

UNIVERZITET SINGIDUNUM

BEOGRAD

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I MEĐUNARODNU SARADNJU

DOKTORSKA DISERTACIJA

**MODELOVANJE, ANALIZA I DIZAJN 3D EDUKACIONOG OKRUŽENJA ZA
DIGITALNU FORENZIKU**

MENTOR

Prof. dr Ranko Popović

KANDIDAT

mr Igor Franc

BEOGRAD, 2013. godina

Sadržaj

1	Uvod	7
1.1	Uvodna razmatranja	8
1.2	Predmet i cilj istraživanja	8
1.3	Motivacija za izradu rada	9
1.4	Definisanje problema i predlog rešenja	9
1.5	Rezultati i doprinos	11
2	Prethodna istraživanja	13
2.1	Istorijski pregled i radovi za digitalnu forenziku	14
2.2	Istorijski pregled i radovi za virtuelna okruženja, vizualizaciju i virtuelizaciju	16
2.3	Istorijski pregled i radovi za virtuelna okruženja	17
2.3.1	Početak	17
2.3.2	Prva virtuelna okruženja	18
2.3.3	“Naseljena” virtuelna okruženja (IVW)	20
2.3.4	Kriza i preporod virtuelnih okruženja	20
3	Digitalna forenzika	22
3.1	Definicije	22
3.1.1	Zvanična istraga kompjuterskog kriminala	23
3.1.2	Korporacijska digitalna forenzička istraga	24
3.1.3	Digitalni dokaz	24
3.1.4	Modeli digitalne forenzičke istrage	25
3.1.5	Anti-forenzika	28
3.2	Akvizicija digitalnih podataka	29
3.2.1	Lokardov princip razmene	30
3.2.2	Redosled sakupljanja nestabilnih podataka	30
3.3	Forenzička analiza digitalnih podataka	31
3.4	Forenzički alati	32
3.4.1	Hardverski forenzički alati	33
3.4.2	Softverski forenzički alati	35
3.5	Izveštavanje – svedočenje	38
3.5.1	Edukovanje pravosudnih organa	39
3.6	Izbor postojećih alata	40
4	Virtuelna okruženja	41
4.1	Definicije	41
4.1.1	Fizikalnost	42
4.1.2	Konstantnost	42
4.1.3	Interaktivnost	42
4.1.4	Predstavljanje	42
4.2	Tipovi virtuelnih okruženja	43
4.2.1	“Full-Immersive” Virtual Environment	43
4.2.2	“Semi-Immersive” Virtual Environment	45
4.2.3	“Desktop-Immersive” Virtual Environment	45
4.2.4	“Tele-Immersive” Virtual Environment	45
4.3	Svrha virtuelnih okruženja	46

4.3.1	Virtuelna okruženja u obrazovanju	47
4.3.2	Učenje u virtuelnom okruženju	48
4.3.3	UTBot–3D kao pedagoško sredstvo	48
4.4	Primena Second Life-a u edukaciji, zabavi, nauci	49
4.5	Primena Open Wonderland-a u edukaciji, industriji, zabavi	53
4.5.1	Virtuelno okruženje za eksperimente iz fizike	54
4.5.2	QuizMAster	55
4.5.3	Virtuelno okruženje „Folkways in Wonderland “	55
4.5.4	Sheet suite	56
4.5.5	MiRTLE	57
4.5.6	SIMILLE	58
4.5.7	WonderSchool	58
4.5.8	Games Village	58
5	3D okruženja u edukaciji	60
5.1	Uvod u virtuelna 3D okruženja	60
5.2	E-učenje i 3D okruženja	61
5.3	Postojeća 3D virtuelna okruženja	62
5.3.1	Prikaz postojećih 3D virtuelnih okruženja	63
5.3.2	Detaljan prikaz postojećih 3D virtuelnih okruženja koja se koriste za edukaciju	65
5.4	Poređenje postojećih i izbor okruženja	71
5.4.1	Poređenje postojećih 3D virtuelnih okruženja	71
5.4.2	Izbor 3D virtuelnog okruženja	74
6	Modelovanje i analiza	75
6.1	Komponentno kompozitni model digitalne forenzičke (DF) laboratorije	75
6.2	Realizovano 3D okruženje	76
6.2.1	Elementi okruženja	76
6.2.2	Okruženje za akviziciju i analizu digitalnih podataka	85
6.2.3	Okruženje za simulacije izveštavanja – svedočenja	86
6.3	Semantički Web	87
6.4	Ontologija	89
6.5	Hardverska platforma	89
7	Realizacija	92
7.1	Dizajn 3D okruženja	94
7.2	Opis softverskog sistema	94
7.3	Ontologija realizovanog 3D okruženja	95
7.4	Karakteristike realizovanog rešenja	97
7.5	Forenzička laboratorija	97
7.5.1	Biblioteka forenzičkih slučajeva FCL – Forensic Case Library	97
7.5.2	Biblioteka forenzičkih scenarija FSL – Forensic Scenario Library	99
8	DF silabusi i kurikulumi	101
8.1	DF silabus	101
8.1.1	DF silabus za osnovne studije	101
8.1.2	DF silabus za master studije	104
8.1.3	DF silabus za doktorske studije (Phd)	105

8.2	Dinamički kurikulumi	106
9	Procena znanja i analiza postignutih rezultata i doprinosa.....	108
10	Zaključak i smernice za budući rad	115
11	Literatura	116

SPISAK SLIKA

- Slika 2.1 Maze War prikaz pokrenut u ranim 1970-tim na Imlac PDS-1
- Slika 2.2 Sala za konferenciju (levo) i podijum za govornike (desno)
- Slika 3.1 Trajnost podataka u sistemu
- Slika 3.2 Hardverski blokatori
- Slika 3.3 FRED računar
- Slika 3.4 FREDDIE računar – portabl
- Slika 3.5 FRED-L računar – laptop
- Slika 3.6 SIFT workstation
- Slika 3.7 DEFT Linux
- Slika 4.1 Izgled HMD-a
- Slika 4.2 Finalni meč na turniru na kraju kursa
- Slika 4.3 Amfiteatar za virtuelno predavanje
- Slika 4.4 Primer učionice sa postavljenim lekcijama
- Slika 4.5 Virtuelna konferencija
- Slika 4.6 Vežbe u virtuelnoj ambulanti
- Slika 4.7 Šematski prikaz QuizHAD-a
- Slika 4.8 Prikaz Second Life učionice univerziteta Pacifik
- Slika 4.9 Prikaz elektromagnetnog polja
- Slika 4.10 Grupa igrača i proglašenje pobednika u QuizMAster-u
- Slika 4.11 Prikaz mape na kojoj su locirane muzičke numere (slika levo); Mapa sa avatarima koji se trenutno nalaze u Zapadnoj Africi (slika desno).
- Slika 4.12 Virtuelno okruženje „Sheet suite“
- Slika 4.13 Virtuelna učionica u ranoj fazi projekta MiRTLE
- Slika 4.14 Wonder School
- Slika 4.15 Games Village
- Slika 5.1 Second Life virtuelno okruženje
- Slika 6.1 Osnovne komponente i kompozicije u digitalnoj forenzici
- Slika 6.2 Primer korišćenja PDF viewera
- Slika 6.3 PDF viewer kontrole
- Slika 6.4 Video plejer u Wonderlandu
- Slika 6.5 Movie player kontrole
- Slika 6.6 Crtanje po tabli
- Slika 6.7 Izolovano mesto u podrazumevanom okruženju Wonderlanda
- Slika 6.8 Konektovani VNC Viewer na server
- Slika 6.9 Izbor načina prikaza PDF fajla
- Slika 6.10 Otvoreni PDF fajl u PDF Sprederu
- Slika 6.11 Microphone u Open Wonderlandu
- Slika 6.12 Unos HTML koda u Poster modul
- Slika 6.13 Prikaz Poster modula u Open Wonderlandu

Slika 6.14 Izbor dela ekrana za deljenje
 Slika 6.15 Screen Share u Open Wonderlandu
 Slika 6.16 Kolaborativni text editor u Open Wonderlandu
 Slika 6.17 Webcam viewer u Open Wonderlandu
 Slika 6.18 Chat koji omogućava tekstualnu komunikaciju kroz čitavo 3D okruženje
 Slika 6.19 Softphone sa globalnom konekcijom na liniji 1
 Slika 6.20 Prikaz okruženja za akviziciju i analizu u Open Wonderlandu
 Slika 6.21 Prikaz okruženja za simulaciju svedočenja u Open Wonderlandu
 Slika 6.22 IBM System x3650 M3
 Slika 7.1 Arhitektura DF-lab i komponente
 Slika 7.2 DF-lab model
 Slika 7.3 Arhitektura DF modela
 Slika 7.4 Ontologija za digitalnu forenziku
 Slika 7.5 Ontologija visokoškolske institucije (Univerziteta)
 Slika 8.1 Softverski sistem virtuelni univerzitet
 Slika 9.1 Izgled virtuelne učionice
 Slika 9.2 Model otvorenog računara u virtuelnoj učionici
 Slika 9.3 Model na kome se vidi forenzički laptop i write blocker
 Slika 9.4 Model računara koji je pokrenut
 Slika 9.5 Model forenzičke radne stranice u virtuelnom okruženju

SPISAK TABELA

Tabela 3.1 Uporedni pregled osnovnih funkcija relevantnih forenzičkih alata
 Tabela 4.1 Stepen vidljivosti u različitim vrstama okruženja
 Tabela 5.1 Pregled dostupnih virtuelnih okruženja
 Tabela 5.2 Minimalna hardverska konfiguracija za Open Wonderland
 Tabela 5.3 Minimalna hardverska konfiguracija za Second Life
 Tabela 5.4 Minimalna hardverska konfiguracija za Activeworlds
 Tabela 5.5 Poređenje virtuelnih okruženja
 Tabela 5.6 Mogućnosti virtuelnih okruženja
 Tabela 5.7 Poređenje virtuelnih okruženja za korišćenje u edukaciji
 Tabela 5.8 Prednosti i mane virtuelnih okruženja
 Tabela 7.1 Specifičnosti različitih forenzičkih slučajeva
 Tabela 8.1 DFCB kategorije
 Tabela 8.2 Beebe i Clark kategorije
 Tabela 9.1 Statistička analiza rezultata

1 Uvod

U poslednjih nekoliko godina došlo je do većih promena u metodama učenja i digitalnoj forenzici (DF). Primećeno je da nove generacije studenata koje odrastaju uz računare i društvene mreže ocenjuju tradicionalne metode učenja kao “dosadne” jer ne ispunjavaju njihove zahteve. Nove generacije, upotrebu tehnologija vide kao sastavni deo svakodnevnih aktivnosti, samim tim i neophodno sredstvo za uspešno učenje. Za te „digitalne generacije“ studenata neophodan je razvoj interaktivnog okruženja za edukaciju. Studentima se pruža mogućnost da uče koristeći različita znanja i veštine u virtuelnom okruženju. Još jedna karakteristika „digitalne generacije“ studenata je da se sa što manje uloženog vremena i truda postigne što bolji rezultat. Da bi se to ostvarilo predavači treba da unaprede komunikaciju i odnose sa studentima. Istraživanja pokazuju da se studenti lakše zainteresuju za izazovne simulacije ukoliko ih predavači prikažu na jednostavan i zanimljiv način.

Problemi tradicionalnog učenja su predavač u centru pažnje i nedovoljna integracija savremenih tehnologija u okruženje za učenje. Ovakav vid učenja zasnovan je na potpunoj kontroli procesa učenja i prenošenju znanja putem lekcija. Savremene metode učenja zasnovane su na definisanju i rešavanju teorijskih i praktičnih problema i zahtevaju razvoj novih interaktivnih, integriranih virtuelnih i realnih okruženja.

Digitalna forenzika (DF) je počela naglo da se razvija krajem prošlog veka uz nepostojanje standarda i nedostatak adekvatnog kadra. Većina univerziteta je počela intenzivno da uvodi ovu naučnu oblast u planove i programe.

Postoji veliki broj radova koji se bave istraživanjima u ovoj naučnoj oblasti. Ovaj rad je pokušaj da se prikaže trenutno stanje u digitalnoj forenzici, sistematizuju znanja iz ove oblasti, definišu problemi, ponudi savremeno rešenje za model 3D edukacionog okruženja i njegove primene u praksi.

1.1 Uvodna razmatranja

Da bi se edukovali digitalni forenzičari neophodno je da postoji dobra teorijska podloga. Ono što je još važnije, neophodno je razviti različite vrste laboratorijskih vežbi gde bi se budući digitalni forenzičari kroz realne slučajeve iz prakse obučavali i sticali potrebna znanja i veštine.

Razvoj digitalnih forenzičkih alata i njihova primena u obrazovanju “digitalne generacije” studenata bio je osnovni motiv za izradu ovog rada. Definisan je generički model virtuelnog okruženja za obuku digitalnih forenzičara od osnovnih studija, preko master pa sve do sticanja zvanja doktora nauka. Definisani su silabusi i kurikulumi za osnovne i posleddiplomske studije u oblasti DF-a. Takođe, kreiran je veliki broj slučajeva iz prakse i scenarija koji su povezani kompozitno komponentnim modelom i omogućavaju studentima interaktivno učenje.

1.2 Predmet i cilj istraživanja

Predmet istraživanja doktorske disertacije je kreiranje modela 3D edukacionog okruženja za digitalnu forenziku. Okruženje se sastoji od virtuelnih učionica i laboratorija koje obezbeđuju interaktivnost između učesnika. Posledice interaktivnosti su specifični pedagoški pristupi koji su bazirani na povratnim informacijama učesnika u procesu obrazovanja. Okruženje se koristi kao pomoćno sredstvo za edukaciju u oblasti digitalne forenzike.

Digitalna forenzička laboratorija (DF-lab) omogućava interakciju između fizički prisutnih i udaljenih profesora i studenata sa edukacionim resursima, korišćenjem integrisanih virtuelnih i realnih laboratorija. Studentima je omogućeno da rade istovremeno na istom projektu i da koriste postojeće desktop aplikacije u višekorisničkom distribuiranom okruženju.

Interaktivne simulacije i virtuelna okruženja omogućavaju proces učenja kroz praktičnu obuku. Okruženja su kreirana da bi omogućila: modelovanje, prikaz, kolaboraciju, kombinaciju različitih korisničkih interfejsa (User Interface) itd. Studenti mogu da se kreću unutar 3D okruženja uz interakciju sa drugim studentima, predavačima i ostalim objektima okruženja.

1.3 Motivacija za izradu rada

Glavni razlozi za istraživanje su nedostaci: integrisanih realnih i virtuelnih učionica ili laboratorija za edukaciju u oblasti digitalne forenzike; interaktivnosti između studenata koji rade istovremeno na istom forenzičkom zadatku; specifičnih pedagoških pristupa sa povratnim informacijama učesnika u procesu obrazovanja; dinamičkog kurikuluma za osnovne i poslediplomske studije u oblasti DF-a.

1.4 Definisanje problema i predlog rešenja

Osnovni problem je proistekao iz prakse, odnosno, iz višegodišnjeg rada sa studentima na Univerzitetu Singidunum. Primećeno je da postoje određeni problemi koji se mogu prevazići uvođenjem novih tehnologija.

Silabus koji se trenutno koristi na Fakultetu za elektrotehniku i računarstvo (FER) na predmetu Digitalna forenzika koncipiran je kroz XV nastavnih nedelja:

- Uvod u kompjuterski kriminal;
- Osnove istrage kompjuterskog kriminala;
- Proces korporacijske istrage kompjuterskog incidenta;
- Funkcionalni modeli digitalne forenzičke istrage;
- Kolokvijum I;
- Digitalni dokazi;
- Osnove digitalne forenzičke nauke;
- Forenzička akvizicija digitalnih podataka;
- Funkcionalni modeli forenzičke akvizicije (statički, dinamički, virtuelni model);
- Forenzička analiza digitalnih podataka;
- Kolokvijum II;
- Antiforenzičke tehnike i alati;
- Alati za digitalnu forenzičku istragu;
- Primene virtuelnih mašina u digitalnoj forenzici;
- Veštačenje digitalnih dokaza.

Cilj predmeta je:

- Sticanje novih teorijskih i praktičnih znanja iz interdisciplinarne oblasti kompjuterskog kriminala.
- Detaljno upoznavanje i proučavanje metodološko-tehnoloških osnova istrage digitalnih podataka u računarskom sistemu, mreži i na Internetu.
- Detaljno upoznavanje sa tehnologijama, tehnikama i alatima za digitalnu forenzičku analizu.
- Razumevanje značaja digitalne forenzičke nauke za korporacijsku istragu kompjuterskog incidenta i nezamenljive uloge digitalne forenzike u zvaničnoj istrazi kompjuterskog kriminala.
- Proučavanje savremenih forenzičkih tehnika i alata za oporavak digitalnih podataka, forenzičku akviziciju i analizu, zasnovano na strogo naučnim principima.
- Samostalan praktični rad sa najznačajnijim forenzičkim alatima za uzimanje forenzičke kopije isključenog računarskog sistema, virtuelne mašine i aktivnog računara u radu.
- Razumevanje forenzičkih izazova u savremenim virtuelizovanim sistemima distribuiranog Internet računarstva (Cloud Computing) i primena virtuelne mašinske introspekcije u digitalnoj forenzici.

Ishod predmeta:

Student stiče teorijska, praktična, metodološka i tehnološka znanja za samostalnu forenzičku istragu. Praktična znanja se odnose na samostalan izbor relevantnih forenzičkih tehnika i alata za uzimanje forenzičke kopije i akviziciju digitalnih podataka iz različitih digitalnih uređaja (računara, mobilnog uređaja, digitalne foto i video kamere itd.).

Iz navedenog silabusa se može primetiti da su osnovni problemi koji se javljaju u toku realizacije nastave nemogućnost vežbanja na realnim slučajevima kao i nemogućnost međusobne saradnje više studenata (grupni rad) na zajedničkom slučaju. Predavači (profesori i asistenti) moraju pripremati kompletne vežbe koje se sastoje od “imidža“ napadnutog računara što zahteva mnogo vremena. Još jedan ne manje bitan problem je komplikovana detekcija pravilnog procesa istrage od strane studenta, odnosno da li je u toku istrage uništio neki od potencijalnih dokaza.

Navedeni problemi se mogu rešiti uvođenjem vizualizacije preko virtuelnih mašina i 3D modela u vidu virtuelne 3D laboratorije za digitalnu forenziku koja bi se koristila kao pomoćno sredstvo u nastavi. Na osnovu ovih poboljšanja studenti su u mogućnosti da efikasno vežbaju na realnim slučajevima iz prakse uz obavezno čuvanje u repozitorijumu slučajeva i scenarija. Predavači mogu da prate rad studenata da čuvaju njihove rezultate kako bi na kraju mogli da dobiju izveštaj u jednostavnom formatu o napredovanju studenata. Postoji mogućnost i pretraživanja slučajeva iz repozitorijuma na osnovu ključnih reči. Još jedan od bitnih aspekata je i mogućnost jednostavne adaptacije na 3D prostor koji je vrlo sličan realnom okruženju. Na taj način smanjuje se potreban period privikavanja na korišćenje navedenog sistema.

1.5 Rezultati i doprinos

Doprinosi ovog rada mogu se posmatrati sa dva aspekta, stručnog i naučnog.

Stručni:

- pregled svetskih iskustava u oblasti 3D edukacionih virtuelnih okruženja,
- pregled i analiza postojećih softverskih alata za 3D virtuelna okruženja,
- kreiranje modela 3D edukacionog okruženja za digitalnu forenziku,
- kreiranje dinamičkog silabusa i kurikuluma za obuku digitalnih forenzičara,
- kreiranje simulacija koje se koriste u toku obuke digitalnih forenzičara,
- korišćenje 3D virtuelnih okruženja u oblasti obuke digitalnih forenzičara.

Naučni:

- pregled i analiza dosadašnjih istraživanja i dostignuća u oblasti 3D virtuelnih okruženja,
- pregled i analiza postojećih implementacija 3D virtuelnih okruženja za učenje,
- analiza nedostataka postojećih 3D virtuelnih okruženja za učenje,
- analiza raspoloživih tehnologija za realizaciju softverskog rešenja,
- kreiranje i dizajn generičkog 3D modela za obuku digitalnih forenzičara,
- projektovanje, razvoj i realizacija hardversko-softverskog sistema koji omogućava korišćenje 3D modela,
- predlog smernica za dalji razvoj.

Rad je podeljen u 10 celina. U prvom delu rada dat je uvod u problematiku istraživanja, motivacija za izradu rada, preciziran je predmet istraživanja i dati rezultati i doprinosi rada. U drugom delu prikazana su prethodna istraživanja u oblasti digitalne forenzike, virtuelnog okruženja (VE), vizualizacije i virtuelizacije. Treći deo rada predstavlja uvod u polje DF-a, dati su osnovni koncepti i definicije. U četvrtom delu predstavljena su VE, tipovi okruženja, svrha i dati su primeri primene okruženja u edukaciji, zabavi i nauci. Peti deo rada bazira se na primeni 3D virtuelnih okruženja u edukaciji, predstavljena je komparativna analiza postojećih virtuelnih okruženja i na osnovu nje je izabrano odgovarajuće rešenje za realizaciju. Šesti deo rada su: modelovanje i analiza, opis okruženje, elementi okruženja, ontologije okruženja i hardverska platforma na kojoj je okruženje realizovano. Sedmi deo rada je realizacija, dat je dizajn okruženja, karakteristike okruženja, opis softverskog sistema i prikazana je kompletna forenzička laboratorija (biblioteke forenzičkih scenarija i slučajeva). U osmom delu rada predstavljeni su silabusi za osnovne, master i doktorske studije kao i dinamički kurikulumi. Deveti deo rada bavi se procenom znanja i analizom postignutih rezultata i doprinosa. Deseti deo rada je zaključak i smernice za budući rad.

2 Prethodna istraživanja

Razvoj digitalne forenzike može da se podeli u dve faze. Prva faza je poznata kao “zlatno doba DF-a” i podrazumeva se vremenski period od 1999. do 2007. godine kada je došlo do naglog razvoja DF-a. Ovaj period karakterišu:

- Velika rasprostranjenost Microsoft Windows operativnog sistema (najviše Win XP).
- Relativno mali broj tipova fajlova koji su bitni za DF istragu (MS office, jpeg, avi, wmv...).
- Istraga se uglavnom bazira na jednom računarskom sistemu.
- Uređaji za skladištenje podataka uglavnom koriste standardne interfejsa (IDE/ATA).
- Mnogi proizvođači prodaju alate pomoću kojih se lako mogu povratiti alocirani i obrisani fajlovi.
- Uvodi se DF na univerzitete.

Posle navedenog perioda, od 2007. godine DF ulazi u doba „krize“ koja je izazvana razvojem informacionih tehnologija. Posledice su:

- Povećanje veličine prostora za skladištenje podataka, što se u startu odražava na obim i dužinu DF istrage.
- Povećava se broj različitih vrsta ugrađenih flash uređaja, što onemogućava da se uređaj “imidžuje” (pravi se kopija bit po bit).
- Povećava se broj različitih operativnih sistema i fajl formata (Android je sve popularniji), što zahteva sve kompleksnije softvere za DF istragu.
- Za razliku od prethodne faze, gde je istraga uglavnom bila bazirana na jednom računaru, ova faza se bazira na više povezanih uređaja.
- Učestalije korišćenje enkripcije (TrueCrypt), što otežava dešifrovanje podataka za DF istragu.
- Korisnici sve češće koriste “Cloud” za čuvanje svojih podataka, što dovodi do mnogo težeg “imidžovanja” podataka.
- Malver se sve češće ne upisuje u standardno skladište podataka (HD) već se mora ispitivati RAM memorija (RAM forensics).

- Zakonski propisi se menjaju i sve više ograničavaju DF istragu.
- DF silabusi i kurikulumi nisu standardizovani.

U ovom delu rada predstavljena su dosadašnja istraživanja u oblasti digitalne forenzike, virtuelizacije, vizualizacije i 3D virtuelnih okruženja i primena u oblasti edukacije.

2.1 Istorijski pregled i radovi za digitalnu forenziku

Pregled radova počinje od primenjenih tehnologija koje se ili koriste za digitalnu forenziku (kao platforme), ili su same cilj primene digitalne forenzičke istrage (kao objekti).

Cloud forenzika je disciplina koja kombinuje Cloud computing i digitalnu forenziku. U radu [67] fokus je na trenutnom stanju razvoja (state-of-the-art) u oblasti Cloud forenzike. U radu [68] fokus je na tehničkim aspektima digitalne forenzike u distribuiranom Cloud okruženju. U radu [69] dati su razlozi za i protiv korišćenja Cloud Computinga u DF-u. Potrebno je da se promeni i usvoji drugačiji skup procedura za istragu koja se sprovodi na Cloud sistemu. Forenzička istraga može imati koristi jer Cloud provajder može pomoći u forenzičkoj istrazi. U radu [70] Cloud se tretira kao objekat digitalne forenzičke istrage. Digitalna forenzika predstavlja primenu principa iz računarskih nauka za “vraćanje” digitalnih dokaza u svrhu prezentacije na sudu. Takođe Cloud forenzika se bazira na glavnim fazama mrežne forenzike (network forensics) zajedno sa preporučenim tehnikama za Cloud okruženja [71].

Forenzika kao Cloud servis može koristiti moćne računarske resurse iz Clouda za podršku istrazi cyber kriminala na svim nivoima [72]. U radu [73] dat je opis hardvera-storage za korišćenje platforme Eucalyptus na Amazon EC2 i S3 Cloud servisima.

U radu [74] autori daju osnove akvizicije i analize imidža sa Android smart telefona. Model forenzičke istrage smart telefona (SPFIPM) kreiran je u radu [75].

U radu [76] autor je nabrojao alate za digitalnu forenzičku istragu i opisao njihovo korišćenje u pravnim okvirima. Isti autor u radu [77] koristi teoriju apstraktnih lejera da objasni svrhu i ciljeve alata za digitalnu forenzičku analizu. U radu [78] autor daje kratak prikaz metodologije, modela, analize i primene alata u digitalnoj forenzici.

