom. Svaki pojedinačni kompjuter, uključen u incident, najbolje je tretirati kao zasebnu digitalnu scenu zločina.

Termini “*pregled (revizija*) ” i “*analiza*” koji se koriste u ovom radu znače da se neki objekat računarskog sistema ili računansrkse mreže, može procesirati u nekom smislu i da se mogu prikupiti informacije iz njega.

Model integrisanih procesa ima 17 faza organizovanih u pet grupa (Sl. 1):

1. Faza pripreme;
2. Faza razvoja;
3. Faza istrage fizičke scene zločina;
4. Faza istrage digitalne scene zločina;
5. Faza provere (kontrole).



Sl. 1. Faze modela integrisanih procesa digitalne forenzičke istrage

Primetimo da se na slici *Faza Istrage Fizičke Scene Zločina* izvodi uporedo sa *Fazom Istrage Digitalne Scene Zločina.* Rezultati *Istrage Digitalne Scene Zločina* koriste se u *Istrazi Fizičke Scene Zločina.*

2.1 Faza pripreme

Cilj faze pripreme je da osigura da operacije i infrastruktura mogu u potpunosti podržati proces istrage. Digitalni i fizički dokazi mogu biti izgubljeni ukoliko nisu prikupljani i čuvani na pravi način. Ova faza je u stalnom trajanju i nije vezana za bilo koji zločin ili incident, 9.

Operacije faze pripreme obezbeđuje obuku i opremu za lica koja će biti uključena u istragu incidenta. Ovo uključuje obuku interventnog tima za odgovor (eng.“*responders*”), forenzičkih laboratorijskih analitičara i lica koja će primati inicijalne izveštaje o incidentu. Forenzička oprema sa kojom interventni tim pretražuje scenu zločina mora biti ispravna, potpuno sanirana (čista) i da predstavlja poslednja tehnološka rešenja. Oprema u laboratoriji za digitalnu forenzičku analizu mora, takođe, da bude održavana na visokom nivou pouzdanosti i spremna za analizu svih dospelih podataka o incidentu.

Infrastruktura faze pripreme obezbeđuje da se generišu potrebni digitalni i drugi podaci da bi se izvršila potpuna istraga, jer ukoliko podaci ne postoje nemoguće je izvršiti istragu. Ova faza odnosi se samo na one koji održavaju okruženje koje bi potencijalno moglo biti scena kompjuterskog kriminala. Fizički primeri za ovu fazu su instalacije i raspoređivanje video nadzora i čitača kartica da bi se snimili pristupi prostoru za vreme kriminalnog akta. Digitalni primeri za ovu fazu su skladištenje log datoteka servera i drugih mrežnih uređaja na zaštićeni “log host”, sinhronizacija unutrašnjih satova na serverima i računarima sa NTP (*Network Time Protocol*), kreiranje sistema osnovne zaštite integriteta sa heš algoritmom MD5, 9 i održavanje upravljanja promenama baze log podataka.

2.2 Faza razvoja

Cilj faze razvoja je da obezbedi mehanizam za detekciju i potvrdu incidenta. Zadaci koji se izvode u ovoj fazi dosta se razlikuju za zvaničnu i korporacijsku istragu.

Faza detekcije i izveštavanja detektuje incident i izveštava odgovorna lica o incidentu. Ovo se može obaviti putem poziva 92, preko alarma mrežnog detektora upada - IDS (*Intrussion Detection System*), ili *online* od agenta policije, koji istražuje ilegalne aktivnosti. Ova faza definiše početak procesa istrage.

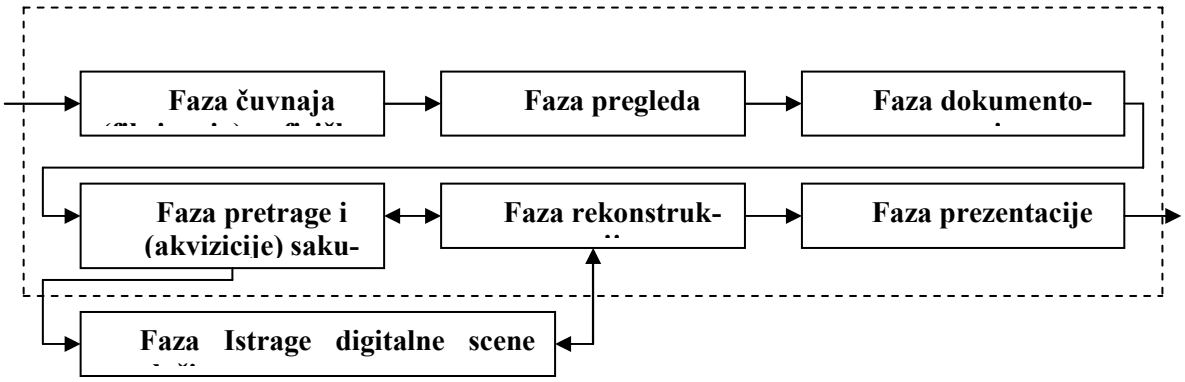
Faza potvrde i autorizacije nastavlja se u različitim smerovima, zavisno od situacije. Cilj ove faze je da se dobije ovlašćenje za potpunu istragu incidenta i scene