U istraživanju [84] autor diskutuje o tehnici analize koja je uspešno unapređena za detekciju malicioznosti u skrivenim podacima za istragu NTFS boot sektora. Njihova prednost je da se backtracking tehnikom beleže dodatni parametri sistema u toku normalnih operacija (real-time) i istrage u toku faze analize. Glavni fokus rada [85] je digitalna forenzička istraga različitih lokacija Windows fajl sistema i Oracle baze podataka.

U radu [95] fokus je na digitalnoj forenzičkoj mrežnoj laboratoriji koja bi se uvela sa ciljem da omogući studentima i fakultetima idealno konfigurabilno okruženje za istraživanja i testiranja preko TCP/IP mrežnog protokola. Istraživanja sigurnosti i privatnosti u Cloud računarstvu u više zemalja prikazana su u radu [96].

U radu [105] objašnjena je i prikazana primena tehnika etičkog hakinga u digitalnoj forenzičkoj istrazi. Prikazan je primer korišćenja tehnike u udaljenom prikupljanju podataka sa živog računara (remote live forensic). Kao platforma za virtuelizaciju korišćen je VMWare Workstation 9.

Posebno su važni radovi iz oblasti edukacije i istraživanja. U radu [86] autori predlažu agendu koja bi se koristila u forenzičkom treningu.

U radu [91] autor izveštava o stanju Falcone programa (Falcone Programme) i AGIS projekta i inovativnim akademskim partnerstvima gde bi se zajedničkim snagama kreirao trening (Cyber crime Forensic Investigation Training) i specijalistička edukacija u Engleskoj.

U radu [92] opisuje se online master program na Champlain koledžu u oblasti upravljanja digitalnom istragom. Predloženi kurikulum je objašnjen zajedno sa načinima za učenje i pedagoškim pristupom, koji su predviđeni za dizajn kursa.

Na California Sciences Institutu je kreiran savremeni kurikulum za doktorat u oblasti digitalne forenzike i razmatra se uvođenje predmeta na osnovne studije [93].

U radu [97] fokus je na tehničkim aspektima digitalne forenzike u distribuiranim Cloud okruženjima. U radu [72] više istraživača je napomenulo da mogućnost primene virtuelnih

mašina (VM) može da bude od pomoći za prikupljanje dokaza iz računarskog okruženja za forenzičku istragu.

U radu [98] fokus je na kreiranju ontologije za specijalizaciju, sertifikaciju i edukaciju u oblasti forenzike. Ova ontologija može da se koristi za kreiranje kurikuluma i edukacionih materijala. U radu [99] predstavljen je ontologija DIALOG (Digital Investigation Ontology). DIALOG ontologija je definisana da objedini sve koncepte u oblasti digitalne forenzike i relacije između njih. U radu [100] autori predlažu sistematski mehanizam koji se bazira na ontologiji DIEAOM za prikupljanje znanja iz različitih heterogenih izvora dokaza, deljenje znanja i ponovno korišćenje i podršku za kriminalne istrage.

2.2 Istorijski pregled i radovi za virtuelna okruženja, vizualizaciju i virtuelizaciju

U radu [79] autori diskutuju o potencijalnoj ulozi virtuelnih okruženja u fazi analize u digitalnoj forenzičkoj istrazi. Oni predlažu nov pristup sa dva okruženja, običnim i virtuelnim koji se koriste nezavisno. U istraživanju [80] cilj je da se pronađu razlike u detekciji „honeypots-a” koji se nalaze u dva različita okruženja, jedan u vidu virtuelne mašine a drugi u vidu standardnog hardverskog sistema.

U radu [81] autori koriste SVL model (Secure model for Virtuelization Layer), koji kombinuje virtuelizaciju i system za detekciju upada. U radu [82] predložena je kombinacija statičke i žive (live) analize. U radu [83] autori su zaključili da je istraga u virtuelnom okruženju jednostavnija nego u fizičkom okruženju.

U radu [87] predstavljen je metod u kome se VR (virtuelna realnost) tehnologija može koristiti za kreiranje realističnih okruženja za forenzički trening kojim bi se mogli smanjiti troškovi i utrošeno vreme studenata i predavača.

U radu [88] autori objašnjavaju ulogu simulacije i različitih aspekata učenja i treninga (simulacije letenja, simulacije u medicini, simulacije u vojnoj primeni, simulacija edukacije u računarskim naukama). U radu [89] isti autor predstavlja sistem za edukaciju eksperata u oblasti

digitalne forenzike koji se bazira na Second Life okruženju za simulacije. Glavni nedostatak sistema koji je predstavljen jeste to što se bazira na okruženju Second Life koje nije open source i kod koga nisu sve funkcionalnosti besplatne za korišćenje.

U radu [90] autor je kreirao i implementirao laboratoriju za učenje u oblasti digitalne forenzike, za akviziciju digitalnih dokaza. U radu su uključene i specifikacije treninga, hardvera i softvera za pokretanje praktičnih vežbi na kursu u školi Information and Library Science (SILS) na University North Carolina.

U radu [94] fokus je na primeni virtuelne realnosti (VR) za dizajniranje interaktivnog prototipa za vizualizaciju i rekonstrukciju forenzičkih istraživanja.

U radu [104] predstavljen je novi model za obuku digitalnih forenzičara. Predstavljena laboratorija se bazira na X3D okruženju sa VNC protokolima za pristup virtuelizovanim klijentima.

2.3 Istoriijat virtuelnih okruženja

Razvoj i dizajn virtuelnih okruženja je snažno povezan sa “snovima i vizijama” [19]. Razvoj virtuelnih okruženja [20] se bazira na dve različite perspektive:

- Hardverski stručnjaci pokušavaju da uspostave temelje za programere koji bi im omogućili da kreiraju realistične 3D objekte i 3D okruženja.
- Programeri virtuelnih okruženja pokušavaju da stvore nove mogućnosti za korisnike koje su neostvarive u stvarnosti.

2.3.1 Početak

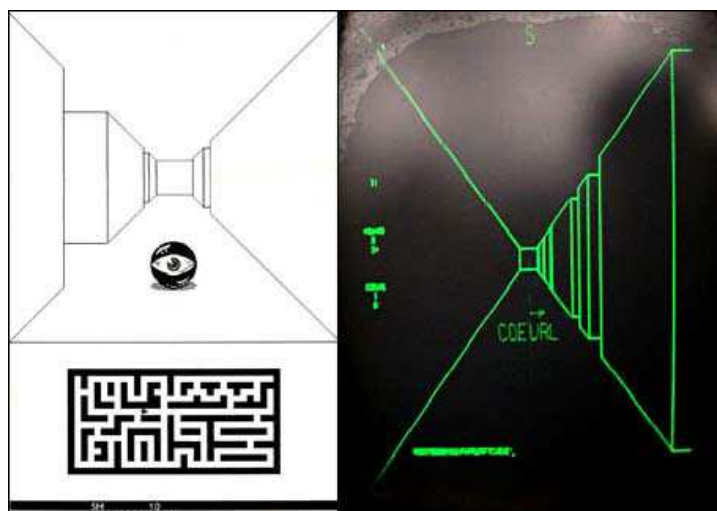
Koncept postavljanja lica u kompjutersko-generisano okruženje ili životnu sredinu je uveo Ivan Sutherland 1965. godine [21]. Sutherland je realizovao svoju ideju 1968. godine pomoću ručno napravljenog stereoskopskog displeja [22]. Ubrzani razvoj i poboljšanje performansi računara dodatno su ubrzali razvoj virtuelnih okruženja [23].

Tekstualni programi kao što su časkanje, e-mail klijenti i Usenet su bili osnovni elementi prvih virtuelnih okruženja. Okruženje bazirano na tekstu MUD¹ napravljeno je prvi put 1978. godine. To je višekorisničko virtuelno okruženje za rad u realnom vremenu koje se bazira na tekstu. Prema rečima Richarda Bartlea “virtuelna okruženja se često nazivaju MUD” [7]. Ovo okruženje je programirano u MACRO-10 assembleru na DecSystem-10 mainframe na Essex Univerzitetu u Engleskoj (Roy Trubshaw). Prva verzija je bila samo program za testiranje osnovnih principa virtuelnog okruženja a tehnički zahtevi za virtuelnost nisu bili ispunjeni u tom trenutku.

Endžin igrice MUD v3 je napisan u BCPL (preteča programskog jezika C), a ostatak igre je napisan na jeziku MUDDL (Multi-User Dungeon Definition Language) [7]. Bartle napominje da postoje dve motivacije zbog čega je Roy Trubshaw napisao MUD. Na prvom mestu Trubshaw je “imao snažan akademski interes da napiše program za parser i interpreter”. Drugi razlog je taj što je kao zaljubljenik u “single-player” avanturističke igre prema sopstvenoj zamisli realizovao “multiplayer” igru. Nakon toga veliki broj programera je razvijajući kompjuterske igre kreirao i odgovarajuća virtuelna okruženja.

2.3.2 Prva virtuelna okruženja

Prvi softver koji je koristio “nešto što podseća” na virtuelno okruženje bio je Maze War (1974. godina) [24]. Maze je pružao korisniku osećaj da je “prisutan i da se kreće” kroz virtuelno okruženje. Podržavao je osam igrača (robota) [25].



Slika 2.1 Maze War prikaz pokrenut u ranim 1970-tim na Imlac PDS-1

¹ (multi-user dungeon)

Maze War (slika 2.1) je “jedini poznati originalni screen shot Maze War u akciji”. Kao što se vidi drugi korisnici u okruženju su predstavljeni kao jednostavni likovi (oko) [26]. U radu [24] Damer je istakao da Maze prvi definiše virtuelna okruženja. Sledeći korak u stvaranju virtuelnih okruženja napravljen je 1980. godine. Bar-Zeev je prikazao i testirao osnove tehnoloških koncepata virtuelnih okruženja [19]. Okruženje za video igru “Massively-Multiplayer Online Role-Playing Games” (MMORPGs) je višekorisničko i pruža mogućnost virtuelne interakcije [27].

Nivo tehnološkog razvoja iz kasnih 70-tih i ranih 80-tih godina prošlog veka nije davao mogućnost komercijalizacije video igara. Pojavom personalnih kolor računara (PC) kao što je Commodore 64 i dial-up mrežnih interfejsa, stvorili su se uslovi za pojavu prvog grafičkog društvenog virtuelnog sveta (Habitat) [24]. U radovima [28], [29], [30] navodi se da je Habitat bio prvi grafički onlajn virtuelni svet koji podržava više igrača odjednom (više od 16). Po prvi put se uvodi pojam avatar [8].

Prva generacija društvenih virtuelnih okruženja na Internetu

U ranim 90-tim god prošlog veka došlo je do povećanja snage centralne procesorske jedinice (CPU) i performansi sistema. Postalo je moguće da se okruženje pokrene u realnom vremenu sa 3D teksturom na standardnom PC računaru [24]. Činjenica da su računari i Internet stigli u domove ljudi, otvorila je vrata ne samo industriji igara i programerima i istraživačima društvenih virtuelnih okruženja [7].

Worlds Chat je jedno od prvih virtuelnih okruženja pokrenuto na Internetu 1995. godine. Korisnici su u mogućnosti da se teleportuju sa jednog mesta na drugo [8]. Virtuelni Alfa svet se koristi kao “eksperimentalna platforma koja dozvoljava korisnicima da izgrade u virtuelnom okruženju montažne objekte”.

Kontakt Konzorcijum

Kontakt Konzorcijum je neprofitna organizacija koja se nalazi u severnoj Kaliforniji, a osnovao ju je Bruce Damer 1995. godine [24]. To je prva globalna organizacija fokusirana na virtuelne prostore na Internetu, koja podržava specijalne interesne grupe, organizuje konferencije i

sponzoriše istraživanja [31]. Ova organizacija je bila domaćin prve svetske konferencije i sajma unutar sajber prostora 1998. godine sa preko 500 polaznika u San Francisku.



Slika 2.2 Sala za konferenciju (levo) i podijum za govornike (desno)

Slika desno 2.2 pokazuje avatara koji predstavlja sadržaj na jednom od šest dostupnih podijuma za govornike na Avatar98 konferenciji. Sajber konferencije su uzastopno održavane u periodu od 1999. do 2004. godine. Na osnovu iskustava stečenih na ovim konferencijama postalo je moguće realizovati virtuelna okruženja za obrazovanje (Vlearn3D) [32].

2.3.3 “Naseljena” virtuelna okruženja (IVW)

Centralni koncept IVW su avatari (vizualno predstavljanje ljudi u sajber prostoru). Avatari čine mogućim da se korisnici pridruže virtuelnim sastancima i prošetaju kroz različite lokacije u virtuelnom okruženju, kao i da razgovaraju licem u lice, koristeći gestove i emocije. Mogućnost da se izgrade različite vrste virtuelnih mesta za sastanke je važna karakteristika. Moguće je korišćenje javnih lokacija koje treba da posluže kao informaciona čvorišta i pokažu put ka novim zasebnim događajima. Razlika između virtuelnosti i realnosti u ovom kontekstu je da korisnici mogu da se “teleportuju” sa jedne lokacije na drugu. Svaki događaj u sajber prostoru mora da bude dobro organizovan i koordiniran kao u stvarnosti. Dakle, sledeća osobina je da fizički timovi koordiniraju akciju u virtuelnom okruženju [33].

2.3.4 Kriza i preporod virtuelnih okruženja

U prelaznom periodu između dva milenijuma mnoge kompanije i investitori su bankrotirali u ranoj fazi usvajanja Internet društvenih virtuelnih okruženja [24]. Bilo je postavljeno pitanje da li

su društvena okruženja održiv medij ili evolutivni promašaj. Odgovor je bio uspon društvenih mreža (My Space, Facebook, LinkedIn), kucanje poruka (Twitter), grafika na mobilnim uređajima, glas i video preko IP protokola (Skype, YouTube), i grupno deljenje znanja (Wikipedia). Ove vrste softvera i medija su odgovorne za izlazak društvenih okruženja iz krize sa kojom su bili suočeni [24]. Početkom 2003. godine pojavile su se beta verzije virtuelnih okruženja (Second Life, There ...) [34].

3 Digitalna forenzika

U ovom delu rada biće date definicije osnovnih pojmova u oblasti digitalne forenzike (DF), zatim vrste DF istrage, pojam anti-forenzike i anti-forenzičkih tehnika a na kraju su prikazani i forenzički alati koji se najčešće koriste u toku DF istrage.

3.1 Definicije

Digitalna forenzička nauka definiše se kao „korišćenje naučno izvedenih i dokazanih metoda za sakupljanje, čuvanje, identifikaciju, analizu, interpretaciju, dokumentovanje i prezentaciju digitalnih dokaza izvedenih iz izvora digitalnih podataka, a namenjenih za lakšu rekonstrukciju događaja koji se smatraju krivičnim delom, ili neovlašćenim ometanjem planiranih operacija računarskih sistema i mreža“ [48].

Kao što se može videti u prethodnoj definiciji digitalna forenzička nauka ili digitalna forenzika uključuje otkrivanje i sakupljanje (akviziciju), čuvanje (upravljanje), dokazivanje (analizu) i ekspertske svedočenje/veštačenje (prezentaciju) digitalnih dokaza pred sudom, u slučajevima zloupotrebe IKT (informaciono komunikacione tehnologije) sistema.

Najveći deo digitalne forenzike odnosi se na forenziku računarskih sistema, ili kompjutersku forenziku, bilo da su računari samostalni ili umreženi u neki oblik računarske mreže. Digitalna forenzika računarskog sistema obuhvata naučno ispitivanje i analizu podataka sa čvrstih diskova - HD (Hard Drives), fajl sistema i drugih medija i prostora za skladištenje podataka u računarskom sistemu, tako da se podaci mogu koristiti kao čvrsti i neoborivi dokazi pred sudom [48].

Digitalna forenzika računarske mreže, uključujući i Internet forenziku, otkriva i sakuplja informacije o tome kako je napadač, ili haker dobio pristup računarskoj mreži i računarskom sistemu. Analiziraju se log fajlovi da bi se odredilo kada se korisnik ulogovao ili poslednji put koristio svoj lični identifikator (ID) za logovanje. Digitalni forenzičar nastoji da odredi kojim URL² je korisnik pristupio, kako se ulogovao na računarsku mrežu i sa koje lokacije.

² *Unified Resource Location*

Važno je napomenuti da se digitalna forenzika računarskog sistema razlikuje od procesa oporavka podataka, slučajno izgubljenih ili izbrisanih. Digitalna forenzika oporavlja podatke, koje je korisnik namerno sakrio ili izbrisao, sa ciljem da obezbedi validnost oporavljenih podataka za dokaze pred sudom. Digitalni dokazi mogu biti optužujući, oslobađajući, ili da ukazuju na osnovanu sumnju. Forenzičar mora ispitivati čvrsti disk (HD) i sve druge sekundarne medije za skladištenje i iz velike količine digitalnih podataka izvući relevantne i održive dokaze.

3.1.1 Zvanična istraga kompjuterskog kriminala

Zvanična istraga uključuje policijske organe istrage, specijalno tužilaštvo i specijalno sudstvo za borbu protiv visokotehnološkog (kompjuterskog) kriminala. Ovi organi u našoj zemlji rade prema Zakonu o krivičnom postupku, Zakonu o borbi protiv visokotehnološkog kriminala Republike Srbije i strogo utvrđenim procedurama za pretragu, privremeno oduzimanje i ispitivanje računarskih sistema i drugih mrežnih uređaja, u cilju otkrivanja validnih digitalnih dokaza. Bitno je istaći da u slučaju zvanične istrage istražni organi moraju dobro poznavati i razumeti zakon i propise koji se odnose na kompjuterski kriminal, uključujući standardne lokalne procedure za pretragu i utvrđivanje slučaja kriminalnog dela.

U procesu utvrđivanja karaktera krivičnog dela kompjuterskog kriminala, istražni organ mora tražiti odgovore na brojna pitanja, kao što su na primer:

- Šta je bilo sredstvo izvršavanja krivičnog dela?
- Da li su računarski sistem i mreža poslužili kao jednostavan prolaz za izvršavanje krivičnog dela?
- Da li je u pitanju krađa, provala ili vandalizam u sistemu?
- Da li je napadač ugrozio nečiju privatnost i druga prava, ili uznemiravao korisnike?

Ovde je bitno istaći paralelu da računarski sistem i računarska mreža mogu biti sredstva za izvršavanje krivičnog dela i u tom smislu ne razlikuju se od alata provalnika za upad u tuđi stan. Računarski sistemi koriste se kao sredstvo za izvršenje krivičnog dela ili mogu biti predmet krivičnog dela.

3.1.2 Korporacijska digitalna forenzička istraga

Pored zvanične istrage postoji i korporacijska istraga koja se radi uglavnom u tajnosti i rezultati se šalju naručiocu istrage, najčešće upravi korporacije. Takođe se može desiti i da istragu sprovodi neko ko je zaposlen u firmi koja je naručilac DF istrage. Kada se kompjuterski incident dogodi, kritičan faktor je brzina reakcije. U početnoj praksi forenzičke istrage kompjuterskog kriminala, pokazalo se da su podaci otkriveni u toku prvih sedam dana bili kritični za uspešan oporavak.

Za donošenje odluke o uključivanju internog ili eksternog tima u digitalnu forenzičku istragu, organizacija treba da razmotri i izbalansira sledeće faktore:

- **Troškovi:** nabavke, ažuriranja i održavanja forenzičkog softvera, hardvera i opreme koja se koristi za sakupljanje i ispitivanje podataka, a može uključivati i dodatnu fizičku zaštitu od njihove kompromitacije. Drugi značajni troškovi uključuju obuku osoblja i troškove rada, koji su posebno značajni za profesionalne forenzičare. Generalno, retko su troškovi angažovanja spoljnih forenzičara skuplji od troškova interne forenzičke istrage.
- **Vreme odgovora:** osoblje locirano na lokaciji incidenta može inicirati forenzičku istragu znatno brže od iznajmljenog tima. Takođe, za fizički distribuirane organizacije osoblje na lokaciji incidenta može brže reagovati nego tim iz centra organizacije.
- **Osetljivost podataka:** zbog osetljivosti podataka organizacija može oklevati da angažuje spoljni forenzički tim koji treba da uzme fizičku kopiju (imidž) čvrstog diska i pri tome ima pristup svim podacima, pošto na disku mogu biti važne zdravstvene informacije, finansijski izveštaji, ili druge osetljive informacije. Međutim, ako postoje indicije da je član internog tima umešan u incident, bolje je angažovati spoljni forenzički tim.

3.1.3 Digitalni dokaz

Digitalni dokaz predstavlja digitalni podatak koji može potvrditi da je kompjuterski kriminal počinjen i koji može da omogući vezu između kriminala i njegovog izvršioca. Primeri digitalnog dokaza su podatak u RAM memoriji, na čvrstom disku, ili u mobilnom uređaju.

Prema definiciji međunarodne organizacije IOCE u oblasti digitalne forenzičke nauke, digitalni dokaz je svaka informacija u digitalnom obliku koja ima dokazujuću vrednost, a koja je ili uskladištena ili prenesena u takvom obliku. Pojam digitalnog dokaza uključuje kompjuterski

uskladištene i kompjuterski generisane dokazne informacije, digitalizovane audio i video dokazne signale, signale sa digitalnog mobilnog telefona, informacije sa digitalnih faks mašina i signale drugih digitalnih uređaja. Digitalni dokaz je bilo koja informacija generisana, obrađivana, uskladištena, ili prenesena u digitalnom obliku na koju se sudski organi mogu osloniti kao validnu, tj. svaka binarna informacija, sastavljena od digitalnih nula i jedinica, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije originalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije.

U kompjuterskom incidentu postoje tri osnovne kategorije digitalnih podataka koji mogu činiti digitalni dokaz:

- Promenljivi podaci ili informacije koje se gube nakon isključivanja računara, kao što su podaci u radnoj memoriji (RAM), rezidentni memorijski programi itd. Ovi podaci se mogu izgubiti u toku procesa isključivanja računara. Zbog toga je veoma važno do kraja precizno sprovoditi proceduru akvizicije. Pre isključivanja računara treba odmah ispitati, locirati i izvući osetljive i šifrovane podatke, jer se može desiti da se posle isključivanja računara ne može doći do njih (npr. vlasnik ključa ili smart kartice ne želi da sarađuje ...).
- Osetljivi podaci ili podaci uskladišteni na čvrstom disku koji se lako mogu izmeniti, kao što je, npr. poslednje vreme pristupa log datoteci itd.
- Privremeno dostupni podaci, ili podaci uskladišteni na čvrstom disku kojima se može pristupiti samo u određeno vreme (npr. šifrovani podaci).

3.1.4 Modeli digitalne forenzičke istrage

U ovom delu rada su opisana tri modela digitalne forenzičke istrage sa prednostima, ograničenjima i mogućnostima forenzičkih tehnika i alata [54].

Model tradicionalne digitalne forenzike (statičke)

Model tradicionalne digitalne forenzike, ili analize neaktivnog računarskog sistema, uključuje preuzimanje kontrole nad kompromitovanim sistemom (privremenim oduzimanjem), isključivanje računara (normalnim isključivanjem shut down operacijom, ili isključivanjem

napajanja), off-line uzimanje fizičke slike (imidža) uređaja za skladištenje (čvrsti disk, USB, CD, DVD itd.) i analizu "imidža" pomoću brojnih forenzičkih alata.

Ovakav model digitalne forenzičke istrage ima sledeća bitna ograničenja:

- Može postati praktično neprimenljiv kada kapacitet čvrstog diska raste do reda terabajta. Uzimanje „imidža“ ovakvih diskova nije moguće, ili je ekstremno teško, posebno sa velikih RAID diskova.
- Proces uzimanja „imidža“ čvrstog diska zahteva da računarski sistem bude isključen, što za savremene organizacije i e-poslovanje u većini slučajeva nije prihvatljivo. Činjenica je i da sudije sve ređe izdaju naloge za isključivanje i privremeno oduzimanje kompromitovanih servera radi forenzičkog ispitivanja.
- Gubi se najveći broj informacija o tome šta se događalo u računarskom sistemu u trenutku njegovog isključivanja. Ove informacije obezbeđuju neophodan kontekst za dokaze sa čvrstog diska i od presudnog su značaja za rekonstrukciju događaja.

Zbog navedenih i drugih ograničenja tradicionalnog modela tzv. statičke digitalne forenzike, došlo je do razvoja modela aktivne digitalne forenzike.

Model aktivne digitalne forenzike

Dok prethodni model digitalne forenzičke istrage pokušava da sačuva sve dokaze na fizičkom disku u nepromenjenom stanju, model aktivne digitalne forenzike zahteva da se uzme jedan snimak aktivnog stanja, slično uzimanju digitalne fotografije mesta krivičnog dela (crime scene). Aktivna istraga prikuplja podatke iz sistema u radu, obezbeđujući dodatne informacije koje nisu dostupne u statičkoj analizi.

Masovna upotreba Interneta čini te informacije još značajnijim. Date informacije uključuju i aktivne procese, mrežne konekcije, sadržaj procesne i fizičke memorije, sadržaj keš memorije, logovanja na korisničke naloge, sistemska opterećenja i dr.

Generalno ovaj model može obezbediti forenzičaru pristup promenljivim informacijama, koje su u statičkoj analizi nedostupne, ali pored pomenutih prednosti, ima nekoliko ozbiljnih nedostataka od kojih su najznačajniji:

- Efekat opservatora, koji se odnosi na činjenicu da svaka operacija izvršena u toku procesa aktivne analize, modifikuje stanje ispitivanog sistema, uključujući sadržaj memorije i medija za skladištenje i kojim se može kontaminirati svaki dokaz otkriven u istrazi.
- Delimično oslanjanje na systemske uslužne programe, koji se nalaze na potencijalno kompromitovanom sistemu, pa napadač može manipulirati rezultatima analize i otežati istragu.

Model distribuirane digitalne forenzike

Tekući trendovi u računarskim i komunikacionim tehnologijama omogućavaju običnim korisnicima računara upotrebu čvrstog diska za skladištenje veoma visokog kapaciteta i komunikaciju velikog propusnog opsega. Iz tog razloga mogu biti premašeni tekući kapaciteti prva dva modela digitalne forenzike u kojima forenzičari koriste jednu radnu stanicu kao forenzičku platformu. Operacije pretprocesiranja, kao što su indeksiranje ključnih reči i generisanje sličica (thumbnails) sa uzetog „imidža” čvrstog diska, zahtevaju mnogo vremena, pre nego što analiza uopšte i počne.

Takođe, pretraga po ključnoj reči može biti spora i potpuno neprihvatljiva. Upotreba samo jedne forenzičke mašine ne omogućava upotrebu sofisticiranih alata za analizu. Zato postaje neizbežno da alati za forenzičku istragu koriste distribuirane resurse klastera računarskih sistema, da bi se istragom moglo centralizovano upravljati. Ključna tehnologija koja omogućava primenu ovog modela digitalne forenzičke analize je virtuelizacija, koja dopušta instalaciju brojnih VM [55] na jednom fizičkom serveru.

Ovaj pristup ima dodatne prednosti u odnosu na standardne metode forenzičke analize:

- U statičkoj forenzičkoj analizi „imidža”, forenzičar gubi sadržaj RAM memorije, što može biti kritično za rekonstrukciju događaja [56].
- U dinamičkoj, aktivnoj forenzičkoj analizi sistema u radu, dobijeni podaci mogu biti pogrešni, ako su jezgro (kernel), biblioteke ili sami programi kompromitovani (npr., trojancem prikrivenim sa rutkit tehnikom).

- Ako se forenzička analiza vrši sa VMM (Virtual Machine Monitor), bilo koja kompromitovana komponenta operativnog sistema, biblioteka, ili programa na VM, biće irelevantna, pošto je alati zaobilaze i rade samo na VMM. U ovom slučaju, forenzičar dinamičkom analizom može „gledati” u memoriju, ali zato što VM nije isključena, ona je praktično statička jer je sadržaj memorije zadržan.

3.1.5 Anti-forenzika

Anti-forenzika je termin uveden poslednjih godina, a označava tehnike hakera i kibernetičkih kriminalaca namenjene za borbu protiv forenzičke istrage – otežavanje, ili onemogućavanje te istrage.

Relativno velika dostupnost forenzičkih alata i znanja može kontra-produktivno delovati na uspeh forenzičke analize. Sa jedne strane, forenzičari mogu lakše razrešiti problem na koji naiđu u radu, koristeći brojne baze znanja i informacija i alate različitih mogućnosti, sa druge strane istim alatima i znanjima mogu pristupiti razni korisnici i vešti hakeri. Da bi se ilustrovale ove mogućnosti, između brojnih potencijalnih aktivnosti, dovoljno je detaljnije opisati primenu tehnike brisanja sa prepisivanjem (wiping) i primenu anti-forenzičkih alata (counter-forensic) [49].

Termin "wiping" pozajmljen je iz zajednice digitalnih forenzičara, da bi se moglo razlikovati kompletno uklanjanje podataka od običnog brisanja sa rutinskim komandama računara. Kao što je poznato, brisanje nekog fajla obično ne briše podatke tog fajla, nego samo menja deo imena fajla u direktorijumu, i to je znak OS-u, da su ti sektori i klasteri koje je fajl koristio sada na raspolaganju za neki novi fajl. Međutim, koristeći funkciju oporavka izbrisanog fajla, podaci iz tog fajla mogu se lako oporaviti. Čak ni formatiranje ne prepisuje većinu podataka na disku. Sa druge strane, wiping je proces koji prepisuje korišćeni prostor fajla koji se 'briše' sa beznačajnim podacima, najčešće nulama.

Podaci se sa diska mogu trajno ukloniti fizičkim uništavanjem diska, ili demagnetizacijom diska snažnim magnetnim poljima, što nije uvek prihvatljiv način. Brisanje sa prepisivanjem podataka vrši se forenzičkim alatima i prepisivanjem podataka fajla sa nulama, jedinicama, ili slučajnim nulama i jedinicama, što efektivno uništava podatke.

3.2 Akvizicija digitalnih podataka

Akvizicija digitalnih podataka predstavlja prvu i glavnu fazu digitalne forenzike, analogna je uzimanju otiska prsta, obuhvata procese otkrivanja, identifikacije i izvlačenja digitalnih podataka za potrebe forenzičke analize digitalnih dokaza.

U procesu akvizicije digitalnih podataka iz osumnjičenog računarskog sistema na fizičkom mestu krivičnog dela, digitalni forenzičar uobičajeno preduzima sledeće korake:

- sprovodi formalnu proceduru pretrage fizičkog i digitalnog mesta krivičnog dela,
- fiksira fizičko i digitalno mesto krivičnog dela,
- dokumentuje fizičko i digitalno mesto krivičnog dela,
- sprovodi zaštitu „osumnjičenog“ računara od izmene podataka i unošenja virusa/trojanca,
- isključuje računarski sistem,
- označava i pakuje sve komponente računarskog sistema,
- privremeno oduzima računarski sistem, ili „imidž“ čvrstog diska i svih drugih medijuma (radnu i referentnu kopiju), a ako to nije moguće
- prenosi privremeno oduzeti računarski sistem u forenzičku laboratoriju za forenzičku analizu.

U nekim slučajevima, pre ulaska u klasično forenzičko ispitivanje računara, forenzičar ima potrebu da sakupi neke informacije iz sistema koji je još u radu pre njegovog isključivanja i akvizicije bit-po-bit „imidža“ čvrstog diska. Informacije za koje forenzičar može biti najviše zainteresovan su promenljive, nestabilne i kratkotrajne informacije, koje prestaju da postoje kada se napajanje računara isključi. Ove nestabilne informacije obično postoje u fizičkoj memoriji (RAM-u) i sastoje se od informacija o procesima, mrežnim konekcijama, sadržajima clipboard-a itd. Ove informacije opisuju stanje sistema u trenutku kada je forenzičar pristupio računaru. Forenzički istraživač može često biti u situaciji da izvrši brzo akviziciju podataka da bi odredio prirodu incidenta.

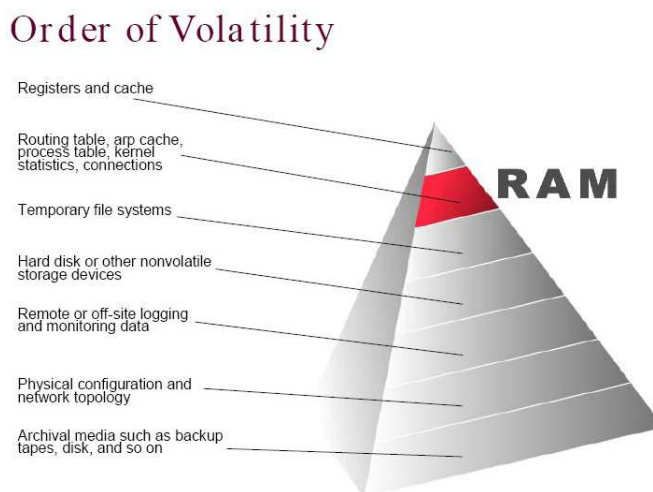
3.2.1 Lokardov princip razmene

U procesu forenzičkog ispitivanja računara u radu, forenzičari i članovi interventnog tima treba da imaju na umu važan princip – da će doći do promene u sistemu koji je u radu posle interakcije korisnika, ili forenzičara sa sistemom. U sistemu koji je u radu promene će se dogoditi jednostavno zbog protoka vremena, rada procesora, skladištenja i brisanja podataka, uspostavljanja i ukidanja mrežnih konekcija itd. Neke promene se dešavaju i kada je sistem samo uključen i nema nikakvih aktivnosti. Promene se dešavaju i kada forenzičar pokrene forenzički alat za uzimanje “imidža”.

Aktiviranje nekog programa izaziva upisivanje informacija u fizičku memoriju, a fizička memorija koju već zauzima neki proces u radu može isprazniti svoj sadržaj u page fajl. Kada forenzičar sakupi informacije i pošalje ih izvan sistema, kreira se nova mrežna konekcija. Sve ove promene mogu se zajedno objasniti Lokardovim³, principom razmene materije: kada dva objekta dođu u kontakt između njih se razmenjuje ili prenosi materija.

3.2.2 Redosled prikupljanja nestabilnih podataka

Forenzičar prvo treba da sakupi informacije o statusu mrežnih konekcija, a najmanje promenljive informacije kao što je fizička konfiguracija sistema, treba sakupljati poslednje.



Slika 3.1 Trajnost podataka [105]

³ Dr. Edmond Locard početkom 20. veka

Iz RAM memorije mogu se izvući sledeće informacije [51]:

- sistemsko vreme,
- logovani korisnici,
- otvoreni fajlovi,
- mrežne informacije,
- mrežne konekcije,
- informacije o aktivnim procesima,
- mapiranje procesa i portova,
- memorija procesa,
- status mreže,
- sadržaj Clipboard-a,
- informacije o servisu/drajveru,
- istorija komandi,
- mapirani drajvovi,
- deljeni fajlovi/direktorijumi.

3.3 Forenzička analiza digitalnih podataka

Forenzička analiza digitalnih podataka, prema izvoru podataka, generalno se deli u tri glavne oblasti:

- forenzička analiza softvera,
- forenzička analiza računara,
- forenzička analiza kibernetičkog prostora (računarskih mreža i Interneta).

Analiza softvera je uglavnom visoko teoretski posao, najosetljiviji je deo digitalne forenzičke analize. Izrada softverskih alata za forenzičku analizu softvera je težak i složen posao. Ključ za identifikaciju autora malicioznog koda je u selekciji odgovarajućeg korpusa koda i identifikaciji odgovarajućih karakteristika za upoređivanje.

Forenzička analiza računara obuhvata ispitivanje računara i tehnika analize u cilju određivanja potencijalnih dokaza, generisanih, ili uskladištenih u računaru. Kompjuterski specijalisti mogu primeniti brojne metode za otkrivanje podataka koji se nalaze u računarskom sistemu, ili za oporavak slučajno izbrisanih, šifrovanih, ili oštećenih fajlova podataka, koje mogu pomoći kod izgradnje neoborivog digitalnog dokaza za pravosudni postupak. Međutim, za otkrivanje, izvlačenje i oporavak namerno izbrisanih, oštećenih ili sakrivenih podataka u računarskom sistemu, potrebna su dodatna znanja, veštine i forenzički alati i iskusni digitalni forenzičari.

Bitno je napomenuti da je forenzička analiza računara najobimniji deo digitalne forenzike, jer se brojni tragovi napada iz ili van lokalne mreže ili sa Interneta uvek nalaze u nekom računarskom sistemu.

Forenzička analiza kibernetičkog prostora bez sumnje je najkompleksnija oblast digitalne forenzike i može biti veoma spor proces. Osnovni zahtev je uspostavljanje legalne saradnje država u borbi protiv kompjuterskog kriminala, uključujući usklađivanje standarda za kvalitet, akviziciju, analizu, prezentaciju i upravljanje digitalnim dokazima. Dodatni problem jeste to što je neophodna saradnja telefonskih kompanija i Internet servis provajdera (ISP), kao i zvaničnih istražnih organa.

3.4 Forenzički alati

Za digitalnu forenzičku akviziciju i analizu potrebno je obezbediti adekvatne forenzičke hardverske i softverske alate - specifične forenzičke alate, ili softverski set alata, koji obezbeđuje izvršavanje nekoliko zadataka istovremeno.

Za nabavku forenzičkog softvera potrebno je proveriti karakteristike potencijalnih alata kao što su:

- OS na kojem forenzički alat radi,
- mogućnost rada verzije alata na jednom ili više OS-a i da li proizvode iste rezultate u višenamenskom radu,
- mogućnost analize više fajl sistema kao što su FAT, NTFS, Ex3, RaiserFS ...
- mogućnost korišćenja nekog programskog alata za automatizaciju funkcija i zadataka koji se u alatu ponavljaju,
- mogućnost automatizovanog obavljanja nekih funkcija, koje mogu smanjiti vreme analize podataka,
- reputacija proizvođača alata i dr.

3.4.1 Hardverski forenzički alati

Hardverski forenzički alati kreću se od jednostavnih jedno-namenskih komponenti do kompletnih forenzičkih računarskih sistema i servera. Jedno-namenske komponente mogu biti uređaji namenjeni za sprečavanje upisivanja podataka na HD koji su poznati kao blokatori upisivanja i predstavljaju hardversko-softverski uređaji za sprečavanje upisivanja podataka na ispitivani disk (slika 3.2).



Slika 3.2 Hardverski blokatori

Primer kompletnog računarskog sistema je radna stanica pod nazivom FRED postoji u više različitih varijanti. Većina proizvođača računarskih sistema i komponenti nudi širok asortiman forenzičkih radnih stanica, koje korisnik može prilagoditi svojim potrebama. Generalno, forenzičke radne stanice mogu se podeliti u sledeće tri kategorije:

- Stacionarna radna stanica: računarski sistem sa nekoliko kućišta za eksterne HD i mnogo perifernih uređaja visokih performansi (slika 3.3).



Slika 3.3 FRED računar

- Portabl radna stanica: laptop računar sa ugrađenim LCD monitorom i skoro istim brojem kućišta i perifernih uređaja kao stacionarna radna stanica (slika 3.4).



Slika 3.4 FREDDIE računar - portabl

- Prenosna radna stanica: obično laptop ugrađen u transportnu torbu sa manjim brojem perifernih uređaja (slika 3.5).



Slika 3.5 FRED-L računar - laptop

3.4.2 Softverski forenzički alati

Postoji veći broj podela softverskih forenzičkih alata u zavisnosti od kriterijuma za kategorizaciju. Najčešća podela je na softverske forenzičke alate koji poseduju ili ne poseduju grafički korisnički interfejs (GUI). Druga važna podela jeste na softverske forenzičke alate koji su besplatni (Open Source) i one koji nisu besplatni (Commercial).

Forenzički alati komandne linije (bez GUI interfejsa)

Forenzički alati sa komandnom linijom MS DOS za IBM PC fajl sisteme bili su prvi alati za analizu i ekstrakciju podataka sa flopi i čvrstog diska. Prvi među tim alatima bio je Norton DiskEditor. Jedna od osnovnih prednosti alata komandne linije je što zahtevaju malo sistemskih resursa, većina njih zauzima jedan butabilni flopi disk (odnosno par megabajta prostora) i proizvodi izveštaj u tekst formatu. Bitno je napomenuti da postoje i forenzički alati komandne linije na Unix/Linux sistemu koji rade na platformama koje se značajno razlikuju od DOS/Windows sistema.

Forenzički alati GUI tipa

Forenzički alati sa GUI interfejsom pojednostavljaju forenzičku akviziciju i analizu. Većina GUI alata dolazi u kolekciji alata za više zadataka (EnCase, FTK). GUI alati imaju nekoliko prednosti:

- jednostavna upotreba,
- mogućnost obavljanja više zadataka,

- ne zahtevaju učenje starijih OS.

Dva najčešće korišćena alata su EnCase i FTK. To su programski alati namenjeni forenzičkoj istrazi digitalnih dokaza. Smatraju se najboljim i najčešće korišćenim softverskim forenzičkim alatima. U tabeli 3.1 može se videti uporedni prikaz osnovnih funkcija navedenih forenzičkih alata:

Funkcija forenzičkog alata	<i>Access Data</i> Ultimate Kit (FTK)	<i>Guidance Software</i> EnCase
Akvizicija		
Fizičko kopiranje podataka	√	√
Logičko kopiranje podataka	√	√
Formati akvizicije podataka	√	√
Proces komandne linije		√
GUI proces	√	√
Udaljena akvizicija		√*
Verifikacija	√	√
Validacija i diskriminacija		
Heširanje	√**	√**
Filtriranje	√	√
Analiza hедера fajlova	√	√
Ekstrakcija		
Čitanje podataka	√***	√***
Pretraživanje po ključnoj reči	√	√
Dekompresija	√	√
Rekonstrukcija fragmentovanog fajla	√	√
Dešifrovanje	√	
Označavanje dokaza	√	√
Rekonstrukcija bezbednosnog događaja		
kopiranje diska na disk	√	√
Kopiranje imidža na disk	√	√
Kopiranje particije na particiju		√
Kopiranje imidža na particiju		√
Izveštavanje		
Log izveštaj	√	√
Generator izveštaja	√	
Legenda: * Zahteva se nabavka <i>Enterprise Edition</i> ** Koristi MD5 i SHA1 algoritme za heširanje *** Varira format fajlova koje podržava		

Tabela 3.1 Uporedni pregled osnovnih funkcija relevantnih forenzičkih alata

Open-source forenzički alati

Ovoj kategoriji alata pripadaju alati koji su besplatni za korišćenje. Uglavnom se baziraju na Linux operativnom sistemu i podležu GPL licencama. Postoji veći broj kvalitetnih alata koji su prihvaćeni od strane pravosudnih organa a među njima prednjači Sleuth Kit/Authopsy browser. Bitno je napomenuti da postoji veći broj Linux distribucija čija je namena DF istraga. Dve najpoznatije takve distribucije su (SIFT Workstation iz SANS-a i DEFT Linux distribucija) [52].

SIFT Workstation je distribucija SANS-a koja poseduje veliki broj besplatnih alata koji se mogu koristiti za DF istragu. Takođe je bitno napomenuti da je distribucija veoma dobro zamišljena za edukaciju forenzičara jer ima dosta dobar help i koristan blog na SANS-ovom sajtu. Na slici 3.6 može se videti kako izgleda ekran posle pokretanja distribucije.



Slika 3.6 SIFT workstation

DEFT Linux je distribucija koja u odnosu na SANS-ovu ima više korisnih alata za DF istragu i mogućnosti su mnogo veće. Bitno je istaći da se ova distribucija konstantno razvija i trenutno u verziji 8 je dopunjena novim savremenim alatima. Na slici 3.7 može se videti kako izgleda ekran posle pokretanja distribucije.



Slika 3.7 DEFT Linux

3.5 Izveštavanje – svedočenje

U međunarodnoj praksi razvijeno je više preporuka za ispitivanje mišljenja - svedočenja ili veštačenja IKT eksperta i prihvatanje istih kao dokaza na sudu. U praksi IKT veštačenja najčešće se prihvataju dokazi utvrđeni naučnim principima. Po ovim principima sudija prihvata digitalni dokaz na osnovu njegove relevantnosti, pouzdanosti i proverljivosti predloženih naučnih metoda, tehnika akvizicije i analize i prezentacije digitalnih dokaza na sudu, za svaki konkretan slučaj. Sud odlučuje da li je svedočenje IKT veštaka bilo od pomoći za utvrđivanje odlučujućih činjenica i istine [53].

Generalno, sud može prihvatiti svedočenje eksperata, gde IKT ekspert na poziv suda, iznosi svoje stručno mišljenje o digitalnim dokazima koji optužuju ili oslobađaju, ali ne iznosi mišljenje o utvrđenim činjenicama, koje su relevantne za slučaj. Tehničko ekspertsko mišljenje treba da bude prihvatljivo za sud i kada ekspert/ forenzičar uvodi nove softverske alate ili nove verzije starijih softverskih alata za akviziciju i analizu digitalnih medija, ali kada primenjuje naučne principe digitalne forenzike i kada to na zahtev suda može potvrditi. Takođe, tehnike za primenu alata za akviziciju i analizu digitalnih dokaza, na osnovu kojih forenzičar izvlači zaključke, moraju biti za sud relevantne, pouzdane, proverljive i u skladu sa usvojenim principima, kao i da se na zahtev suda mogu testirati i verifikovati.

Suđenja koja uključuju digitalne dokaze razlikuju se od svih drugih suđenja u dva glavna aspekta:

- često se pokreće pitanje legalnosti prihvatanja digitalnih dokaza i
- ovaj proces uključuje kompleksan skup nepoznatih pojmova i termina.

Dobar metod prezentacije kompleksnih digitalnih dokaza, uključuje [53]:

- Korišćenje vrlo jednostavnih analogija za objašnjenje generalnog koncepta (npr. slanje e-maila je kao slanje poštanske razglednice).
- Definisanje tehničkih reči pojmovima koje pravosudni organi i porota mogu razumeti.
- Korišćenje slika, crteža ili grafikona za demonstraciju kompleksnih sistema.

- Izgradnju svedočenja koja počinje kroz uvodnu reč sa jednostavnim konceptima, a zatim prelazi na kompleksnija pitanja koja treba objasniti u detalje.
- Povezivanje tehnologije sa tehnologijama koje su prisutni pravosudni organi i drugi u sudnici već upoznali ili koristili, tamo gde je to moguće.

3.5.1 Edukovanje pravosudnih organa

Ako je slučaj kompleksan, potrebno je edukovati sve prisutne u sudnici (sudiju i porotu) u svakoj fazi suđenja (parnice). Edukacija treba da obuhvati [53]:

- proveru usklađenosti sa naučnim principima,
- proveru zakonske prihvatljivosti digitalnih dokaza i saslušanja IKT veštaka pre glavnog pretresa,
- primenu principa uviđaja; uvodnu izjavu,
- svedočenje/veštačenje IKT eksperta,
- unakrsno ispitivanje i završnu reč (izjavu) i
- zatvaranje svedočenja/veštačenja.

Važno je napomenuti da je potrebno da poznavanje alata sudije i porote bude na minimalnom nivou razumevanja, da nije neophodno da budu eksperti za svedočenje ili veštačenje.

Svaki slučaj zahteva da tužilac pažljivo razmotri šta treba da bude dokazano/opovrgnuto i ispita sve elemente optužnice, da bi obezbedio prezentaciju ubedljivih dokaza za svaki elemenat optužnice. Često postoji konflikt između praktičnih ograničenja na to šta se može dokazati ili opovrći (pobiti) i šta od alternativnih objašnjenja advokat odbrane može iskoristiti da unese razumnu sumnju u dokazni postupak ili dokaze.

Šta jedan tužilac treba da opovrgne zavisi od samog pitanja i snage preostalih dokaza u slučaju. Na primer, u slučaju dečije pornografije, kada je bitan elemenat poznat, može se opovrći tvrdnja odbrane da su slike uskladištene u računar osumnjičenog bez njegovog znanja, jer nije razumno prihvatiti alternativu, tj. da su se u njegovom računaru slike pojavile same po sebi.

Važno pitanje je kada izabrati trenutak pobijanja tvrdnji odbrane. Na primer, ako je znanje osumnjičenog o sadržaju računara značajno, ponekad je „mudro” dopustiti da osumnjičeni pokrene pitanje i da sami dokazi (bilo kroz unakrsno ispitivanje, ili u ponovljenom procesu) pobiju ovu tvrdnju, pre nego što se opovrgavanje dokaza izvrši u glavnom pretresu.

3.6 Izbor postojećih alata

Na osnovu iskustva u radu sa studentima i mogućnostima različitih alata izabrani su sledeći alati za korišćenje u 3D virtuelnoj forenzičkoj laboratoriji:

- Od komercijalnih alata dva najzastupljenija koja predstavljaju standard (Encase v7 i FTK v4).
- Od besplatnih (open source) DF distribucija koje sadrže bogatu kolekciju DF alata (DEFT 7.2, SIFT 2.14).
- Od besplatnih (open source) distribucija opšte namene sa dosta korisnih alata za DF Backtrack R5.

4 Virtuelna okruženja

Ovo poglavlje daje pregled virtuelnih okruženja. Date su osnovne definicije, prikazana su virtuelna okruženja, potrebni uslovi za početak njihovog razvoja, vrste 3D virtuelnih okruženja i njihova razlika.

4.1 Definicije

Postoje mnoge definicije za pojam “virtuelno okruženje”. Neki autori su veoma restriktivni i definišu virtuelno okruženje kao “trodimenzionalno, multisenzorsko, „immersive“, „real time“ (okruženje za rad u realnom vremenu) i interaktivno okruženje koje se može „doživeti“ od strane korisnika putem trodimenzionalnih ulaznih i izlaznih uređaja” [1].

Schroeder je opisao virtuelno okruženje kao “kompjuterski generisani ekran koji dozvoljava ili primorava korisnika (ili korisnike) da imaju osećaj da su prisutni u okruženju u kome se stvarno ne nalaze, i da komuniciraju sa tim okruženjem.” [2] Ukratko, on je dao više apstraktnu definiciju koristeći frazu “biti tamo”. Kasnije je definicija proširena za višekorisnička okruženja za saradnju i učenje gde su korisnici prisutni u istom okruženju u interakciji sa drugim učesnicima, i koristi izraz “biti tamo zajedno” [3]. Schroeder je napisao da se njegova definicija “fokusira na čulno iskustvo”. Ako se senzorski element doživljava kao mesto ili prostor u kome korisnik nije fizički prisutan, ili kao doživljaj da drugi ljudi nisu tamo, tada sve što je navedeno u ovoj definiciji postaje besmisleno.” On je definisao virtuelne svetove kao konstantno virtuelno okruženje “u kome ljudi doživljavaju druge ljude kao da su tamo zajedno – i gde oni mogu da komuniciraju sa njima”. Prema tome, virtuelna okruženja ljudi doživljavaju posle nekog vremena kao veliku zajednicu sa kojom će zajedno postati okruženje za društvenu interakciju [4].

Postoje tri aspekta definisanja virtuelnih okruženja:

- Prisutnost,
- Konstantnost,
- Društvena interakcija.

Castronova je napravio rezime o funkcijama virtuelnih okruženja koja takođe moraju da imaju pomenuta tri aspekta koje on naziva: fizikalnost, upornost i interaktivnost [5].

Prentice je uneo još jednu dodatnu stavku, a to je interakcija sa drugima u okruženju koja podrazumeva korišćenje onlajn ličnosti preko “avatara” [6].