zločina. Za slučaj zvanične istrage, ovaj korak podrazumeva obezbeđivanje naloga za pretres ili drugo legalno odobrenje, koje je mora biti potkrepljeno sa dovoljno dokaza ili osnovanom sumnjom.

Za slučaj ***korporacijske istrage incidenta***, nalozi za pretres nisu potrebni dok god se ne krše prava privatnosti ili slučaj preraste kapaciteta i sposobnosti korporacijskog tima za istragu (npr. međunarodni incident, zahtev za prisluškivanje telefona osumnjičenog, hapšenje i dr.). U situaciji upada u server, ovaj korak uključuje interventni tim za odgovor na incidente koji proverava da li je sistem kompromitovan, tako što ispituju sumnjive aktivnosti na mreži ili traže maliciozne programe (*rootkit*-ove) u sistemu. U toku ove analize uživo, važno je da se prema sistemu ophodi kao prema sceni zločina, da se primenjuje kompletna *standardana operativna procedura* pristupa kompromitovanom računaru i da se minimizira uticaj na ispitivani sistem. Posle potvrde da se incident zaista dogodio, neophodan je pristanak vlasnika sistema da bi se preduzele naredne akcije: uključili zvanični organi istrage ili ne iz bilo kojeg razloga. Za servere čiji je vreme aktivnog rada kritično za kompaniju, odobrenje mora da se traži na nivou izvršne vlasti, [9].

2.3 Faza istrage fizičke scene zločina

Cilj ove faze je da prikupi, analizira fizičke dokaze i rekonstruiše akcije koje su dovele do incidenta. Jedan od najvažnijih ciljeva forenzičke digitalne istrage je da se identifikuju ljudi koji su odgovorni za incidente i zbog toga su potrebni fizički dokazi. Za zvanični model istrage, ekspert za fizičku scenu zločina izvršava većinu ovde navedenih zadataka. U korporacijskoj istrazi, ove zadatke će izvršiti interventni tim za odgovor na kompjuterski incident ili tim za fizičku bezbednost. Faze za istragu fizičke scene zločina prikazane su na slici 2.



Slika 2: Šest faza istrage fizičke scene zločina i interakcija sa istragom digitalne scene zločina

Faza čuvanja (fiksiranja) je ista za svaki tip zločina. Osnovne aktivnosti koje se preduzimaju su: *osiguranje izlaza, pomoć ranjenima, zadržavanje osumnjičenih i identifikovanje svedoka.* U digitalnom incidentu, fizička scena zločina trebalo bi da se osigura koristeći iste procedure kao i kod fizičkog incidenta (koji nije digitalni). U istrazi upada u server, ova faza uključuje identifikovanje, ko je bio u centru za obradu podataka i sprečavanje drugih da uđu u centar zbog toga što je možda neko od zaposlenih odgovoran za incident. Primetimo da ova faza čuva scenu zločina od izmena da bi se

kasnije mogli sakupiti i identifikovati dokazi. Ova faza ne čuva određene delove dokaznog materijala, već celokupnu scenu zločina.

Faza pregleda fizičke scene zločina odvija se tako što organ istrage prolazi i opservira scenu zločina i obično je prva osoba koja odgovara na incident. Cilj je da se identifikuju očigledni delovi dokaznog materijala, osetljivi delovi fizičkog dokaza i razvije početna teorija (hipoteza) o zločinu. Na primer, u istrazi ubistva, u ovoj fazi se ide kroz stan i identifikuje kako je napadač ušao, na kom mestu se ubistvo dogodilo i šta se dogodilo sa žrtvom posle ubistva. Osetljivi digitalni dokazi moraju se odmah dokumentovati i sakupiti da se ne bi oštetili. U digitalnom incidentu, primeri fizičkih dokaza koji su identifikovani u pretrazi uključuju broj i lokaciju kompjutera, mrežne konekcije kompjutera, PDAs, mobilni telefoni, lozinke na papiru, razne zabeleške i odštampani materijali i CD-romovi ili neki drugi prenosivi mediji. Pri završetku ove faze istražni organi imaju ideju kako da obradi fizičku scenu zločina i koje specijalne veštine su im potrebne za obradu. Ukoliko digitalni forenzičar - specijalista za kompjuter nije na uviđaju u tom trenutku, treba ga pozvati da dođe i izvrši forenzičku akviziciju dokaza (uzme dokaze). Kompjuter koji je uključen tj. koji radi i koji je priključen na mrežu smatra se osetljivim dokazom, jer se digitalni dokazi koji se nalaze u njemu mogu izbrisati daljinski, komandom sa udaljenog računarskog sistema. Zbog toga se obavezno koriste neke standardne procedure kao što je isključivanje kompjutera sa mreže (zavisno od vrste platforme: Windows, Linux/ Unix,...) dok ne počne potpuna forenzička istraga.

Faza dokumentovanja fizičke scene zločina izvodi se tako što se prave fotografije, skice i video snimci scene zločina i fizičkih dokaza. Cilj je da se prikupi što više informacija tako da se razmeštaj i važni detalji scene zločina sačuvaju i zabeleže. Kod digitalnog incidenta važno je da se dokumentuju i fotografišu konekcije na računaru i stanje računara. Takođe bi moglo biti značajno da se dokumentuje broj i veličina hard diskova i količina memorije. U nekim slučajevima, treba sačuvati MAC adresa hardvera mrežnih kartica da bi se DHCP logovi mogli koristiti za identifikovanje sistemske aktivnosti. Korisno je sačuvati serijske brojeve i "jednoznačne oznake objekata sistema" u ovoj fazi. Da bi se identifikovalo šta treba sačuvati, treba uzeti u obzir da forenzičke labaratorije za analizu ne mogu dobiti originalni fizički hardver, već samo fizičku (*miror*) kopiju hard diska. Bilo šta što bi moglo biti od koristi za forenzičku laboratoriju za analizu, ili kasniju rekonstrukciju trebalo bi da se zabeleži. Na kraju *Faze Dokumentacije* izrađuje se konačni izveštaj o incidentu.

Faza pretrage i prikupljanja (akvizicije) dokaza iz fizičke scene zločina obuhvata pretragu i detaljno prikupljanje dodatnih fizičkih dokaza iz dubine scene. Pretraga može biti usmerena prema nestalim delovima fizičkih dokaza, kao što su oružje, ili može biti metodična i imati striktne obrasce pretrage. Svaki tip dokaza treba da ima specifične standardne procedure, za prikupljanje (akviziciju). Za digitalni incident u ovoj fazi traže se dodatni mediji i digitalni uređaji sa mesta zločina. Ova faza takođe uključuje kontaktiranje administratora radi očuvanja i obezbeđivanje logova za pristup (*access logs*) centru podataka, promenljivih logova za "*update*" servera, logove *firewall*-ova, logova IDS, i logove udaljenog pristupa (*remote access logs*). Ovo je poslednja faza koja se vrši na realnoj sceni zločina. Fizički dokazi koji su prikupljeni sa scene zločina, šalju se u forenzičku laboratoriju radi analize, a rezultati se koriste u sledećoj fazi, rekonstrukcije incidenta.

Faza pretrage i prikupljanja dokaza iz fizičke scene zločina je faza u kojoj počinje digitalna forenzička istraga scene zločina. Kompjuterski sistem se smatra za fizički dokaz pa će se i on uzeti kao dokazni materijal gde god je moguće. Procedura prikupljanja dokumentuje kako se prikupljaju važni podaci sa sistema koji je aktivan i kako se sistem isključuje.