Ova četiri aspekta su detaljnije objašnjena u nastavku rada.

4.1.1 Fizikalnost

Ljudi pristupaju programu preko interfejsa koji simulira za njih fizičko okruženje na njihovom kompjuterskom ekranu. U virtuelnom okruženju vladaju isti prirodni zakoni kao i na Zemlji. Zato na primer chat soba ne bi mogla biti virtuelni svet jer tu nema zakona fizike. Bartle kaže da to može biti samo deo virtuelnog sveta koji se koristi kao drugi komunikacioni kanal slično kao glas ili video [7].

4.1.2 Konstantnost

Program mora da ima opciju za nastavak rada bez obzira da li neko trenutno koristi okruženje ili ne. Mora da pamti lokaciju ljudi i stvari kao i vlasništvo nad određenim objektima. Dakle virtuelni svet radi odvojeno, ali u realnom vremenu paralelno sa stvarnim svetom. Osoba u stvarnom svetu sarađuje sa osobom u virtuelnom svetu koja predstavlja realnu osobu.

4.1.3 Interaktivnost

Virtuelni svet može biti pokrenut na jednom kompjuterskom sistemu, ali mu istovremeno veliki broj ljudi može pristupiti na daljinu (preko Internet konekcija), gde ulazna komanda jednog korisnika može uticati na komandne rezultate drugih ljudi. Dakle, interakcija sa svetom se odvija u realnom vremenu [6]. Interaktivnost je jedan od glavnih aspekata za korišćenje virtuelnih okruženja za saradnju, edukaciju i sticanje veština.

4.1.4 Predstavljanje

Jedna od osnovnih mogućnosti virtuelnog okruženja je da se prikaže pogled korisnika gde svaki korisnik ima sopstveni pogled na isto okruženje i gde se avatari korisnika personalizovani. Avatari su prvi put uvedeni još 1985-te za opisivanje vizualno “prisutnih” korisnika u sajber prostoru tj. u virtuelnom svetu “Habitat”. Originalni termin avatar je iz Hindu mitologije i to je naziv za privremeno telo koje bog “nastanjuje” tokom posete zemlji. Drugi sinonimi za avatara su: likovi, igrači, virtuelni glumci ili virtuelni ljudi [8]. Govor tela čoveka je veoma važan za

dobijanje više informacija o osećanjima i može se dogoditi ako osoba govori o nečemu pozitivnom ili negativnom kao i da li je srećna ili tužna. Govor tela takođe intenzivira govor i čini komunikaciju izraženijom. Avatari su potrebni da bi obezbedili takvu informaciju u virtuelnom prostoru. U vreme društvenih okruženja i povećanjem performansi računarske grafike avatari su postajali sve više i više „realni”. Oni su u mogućnosti da se izraze kroz govor tela kao što su gestovi ili izrazi lica.

Perlin je opisao skup alata i tehnika na Univerzitetu u Njujorku krajem 1990. godine. On je takođe ukazao na značaj da se “kreiraju aplikacije koje uključuju animirane likove koji se ponašaju, reaguju i odgovaraju korisniku na način koji prenosi raspoloženje i emocije” [9].

4.2 Tipovi virtuelnih okruženja

Korisnik kroz virtuelno okruženje koristi tehnike kompjuterske grafike da predstavi model okruženja od „full-Immersive“ virtuelnog okruženja do tradicionalne desktop aplikacije koja nije u potpunosti „immersive“. Razlike između okruženja postaju nebitne, ali sve varijante virtuelnih okruženja biće važne u budućnosti. Pregled različitih vrsta virtuelnih okruženja dat je u nastavku rada.

4.2.1 “Full-Immersive” Virtual Environment

Rano interesovanje za istraživanja 3D okruženja bila su fokusirana na “Immersive virtuelna okruženja”. Termin “immersive” ili “sensor-immersive” su okruženja koja zahtevaju skupi hardver i kompjuterski generisan senzorski ulaz, kao što je head-mounted displej (HMD) [10]. Takvo okruženje omogućava korisniku da stekne puni osećaj svesnosti (prisutnosti, postojanja) u veštačkom simuliranom trodimenzionalnom okruženju, koji je u potpunosti generisan od strane kompjutera.

Sa tehničke strane gledišta, zahtevi “immersive” virtuelnog okruženja su izolacija ljudske percepcije od uticaja realnog sveta, kao i stimulisanje ljudske percepcije da se postigne željena iluzija o nepostojećem okruženju [11].



Slika 4.1 Izgled HMD-a

HMD je bio prvi uređaj koji je obezbedio korisnicima vizualni “immersion” (slika 4.1). Godine 1965. Evan i Sutherland su prikazali HMD. Prošlo je više od 20 godina od uvođenja prvog komercionalno dostupnog HMD-a (“EyePhone” sistem). Važne karakteristike HMD-a koje ih razlikuju od drugih displeja su kao prvo korisnikov pogled na virtuelno okruženje. HMD se montira na glavu tako da korisnik može da razgleda okolo realno okruženje. Drugo, oni daju stereoskopsku sliku gde korisnik okreće glavu da razgleda simuliranu okolinu [12]. Međutim, korišćenje HMD-a nije moguće sa standardnom tastaturom i mišem. Zbog ove činjenice potrebni su novi uređaji za unos i interakciju u “immersive” okruženjima (rukavice - gloves koje omogućavaju šest stepeni slobode za interakciju sa virtuelnim objektima). Za razliku od tradicionalna dva stepena slobode (kao što je slučaj kod miševa), upotreba takvih ulaznih uređaja omogućava više intuitivnu navigaciju kroz “immersive” okruženje i informacije tri najvažnija čula vida, sluha i dodira [13].

Još jedan popularan koncept alternativa za “immersive” prikazivanje je “Cave Automatic virtuelna okruženja” (CAVE – virtuelna pećina) koja pruža iluziju “immersive” u sobi veličine kocke. CAVE je razvijena od strane Eletronic Visualization Laboratory (EVL) na Univerzitetu Illinois početkom devedesetih godina prošlog veka i bila je prvo virtuelno okruženje koje dozvoljava učešće više korisnika istovremeno. Stereo slike se projektuju na tri ili četiri zida i pod kocke. Koristeći posebne naočare sve je naizgled kao 3D slika gde jedan ili više korisnika ulaze i kreću se unutar CAVE-a. Pored toga sistemi za praćenje kontinuirano prilagođavaju stereo projekciju na osnovu trenutne pozicije korisnika [14]. U zavisnosti od različitog broja strana, virtuelno okruženje može biti “full-immersive” (pet zidova), ili “semi-immersive” (tri zida).

4.2.2 “Semi-Immersive” Virtual Environment

“Semi-immersive” sistem podrazumeva veliki ekran za projekcije, to je mali bioskop poput studija, gde publika može da deli osećaj kao da je na sceni, iako je navigacija obično u rukama iskusnog operatera [15]. Ovaj tip virtuelnih okruženja omogućava da više učesnika doživi simulirano okruženje projektovano na jedan ekran i predstavlja alternativu za korišćenje desktop “non-immersive” ekrana ili HMD-a. To znači da se pogled na okruženje projektuje na jedan ili više zidova prostorije. Veličina zida nije relevantna zbog perifernog vidnog polja (Field Of View FOV) korisnika, ukoliko virtuelni svet okružuje korisnika. Ključni faktor kod ovakvog virtuelnog okruženja je FOV, koji opisuje koliko korisnik može biti pokriven prikazom.

„Fully-immersive” virtuelna okruženja mogu da proizvedu potpuno virtuelno praćenje koristeći FOV tehnologiju. Kod „semi-immersive” virtuelnih okruženja, ukoliko korisnici okreću glave, praćeni ili ne, oni će naglo izaći iz virtuelnog okruženja jer ekran ispred njih ne može da prati njihovo kretanje.

4.2.3 “Desktop-Immersive” Virtual Environment

Iako su “fully-immersive” virtuelna okruženja okupirala pažnju mnogih istraživača tokom devedesetih godina prošlog veka, istraživanja u “non-immersive” odnosno “desktop-immersive” virtuelnim okruženjima su takođe postala veoma važna. Budući da su grafičke mogućnosti standardnih računara poboljšane a i smanjena je cena za jake računare i grafički hardver, omogućeno je korišćenje desktop računara. Razvoj “desktop-immersive” virtuelnih okruženja zahteva hardver koji je deo tradicionalnih kompjuterskih sistema, a najveći deo njih je relativno jeftin.

VR tehnologija je dostupna svima koji poseduju “običan” računar [10] sa tradicionalnim ulaznim uređajima kao što su miš i tastatura. Ipak ekran na “desktop-immersive” okruženju pokriva samo mali deo korisničkog FOV-a i prikaz vizualnog “immersion” je ograničen.

4.2.4 “Tele-Immersive” Virtual Environment

Posebna grupa “immersion” se zove “Tele-immersion” ili “immersive tele-presence” i koristi se za svakodnevnu upotrebu u telekomunikacijama i drugim oblastima mrežnih usluga. “Tele-immersion” se definiše kao zajednica audio i video konferencije, umrežena kolaborativnim okruženjem. Cilj “tele-immersion” nije da reprodukuje licem u lice sastanak, već da omogući saradnicima širom sveta da rade zajedno u zajedničkom virtuelnom okruženju [16]. Ovo

zajedničko okruženje može biti trodimenzionalno okruženje koje fizički ne postoji ili se fizički ne može posetiti, ali je u stanju da pruži snažan osećaj prisustva u zajedničkom prostoru [17]. Na primer, “immersive” telekonferencijski sistem obezbeđuje “immersive” telesnu prisutnost u zajedničkom virtuelnom okruženju u kojem učesnici imaju utisak prisutnosti. “Tele-immersion” ne znači samo da učesnici sede ispred displeja na kome se prikazuje snimak njihovih kolega. U stvari, oni sede oko zajedničkog virtuelnog stola, jedan pored drugog koristeći veliki displej, koji pokriva skoro ceo ugao gledanja od strane korisnika, prikazujući prirodnu veličinu slike učesnika. Ove okolnosti obezbeđuju prirodnu reprodukciju kontakata očima i govora tela, kao da sarađuju na efikasan i prirodan način [11].

“Tele-immersive” teži kolaborativnom pristupu, međutim ova vrsta tehnologije se fokusira na potpuno “immersed” telesnu prisutnost baziranu na avataru. Potpuna “immersive” telesna prisutnost znači simulirano zajedničko okruženje koje koristi displej korišćenjem FOV-a i CAVE-a. Tabela 4.1 pokazuje vidno polje različitih tipova displeja koji se koriste u prethodno objašnjenim virtuelnim okruženjima [18].

Tip displeja	Ugao vidljivosti (aproksimativno)
Standardni kompjuterski monitor	20-40°
HMD	30-80°
Veliki monitor na zidu	100-140°
CAVE	više od 360°

Tabela 4.1 Stepen vidljivosti u različitim vrstama okruženja

4.3 Svrha virtuelnih okruženja

“Projektovanje, izgradnja, i upravljanje virtuelnim okruženjima je jedan od najizazovnijih zadataka za korisnike računara i Interneta“. Programeri mogu uzeti u obzir mnoge aspekte kreiranja virtuelnih okruženja, ali prvo pitanje na koje moraju da odgovore je: Zašto neko želi da izgradi virtuelni svet i šta je njegova svrha [8]. Ranije tehnologije su bile telefon, radio, film a kasnije TV. Potom su došli kompjuteri sa softverom, kao i virtuelni svetovi. Virtuelno okruženje kombinuje sve aspekte svih tih ranijih tehnologija, stvarajući novo iskustvo [24].

Steve Prentice (potpredsednik Gartner, Inc.) opisuje svoju firmu kao vodeću svetsku firmu za informacione tehnologije i konsalting. U njegovom radu “Virtuelni svetovi – Šta da očekujete u 2009” Prentice navodi uloge virtuelnih okruženja i njihova ciljna tržišta. “Virtuelni svetovi obuhvataju širok spektar okruženja, namenjen za izrazito različite svrhe” [6], a to su:

- Virtuelni svetovi fokusirani na potrošače (Consumer focused virtual worlds),
- Virtuelni svetovi fokusirani na edukaciju (Education focused virtual worlds),
- Virtuelni svetovi fokusirani na preduzeća (Enterprise focused virtual worlds).

4.3.1 Virtuelna okruženja u obrazovanju

Virtuelna okruženja se koriste u akademskim istraživanjima i simulacijama već dugi niz godina.

Simulacije

Virtuelna okruženja su kreirana da simuliraju realna okruženja kao što su na primer simulacije letenja. Prentice je istakao da imaju posebnu vrednost u realnom svetu gde je delatnost opasna, skupa ili kompleksna [6].

Uloge i scenariji

Na osnovu simulacije realnog okruženja za obuku, uloge i scenarija, pojedincima je omogućena višestruka interakcija u zajedničkom virtuelnom prostoru. Oni je često koriste i priznaju za efikasne obuke u okruženju (vojne vežbe, hitne službe i katastrofalni scenariji) [6].

Prednosti su niski troškovi, bezbednost i sposobnost da se ponovi scenario više puta. Lako je kreirati pomoću virtuelnih okruženja različite scenarije za više uloga i prilagoditi ih određenim situacijama.

Podučavanje

Kluge i Riley su istakli da je pojava onlajn virtuelnih okruženja stvorila nove uzbudljive mogućnosti kao izazov za predavače. Zbog ovakvih okolnosti mnogi univerziteti koriste informacione tehnologije i eksperimentišu sa virtuelnim okruženjima [35]. Steve Prentice je napisao u izveštaju za Gartner da se “virtuelna okruženja sve više koriste za nastavu na svim nivoima obrazovanja od osnovnog do visokog i šire” [6].

4.3.2 Učenje u virtuelnom okruženju

Cynthia M. Calongne, profesor kompjuterskih nauka na Kolorado Tehničkom Univerzitetu, predavala je devet univerzitetskih kurseva uz pomoć okruženja Second Life kao obrazovne učionice do 2008. godine. Iz iskustva stečenih tokom ovih kurseva, došla je do zaključka da “uspešna virtuelna grupa zahteva mešavinu iskustava, tehnologija, alata, sadržaja, identiteta, angažovanja, strukture kursa, upravljanja rizikom, mentorstva, dobre orijentacije, kao i povratne informacije pri korišćenju alata”. Virtuelna okruženja pružaju “nove načine studiranja, diskutovanja, kreiranja i izražavanja studenata pod nadzorom i uz podršku instruktora” [36]. Virtuelni svet je kombinacija sledećih funkcija:

- Lično: prilagođavanje avatara;
- Istraživanje: kretanje po svetu;
- Komunikacija: razmena informacija sa drugima;
- Navigacija: gledanje 3D sadržaja;
- Interakcija: korišćenje 3D objekata;
- Kreiranje: dizajn grupnog projekta;
- Isporuka: davanje projekata instruktoru;
- Procena: ocenjivanje projekta u Second Life;
- Povratna informacija: izveštaj o napretku.

4.3.3 UTBot–3D kao pedagoško sredstvo

Drugi pristup za korišćenje virtuelnih okruženja kao pedagoškog sredstva u obrazovanju jeste da studenti razviju osnovne delove ili objekte virtuelnog okruženja. Prednost je u tome što su oni u stanju da odmah vide rezultate.

Sledeći primer opisuje ovu ideju: odsek za računarske nauke na univerzitetu Kyonggi u Južnoj Koreji održao je kurs za dizajn platforme nastavnog agent sistema. Iz tog razloga oni su uveli UTBot virtuelnu agent platformu koja “predstavlja klijenta za Unreal Tournament server igre i Gamebots sistem.”

Trebalo je da studenti razviju inteligentne virtuelne agente na toj platformi i da samostalno igraju UT igre [37]. Za početnike je bilo prilično teško da izgrade inteligentni virtuelni softverski agent, jer je dosta posla na niskom nivou bilo potrebno uraditi. Ovo je izazvalo probleme početnicima da završe svoj projekat u trajanju kursa od tri meseca. Iako je bio težak zadatak studenti su i dalje radili sa velikim podsticajem (konkurencija između različitih studentskih timova). Ocena za projekat je bila određena položajem tima na turniru i kvalitetom njihovog konačnog izveštaja i prezentacije” [37].



Slika 4.2 Finalni meč na turniru na kraju kursa

Iskustva učenja pomoću UT Bota kao sredstva, su bila izuzetno pozitivna (slika 4.2).

4.4 Primena Second Life-a u edukaciji, zabavi, nauci

Zbog velike popularnosti Second Life (SL) okruženja dat je pregled značajnijih primena u različitim oblastima.

„Kinesko selo“

Na kineskom univerzitetu kreirano je drevno kinesko selo (primena 3D virtuelnog okruženja u edukaciji). 3D okruženje za virtuelno učenje je podeljeno na 6 celina. U svakoj celini okruženja za virtuelno učenje se nalazi 6 zgrada, u kojima se nalaze materijali vezani za svako predavanje. Svako predavanje odgovara jednom od 6 specifičnih strategija koje se dešavaju u nekoj od 6 „ratnih” situacija [57].

Šest “ratnih” situacija:

1. “superiorna pozicija”,
2. suočavanje,
3. napad,
4. „zbunjujuća situacija“,
5. zauzimanje teritorije,
6. “očajna situacija”.



Slika 4.3 Amfiteatar za virtuelno predavanje



Slika 4.4 Primer učionice sa postavljenim lekcijama

Konferencija na temu „edukacija u virtuelnoj realnosti“

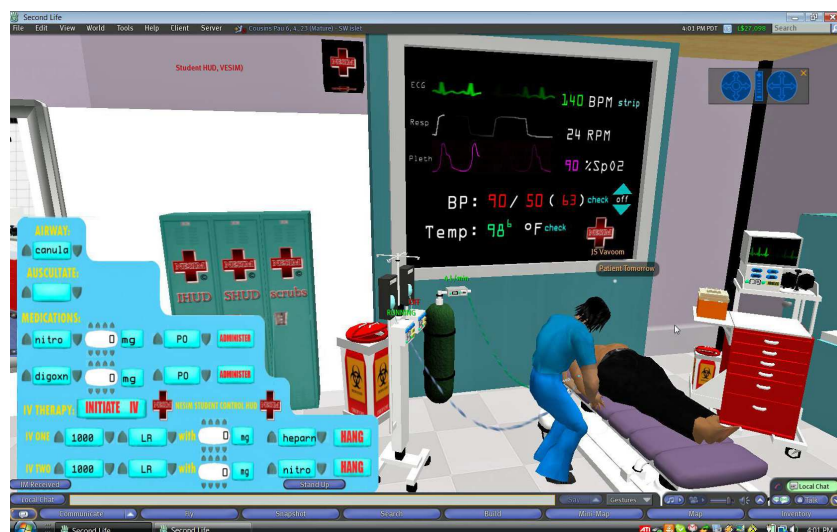
Još jedna interesantna primena 3D okruženja za edukaciju je konferencija koja je organizovana u Second Life-u na temu „*edukacija u virtuelnoj realnosti*“ a koju je za dva dana posetilo preko 5000 avatara. Konferencija je prvi put održana 2007. godine. Prošle godine je održana u decembru i privukla je veliki broj ljudi zaposlenih na fakultetima, nastavnike, trenere, administratore, programere, tehničke stručnjake, profesionalce koji stvaraju virtuelna okruženja ... Glavne teme konferencije su bile: šta je obrazovanje, šta je učenje, kako poboljšati kvalitet učenja u Second Life-u.



Slika 4.5 Virtuelna konferencija

Virtuelna ambulanta Tacoma Univerziteta

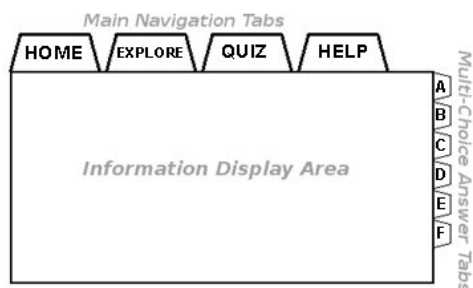
Studenti internisti Tacoma univerziteta mogu da prisustvuju laboratorijskim vežbama, i mogu kontaktirati virtuelne pacijente čiji je život ugrožen. Nakon prikupljanja informacija o pacijentu studenti leče pacijenta koristeći sopstveno znanje. Simulacija dozvoljava da studenti reaguju u odnosu na situaciju. Oni mogu da izaberu koji lek i instrumente da koriste, a zatim da prate posledice i shodno tome prilagode lečenje. Ovo je veoma značajno zbog toga što se komplikovane i teške vežbe odigravaju u bezbednom okruženju gde život pacijenta nije ugrožen [58].



Slika 4.6 Vežbe u virtualnoj ambulanti

SLOODLE

Jedan od najzanimljivijih rešenja sistema za obrazovanje na daljinu je stvoren u okviru univerziteta West of Scotland Paisley. Oni su spajanjem Moodlea (Modular Object-Oriented Dynamic Learning Environment) i Second Life-a napravili novo okruženje SLOODLE (Simulation-Linked Object-Oriented Dynamic Learning Environment), koje je bazirano na radu sa kvizovima. Skraćeni naziv je QuizHUD (Heads-Up-Display). Kvizovi su kombinacija teksta i slika. Svaki student vidi QuizHUD na svom ekranu, koji prikazuje posebno izrađen Web sadržaj sa relevantnim informacijama i pitanjima vezanim za određenu lekciju. Student prolazi kroz kviz onim tempom koji mu odgovara i ne smetaju mu ostali studenti koji se mogu nalaziti pored istog objekta u virtuelnom okruženju [59].



Slika 4.7 Šematski prikaz QuizHAD-a

Virtuelno ostrvo Pacifik Univerziteta

Veliki broj univerziteta širom sveta je kreirao sopstveni virtuelni univerzitet na zasebnim ostrvima. Univerzitet Pacifik iz Tenesija je među prvima uporedio klasičan način učenja sa učenjem u okruženju Second Life. Univerzitet ima ostrvo u Second Life-u sa kompleksom koji se sastoji od nekoliko zgrada. U jednoj od tih zgrada se nalaze amfiteatri za predavanja. Učionica se sastoji od podijuma na kojem se nalazi mesto za avatara predavača, velike table na kojoj se prikazuju Power Point prezentacije i mesta za avatare studenata.



Slika 4.8 Prikaz Second Life učionice univerziteta Pacifik

Prilikom diskusije o iskustvu prilikom korišćenja Second Life-a, studenti su izneli sledeće nedostatke: prevelika sloboda avatara i nemogućnost profesora da ih kontroliše, usporavanje aplikacije za četovanje zbog preterivanja u vođenju razgovora koji se ne odnose na temu predavanja i nemogućnost da se uvek razlikuje tekst predavača od teksta studenata.

4.5 Primena Open Wonderland-a u edukaciji, industriji, zabavi

Open Wonderland je besplatan skup alata otvorenog koda baziran na programskom jeziku Java za kreiranje kolaborativnih 3D virtuelnih okruženja.

4.5.1 Virtuelno okruženje za eksperimente iz fizike

Tehnološki univerziteti iz Graca, Perta i Kembridža (SAD) su kreirali VE za eksperimente iz fizike. Njihovo zajedničko virtuelno okruženje daje dobre rezultate zahvaljujući integraciji eksperimenata iz fizike dostupnih na Internetu (ILabs) i alata dostupnih u Wonderland-u. Studenti i profesori su predstavljeni kao avatari, i zahvaljujući virtuelnom okruženju mogu da kontrolišu opremu koja se koristi za eksperimente, da vide rezultate svog rada i da o tome diskutuju.

Ovo virtuelno okruženje omogućava dostupnost laboratorije studentima 24 sata svakog dana. Korišćenje virtuelne laboratorije je znatno jeftinije od prave laboratorije. Korisnici mogu pristupiti online laboratoriji iz bilo kog dela sveta. Između ostalog ciljevi ovog projekta su da olakša razumevanje prirode i dinamike elektromagnetnog polja i pojava koje se u njemu dešavaju [60].

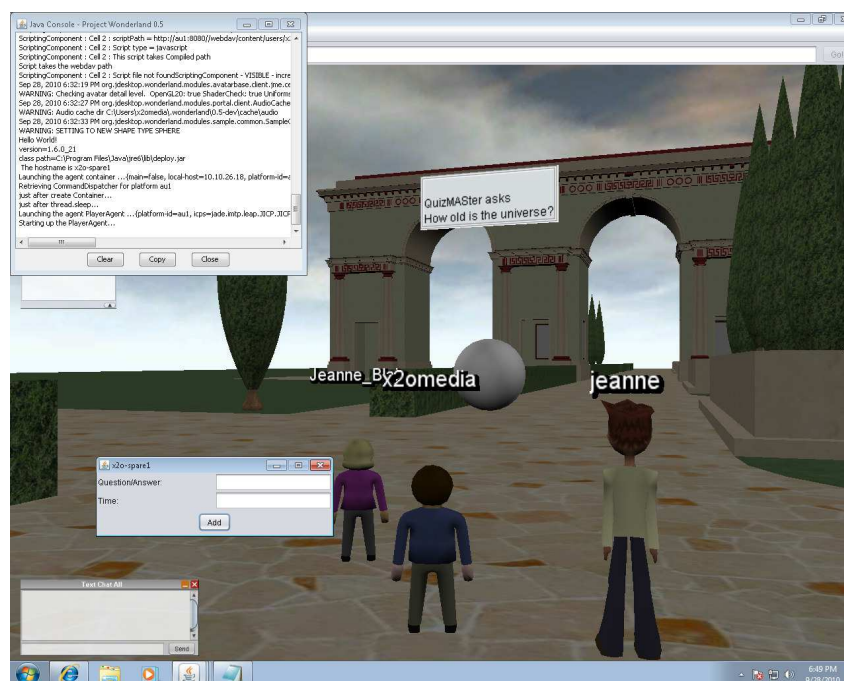


Slika 4.9 Prikaz elektromagnetnog polja

Tokom eksperimenta u virtuelnom okruženju studentima je omogućeno da vide nevidljive linije magnetnog polja (što u realnom eksperimentu nije moguće). Studentima je u virtuelnom okruženju omogućeno da menjaju parametre kao što su amplituda i frekvencija. Ovo okruženje ima opciju tekstualnog chat-a koja studentima pruža mogućnost komunikacije u toku i nakon eksperimenta.