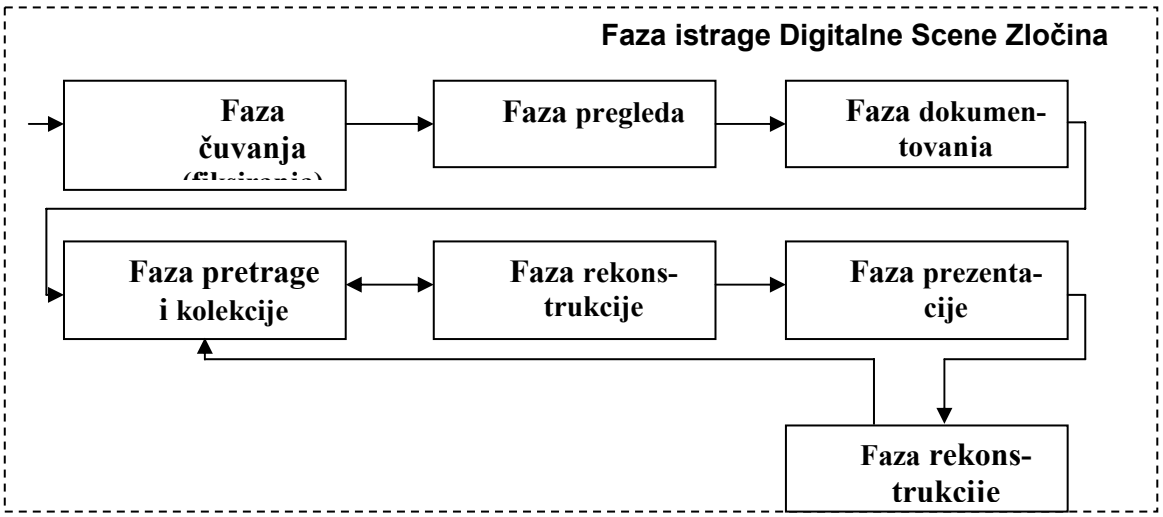
Faza rekonstrukcije fizičke scene zločina uključuje organizovanje rezultata analize prikupljenih fizičkih i digitalnih dokaza i korišćenje fotografija sa scene zločina da bi se razvila teorija (hipoteza) o incidentu. Za rad sa dokazima mora se koristiti naučni metod, da bi se mogle testirati teorije o incidentu. Kod digitalnog incidenta, rezultati istrage digitalne scene zločina su u vezi sa fizičkim dokazima, da bi se povezala osoba

sa digitalnim događajima. Primeri u ovoj fazi su povezivanje logova sa servera u centru za obradu podataka sa *login*-ovima u radnoj stanici (napadnutom računaru) i drugim mrežnim uređajima, povezivanje *chat* aktivnosti otkrivenih u sistemu sa aktivnošću detektiva i povezivanje aktivnosti na kompromitovanom serveru sa aktivnošću na kućnom računarskom sistemu osumnjičenog i mrežnom aktivnošću sačuvanoj na serveru ISP-a. Da bi imala najveći efekat, ova faza treba da uključi eksperte za digitalnu forenziku, radi pomoći oko povezivanja i konsultovanja događaja sa više izvora digitalnih dokaza. Treba zapaziti da rekonstrukcija fizičke scene zločina nije isto što i "ponovno kreiranje", koje podrazumeva izradu fizičkog modela scene zločina.

Faza prezentacije (veštačenja) fizičke scene zločina prezentuje fizičke i digitalne dokaze sudu ili upravi korporacije. Ova faza prezentuje dokaze i teoriju koja je razvijena u fazi rekonstrukcije fizičke scene zločina.

2.4 Faza istrage digitalne scene zločina

Faza istraga digitalne scene zločina počinje kada su fizički digitalni uređaji prikupljeni kao i fizički dokazi sa fizičke scene zločina, ili kada je sačuvani mrežni saobraćaj analiziran radi obezbeđivanja dokaza. Ova faza prilazi kompjuterskom sistemu kao sceni zločina i pretražuje ga radi izvlačenja dokaza. Cilj je da se identifikuju elektronski događaji koji su se dogodili na sistemu i prezentuju istražnom organu fizičke scene zločina. Specijalista za rad sa forenzičkim alatima i tehnikama za analizu vrši forenzičku digitalnu analizu u sledećim fazama, (Sl. 3).



Sl. 3. Faze forenzičke istrage digitalne scene zločina, čiji se rezultati vraćaju u fazu istragu fizičke scene zločina

U ovom modelu, svaki digitalni uređaj smatra se posebnom (odvojenom) fizičkom scenom zločina. Konačni rezultati analize svakog digitalnog uređaja šalju se u *Fazu rekonstrukcije fizičke scene zločina,* u kojoj će biti identifikovane veze između digitalnih uređaja. Ovo omogućava da se analize različitih tipova uređaja izvrše na različitim mestima. Fizičke scene zločina organizovane su u primarne i sekundarne scene, gde su primarne one gde se prvi kriminalni akt dogodio, 9. Digitalne scene zločina mogu takođe da se organizuje u primarne i sekundarne scene zločina. Na primer, server koji je kompromitovan bio bi primarna scena zločina, a log server koji je bio kompromitovan kasnije zbog izmene log-ova koji su u vezi sa upadom, bio bi sekundarna digitalna scena zločina.