4.5.2 QuizMAster

Zanimljivo 3D virtuelno okruženje napravljeno je na univerzitetu Athabasca u Kanadi. Došli su do zaključka da bi virtuelno okruženje koje podseća na video igrice davalo bolje rezultate od klasičnih virtuelnih okruženja. Koriste kvizove za proveru znanja i zbog toga su stvorili QuizMAster koji po uzoru na TV kvizove omogućava takmičenje većeg broja studenata. QuizMAster se sastoji iz dva osnovna elementa, QuizMAster posrednika i igrača. QuizMAster posrednik kontroliše igru i šalje pitanja svim takmičarima. Takmičari odgovaraju na pitanja koja se prosleđuju QuizMAster-u preko FIPA protokola. Igrači imaju ograničeno vreme za davanje odgovora. Ukoliko ne znaju odgovor na postavljeno pitanje ne moraju da odgovore, a pobednik je onaj koji najbrže da tačne odgovore [61].

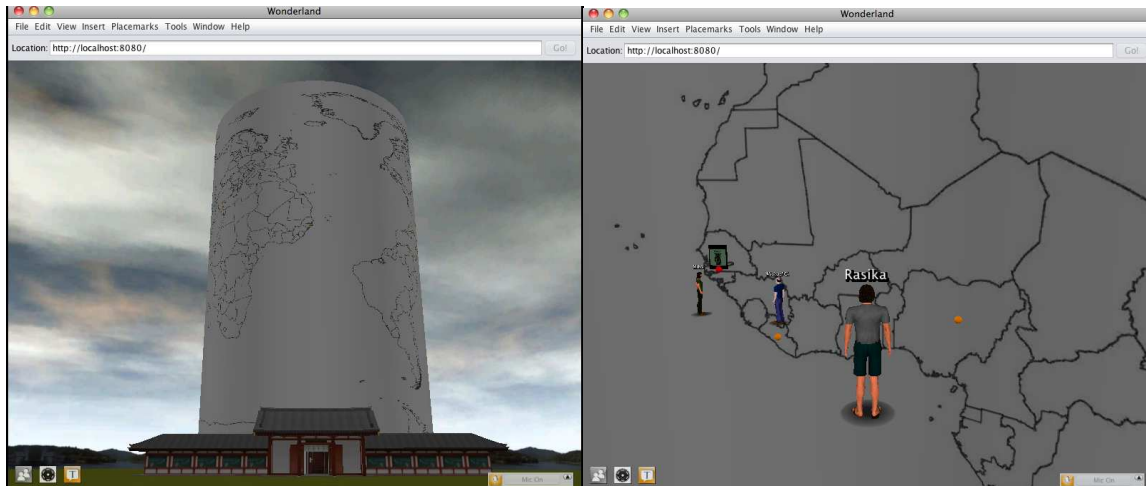


Slika 4.10 Grupa igrača i proglašenje pobednika u QuizMAster-u

4.5.3 Virtuelno okruženje „Folkways in Wonderland“

U Japanu je stvoreno virtuelno okruženje „Folkways in Wonderland“ za istraživanja u etnomuzikologiji. Pretraživanje muzike u ovom virtuelnom okruženju se obavlja preko karte sveta koja je postavljena na cilindru. Muzičke numere su postavljene u zavisnosti od geografskog

položaja (mesto izvođenja, stil...), track markeri su postavljeni na mapi na tačnoj geografskoj širini i dužini. Ovi markeri su u isto vreme i izvori zvuka [62].



Slika 4.11 Prikaz mape na kojoj su locirane muzičke numere (slika levo); Mapa sa avatarima koji se trenutno nalaze u Zapadnoj Africi (slika desno).

Virtuelno okruženje omogućava da više korisnika u istom trenutku sluša muziku a komunikacija glasom im je omogućena preko chat-a. Avatari čuju sve izvore zvuka unutar virtuelnog okruženja i slobodno istražuju virtuelno okruženje koristeći tastaturu i miš.

4.5.4 Sheet suite

Ovo okruženje daje mogućnost predavaču da kreira veći broj pitanja, kako otvorenog tako i zatvorenog tipa. Pitanja su prikazana u virtuelnom okruženju na malim ekranima koji se nalaze iznad avatara [63].



Slika 4.12 Virtuelno okruženje „Sheet suite“

Osim Web alata koji se koristi za uređivanje pitanja postoji i alat za prikupljanje ostvarenih rezultata koji se mogu prikazati u tabelama.

4.5.5 MiRTLE

Interesantno rešenje je napravljeno na Univerzitetu Essex pod nazivom MiRTLE koje obezbeđuje mešovito realno okruženje sa kombinacijom lokalnih i udaljenih učenika koji istovremeno slušaju predavanja. Cilj je da se kod udaljenih studenata podstakne osećaj zajedništva i da se poveća motivacija za učenje u virtuelnom okruženju. Ovaj projekat je pokazao da je uticaj na lokalne studente mali ali se broj studenata u virtuelnom okruženju naglo povećao. Glavni razlog povećanja broja studenata u virtuelnom okruženju jeste mogućnost spontane interakcije između udaljenih i fizički prisutnih studenata [64].



Slika 4.13 Virtuelna učionica u ranoj fazi projekta MiRTLE

4.5.6 SIMiLLE

SIMiLLE projekat ima drugačiji pristup u tome što koristi jednu od ključnih karakteristika virtuelnih okruženja, a to je da bude u mogućnosti da simulira nova i postojeća okruženja što dovodi do povećanja efikasnosti učenja. Jedan od ciljeva ovog projekta je da ispita tehničku mogućnost i pedagošku vrednost korišćenja virtuelnih okruženja za pružanje realnog socio-kulturnog sadržaja za učenje drugog stranog jezika [65]. Projekat je napravljen radi olakšanog učenja jezika, zato što se optimalan nivo učenja distiže tek kada studenti uđu u srž kulture naroda koji govori taj jezik.

4.5.7 WonderSchool

Online škola koja koristi mogućnost Open Wonderland-a da pokreće deljene aplikacije unutar samog virtuelnog okruženja [66].



Slika 4.14 Wonder School

4.5.8 Games Village

Programerima video igara je omogućeno da predstavljaju svoje igre u okruženju Singapore Games Village razvijenom od strane Games Solution Center iz Singapura. Oni ne nude samo prostor za prikazivanje već i tehnološku podršku: softver, hardver, alate, pomoć iskusnih programera, testiranje igrica ... Games Village je “napravljen” oko reklamnog stuba na kome se prikazuju igrice koje se mogu igrati koristeći browser ili mobilni uređaj. Ukoliko neko igra igru, ostali koji se nalaze u blizini mogu da posmatraju kao i da sami odigraju deo igre (preko svojih avatara).



Slika 4.15 Games Village

Pored toga reklamni stubovi mogu biti napravljeni tako da se na njima prikazuju reklamni spotovi koje posetioци virtuelnog okruženja mogu da vide. Moguće je staviti plakate sa obe strane prostora za igranje, podatke o igrici i programeru, kao i eksterni link ka Web stranici programera.

5 3D okruženja u edukaciji

U ovom poglavlju je definisan koncept 3D okruženja i posebno kolaboracija i učenje. Predstavljena su 3D virtuelna okruženja i dat je uporedni pregled njihovih mogućnosti. Na kraju poglavlja izabrano je odgovarajuće okruženje za realizaciju.

5.1 Uvod u virtuelna 3D okruženja

Višekorisnička virtuelna okruženja (MUVE Multi User Virtual Environment) se definišu kao kompjuterski programi koji pružaju mogućnost simulacije, vizualizacije, virtuelizacije, animacije ... Virtuelni prikaz korisnika (avatar) može da se kreće i gleda na objekte iz različitih uglova u određenom VE. Da bi razvio odnos prema okruženju i drugim učesnicima, svaki korisnik ima svoj sopstveni virtuelni identet i mora biti online vidljiv drugim korisnicima. MUVE okruženja podržavaju asinhronu i sinhronu komunikaciju. Korisnici svesni prisustva drugih korisnika mogu da koriste ćaskanje i ponekad VOIP za komunikaciju sa drugima [38].

Postoji više definicija za 3D okruženja. U radu [39] data je sledeća definicija: "Virtuelno okruženje je kompjuterski zasnovano, simulirano multimedijalno okruženje, koje se obično prikazuje preko Weba, i dizajnirano je tako da korisnici mogu da "stanuju" i vrše interakciju preko avatara".

Trodimenzionalno virtuelno okruženje [40] je nova tehnologija u razvoju i koristi se za učenje i nastavu. 3D virtuelno okruženje se definiše i kao: "umrežena desktop virtuelna stvarnost u kojoj se korisnici kreću i komuniciraju u simuliranom 3D prostoru."

Radovi [40], [41] uključuju u definiciju 3D edukacionih okruženja i sledeće karakteristike:

- Interaktivnost

3D okruženje u kome učesnici mogu da komuniciraju sa virtuelnim objektima i međusobno.

- "Embodiment"

Avatar se može objasniti kao vizualno predstavljanje korisnika u 3D virtuelnom okruženju. Avatari međusobno komuniciraju, slobodno se kreću u okruženju i komuniciraju sa postojećim objektima uz prisustvo kamere.

- Podrška komunikaciji

Obavezne su sinhronne aplikacije kao što je tekstualni čat ili glas preko IP-a. Asinhroni alati takođe mogu biti dostupni.

Virtuelni 3D svetovi su dostupni ili koristeći browser ili preko samostalnih klijentskih aplikacija i ispunjavaju Web 3D standarde. Prema rečima Nigel (2007) Web 3D se definiše kao: “generički termin koji se obično odnosi na trodimenzionalnu (3D) grafičku tehnologiju podržanu od strane World Wide Weba (WWW).” Primeri za takve tehnologije su Virtual Reality Modeling Language (VRML), eXtensible 3D (X3D) i Java3D.) VRML i X3D otvoreni ISO standard.

5.2 E-učenje i 3D okruženja

3D virtuelna okruženja se koriste za učenje kada su korisnici međusobno udaljeni ili kada korisnici imaju određena ograničenja, a sve u cilju smanjenja troškova i ispunjenja odgovarajućih uslova [42]. Pojedini autori tvrde da za razliku od tradicionalnog obrazovanja (licem u lice), obrazovanje putem 3D virtuelnih okruženja navodno koristi manje vremena za sticanje znanja i postiže bolje efekte učenja [43]. U radu [44] su prikazani pozitivni rezultati korišćenja 3D okruženja:

- Jednostavnost komunikacije

Virtuelna okruženja koja se trenutno koriste obično nude ugrađeni VOIP koji olakšava komunikaciju između samih studenata kao i studenata i nastavnika.

- Osećaj zajedništva

Student se emotivno vezuje za svog avatara i u stanju je da komunicira sa drugim avatarima. On ima svoju sopstvenu percepciju pripadnosti datoj zajednici.

- Mogućnost kombinovanja kompjuterskih aplikacija

Integrisanje postojećih Learning Management Systems (LMS) u virtuelno okruženje nudi prednosti obe tehnologije. Primer takve implementacije je SLOODLE platforma.

- Simulacija

Daleko je lakše i jeftinije koristiti simulatore u 3D okruženjima za učenje dok se ne postignu određeni rezultati a onda nastaviti sa realnim uređajima u fizičkom okruženju.

- Uglovi gledanja

Uglovi gledanja su veoma bitni za dizajn složenih objekata kao i za kretanje u kompleksnim okruženjima.

- Nezavisnost od mesta i vremena

Sposobnost avatara da se teleportuju sa jednog mesta na drugo čini mogućim da se virtualno putuje kroz vreme i prostor. To se može iskoristiti u predmetima kao što su istorija, geografija ili arhitektura, kao i jezik, kulturna edukacija itd.

- Deljenje znanja

Mogućnost posmatranja studenata dok rešavaju složene probleme izaziva kod drugih studenata osećaj da i oni mogu to da savladaju na isti način.

Sanders i McKeown predstavljaju prednosti virtuelnog društvenog prostora koji studenti doživljavaju koristeći svoje 3D edukaciono okruženje. “Studenti znaju i mogu da vide kada su njihove kolege prisutne u VE. Oni mogu da se kreću, komuniciraju i kroz interakciju kreiraju zajedničko znanje” [46].

Ang i Wang [45] tvrde da IKT a naročito virtuelna okruženja povećavaju interesovanje studenata za rešavanje složenih problema. Oni su testirali svoju tvrdnju tako što su studenti sa slabijim uspehom koristili 3D virtuelna okruženja za rešavanje određenih problema i projekata i postigli bolje rezultate.

U istraživačkom radu [47] K. Holmberg i Huvila su izjavili: “Second Life stvara realniji osećaj prisustva nego diskusioni forumi ili čet sobe”.

5.3 Postojeća 3D virtuelna okruženja

U prethodnom delu rada dat je pregled primene 3D okruženja (Second Life i Open Wonderland) u različitim oblastima primene. U sledećem delu rada biće dat opis i poređenje najčešće korišćenih 3D okruženja.

5.3.1 Prikaz postojećih 3D virtuelnih okruženja

Second Life

Second Life je najpoznatije virtuelno okruženje dostupno na Internetu. Kreirano je 2003. godine od strane kompanije Linden Research Inc. (Linden Lab). Postoje dve vrste korisničkih naloga: besplatni (Basic) i Premium nalozi koji se od besplatnih razlikuju po tome što se, uz fiksni iznos koji se plaća mesečno za održavanje, korisnicima dodeljuje virtuelno zemljište površine od 512 m². Moguće je kupiti i veće parcele, pa čak i cela ostrva, ali su cene vrlo visoke. Takva virtuelna okruženja najčešće iznajmljuju velike firme, fakulteti, i drugi korisnici koji žele da investiraju u svoj virtuelni identitet.

Second Life je zamišljen kao virtuelni svet u kojem apsolutno sav sadržaj stvaraju korisnici. Kako bi se kreirala virtuelna okruženja, firma Linden Lab je ponudila LSL (Linden Scripting Language) jezik koji je po sintaksi sličan C-u i koji služi za proširenje funkcionalnosti virtuelnih objekata, a omogućuje i komunikaciju objekata s Internetom korišćenjem HTTP protokola.

Active Worlds

Active Worlds je vrlo fleksibilna tehnologija koja se temelji na nizu virtuelnih okruženja. Klijentska i serverska aplikacija su besplatne, ali kreiranje sopstvenih virtuelnih okruženja moguće je samo uz plaćanje naknade. Vlasnici virtuelnih okruženja naknadu plaćaju u zavisnosti od veličine svog okruženja i broja korisnika koji mogu istovremeno pristupiti virtuelnom okruženju. Klijentski softver je napravljen isključivo za Windows operativne sisteme. Komunikacija korisnika u virtuelnom okruženju je omogućena korišćenjem chata (tekst, glas). Za razliku od klijentskog, serverska aplikacija je dostupna na Windows, Linux i Solaris operativnim sistemima.

There

There (u vlasništvu firme Makena Technologies) je zamišljen prvenstveno kao mesto za razonodu i odmor. U osnovi There predstavlja društvenu mrežu, smeštenu u virtuelno okruženje. Korisnici mogu besplatno postati članovi There zajednice, što im pruža osnovnu funkcionalnost, slušanje radija, mogućnost kupovine virtuelnih objekata i pristupanja ograničenom broju

korisničkih grupa. Premium korisnički paket se plaća i nudi glasovnu komunikaciju, mogućnost prodaje objekata i održavanja društvenih događaja u virtualnom okruženju. Za kreiranje objekata koristi se jednostavan alat koji je također u vlasništvu firme Makena Technologies, a prodaja se obavlja aukcijski unutar samog virtualnog okruženja. Klijentski softver napravljen je isključivo za Windows operativne sisteme.

Open Wonderland

Projekat Open Wonderland pripada nizu Java Desktop open source projekata, a nastao je s ciljem izrade umreženih virtualnih okruženja namenjenih poslovanju i edukaciji. Klijentski softver omogućava svakom korisniku da unutar virtualnog okruženja u za to unapred određenom okviru koristiti 2D desktop aplikacije, bilo da se radi o komponentama raznih Office paketa, programima za pregled slika, filmova, zvuka ... To omogućava korisnicima da svoje dnevne poslove obavljaju unutar virtualnog okruženja. Za modeliranje se koriste poznati 3D alati kao što su Blender, 3Ds Max, Lightwave i Maya.

Croquet

Croquet predstavlja open source projekat nastao s ciljem stvaranja umreženih virtualnih okruženja namenjenih upravljanju projektima, obrazovanju, arhitekturi, dizajnu i kreiranju MMOG (Massive Multiplayer Online Game) igara.

Kaneva

Kaneva je vrlo fleksibilna tehnologija namenjena brzom i jednostavnom kreiranju virtualnih okruženja, sa naglaskom na MMORPG (Massive Multiplayer Online Role Playing Game) i MMOFPS (Massive Multiplayer Online First Person Shooter) igre. Postoji samo jedan tip korisničkih naloga, i to besplatan, za razliku od većine ostalih okruženja u kojima se to plaća. Korisnici pri registraciji dobijaju i svoje virtualne kuće. Iako je prvenstveno zamišljena kao rešenje za razvoj igara, Kaneva platforma može poslužiti i za razvoj virtualnih okruženja u oblasti obrazovanja.

Entropia Universe

Entropia Universe proizvod je švedske firme MindArk, a nastao je iz kompjuterske igre Project Entropia. Ovo virtualno okruženje nije opšte namene, već pripada porodici MMOG igara smeštenih u 3D virtualno okruženje. Entropia Universe nudi samo jedan tip korisničkih naloga (besplatan). Klijentski softver napravljen je samo za Windows operativne sisteme, a instalacioni paket zauzima čak 1 GB, zato što softver koristi veliki broj lokalno snimljenih tekstura i modela. Klijentski softver zahteva relativno moćan računar, ali nudi više mogućnosti.

Virtualni svet	Namena	Klijentska platforma	Serverska platforma	Podrška za kreiranje objekata
Second Life	opšta	Linux, Windows, Mac	Linux	odlična
Active Worlds	opšta	Windows	Windows, Linux	odlična
There	opšta	Windows	-	slaba
Open Wonderland	opšta	Linux, Windows, Mac	Linux, Windows, Mac	odlična
Croquet	opšta	Linux, Windows, Mac	Linux, Windows, Mac	odlična
Kaneva	sa podrškom za igranje	Windows	Windows	odlična
Entropia Universe	sa podrškom za igranje	Windows	-	nepostoji

Tabela 5.1 Pregled dostupnih virtualnih okruženja

5.3.2 Detaljan prikaz postojećih 3D virtualnih okruženja koja se koriste za edukaciju

Open Wonderland

Do februara 2010. godine Open Wonderland je bio projekat vođen od strane firme Sun Microsystems, zatim je prešao u neprofitnu organizaciju pod nazivom Open Wonderland

Foundation. Open Wonderland je otvorenog koda i koristi se besplatno. Baziran je na Java programskom jeziku i svako ko ga je savladao može da kreira i prilagodi virtuelno okruženje sopstvenim potrebama. Open Wonderland radi sa modulima koji omogućavaju potpunu promenu serverske aplikacije, administrator može da kreira sopstvene module, kao i da koristi već postojeće koji se nalaze u „skladištu modula“. Ovo omogućava potpunu promenu interfejsa i kao rezultat se može dobiti potpuno jedinstveno 3D virtuelno okruženje. Kao što je već ranije navedeno za modeliranje se koriste poznati 3D alati kao što su Blender, 3Ds Max (ColladaMax), Lightwave i Maya, Solid Works.

Klijentska aplikacija omogućava svakom korisniku da unutar virtuelnog okruženja u za to predviđenom okviru koristi nemodifikovane 2D desktop aplikacije, bilo da se radi o programima iz Office paketa, browserima, programima za pregled slika, filmova, muzike itd. Ove aplikacije daju veliku prednost ovom okruženju u odnosu na druge za korišćenje u oblasti obrazovanja. Cilj je obezbediti krajnjem korisniku funkcionalnu, sigurnu, stabilnu platformu za složene aktivnosti na polju obrazovanja.

Grafičko okruženje - Instaliranje klijentske aplikacije je veoma jednostavno. Po preuzimanju aplikacija se instalira automatski, jedini preduslov je da na računaru bude instaliran paket Java.

Glavni meni – Nalazi se u gornjem delu prozora i nudi širok spektar opcija, adaptaciju klijentskog interfejsa dodavanjem novih opcija na osnovnom prozoru i ubacivanje objekata i modula.

Korisnička lista - Predstavlja spisak svih aktivnih korisnika. Kada se izabere avatar moguće je izvršiti određena podešavanja (npr. jačina glasa na chat-u).

Chat panel - U ovom prozoru se prikazuje tekstualna komunikacija između korisnika.

Sistemske zahteve

Pokretanje aplikacije bilo da je u pitanju klijentska ili serverska, omogućeno je na svim operativnim sistemima što takođe predstavlja jedan od bitnih preduslova za korišćenje. Do skoro je serverska aplikacija mogla da radi isključivo na Linux ili Solaris operativnom sistemu. U tabeli 5.2 dat je prikaz minimalne hardverske konfiguracije za korišćenje Open Wonderland-a.

Sistemske zahteve – minimalna hardverska konfiguracija	
Operativni sistem	XP, Vista, Windows 7 MacOS, Linux, Solaris
Memorija	1GB
Procesor	1,5GHz
Internet	brzi link mora da postoji mrežna konekcija
Grafička karta	NVIDIA sa najmanje 128 MB 256 MB za bolje performanse

Tabela 5.2 Minimalna hardverska konfiguracija za Open Wonderland

Ograničenja u Open Wonderland-u

Open Wonderland zahteva minimum 1GB radne memorije, što isključuje korišćenje starijih računara. Međutim da bi sistem radio optimalnom ili zadovoljavajućom brzinom neophodno je imati 2GB radne memorije. Takođe preporučljivo je koristiti grafičke kartice NVidia ili ATI a ne integrisane grafičke kartice. Ovakvi hardverski zahtevi smanjuju broj potencijalnih korisnika.

Second life

Second Life je napravila Linden laboratorija, juna 2003. godine i prema poslednjim podacima ima oko 15 miliona registrovanih korisnika. To je virtuelno 3D digitalno okruženje, koje koristi sve mogućnosti Interneta. Second Life pruža korisnicima mogućnost slobodnog kretanja i stvaranja sopstvene realnosti. Danas se koristi u komunikacijama, obrazovanju, ekonomiji, marketingu ... U Second Life-u su kreirani digitalni kontineti (ostrva) na kojima žive ljudi, gde se nalaze predstavništva raznih zemalja, velike svetske kompanije, kao i veliki broj fakulteta koji svojim studentima nude potpuno novi vid učenja.

Kada se putem Interneta pristupi ovom virtuelnom okruženju, prvo je potrebno kreirati svog avatara odnosno svoje digitalno ja, zatim se može početi "drugi život". Mogućnosti koje se, u ovom "drugom životu" pružaju su mnogobrojne: ovde je moguće pronaći savršeno mesto za

izgradnju kuće ili poslovnog prostora, mogućnost putovanja, organizacije različitih događaja i poslovnih sastanaka ... Osnovni nalozi su besplatni a postoje i premijum nalozi koji se plaćaju. Vlasnicima premijum naloga je dozvoljeno da kupuju i prodaju delove zemlje, čak i cela ostrva. Kao i u stvarnom životu postoje mesečni troškovi održavanja zemlje (takse), a vlasnik dobija određena prava kao što su izgradnja i uređenje zemljišta, ali i mogućnost da ostalima zabrani pristup na svoju teritoriju. Okruženje SL je postalo toliko popularno da se u njemu organizuju “prava” predavanja, treninzi i edukacije, sreću se naučnici, profesori i studenti. Na njemu se nalaze i najpoznatiji svetski univerziteti.

Jedinstvena valuta u SL je Linden dolar koji se može razmeniti za prave US dolare na nekoliko online LINDEN menjačnica u USA. Poslovanje u SL i mogućnost promene Lindena za US dolare je omogućilo stvarnu zaradu. Novembra 2005. godine pojavio se prvi stvarni milioner u SL, dvadesetpetogodišnji student koji je trgovinom nekretnina u SL-u uspeo da zaradi preko milion US dolara.



Slika 5.1 Second Life virtuelno okruženje

Sve veći broj škola, fakulteta i univerziteta istražuje mogućnost upotrebe virtuelnog sveta kao dopunu predavanjima i vežbama, kako bi studenti uspešno savladali sve zadatke. Više od 700 univerziteta, uključujući i jedan od najpoznatijih u realnom svetu Harvard, koriste Second Life kao obrazovni alat.

Sistemiški zahtevi

Second Life klijentska aplikacija je dostupna na Windows, MacOS, Linux operativnim sistemima. U tabeli 5.3 dat je prikaz minimalne hardverske konfiguracije za korišćenje Second Life-a.

Sistemiški zahtevi – minimalna hardverska konfiguracija	
Operativni sistem	XP, Vista, Windows 7 MacOS Linux
Memorija	512MB
Procesor	800 MHz Pentium III or Athlon
Internet	Cable, DSL
Grafička karta	NVIDIA GeForce 6600 ATI Radeon 8500, 9250 Intel 945 chipset

Tabela 5.3 Minimalna hardverska konfiguracija za Second Life

Ograničenja u Second Life-u

Za napredno korišćenje Second Life-a potrebno je naučiti novi i za ovo okruženje ograničeni programski jezik Linden Script Language (LSL), koji omogućava ograničeno dizajniranje prostora jer je u pitanju serverska aplikacija zatvorenog koda. Second life nije kompatibilan sa mnogim aplikacijama. Iako se dosta koristi u obrazovne svrhe finansijski aspekt Second Life-a može da predstavlja problem (neophodno je platiti zakup zemljišta).

Activeworlds

Activeworlds kompanija je stvorila virtuelno okruženje čiji server trenutno hostuje preko 1000 virtuelnih 3D okruženja. U zavisnosti od novca koji se izdvoji, kupac može da bira određene pakete koji se razlikuju. Pojedini paketi nude mogućnost uvoza 3D objekata kreiranih sa 3D alatima za modelovanje. Za kreiranje dodatnih opcija u ovom virtuelnom okruženju mora se koristiti isključivo programski jezik C. Modul VOIP nije deo osnovnog paketa ali kompanija Activeworlds daje mogućnost kupovine alata koji omogućava njegovo korišćenje.

Korisnicima je omogućeno da ovo virtuelno okruženje posete kao gosti („guest account“) ili kao građani („citizen account“). Korisnici imaju klasične mogućnosti kretanja kroz svet (trčanje, letenje, skakanje igranje i teleportacija). Gosti imaju ograničene dozvole za razliku od građana. Vlasnici virtuelnih okruženja plaćaju „taksu“ u zavisnosti od veličine zemljišta, ali i u zavisnosti od najvećeg broja „stanara“. Zbog sve većeg interesovanja obrazovnih institucija za ovo virtuelno okruženje, kompanija Activeworlds je umanjila naknade za korišćenje zemljišta u oblasti edukacije.

Grafičko okruženje

Glavni meni - Nudi mogućnost podešavanja parametara klijentske aplikacije, kao i korišćenje funkcija za komunikaciju i interakciju u virtuelnom okruženju.

Okvir Tabs - Ovaj deo osnovnog prozora se uključuje iz glavnog menija. Korisniku se nudi mogućnost brzog izbora određenih opcija koje ovo virtuelno okruženje podržava.

Gesture meni - Naknadno se uključuje iz glavnog menija. Ovaj meni omogućava prikazivanje gestikulacije avatara (npr. osmeh, plač ...).

Sistemske zahteve

Klijentski softver napravljen je isključivo za Windows operativne sisteme što predstavlja jedno od ograničenja, a funkcioniše i kao browser sa mogućnošću korišćenja HTTP protokola. Za razliku od klijentskog, administratorski softver namenjen je upotrebi na Windows, Linux i Solaris operativnim sistemima. Administratorski softver nudi jednostavno, ali moćno okruženje za konfiguraciju i administraciju virtuelnog okruženja koje vlasnicima, odnosno administratorima okruženja, omogućuje da menjaju postavke vezane za interakciju. Za pristup

potrebnim informacijama administratorski softver koristi integrisanu verziju MySQL baze podataka, ali ga je moguće koristiti i sa eksternom MySQL bazom ukoliko je to potrebno.

Sistemske zahteve – minimalna hardverska konfiguracija	
Operativni sistem	Windows 98 ... Windows 7
Memorija	128MB
Procesor	800 MHz
Internet	može i sporija Internet konekcija
Grafička karta	3D accelerated video card ($\geq$ 64MB)

Tabela 5.4 Minimalna hardverska konfiguracija za Activeworlds

Ograničenja u Activeworlds-u

Jedna od glavnih mana ovog virtuelnog okruženja je naplata korišćenja zemljišta kao i naplata u zavisnosti od broja korisnika. Osim toga ograničen je i broj korisnika koji u isto vreme mogu da budu online. Virtuelno okruženje se nalazi na serveru kompanije Activeworlds, zbog toga su vlasnici virtuelnih okruženja primorani da sa njima podele svoju politiku poslovanja, da im daju osnovne podatke, kao i da se uklape u standarde kvaliteta Activeworlds-a. Jedna od najvećih mana je da se može koristiti isključivo na Windows operativnim sistemima.

5.4 Poređenje postojećih i izbor okruženja

5.4.1 Poređenje postojećih 3D virtuelnih okruženja

Tri najbitnija faktora za poređenje 3D virtuelnih okruženja iz kojih se može izvući zaključak koje okruženje najviše odgovara potrebama DF laboratorije su:

1. Pristup

S obzirom da se 3D virtuelna okruženja koriste u svrhu obrazovanja i istraživanja, neophodno je da bude omogućen pristup velikom broju korisnika. Pristup može biti ograničen zbog visokih zahteva sistema ili kompatibilnosti klijentske aplikacije. Što se tiče sistemskih zahteva najpristupačniji je Activeworlds. Međutim s obzirom da je omogućen samo rad u Windows operativnom sistemu, Second Life u ovom poređenju ima prednost.

2. *Finansijski aspekti*

Od ova tri virtuelna okruženja jedino je server Open Wonderland-a besplatan za korišćenje. Activeworlds i Second Life dolaze sa značajnim troškovima. Povećanje broja studenata koji koriste Open Wonderland ne iziskuje nikakve troškove. U ovom poređenju Open Wonderlend ima prednost.

3. *Rukovanje serverom*

Sa aspekta rukovanja serverom Open Wonderland pruža najviše mogućnosti, pošto se serverska aplikacija (administriranje) nalazi na sopstenom server računaru.

Virtuelno okruženje	Multi platform	Besplatno za korišćenje	Kvalitet grafičkog okruženja	Open sorce	Text - Voice chat	3D/2D	Jezik
Open Wonderland	da	da	vrlo dobro	da	da	3D	Java
Second Life	da	ograničeno	vrlo dobro	ne	da	3D	LSL / C++
Active Worlds	ne	ograničeno	dobro	ne	da	3D	C

Tabela 5.5 Poređenje virtuelnih okruženja

	Open Wonderland	Second Life	Active Worlds
Mogućnosti	Web browsing, voice chat, basic instant messaging		
	deljenje aplikacija	lako kreiranje sadržaja	-

Tabela 5.6 Mogućnosti virtuelnih okruženja

Virtuelno okruženje	Obrazovna zajednica	Mogućnost promene okruženja	Mogućnost dodavanja sopstvenih sadržaja	Može da koristi već gotove sadržaje	Korišćenje eksternih medija i dokumenata
Open Wonderland	mala-u porastu	da	da	da	da

Second Life	veoma velika	da	da	da	da
Active Worlds	mala	da uz nadoknadu	da uz nadoknadu	da	da

Tabela 5.7 Poređenje virtuelnih okruženja za korišćenje u edukaciji

Iz prethodnih tabela u kojima je dato kratko poređenje virtuelnih okruženja koja se mogu koristiti za učenje Open Wonderland i Second Life zauzimaju gotovo isto mesto, dok je Active Worlds zbog mnogih ograničenja otpao kao moguće okruženje za učenje koje će biti implementirano u ovom projektu. Odluka o korišćenju platforme je prikazana u sledećoj tabeli gde je istaknuta stabilnost, kvalitet platforme (interfejsa), veličina zajednice korisnika, dostupnost sadržaja i budućnost ovih virtuelnih okruženja.

Virtuelno okruženje	prednosti	mane
Open Wonderland	Okruženje je bazirano na Javi, veoma kvalitetno i stabilno. Daje mogućnost besplatnog pokretanja privatnih virtuelnih okruženja. Integracija interfejsa je mnogo lakša i bolja u odnosu na Second Life. Broj korisnika je manji nego u Second Life-u ali se iz godine u godinu broj naglo povećava.	Nema gotovih sadržaja na raspolaganju kao što to nudi Second Life zajednica. Open Wonderland projekat je još u razvoju. Za poboljšanje interfejsa mora se koristiti programski jezik Java.
Second Life	Broj korisnika – zajednica koja koristi Second Life je ogromna i konstantno raste. Interfejs je stabilan, sa mogućnošću korišćenja gotovih komponenti koje su besplatne. Široko je korišćen od strane obrazovnih institucija.	Browser je bio jako nestabilan ali se poboljšao od verzije 2. Za kreiranje virtuelnih okruženja mora se platiti zakup zemljišta ili ostrva.

Tabela 5.8 Prednosti i mane virtuelnih okruženja

5.4.2 Izbor 3D virtuelnog okruženja

Kako bi izabrali odgovarajuću platformu za učenje, korišćenjem virtuelnog okruženja potrebno je postaviti niz kriterijuma koje platforma mora da zadovolji.

Na prvom mestu virtuelno okruženje mora biti pouzdano, nudeći studentima i predavačima mogućnost praćenja, odnosno održavanja nastave u realnom vremenu. Važno je napomenuti da virtuelno okruženje mora biti kreirano tako da pruža što verniji osećaj prisutnosti bez korišćenja posebne opreme. Poželjno je da klijentski softver bude dostupan na što većem broju različitih platformi.

Drugi važan kriterijum je da okruženje, kao i prava učionica omoguće prikaz širokog spektra multimedijalnih sadržaja (prikaz prezentacija, Web sadržaja, mogućnost korišćenja bele table, glasovna komunikacija između studenta i predavača itd.).

Treći kriterijum je lakoća razvoja i promene virtuelnih okruženja. Važno je odabrati okruženje koje neće praviti velike probleme predavačima koji nisu previše vešti u programiranju i korišćenju računara, kako bi uspešno mogli da kreiraju virtualna predavanja. Potrebno je da alati koji se koriste za izradu virtualnih predavanja budu što jednostavniji za korišćenje. Veličina zajednice korisnika je veoma važan faktor, jer najbolji izbor za savete i podršku predstavljaju upravo drugi korisnici.

Pored ova tri kriterijuma potrebno je napomenuti da je veoma važno da postoji mogućnost pokretanja lokalnog servera, što olakšava kontrolu i modifikaciju virtuelnog okruženja.

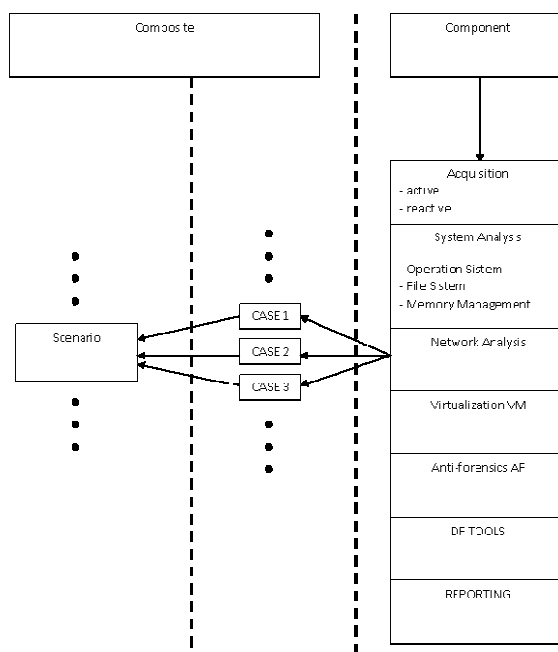
S obzirom na kriterijume koji moraju biti zadovoljeni i koji su navedeni, okruženje Open Wonderland se predlaže kao idealno rešenje.

6 Modelovanje i analiza

U ovom delu rada prvo je opisan komponentno kompozitni model laboratorije koji se koristi u realizaciji. Zatim je prikazano okruženje za realizaciju kao i njegovi elementi. Dat je uvod u semantički Web i odgovarajuće ontologije, a na kraju poglavlja data je hardverska platforma na kojoj je realizovano rešenje.

6.1 Komponentno kompozitni model digitalne forenzičke (DF) laboratorije

Početna tačka u definisanju 3D virtuelne laboratorije je uvoz osnovnih 3D objekata-komponenti (“cells” u Wonderland-u), koji imaju dve komponente (rendering i funkcionalnu komponentu). Biblioteka osnovnih komponenti se može proširiti uvođenjem kompozicija (slika 6.1). Ovaj proces zahteva povezivanje i kombinaciju novih 3D objekata (3D composition components) na svim nivoima, kao i dodavanje novih funkcionalnosti i alata. Interaktivna funkcionalnost se dodaje za svaki objekat [106].



Slika 6.1 Osnovne komponente i kompozicije u digitalnoj forenzici

Definisane su osnovne DF komponente: akvizicija (aktivna i reaktivna), analiza sistema (operativni sistem, fajl sistem i upravljanje memorijom), analiza mreže, virtuelizacija, Antiforenzika, DF alati i izveštavanje. Ove komponente čine slučajeve. Više slučaja čini jednu

scenu (kompoziciju). Više objektno orijentisanih scena može činiti jedan novi slučaj. Moguće su kombinacije i scena i slučajeva.

6.2 Realizovano 3D okruženje

Sledi detaljan opis elemenata koji su korišćeni za realizaciju 3D virtuelne forenzičke laboratorije.

6.2.1 Elementi okruženja

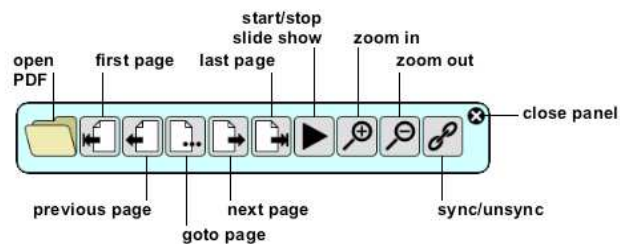
PDF Viewer - pregledač

Aplikacija PDF pregledač pruža funkcionalnost za gledanje PDF fajlova. Važno je da URL za PDF dokumenta mora da bude dostupan svim klijentima. Ako korisnik pokuša da učita PDF koji se nalazi na privatnom hard disku onda je to u osnovi i moguće gde samo korisnik vidi odgovarajući fajl u pregledaču, ali svaki drugi korisnik će videti crni ekran.



Slika 6.2 Primer korišćenja PDF viewera

Sa PDF pregledačem klijent je takođe u mogućnosti da izvrši prezentaciju i napravi slajdove. Kada klijent gleda PDF fajl mora se obezbediti da cela strana bude vidljiva promenom veličine prozora aplikacije, zato što scrolling ne radi. Na slici 6.3 može se videti kontrolna tabla koja se može koristiti za navigaciju kroz dokumenta.



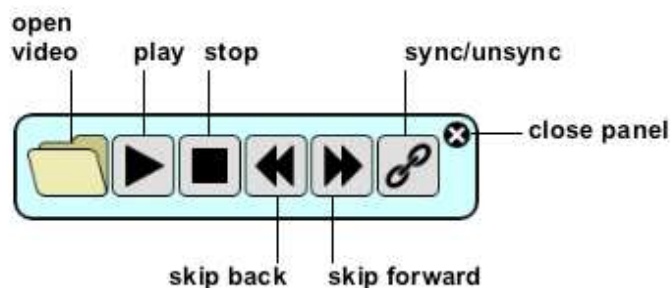
Slika 6.3 PDF viewer kontrole

Video - movie plejer

Identično kao PDF pregledač URL video zapisa mora da bude dostupan svim klijentima. Postoji Web kamera viewer i panorama viewer omogućavaju streaming videa pod uglom video kamere (slika 6.4). Video plejer podržava prikaz video zapisa koji su snimljeni ranije. Najčešće korišćeni formati koji su podržani u Wonderlandu su Quicktime (MPEG-4) i Flash (flv).



Slika 6.4 Video plejer u Wonderlandu

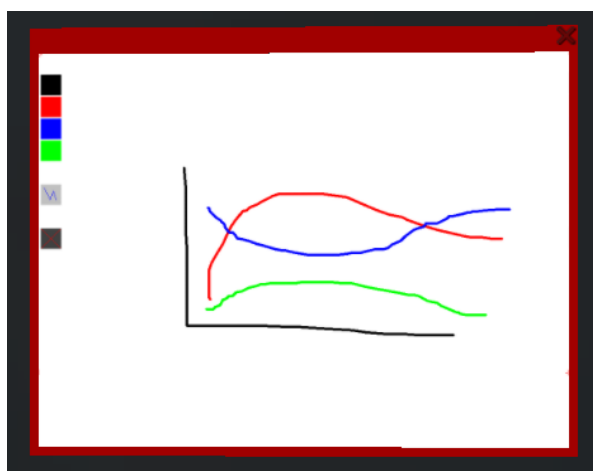


Slika 6.5 Movie player kontrole

Slika 6.5 prikazuje kontrol panel video plejera. Ukoliko video zapis ne počne odmah, to je zbog lošeg propusnog opsega korisničke konekcije. Plejer prepoznaje tu situaciju i počinje sa reprodukcijom tek nakon keširanja dovoljno podataka.

Bela tabla

Bela tabla je verovatno najjednostavniji deo serverske aplikacije i omogućava klijentima crtanje i brisanje jednostavnih linija u više boja kao na slici 6.6



Slika 6.6 Crtanje po tabli

Izolovano mesto

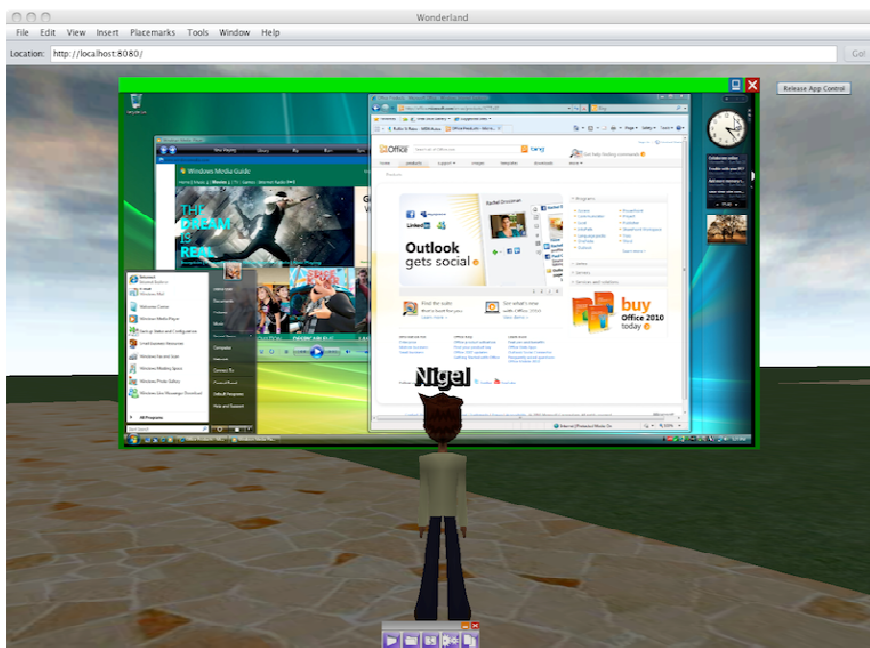
Izolovano mesto je krug gde avatari mogu da odu i imaju privatne razgovore. Mogu da čuju jedni druge, ali ne mogu da čuju zvuk spolja. Klijenti koji se nalaze van tog kruga ne mogu da čuju bilo kakav zvuk unutar kruga (slika 6.7). To se može iskoristiti za kreiranje jednog ili više privatnih mesta u tom okruženju (kancelarije za konsultacije).



Slika 6.7 Izolovano mesto u određenom okruženju Wonderlanda

VNC Viewer - pregledač

Omogućava prikaz udaljenog desktopa i interakciju sa Wonderlandom. VNC Viewer se povezuje na server i prikazuje udaljeni desktop kao što možete videti na sledećoj slici.



Slika 6.8 VNC Viewer konektovan na server

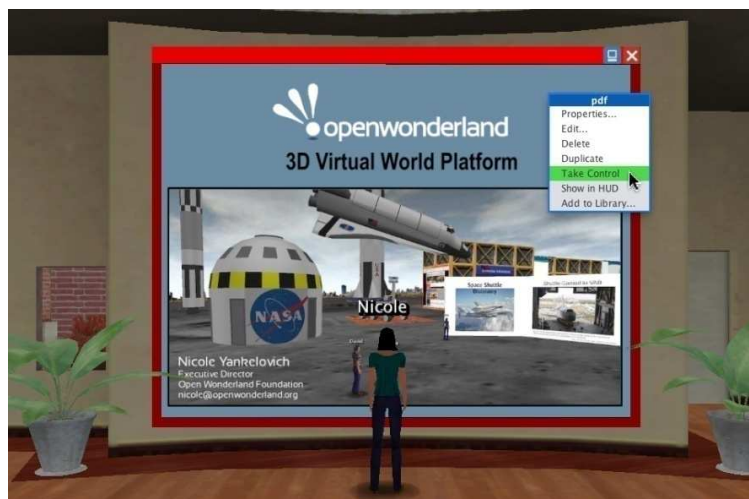
Svaki klijent konektovan na isti Wonderland server ima isti pogled na desktop i može da preuzme kontrolu i interakciju.

PDF Spreader

PDF Spreader zavisi od osnovnog modula Presentation i oba modula moraju biti instalirana. Prevlačenjem (drag i drop opcija) PDF fajla otvoriće se prozor kao na slici 6.9, sa izborom načina prikaza datog fajla (slika 6.10).



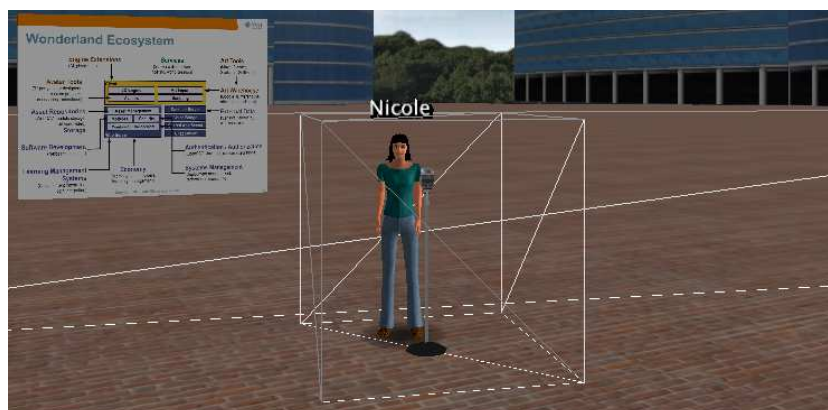
Slika 6.9 Izbor načina prikaza PDF fajla



Slika 6.10 Otvoreni PDF fajl u PDF Sprederu

Microphone

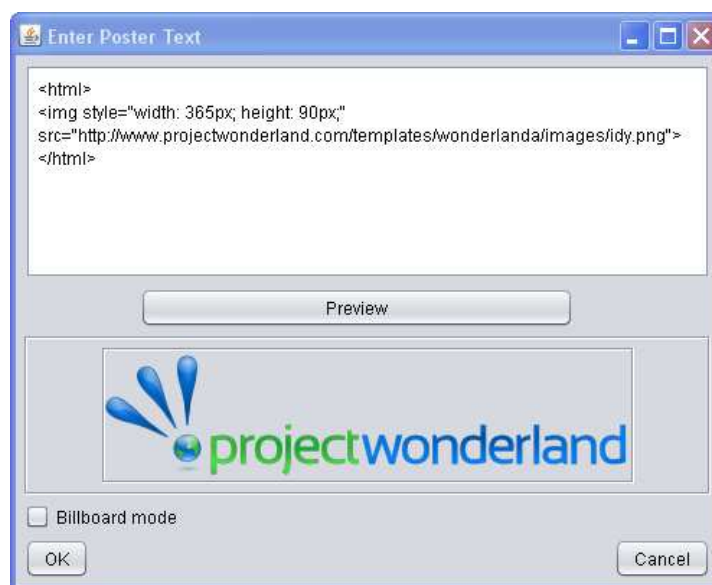
Ovim modulom je definisano korišćenje mikrofona u Open Wonderland okruženju. Na slici 6.11 može se videti prikaz mikrofona u 3D okruženju.



Slika 6.11 Microphone u Open Wonderlandu

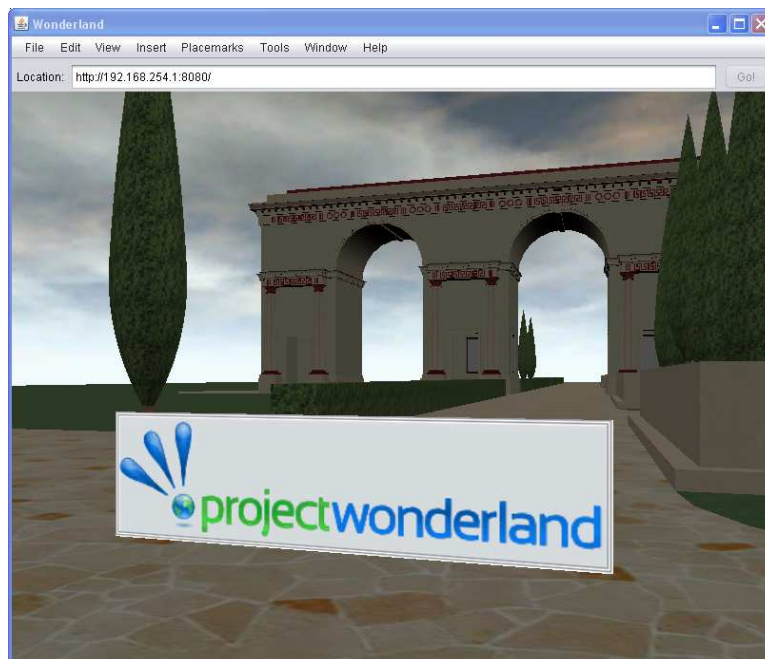
Poster

Izbor opcije “Poster” iz Insert Object dialoga definiše rad sa posterom i automatski se pojavljuje podrazumevani poster sa natpisom “Hello World”. Za složenije postere, može se uneti HTML kod u prozor za unos teksta kao što se može videti na sledećoj slici.