Faza čuvanja digitalne scene zločina sastoji se iz obezbeđivanja ulaza i izlaza ka daigitalnoj sceni zločina i očuvanja digitalnih dokaza koji bi se lako mogli promeniti. U fizičkom svetu, ovome odgovara smanjenje broja otiska stopala i sakupljanje fizičkih dokaza koji bi mogli da se vremenom izgube. U digitalnom svetu ovo bi značilo izolaciju sistema od mreže, sakupljanje nestabilnih (lako promenljivih) podataka koji bi mogli biti izgubljeni kada se sistem isključi i identifikovanje bilo kakvih sumnjivih procesa, koji su aktivni u sistemu. Sumnjive korisnike, koji su ulogovani (registrovani) na sistem, treba registrovati i po mogućnosti ispitati. Log datoteke mogu se smatrati za očevidce *digitalnog zločina* i moraju biti obezbeđene ukoliko postoji pretnja da će biti izbrisane, pre nego što se sistem fizički iskopira. Treba zapaziti da drugi modeli koriste termin "čuvanje" u smislu očuvanje samih digitalnih dokaza u celokupnom lancu od istrage do sudskog procesa. U ovom modelu "čuva se" celokupno digitalno okruženje. U stvari, nijedan digitalni dokaz nije još identifikovan, kada se ova faza izvršava. Jedna od prednosti digitalnog sveta u odnosu na fizički svet je u tome da se digitalno okruženje može lako kopirati. Zato, je uobičajeno u ovoj fazi da se napravi kompletna fizička (*miror*) slika sistema na forenzičkom računaru, da bi se mogao kasnije analizirati u forenzičkoj laboratoriji. Kompletne fizičke kopije diskova očuvaju celokupnu digitalnu scenu zločina, dok kopije koje su samo obični *backup*-ovi sistema čuvaju samo dodeljene podatke u digitalnoj sceni zločina. Kritični sistemi mogu da se povrate posle kreiranja forenzičke fizičke slike tako da se može brzo priključiti na mrežu. Neki slučajevi zahtevaju da originalni hard disk ostane fizički dokaz sve dok je slučaj u toku. Kada monitori mrežnog saobraćaja snime mrežni tok saobraćaja, tada oni imaju efekat čuvanja bezbednog (neizmenjenog) stanja mreže.

Faza pregleda digitalne scene zločina odigrava se u forenzičkoj laboratoriji koristeći jednu od forenzičkih replika scene zločina. Ova faza može da se izvrši na živom sistemu (kompromitovanom sistemu uživo), kao i u fizičkom svetu, ali je poželjno laboratorijsko okruženje, zato što pruža kontrolisane uslove, a rezultati se mogu ponoviti sa drugom replikom sistema, ako to zahtevaju sudski organi. Ukoliko se *Faza pregleda* izvodi na živom sistemu, forenzičku sliku sistema ipak treba napraviti tako da se bilo koji digitalni dokaz može prikupiti i u kontrolisanom laboratorijskom okruženju verifikovati. Ova faza se ponekad radi na terenu da bi se utvrdilo da li sistem treba donositi u laboratoriju na punu forenzičku analizu. Pretrage na terenu obično se izvode na sistemu *boot*-ovanom sa butabilnog CD/ diskete u sigurnom okruženju tako da digitalni dokazi ostanu nepromenjeni.

U *Fazi pregleda* pronalaze se očigledni delovi digitalnih dokaza za datu vrstu zločina. Na primer, u slučaju dečije pornografije istražni organ će prikupiti sve grafičke slike sa sistema i identifikuje one koje bi mogli da se koriste kao dokazi. U upadu na server, istražitelj traži očigledne znakove instalacije *rootkit*-a, analizira logove aplikacija i traži nove konfiguracione datoteke. U drugim slučajevima, mogu se analizirati keš i istoriju na HTML *browser*-u. Kada se analizira mrežni saobraćaj o nekom incidentu, ova faza može analizirati saobraćaj u vremenskom okviru incidenta i filtrirati određene portove i hostove. *Faza pregleda* pokazuje veštinu osumnjičenog i analizira tehnike koje će biti potrebne u istrazi. Istražni organ u ovoj tački može konsultovati eksperte u oblasti kriptologije, digitalne forenzičke analize, ili eksperte za oporavak podataka (povratak podataka ukoliko su neki nestali, ili bili izbrisani).

Faza dokumentovanja digitalne scene zločina sastoji se iz pravilno dokumentovanih digitalnih dokaza koji su akvizicijom otkriveni. Tačne (fizičke) kopije sistema koje su potrebne u toku *Faze očuvanja* imaju istu ulogu kao i skice i video zapisi fizičke scene zločina. Svaki deo digitalnog dokaza koji se pronađe u toku forenzičke analize *miror* slike sistema mora biti jasno dokumentovan. Ova faza dokumentuje pojedinačne delove dokaza i ne kreira finalni izveštaj o incidentu. Finalni izveštaj forenzičke digitalne analize pravi se u *Fazi prezentacije.*

Digitalni dokazi mogu postojati u različitim apstraktnim slojevima računarskog sistema i moraju se dokumentovati pomoću specifičnih forenzičkih alata za te slojeve, 9, 9. Na primer, datoteka može biti dokumentovana koristeći puno ime njene putanje,

cluster-e i sektore na disku koje sistem datoteka koristi. Mrežni podaci mogu biti dokumentovani sa izvornom i ciljnom adresom na raznim mrežnim nivoima. Kako su digitalni dokazi promenljivi i mogu ostaviti malo tragova, dodatni koraci bi trebali da se preduzmu da bi se kasnije proverio integritet. Kriptografsku heš vrednost, kao što je MD5 ili SHA-1, 9, treba primeniti na delove digitalnih dokaza u fazi skupljanja, da bi se mogao dokazati integritet dokaza na sudu. Lanac neprekidnog čuvanja i nadzora dokaza treba formirati u ovoj fazi, da bi se dokazi mogli koristiti na sudu. U praksi, *Faza dokumentovanja* nije posebna faza u digitalnoj istrazi, zato što se digitalni dokazi dokumentuju u trenutku otkrivanja (akvizicije).

Faza pretrage i sakupljanja (akvizicije) dokaza sa digitalne scene zločina sastoji se od potpune digitalne forenzičke analize sistema radi izvlačenja digitalnih dokaza. Ova faza koristi rezultate iz *Faze pretrage* da bi se usredsredila na dodatne tipove analiza. Na primer, u ovoj fazi može se izvršiti pretraga po ključnoj reči ukoliko su ključne reči identifikovane iz drugih dokaza. Nedodeljeni prostori sistema datoteka mogu se izvući i obraditi izbrisane datoteke. Mogu se pratiti i analizirati korisničke aktivnosti nad datotekama, na najnižem nivou vremenske linije aktivnosti. Svi mrežni paketi koji su sakupljeni softverom za monitoring mrežnog saobraćaja mogu se analizirati. U nekim slučajevima, prikladno jee pregledati sadržaj svakog klastera (fizička pretraga) ili svake datoteke (logička pretraga). Kao što postoje različite tehnike pretrage u fizičkoj sceni zločina, tako postoje i različite tehnike forenzičke analize digitalne scene zločina.

Najveći deo vremena digitalne forenzičke istrage potroši se u ovoj fazi. U digitalnom svetu, dokazi su kopirani iz scene zločina, ali nisu uklonjeni sa nje. Za neke tipove kompjuterskih incidenata, uobičajeno je da rade i tehnički i netehnički istražni organi u ovoj fazi, zbog ograničenog broja obučenih organa za digitalnu forenzičku istragu. Na primer, tehnički istražni organi će izvući sve slike iz sistema i poslati ih netehničkim istražnim organima koji će analizirati svaku sliku i identifikovati one koje bi se mogle koristiti kao dokaz. *Faza pregleda* i *pretrage* slične su *Fazi ispitivanja* u drugim modelima.

Faza rekonstrukcije digitalne scene zločina sastoji se iz sastavljanja neoborivog, čvrstog digitalnog dokaza bez pukotina od delova digitalne zagonetke. Digitalni dokazi se mogu razvrstati i proceniti da bi se odredilo koliko su poverljivi i pouzdani, 9. Podaci koji zahtevaju složene tehnike analize, kao što su izvršne analize ili dešifrovanje, izvode se u ovoj fazi i koriste se njihovi rezultati. Ova faza koristi stroge naučne metode da bi se dokazi mogli testirati i da bi se odbacile teorije koje se potencijalno mogu zasnovati na digitalnom dokazu. Ova faza ustanovljava kako je digitalni dokaz dospeo tamo i šta njegovo postojanje (prisustvo) znači. Kada digitalni dokaz i dalje nedostaje, *Faza pretrage* će nastaviti da identifikuje dodatne dokaze. Na primer, u slučaju upada u server, ova faza će dovesti u vezu eksplotaciju ranjivih servisa sa instalacijom *rootkit*-a i razvojem mrežnog *sniffer*-a. Izvorišna IP adresa mrežne konekcije može dovesti do potrebe analize dodatne digitalne scene zločina. Ova faza je slična *Fazi analize* u drugim modelima.