Slika 6.12 Unos HTML koda u Poster modul

Rezultat prethodno unetog koda prikazan je na slici 6.13

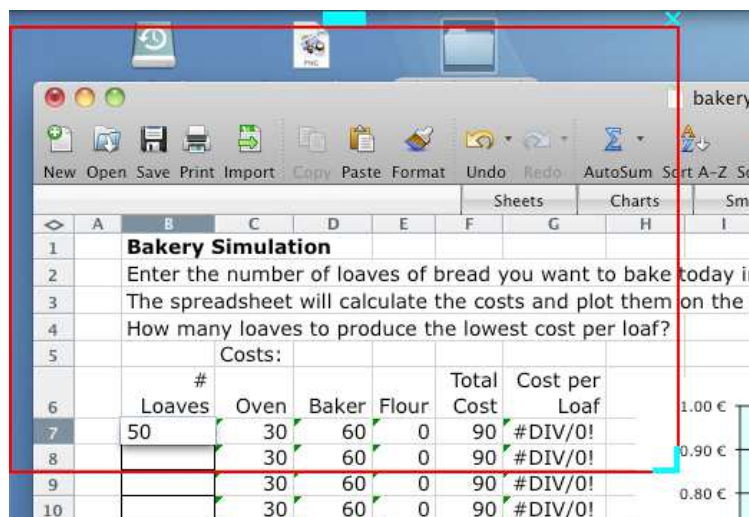


Slika 6.13 Prikaz Poster modula u Open Wonderland

Ažurirana verzija originalnog Poster modula je HTML Poster.

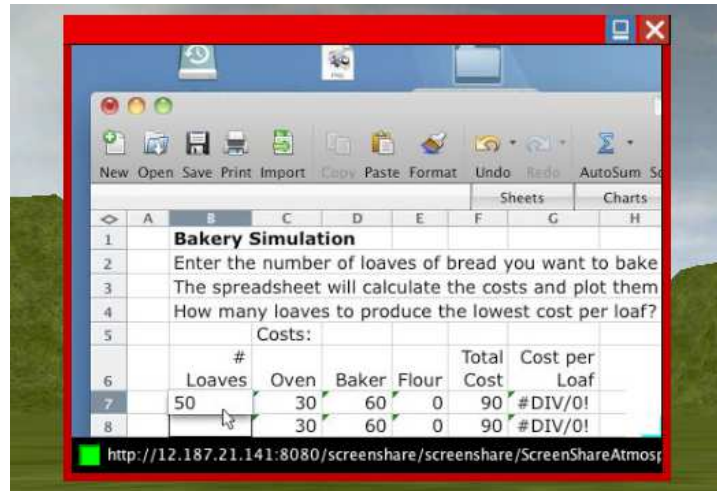
Screen Sharer

Screen Sharer je jednostavan alat za deljenje dela ekrana. Izborom opcije “Share screen” iz menija sa alatima pojavljuje se crveni okvir u gornjem levom uglu ekrana (slika 6.14).



Slika 6.14 Izbor dela ekrana za deljenje

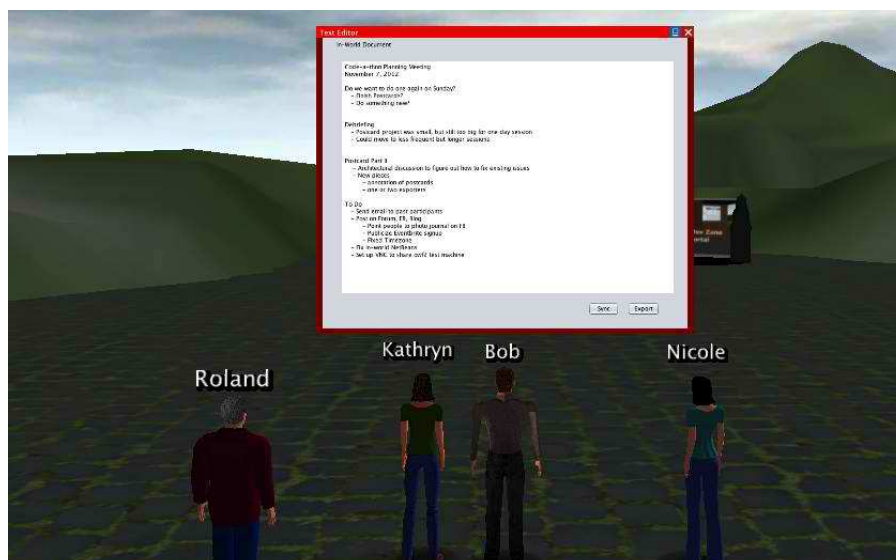
Veličina i položaj ovog okvira može se promeniti korišćenjem plave ručice u donjem uglu. Za prikaz u 3D okruženju ekran se ažurira brzinom jedan frejm u sekundu.



Slika 6.15 Screen Share u Open Wonderlandu

Kolaborativni Text Editor

Text editor koji omogućava većem broju korisnika da ažurira isti tekst (bez formatiranja, samo običan tekst). Mogu da se prevuku fajlovi sa ekstenzijama txt, log, html i xml i ovaj modul kreira novu ćeliju i otvara fajl.



Slika 6.16 Kolaborativni text editor u Open Wonderlandu

Webcam Viewer

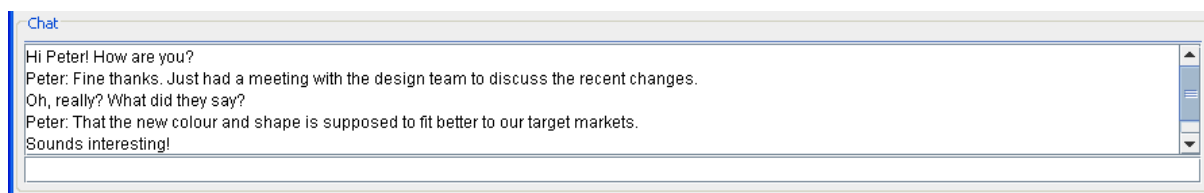
Webcam Viewer je 2D aplikacija koja omogućava gledanje streaming videa sa Web kamere. Ova aplikacija podržava bilo koju kameru koja obezbeđuje Motion-JPEG stream. Kada se Webcam Viewer startuje on se povezuje na podrazumevanu Web kameru. Za povezivanje sa drugom kamerom treba preuzeti kontrolu na aplikacijom desnim klikom na prozor i izabrati Take Control iz menija a zatim izabrati ikonu sa kontrolne table i uneti URL kamere. Webcam Viewer je kolaborativna aplikacija koja omogućava da više korisnika vidi prikaz iste kamere (slika 6.17).



Slika 6.17 Webcam viewer u Open Wonderlandu

Text chat

Osnovni modul za chat komunikaciju koji ima mogućnost skrivanja i ponovnog prikaza (skrivena chat poruke drugih korisnika čuvaju se i biće prikazane kada se chat meni opet prikaže) kao na sledećoj slici.



Slika 6.18 Chat koji omogućava tekstualnu komunikaciju kroz 3D okruženje

Glasovni chat

Glasovni chat je sofisticiraniji modul za komunikaciju, gde ljudski glas omogućava prenos dodatnih informacija (emocija) pored značenja same reči. Postoje dve glavne komponente u Wonderlandu koje se moraju pravilno konfigurisati Voice Bridge (na strani servera) i Softphone (na strani klijenta). Softphone je uređaj za konfigurisanje i testiranje audio postavki za klijente. Izgled Softphone podseća na standardni digitalni telefon sa tastaturom (slika 6.19).



Slika 6.19 Softphone sa globalnom konekcijom na liniji 1

Wonderland koristi topologiju zvezde za opštu glasovnu komunikaciju i postupak registracije.

6.2.2 Okruženje za akviziciju i analizu digitalnih podataka

Okruženje za akviziciju i analizu digitalnih podataka predstavljeno je kroz jednu virtuelnu 3D kompoziciju koja se sastoji od sledećih elemenata:

- PDF Viewer (za pregled pdf dokumenata);
- VNC Viewer (za rad sa DF alatima preko RDP protokola);
- Html Poster (za natpis sa imenom tima koji trenutno radi);



Slika 6.21 Prikaz okruženja za simulaciju svedočenja u Open Wonderland

6.3 Semantički Web

World Wide Web je promenio način na koji ljudi međusobno komuniciraju, posluju, dolaze do informacija i kako se zabavljaju. Trenutno se na računare gleda kao na polaznu tačku globalnog informacionog prostora. Većina današnjeg Web sadržaja je prilagođena ljudskoj upotrebi. Pretraživači koji koriste ključne reči u pretragama kao što su Yahoo i Google su glavni alati za korišćenje današnjeg Web-a. Web ne bi postigao toliki uspeh da nema ovih alata. Međutim, postoje ozbiljni problemi u korišćenju ovih alata:

- Veliki odziv, mala preciznost. U ovom slučaju višak informacija predstavlja problem.
- Mali odziv ili bez odziva. U ovom slučaju manjak informacija predstavlja problem.
- Rezultati su veoma osetljivi na rečnik. Ovo je nezadovoljavajuće, jer slični semantički upiti treba da vrate slične rezultate.
- Rezultati su pojedinačne Web stranice. To je problem jer ako su potrebne informacije koje se nalaze u više raznih dokumenata, korisnik mora da pokrene više upita.

Jedno od rešenja za poboljšanje trenutne situacije u obradi teksta je da se na osnovu sadržaja razvija napredna tehnika na bazi veštačke inteligencije i računarske lingvistike. Ovaj pristup se koristi već neko vreme, ali uprkos napretku zadatak je i dalje previše ambiciozan.

Alternativni pristup je da se Web sadržaj prikaže u formi koju mašine lakše procesiraju i da se koriste inteligentne tehnike kako bi se iskoristio ovaj prikaz. Ovaj pristup se odnosi na “revoluciju” Weba kroz Semantic Web inicijativu. Semantički Web neće biti novi globalni izvor informacija paralelan postojećem Webu. On se postepeno razvija i evoluira iz postojećeg Weba 2.0.

Semantički Web propagira internacionalno telo za standardizaciju Weba, World Wide Web konzorcijum (W3C). Inicijator Semantičkog Weba je Tim Berners-Lee, osnivač WWW u kasnim 1980-tim. Očekuje se realizacija “originalnog” Weba, uz viziju gde značenje informacija ima mnogo veću ulogu u odnosu na današnji Web.

Semantički Web se veoma brzo razvija, i sve je veći broj projekata i programa u svim delovima sveta. Za nas posebno je bitna njegova primena u upravljanju znanjem. Cilj Semantičkog Weba je da omogući sisteme za napredno upravljanje znanjem:

- Znanje će biti organizovano u konceptualnom prostoru u skladu sa svojim značenjem.
- Automatizovani alati će podržavati održavanje proverom nedoslednosti i izdvajanjem novih znanja.
- Pretraživanje na osnovu “ključnih reči” zameniće “odgovori na upite”: traženo znanje će biti izdvojeno i prikazano na način jednostavan za korišćenje.
- “Odgovori na upite” će biti mogući kroz više dokumenata.
- Definisanje ko može da vidi određeni deo informacije (čak i deo dokumenta) će biti moguć.

6.4 Ontologija

Prema Gruberu [110] ontologija je eksplicitna specifikacija procesa konceptualizacije. Izraz je pozajmljen iz filozofije gde je ontologija sistematsko „očitavanje” postojanja. Postoje dva tipa ontologije [111], [112]. Ontologija koja počinje malim slovom “o” objašnjava situacije u kojima se stiču znanja sa ciljem organizacije i klasifikacije [98].

Ontologije su u širokoj upotrebi u mnogim oblastima, i formalno predstavljaju znanje u toj oblasti. Ontologije su razvijene i da podrže digitalnu forenziku. U radu [107] ontologija se koristi za razvoj automatskih digitalnih forenzičkih alata. U radu [108] autori predlažu ontologiju za mrežnu forenzičku analizu. Ova ontologija predstavlja i oblast znanja mrežne forenzike kao i oblast znanja rešavanja problema. U radu [109] predstavljeni su neki izazovi u konceptualizaciji ontologije i specifične tehnike koje su korisne za konstrukciju ontologija. Kreirane su ontologiju za analizu terorizma. U radu [100] opisan je okvir za forenzičku analizu velike količine podataka korišćenjem ontologije i mašinskog učenja.

Ovaj rad predstavlja pokušaj da se primeni ontologija u oblasti DF-a sa ciljem da se pronađe pravi nivo za edukaciju i istraživanje sa jedne strane (academics), i hardvera i softvera sa druge strane (technology).

6.5 Hardverska platforma

U ovom delu rada opisano je korišćene platforme i protokola. Serverska platforma je IBM System x3650 M3

- Procesor: 2x Intel Xeon E5645 (6c/12t);
- Memorija: 4x8GB ECC DDR3 1333MHz;
- Sistemski disk: 2x 300GB 15K 6Gbps SAS 2.5" SFF Slim-HS SED;
- Storage: 4x 1TB 7.2K 6Gbps NL SAS 2.5" SFF HS HDD;
- Mreža: 2x 1Gbps network card (load balancing).



Slika 6.22 IBM System x3650 M3

Osim navedenog hardvera potrebno je obezbediti i softver koji će pokretati laboratoriju. Što se tiče operativnog sistema koristi se Windows 2012 Server koji je osnova sistema i koji preko svog sistema za virtuelizaciju HyperV version 3 pokreće sve potrebne virtuelne mašine.

Na Univerzitetu Singidunum koriste se virtuelne mašine za učenje različitih oblasti i kurseva u informacionim tehnologijama. Različiti operativni sistemi se mogu demonstrirati na jednom studentskom desktop računaru sa vrlo malo vremena potrebnim za pripremu sistema. Prednosti za studente uključuju više informacija i kraći vremenski period potreban za instalaciju.

U laboratoriji se koriste virtuelne mašine sa različitim karakteristikama, namenama i brojem instanci. Virtuelne mašine u laboratoriji se koriste za potrebe korisničkog interfejsa studenata, serversku primenu, isporučivanje edukacionih materijala i razna testiranja. Kreiran je određen broj virtuelnih mašina koje su konfigurisane i smeštene u repozitorijum virtuelnih mašina gde se registruju, i odakle se kopiraju za potrebe instanci u laboratoriji, a to su:

- Windows XP/VISTA/WIN 7/WIN SERVER;
- Linux/Unix, android simulator;
- iOS simulator;
- router iOS simulator;
- DEFT 7.2 live distribution;
- SIFT WORKSTATION 2.14 live distribution;

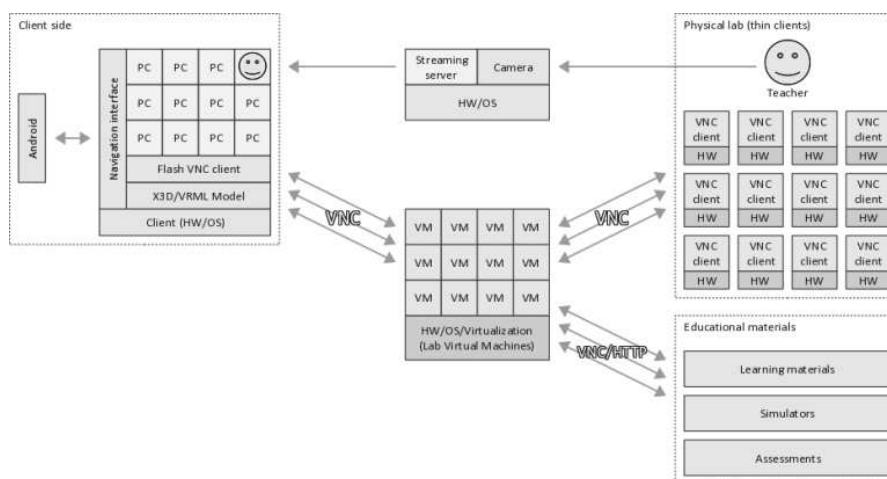
- BACKTRACK 5 R3 live distribution;
- Windows 2012 server with FTK and ENCASE.

Pri prvom pokretanju laboratorije vrši se instanciranje virtuelnih mašina koje podrazumeva kopiranje i podešavanje modela za svaku od definisanih instanci. Kod gašenja laboratorije virtuelne mašine se zamrzavaju, a pri narednim pokretanjima laboratorije se vrši njihovo odmrzavanje.

Protokoli koji se koriste u virtuelnoj laboratoriji su RDP 8.0 i VNC. RDP (Remote Desktop Protocol) je protokol koji se koristi za daljinski pristup desktopu virtuelnog računara i omogućava sigurnu tj. šifrovanu komunikaciju. Aktuelna verzija je 8.0 i ona je podržana od strane MS Windows 8 i Windows Server 2012 operativnih sistema u startu kao i od Windows 7 SP1 i Windows Server 2008 R2 SP1. VNC (Virtuel Network Computing) se koristi za deljenje desktopa a bazira se na RFB (Remote Frame Buffer) protokolu. Izabran je ovaj protokol jer u Open Wonderland-u postoji VNC client koji bez problema iz 3D okruženja može da pristupi bilo kom virtuelnom računaru.

7 Realizacija

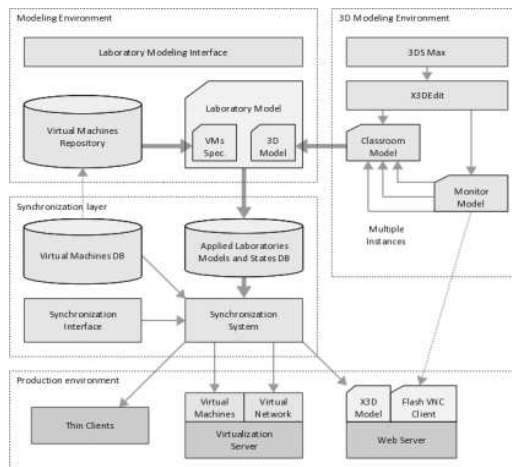
Ovoj realizaciji prethodi prethodno istraživanje i implementacija sistema za edukaciju u oblasti digitalne forenzike. Prethodna implementacija digitalne forenzičke laboratorije (DF-lab) [104] bazira se na X3D okruženju. Arhitekturu laboratorije može da se vidi na slici 7.1



Slika 7.1 Arhitektura DF-lab i komponente

Jezgro laboratorije čini klaster servera na kojima se preko Xen Hypervisor 4.1 izvršavaju klijentske virtuelne mašine sa softverskim konfiguracijama prilagođenim za praćenje planiranih nastavnih procesa (Win XP, 512mb RAM). Virtualizacijom klijentskih računara postiže se napredak po pitanju fleksibilnosti i dostupnosti. Podrazumevani protokol za pristup virtualizovanim klijentima je VNC, kao platformski nezavistan.

Fizički interfejs ka klijentskim računarima laboratorije čine tanki klijenti sa ulazno-izlaznim uređajima i VNC klijentskim softverom. Web interfejs ka klijentskim računarima laboratorije izgrađen je korišćenjem X3D/VRML baziranog 3D okruženja sa ugrađenim VNC klijentima. Osnovna ideja je da 3D okruženje predstavlja repliku realnog fizičkog okruženja forenzičke laboratorije. VNC klijenti ugrađeni u 3D model omogućavaju direktnu vezu sa virtuelnim mašinama i njihovim interfejsima u fizičkoj laboratoriji.

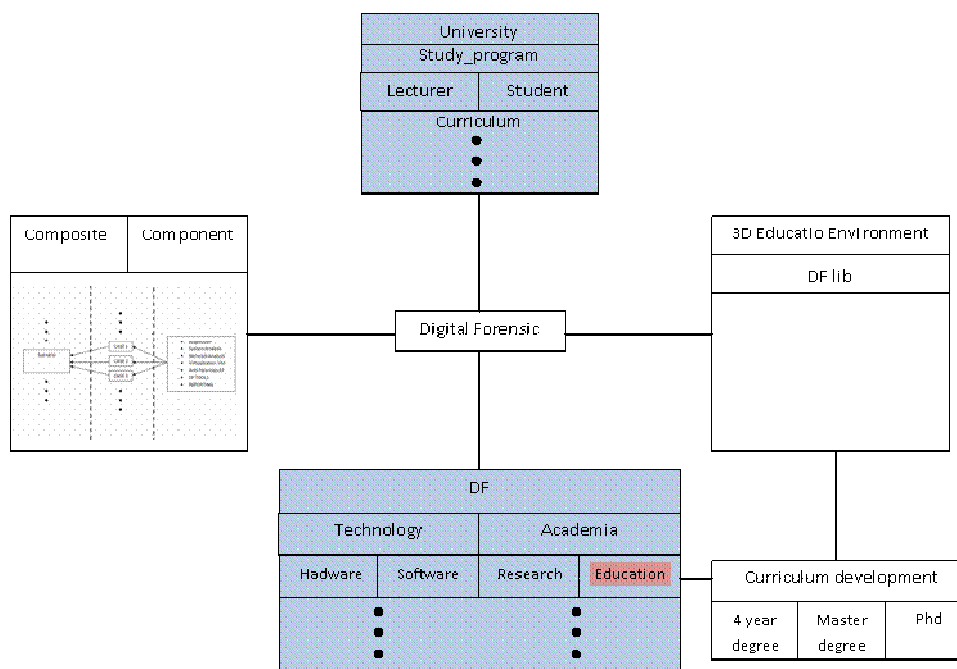


Slika 7.2 DF-lab model [104]

Iako je implementacija uspešna postoji problem što se zahteva znanje programiranja, odnosno neophodno je znati VRML. Korišćenje Open Wonderland platforme ne zahteva znanje programiranja i može se lako implementirati bilo koja funkcionalnost objekata u 3D okruženju.

U radu je dat nov pristup u edukaciji u oblasti digitalne forenzike (slika 7.3):

- Kao platforma se koriste Cloud sistem i virtuelne mašine, gde je ova platforma sastavni deo forenzičke analize.
- Ontološki je opisan model visokoškolske ustanove.
- Ontološki model je komponentno kompozitnog tipa i na osnovu njega je realizovano 3D virtuelno edukaciono okruženje.
- Ontološki model se koristi za dinamički razvoj kurikuluma.



Slika 7.3 Arhitektura DF modela

Obojene oblasti (plave) predstavljaju razdvojene ontologije koje se preklapaju u više kategorija. Ove ontologije i njihovi izvori su detaljno objašnjeni.

7.1 Dizajn 3D okruženja

Projektovanje okruženja koje se koristi za edukaciju se realizuje kao interfejs koji povezuje realan i virtuelan svet. Dizajn uzima u obzir prostorne i vremenske apstrakcije koje definišu kolaborativni radni prostor. Definišu se tri konceptualna elementa u organizaciji okruženja: svet, scene i objekti. Svaka scena se sastoji od objekata sa kojima korisnik može da ostvari interakciju. Elementi mogu da budu objekti koji su namenjeni za učenje ili određeni alati koji pružaju uslugu korisnicima (aplikacije za časkanje ili simulaciju).

7.2 Opis softverskog sistema

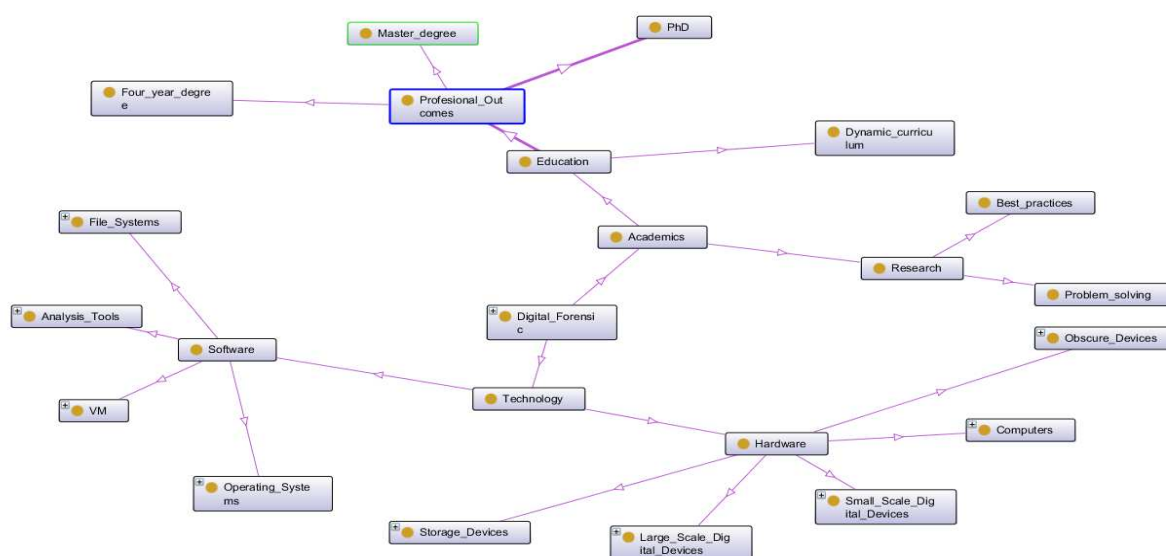
U sistemima virtuelne realnosti objekti koji se koriste za učenje zasnivaju se na određenom skupu alata koji služe kao gradivni blokovi za pravljenje složenijih objekata. Ti alati se mogu podeliti u sledeće grupe:

- Alati za komunikaciju (immersive real-time audio, chat);
- Alati za deljenje prezentacija (2D i 3D slide sharer);

- Alati za upravljanje fajlovima (repozitorijum fajlova koji su poslani na server, podeljen po korisnicima ili grupama);
- Alati za navigaciju (sinhronizacija kontrole nad objektima koje istovremeno može da upotrebi nekoliko korisnika);
- Multimedijски alati (video striming, URL navigacija, snimanje video i audio zapisa unutar okruženja).

7.3 Ontologija realizovanog 3D okruženja

Brinsonov ontološki model prikazan u [98] je poslužio kao osnova za razvoj originalne hijerarhijske strukture sa ciljem da se kreira 3D edukacioni model za digitalnu forenziku. Ontološki model za edukaciju u digitalnoj forenzici kreiran je koristeći Protege editor (slika 7.4).