Faza prezentacije digitalne scene zločina obuhvata prezentovanje otkrivenih digitalnih dokaza timu za istragu fizičke scene. Rezultate iz digitalne istrage tim za istragu fizičke scene zločina koristi u *Fazi rekonstrukcije.* Istražni organ fizičke scene zločina integriše rezultate iz istrage svake digitalne scene zločina. U ovoj fazi dokumentuju se i prezentuju otkrića određene scene zločina drugim organima istrage. Korisno je ako je fizički i digitalni tim za istragu jedinstven, jer se informacije lakše razmenjuju između članova istog tima.

2.5 Faza provere (kontrole)

Finalna faza je **Faza provere** i sastoji se od revizije i kontrole integralnog procesa istrage, da bi se identifikovale oblasti koje se mogu poboljšati. Za digitalni kompjuterski incident, ovo uključuje analizu kvaliteta rada i koliko dobro su izvršene fizička i

digitalna istraga svaka za sebe, koliko dobro su urađene fizička i digitalna istraga zajedno i da li postoji dovoljno fizičkih i digitalnih dokaza da bi se slučaj rešio. Rezultat ove faze mogu biti nove poboljšane procedure, nova obuka, ili ništa ukoliko je sve ispalo kako je planirano.

3. ZAKLJUČAK

Ovaj model daje precizan pogled na proces digitalne forenzičke istrage i razlike između prikupljanja digitalnih dokaza i digitalne forenzičke analize. Fizička forenzička istraga odgovara na komparativna pitanja tipa: “Da li su X i Y slični”, ili identifikaciona pitanja tipa: “Da li možeš identifikovati X”, 9. Postupci koji su potpali pod kategoriju digitalne forenzičke istrage (analize) širi su i uključuju rekonstrukciju događaja (incidenta). Zbog toga je izraz ***digitalna forenzička analiza*** mnogo precizniji, iz perspektive eksperata koji analiziraju sistem. Iz perspektive istražnog organa fizičke scene zločina, koji šalje kompjuter u labaratoriju radi analize, ovaj proces se, takođe, smatra digitalnom forenzičkom analizom.

Model prikazuje i obim napora koje treba žučiniti da bi se ispravno istražio digitalni incident. U većini država gde postoje, zvanični organi istrage imaju samo jedno lice koje analizira svaki deo kompjutera. Ovo je analogno slanju jednog zvaničnog organa istrage na fizičku scenu zločina, očekujući da će otkriti sve vrste dokaza i odrediti tip slučaja. Da bi se kvalitetno istražio digitalni incident potrebno je angažovati multidisciplinarni tim sa specifičnim znanjima i veštinama i adekvatnim forenzičkim alatima.

Sa aspekta faza modela, savremene tehnologije obezbeđuju forenzičke alate za akviziciju i analizu digitalnih dokaza, dozvoljavajući korisniku da potpuno *vidi* digitalnu scenu zločina i prikupi digitalne dokaze sa svih apstraktnih slojeva te scene, 1, 2, 2, [5], 19, 10, 18, 19. Forenzički alati se koriste u *Fazama digitalnog pregleda i pretrage* za prikupljanje dokaza. Analize veza i alati za konsolidaciju vremenskih linija događaja pomažu istražnom organu u *Fazi digitalne rekonstrukcije*. Zato, sa ovim modelom mnogi postojeći alati za digitalnu forenzičku analizu mogu se nazvati alati za forenzičku akviziciju (prikupljanje) digitalnih dokaza. Alati za prikupljanje digitalnih dokaza prevode digitalne podatke na neki nivo apstrakcije koji pomaže istražnom organu da ih vidi, razume i objasni, 19. Forenzički alati najčešće koriste inženjerske tehnike, a ne stroge naučne metode, da bi predstavili digitalne podatke istražnom organu.

Vode se brojne debate da li su pouzdani dokazi sakupljeni sa kompromitovanog kompjutera uživo. Koristeći ovaj model, za prikupljanje dokaza sa kompromitovanog kompjutera uživo, proces se ništa ne razlikuje od skupljanja fizičkih dokaza. Fizička scena zločina se modifikuje kada istražni organ šeta okolo, kao što se digitalna scena zločina modifikuje, kada forenzički istražni organ pokrene softver za prikupljanje digitalnih dokaza. Zadatak IKT eksperata je da se smanje izmene originalne digitalne scene, razume efekat izmena digitalnih podataka i smanji poverenje u operativni sistem u slučaju prikupljanja digitalnih podataka sa sistema uživo.

Ovaj model jasno pokazuje interakciju između fizičkog i digitalnog domena. Mnoge procedure fokusiraju se uglavnom na digitalne dokaze, a uključuju samo osnovne fizičke dokaze, kao što su slike spoljašnje strane sistema. Model se sastoji od jednakog broja faza fizičke scene zločina i digitalne scene zločina. Motiv i mogućnost za ovo leži u tome što je krajnji cilj bilo koje digitalne istrage da se povežu digitalne aktivnosti sa čovekom (napadačem, fizičkim bićem). Zato će fizički dokazi biti potrebni i treba da se uzmu u obzir u toku istrage svakog kompjuterskog incidenta. Digitalna scena zločina može da se smatra *sekundarnom scenom zločina primerne fizičke scene zločina.*

Fizička scena zločina vrlo je jasna i razumljiva za zvanične organe istrage. Uobičajeno, istraga fizičke scene zločina manje je razumljiva za korporacijske istražne organe koji vode forenzičku istragu digitalne scene. Na primer, mnogi interventni timovi

za odgovor na incident nemaju zvanične procedure za analizu fizičkog prostora oko kompromitovanog servera. U praksi, neki nezadovoljni sistem administrator koji ima fizički pristup sistemu, mogao bi sam da izazove incident. Moguće je da preostali fizički dokazi budu izgubljeni, ukoliko ih interventni tim nije otkrio.

Ovaj model pokazuje da se poteškoće sa kojima se digitalni istražni organi susreću slične onima sa kojima se susreću organi istrage fizičke scene. Na primer, *Faze pregleda i pretrage* u oba slučaja moraju da identifikuju korisne delove dokaza. Istražni organ fizičkog kriminala ne može da pošalje svaki fizički objekat u laboratoriju na analizu. Mora da koristi svoje iskustvo da identifikuje šta je uobičajeno (normalno), a šta ne. Slično tome, organ za forenzičku istragu digitalne scene ne može da pošalje svaku datoteku sa sistema na pregled i ispitivanje. Oba organa istrage susreću se sa poteškoćom pronalaženja sitnih delova dokaza, kao što su dlaka na tepihu, ili izbrisanu datoteku u OS sa 100 GB memorije hard diska.

Razdvajanjem procesa analize u *Fazu pregleda* i *Fazu pretrage*, lakše se dokumentuje, shvata i uči proces. Uobičajeni problem za neiskusnog organa za forenzičku istragu digitalnih dokaza je to što ne zna kako da počne *Fazu ispitivanja* koju drugi modeli opisuju. Model istrage fizičke scene, razdvajanjem *Faze ispitivanja* u dve faze čini proces više intuitivnim. Obično istraga digitalne scene započinje pronalaženjem i eliminisanjem dokaza koji dovode do brzih rezultata, isključivanjem očigledno nemogućih i nelogičnih dokaza, a onda se na njima dalje širi, 2.

5. LITERATURA

1. *Access Data: Forensic Toolkit*, http://www.accessdata.com./.
2. *Analyst's Notebook*, http://www.i2.co.uk./ .
3. *ASR Data Acquisition and Analysis: SMART*, http://www.asrdata.com./.
4. Carrier B., *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers*. International Journal of Digital Evidence, Winter 2003.
5. Carrier B., Spafford H. E., *Getting Physical with the Digital Investigation Process,* International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2, CERIAS, Purdue University.
6. *Electronic Crime Scene Investigation: A Guide for First Responders*, http://www.ncjrs.org, July 2001.
7. Casey E., *Digital Evidence and Computer Crime*. Academic Press, 2000..
8. Casey E., *Error, Uncertainty, and Loss in Digital Evidence*, International Journal of Digital Evidence, Summer 2002.
9. Grubor G., *Osnove Kompjuterskog kriminala (Tema 16)*, Univerziitet Singidunum, Fakultet za poslovnu informatiku, 2006, Beograd.
10. *Guidance Software: EnCase Forensic Edition*, http://www.encase.com./.
11. James S., and Nordby J., editors. Forensic Science: *An Introduction to Scientific and Investigative Techniques*, CRC Press, 2003.
12. Lee H., and all, *Henry Lee's Crime Scene Handbook*. Academic Press, 2001.
13. Pettinari D., Cmdr., *Handling Digital Evidence from Seizure to Court Presentation*, IOCE conference, juni 2000.
14. Rivest R., *The MD5 Message-Digest Algorithm*, Network Working Group RFC 1321, April 1992. 15.
15. Saferstein R., *Criminalistics: An Introduction to Forensic Science*. Pearson, 7. editi-on, 2000.
16. *Secure Hash Standard*, National Institute of Standards and Technology, FIPS PUB 180, May 1993.
17. Tan J., *Forensic Readiness*, Technical report, @stake, 2001.
18. Technology Pathways*, Pro Discover DFT*, http://wwww.techpathways.com./.
19. *The Sleuth Kit*, http://www.sleuthkit.org./, 2006.