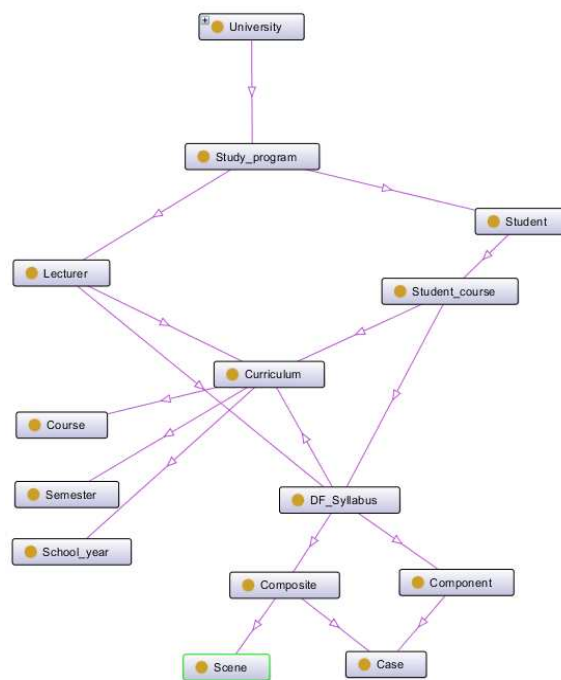


Slika 7.4 Ontologija za digitalnu forenziku

Modelovanje: Materijale i ostale elemente potrebne za virtuelnu edukaciju neophodno je modelovati kao 3D entitete. Koristeći hijerarhijske analize kreiran je 3D model virtuelne laboratorije. Virtuelna laboratoriji se sastoji od velikog broja 3D entiteta i scena i može se u svakom momentu proširiti. Za nov eksperiment ili laboratoriju, korisnik treba da izabere potrebne virtuelne entitete i scene iz biblioteke i kreira novu scenu. Scene (kompozicije) mogu da sadrže različite komponente (objekte) kao i druge scene.

Kombinacijom raznih 3D entiteta dobijamo različite objekte. Njihovom kombinacijom dobijamo scene. Sve se to može snimiti u biblioteku. Virtualni entiteti vezani su za objekte preko njihovih funkcionalnosti i atributa u eksperimentalnoj sceni. Postoje različiti alati koji su uključeni u DF-lab koji mogu simulirati različite forenzičke operacije iz stvarnog sveta.

Ovo se sve uklapa u opšti model visokoškolske ustanove prikazan na slici 7.5



Slika 7.5 Ontologija visokoškolske institucije (Univerziteta)

Ontologiju za digitalnu forenziku na visokoškolskoj instituciji definišu sledeće klase: University, Study_program, Student, Lecturer, Student_course, Curriculum, Course, Semester, School_year, DF_Syllabus, Composite, Component, Case i Scene. Ove klase označavaju prirodne koncepte koji su zajednički za obrazovne institucije. Klase imaju skup instanci (objekti klase). Na primer SingidunumUniversity je instanca klase University. Ontologija takođe sadrži i relacije koje označavaju prirodne odnose između objekata u realnom svetu. Klase se dalje razvijaju u potklase.

Univerzitet ima više studijskih programa. Za svaki studijski program definišemo kurikulume i odgovarajuće silabuse za digitalnu forenziku. Koristimo komponentno kompozitni model sa

odgovarajućim scenama i scenarijima. Istovremeno se definišu i relacije između studenata i predavača i menadžmenta univerziteta.

Model u osnovi uključuje razvijene kurikulume za osnovne studije (4 godine), master i doktorske studije. Ovaj model može da se koristi i za pripremu kurseva i materijala za kurseve. Najviši nivo pokriva sve aspekte u oblasti digitalne forenzike.

7.4 Karakteristike realizovanog rešenja

Virtuelno edukaciono okruženje se bazira na sledećim karakteristikama:

- interaktivno 3D okruženje sadrži grupu pravila koja objašnjavaju odnos elemenata,
- formalna ontologija sadrži sve koncepte,
- svi elementi u okruženju su povezani sa konceptom ontologije,
- grupa korisnika (studenti, profesori) mogu koristiti 3D virtuelno okruženje. Članovi grupe su povezani konceptom ontologije.

Ovakvo 3D okruženje koristimo kao virtuelnu laboratoriju za digitalnu forenziku gde prvo kreiramo osnovne komponente-objekte koje povezujemo i definišemo nove kompozicije i sve smeštamo u biblioteku. Ontološki se definišu veze između svih komponenata i kompozicija.

7.5 Forenzička laboratorija

7.5.1 Biblioteka forenzičkih slučajeva FCL – Forensic Case Library

Forenzička kolekcija za učenje sastoji se od različitih slučajeva koji pokrivaju razne oblasti DF istrage. Svi slučajevi se baziraju na određenom broju koraka:

- Forensic acquisition (Live/Clasic) – forenzička akvizicija;
- Forensic data analisys (Windows, Unix, Mac, Android, network, Internet, VM, anti-forensic) – forenzička analiza podataka;
- Forensic tools (open-source/comercial) – forenzički alati;
- REPORTING / EXPERT WITNESS – izveštavanje i svedočenje.

U nastavku će biti detaljno prikazani izabrani slučajevi iz forenzičke prakse i njihove specifičnosti u odnosu na navedene korake. Sledeća tabela prikazuje slučajeve istrage razvrstane po različitim operativnim sistemima, vrstama memorije iz kojih se uzimaju “imidži”, i fajl sistemu koji se imidžuje:

Forensic Case	File system	Memory	OS
Windows	NTFS, FAT	RAM / Storage	Windows
Unix	ext2, ext3, raiserFS	RAM / Storage	Unix/Linux
Mac OS X	HFS, HFS+	RAM / Storage	Apple Mac OS X
Android smart phone	YAFFS	SD/MMC	Google Android
iOS smart phone	HFSX	SD/MMC	Apple iOS

Tabela 7.1 Specifičnosti različitih forenzičkih slučajeva

Kompletan slučaj istrage računara zahteva sve faze DF istrage od akvizicije podataka, preko analize operativnog sistema i na kraju pisanje forenzičkih izveštaja korišćenjem različitih forenzičkih alata koji su prihvaćeni od strane digitalnih forenzičara i pravosudnih organa. Pored navedenih slučajeva koji su vrlo slični i prikazani u tabeli, postoje i neki specifični slučajevi koji se razlikuju u prethodno navedenim koracima.

Network Intrusion Forensic Case - Kompletan slučaj specifične istrage upada u računarsku mrežu koji zahteva sve faze DF istrage od akvizicije podataka, preko analize mrežnog saobraćaja i na kraju pisanje forenzičkih izveštaja korišćenjem različitih forenzičkih alata koji su prihvaćeni od strane digitalnih forenzičara i pravosudnih organa. Specifičnost ovog slučaja je da se u koraku Forensic acquisition koristi samo Live akvizicija i da se koriste u koraku Forensic data analysis alati i koraci vezani za mrežnu forenziku.

Internet Forensic Case (mail, chat, browser forensic case) - Kompletan slučaj specifične istrage računara koji je povezan na Internet zahteva sve faze DF istrage od akvizicije podataka, preko analize korišćenih online servisa i na kraju pisanje forenzičkih izveštaja korišćenjem različitih forenzičkih alata koji su prihvaćeni od strane digitalnih forenzičara i pravosudnih organa. Specifičnost ovog slučaja je da se koriste u koraku Forensic data analysis alati i koraci vezani za Internet forenziku.

VM Forensic Case - Kompletan slučaj specifične istrage virtuelnih mašina koje su bile meta napada hakera zahteva sve faze DF istrage od akvizicije podataka, preko analize fajlova virtuelne

mašine i na kraju pisanje forenzičkih izveštaja korišćenjem različitih forenzičkih alata koji su prihvaćeni od strane digitalnih forenzičara i pravosudnih organa. Specifičnost ovog slučaja je da se u koraku Forensic acquisition koristi samo Live akvizicija i da se koriste u koraku Forensic data analysis alati i koraci vezani za virtuelne mašine a to su:

- VM forensic
- Memory forensic

Anti-forensic Case - Kompletan slučaj specifične istrage računara koji je bio meta napada hakera i gde su korišćene različite anti-forenzičke tehnike kako bi se sakrili tragovi upada, zahteva sve faze DF istrage od akvizicije podataka, preko analize korišćenih anti-forenzičkih alata i na kraju pisanje forenzičkih izveštaja korišćenjem različitih forenzičkih alata koji su prihvaćeni od strane digitalnih forenzičara i pravosudnih organa. Specifičnost ovog slučaja je da se koriste u koraku Forensic data analysis alati i koraci vezani za anti-forenziku.

7.5.2 Biblioteka forenzičkih scenarija FSL – Forensic Scenario Library

Biblioteka forenzičkih scenarija (FSL) je mesto gde se čuvaju različiti scenariji koji se sastoje od slučajeva (case). Omogućeno je pretraživanje ove biblioteke i student može na osnovu ključnih reči pronaći slične slučajeve koji već postoje sačuvani u biblioteci. U nastavku je dat prikaz jednog scenarija koji je dosta širok i zahteva opsežnu digitalnu forenzičku istragu.

XXX je firma koja se bavi marketing uslugama. Posедуje preko 50 računara i zastupljene su različite vrste računara (laptop, desktop i tablet). Primećeno je da je u toku druge polovine 2012 godine došlo do curenja određenih informacije (špijunaža) sa kompanijske mreže. Svi računari su umreženi i koriste se deljeni resursi na mreži za čuvanje podataka. Takođe postoji brzi link ka Internetu i neki zaposleni razmenjuju podatke preko dropbox i google docs-a. Sumnja se da je došlo do kompromitacije nekog od računara ili naloga na mrežnim servisima za čuvanje podataka. Pretpostavlja se da napad dolazi sa Cloud Systema.

Takođe je bitno istaći da se u kompaniji koriste kako žičani 1Gb tako i wireless mreže, tako da je moguće da je neko uspeo da se ubaci u wireless mrežu i da na taj način pristupa internoj mreži. Sva oprema koja se koristi za umrežavanje je CISCO tako da postoji i određeni broj CISCO rutera sa svojim OS.

Operativni sistemi koji se koriste su uglavnom Micorosftovi: Windows XP i Windows 7 na klijentima dok se na serverima koristi Windows 2008 server. Postoji i jedan Linux RedHat računar koji se koristi kao Webserver. Dizajneri za svoje potrebe koriste u svojoj kancelariji MAC računare koje pokreće iOS 6 dok tablet računari uglavnom imaju instaliran Android 4.1 OS osim par dizajnerskih tableta koji koriste iOS (iPad2).

Locirani su sumnjivi računari i potrebno je sprovesti kompletnu DF istragu. Zadatak je da se ispita gde je došlo do propusta i gde cure informacije i da se detaljan izveštaj dostavi u što kraćem roku menadžentu kompanije.

Potrebni koraci:

- Izvršiti akviziciju svih računara i uređaja (live i klasičnu) koristeći DEFT ili SIFT distribuciju kao i alate komandne linije koji se mogu koristiti za ovu namenu (DD, FTK Imager...);
- Izvršiti forenzičku analizu prikupljenih podataka (Windows, Linux, Mac OS X, Android) koristeći raspoložive alate iz EnCase i FTK alata ili SIFT distribucije;
- Izvršiti analizu mreže i mrežnih servisa (Cloud - Internet, mrežna i ruter forenzika) koristeći alate za analizu mrežnog saobraćaja i za analizu tragova korišćenja Internet servisa;
- Ponoviti prethodne korake u virtuelnom okruženju i proveriti da li u biblioteci postoji slično ili isto rešenje;
- Ako studenti rade u grupama VE iskoristiti za međusobnu interakciju – saradnju;
- Napisati forenzički izveštaj u odgovarajućem formatu, kao i lični utisak o korišćenju VE;
- Snimiti poslednji scenario i izveštaj u DF_lib.

8 DF silabusi i kurikulumi

8.1 DF silabus

8.1.1 DF silabus za osnovne studije

Predloženi ontološki model može se takođe prilagoditi u cilju razvoja kurikuluma. To se može uraditi praćenjem različitih delova modela za pronalaženje oblasti za učenje na nekom kursu. Predmet se sluša u jednom semestru i traje tačno 14 radnih nedelja od kojih je 12 nedelja predavanja i vežbi, dve nedelje su predviđene za redovne kolokvijume. U nastavku je dat prikaz 12 nedelja predavanja:

1. Forensic acquisition – classic

Uvodno predavanje u kome se studenti upoznaju sa osnovnim pojmovima vezanim za DF istragu, procedure koje je neophodno poštovati tokom istrage i uče tehnike klasične akvizicije (reaktivna forenzika) podataka sa različitih vrsta uređaja (desktop, laptop, PDA/TABLET/SMART Phone...).

2. Forensic acquisition – live

Druga nedelja predavanja u kojoj se studenti upoznaju se tehnikama akvizicije podataka sa računara koji radi (aktivna forenzika) a u zavisnosti od uslova (local live response, remote live response i hybrid live response). Takođe u ovoj nedelji studenti uče pravilan redosled prikupljanja podataka sa računara i načinom rukovanja prikupljenim podacima.

3. file system forensic

Treća nedelja predavanja u kojoj se studenti upoznaju sa specifičnostima različitih fajl sistema koji se mogu sresti u toku DF istrage na računarima, tabletima ili smart telefonima. Pokriveni su svi poznatiji fajl sistemi (NTFS, FAT/FAT32, EXT2/EXT3, RAISERFS, YAFFS, HFS+, HFSX...). U ovoj nedelji studenti se upoznaju i sa fizičkim uređajima sa kojih se prikupljaju podaci, uče kako da proračunaju stvarni kapaciteti određenih medija (geometrija diska).

4. memory forensic

Četvrta nedelja predavanja u kojoj se studenti upoznaju sa specifičnostima različitih vrsta memorija koje se mogu pojaviti prilikom DF istrage. Pokrivene su oblasti vezane za RAM memory forensic, SD/MMC card forensic, USB FLASH/NAND forensic, SSD forensic. Studenti uče i kako da rukuju sa podacima koji se prikupljaju sa ovih različitih vrsta memorija.

5. Internet forensic

Peta nedelja predavanja u kojoj se studenti upoznaju sa Internet forenzikom odnosno načinima kako prikupiti podatke sa računara koji je priključen na Internet (Internet artifakti). Oblasti koje su pokrivene su mail forensic, browser forensic (History, Cache, Searches, Downloads), chat client forensic (Facebook live, MSN Messenger, Yahoo, AIM, GoogleTalk chat)... Osim navedenog u ovoj nedelji studenti uče i analizu log fajlova.

6. Kolokvijum 1

Prva provera znanja

7. Network/Cloud forensic

Sedma nedelja predavanja u kojoj se studenti upoznaju sa mrežnom forenzikom odnosno načinima kako prikupiti podatke vezane sa računarsku mrežu i razne mrežne servise. Oblasti koje su prokrivene su network monitoring / sniffing (Wireshark), network logs, router forensic... Osim navedenog studenti se upoznaju i sa Cloud okruženjem i uče kako da prikupe podatke iz ovakvog okruženja.

8. OS forensic

Osma nedelja predavanja u kojoj se studenti upoznaju sa operativnim sistemima odnosno načinima kako prikupiti različite vrste podataka iz različitih OS-a. Oblasti koje su pokrivene su Windows forensic, Linux/unix forensic, android forensic, iOS forensic. Studenti se upoznaju sa specifičnostima različitih operativnih sistema i uče kako da analiziraju Registry bazu u Windows sistemima (Win 7, Windows 2008 Server...).

9. VM forensic

Deveta nedelja predavanja u kojoj se studenti upoznaju sa tehnikama virtuelizacija i načinima kako se vrši istraga virtuelnih mašina ili kako se virtuelna mašina koristiti kao forenzički alat.

Okruženja koja se najčešće koriste su obuhvaćena u ovom delu a to su (VMWare, Microsoft Hyper V i Oracle VirtuelBox). Takođe studenti se upoznaju sa specifičnostima prikupljanja podataka sa ovako pokrenutih virtuelnih računara i sa specifičnim načinom prikupljanja određenih podataka uz pomoć Suspend moda rada virtuelnog računara.

10. Anti-forensic

Deseta nedelja predavanja u kojoj se studenti upoznaju sa anti-forenzičkim tehnikama i alatima koji se često koriste. Oblasti koje su pokrivene su: data hiding, encryption, steganography, artifact wiping, trail obfuscation, attacks against computer forensics... U ovoj nedelji studenti se osim upoznavanja sa različitim vrstama anti-forenzičkih tehnika i alata upoznaju i sa načinom upotrebe virtuelnih mašina i live distribuciju u cilju skrivanja tragova izvršenja krivičnog dela.

11. Forensic tools 1 – open source

Jedanaesta nedelja predavanja u kojoj se studenti upoznaju sa besplatnim odnosno open-source alatima i distribucijama koje u sebi sadrže različite alate za DF istragu. Studenti se upoznaju sa dve najpoznatije distribucije za DF istragu a to su DEFT 7.2 i SIFT WORKSTATION 2.14, zatim sa najpoznatijom hakerskom distribucijom BACKTRACK 5 R3 i sa dostupnim alatima u navedenim distribucijama (AUTOPSY/SLEUTH KIT, DFF, PyFlag...)

12. Kolokvijum 2

Druga provera znanja

13. Forensic tools 2 – comercial

Trinaesta nedelja predavanja u kojoj se studenti upoznaju sa komercijalnim alatima i njihovim mogućnostima u DF istrazi. Studenti se detaljno upoznaju sa mogućnostima dva najpopularnija alata za DF istragu a to su AccesData FTK 4 i EnCase v7. Studenti uče da koriste ove alate u oblastima akvizicije i analize podataka koji su prikupljeni nekom od ranije naučenih tehnika.

14. Reporting/Expert witness

Četnaesta nedelja predavanja u kojoj se studenti upoznaju sa pravilnim pisanjem izveštaja kao i preporukama koje su nastale kao plod višegodišnjeg iskustva veštačenja u oblasti DF istrage. Takođe studenti se uče i pravilima svedočenja odnosno veštačenja na sudu (unakrsnog

ispitivanja) i ekspertize. Razvijena je i virtuelna sudnica gde studenti uče kako da pravilno prezentuju rezultate DF istrage.

8.1.2 DF silabus za master studije

Prvi korak je analiza programa prikazanih od strane DFCB (Digital Forensic Certification Board) [101]. Tabela 8.1 prikazuje nekoliko primera oblasti koje daju bolje razumevanje kategorija.

<u>Legal</u>
<u>Ethics</u>
<u>Storage Media</u>
<u>Mobile & Embedded Devices</u>
<u>Network Forensics</u>
<u>Program & Software Forensics</u>
<u>Quality Assurance, Control, & Management</u>

Tabela 8.1 DFCB kategorije

Još jednu analizu i mapiranje kurseva uradili su Beebe i Clark [102]. Tabela 8.2 daje prikaz nekoliko primera oblasti koje daju bolje razumevanje kategorija.

<u>Computer Science</u>
<u>Conducting Investigations</u>
<u>Data Analysis</u>
<u>Digital Forensic Awareness</u>
<u>Documentation & Findings Communication</u>
<u>Evidence Preservation & Collection</u>
<u>Evidentiary Issues</u>
<u>Incident Response</u>
<u>Law & Ethics</u>
<u>Preparation</u>

Tabela 8.2 Beebe i Clark kategorije

Istraživanje [103] fokusira se na izradu standardnog kurikuluma za master studije. Prikazana je trenutna situacija kroz analizu različitih vrsta master programa za područje USA.

Na osnovu navedinih radova u kojima su prikazani različiti kurikulumi za master u oblasti digitalne forenzike korišćeni na američkim univerzitetima kao i bitnih oblasti koje bi trebalo da budu pokrivene, definisan je sledeći kurikulum. On je prilagođen potrebama Univerziteta Singidunum i predstavlja nadogradnju prethodnog kurikuluma za osnovne studije:

- Napredna forenzička analiza bazirana na Hostu-Hipervizoru;
- Napredna mrežna-Cloud analiza;
- Napredne oblasti istraživanja u Cyber forenzici;
- Rekonstrukcija događaja i povezivanje;
- Hakerske tehnike (Hacking Exploits) i detekcija upada (Intrusion Detection);
- Analiza malvera (Malware) i osetljivosti programa (Software Vulnerability);
- Bezbednost mreže (Network Security), zaštita podataka i telekomunikacije;
- Pravni aspekti digitalne forezničke istrage;
- Istraživanje u oblasti DF/ Praktikum;
- Praksa (Internship).

8.1.3 DF silabus za doktorske studije (Phd)

U radu [93] predstavljen je kurikulum za doktorske studije u oblasti digitalne forenzike i analizirana je implementacija navedenog kurikuluma i na osnovnim studijama. Takođe je data diskusija o tome kako je navedeni kurikulum implementiran na California Sciences institutu. Autori su pronašli da je ključna stvar, nedostatak programa u oblasti digitalne forenzike na nivou master studija i da je kreiranje programa za doktorske studije sličan proces.

Na osnovu navedenog rada i iskustva sa master kurikulumima kreiran je sledeći kurikulum prilagođen potrebama Univerziteta Singidunum:

- Programirana digitalna forenzička analiza (fokus ovog kursa je na pisanju specijalnih programskih procedura za analizu digitalnih dokaza. Uključene su laboratorijske vežbe u rasponu od pisanja jednostavnih skriptova (simple shell and scripts) do pisanja specifičnih programa za forenzičku analizu.
- Izazovi u digitalnoj forenzici (na nivou doktorskih studija).

- Metodologija istraživanja (fokus ovog kursa je na kvalitativnim i kvantitativnim metodama istraživanja).

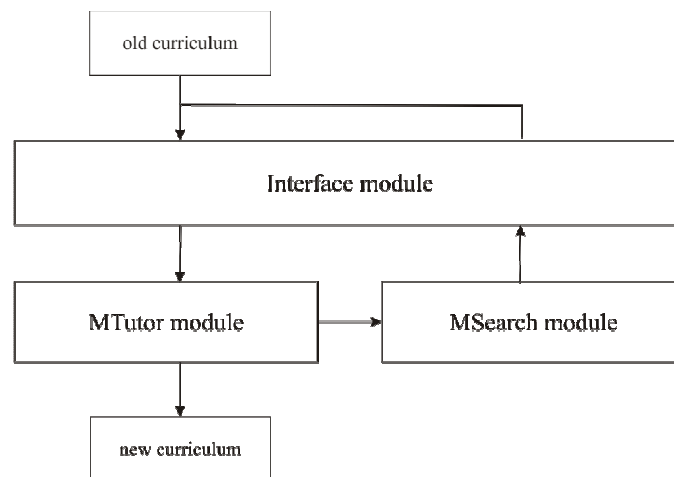
8.2 Dinamički kurikulumi

Kurikulum se definiše kao sadržaj određenog kursa ili kao program učenja u smislu znanja i veština, tj. kurikulum određuju glavne metode podučavanja, učenja i procene znanja. Kurikulum takođe indicira resurse učenja potrebne za efikasno održavanje predmeta (kursa). Silabus opisuje sadržaj određenog studijskog programa i može se posmatrati kao deo kurikuluma.

Elementi kurikuluma su: rezultati učenja, sadržaj, metodi podučavanja i učenja, procena znanja i razni resursi učenja. Postoji veliki broj radova posvećenih razvoju i dizajnu kurikuluma. Na Univerzitetu Singidunum u okviru virtuelnog univerziteta razvijaju se kurikulumi koristeći odoređeni pedagoški pristup baziran na studentskim profilima i edukacionim materijalima koji su dobijeni korišćenjem specijalnog modula uzimajući u obzir prethodna iskustva u učenju [113]. Kurikulum je razvijen modifikovan dinamički kroz monitoring i evaluaciju na kraju svakog semestra kada nastavnici uporede kurseve na matičnom univerzitetu sa kursevima na najuticajnijim univerzitetima na svetu. Polazna tačka u razvoju kurikuluma je IEEE kurikulum standard. Nastavnik bira materijale za predmet na osnovu svojih sklonosti i povratne sprege od studenata. Kreiranje novog kurikuluma je modularno sa ciljem da obezbedi nastavnicima osnovne teorijske principe i integriše pristup najboljeg pokušaja i najnovije trendove u edukacijiračunarskih nauka. Razvoj kurikuluma je iterativni proces sastavljen iz tri faze: evaluacija, izmena sadržaja, dodavanje novih metoda i korekcije.

Softverski sistem virtuelni univerzitet sastoji se od tri softverska modula (slika 8.1)

- Interfejs modul;
- Modul za dobijanje sadržaja (Msearch);
- Modul za procenu znanja (Mtutor).



Slika 8.1 Softverski sistem virtuelni univerzitet [113]

Analiza korišćenja sistema zajedno sa činjenicom da studenti teže da provedu mnogo više vremena u VE, opravdava izbor razvoja virtuelnog sistema orijentisanog ka integraciji virtuelnog i realnog okruženja.

9 Procena znanja i analiza postignutih rezultata i doprinosa

Originalni rezultati primene DF-lab dati su u radu [104]. Studenti prolaze kroz tri različita scenarija, gde stiču osnovna znanja i veštine i gde se vrši njihovo potpuno automatsko ocenjivanje. Scenariji se međusobno nadovezuju tako da svaki student mora redom da prođe kroz sva tri scenarija, gde se svaki od njih vrednuje sa 20 poena (što je ukupno 60). Ostalih 40 poena nosi teorijski deo koji se polaže na kraju preko sistema za testiranje Mtutor.

Scenario 1 – akvizicija podataka (hardware)

Studenti prolaze kroz kompletan postupak akvizicije podataka sa računara, od pristupa samom hardveru računara pa sve do montaže hard diska na blokator upisivanja (write blocker) i korišćenja različitih alata na forenzičkoj radnoj stanici. Vrlo je bitno poštovati standardne postupke i procedure koje su propisane standardima za akviziciju podataka koji se kasnije mogu koristiti kao validni dokazi na sudu. Studenti rade sa virtuelnim mašinama i simulira se pristup ekranu realnog računara. Ovim postupkom se smanjuju troškovi obuke jer nije potrebno fizičko prisustvo kandidata u laboratoriji a moguće je i simuliranje različitih vrsta hardverskih šteta na računaru (posledice vatre, eksplozije ...).

Koraci kroz koje student prolazi:

- Student kroz x3D okruženje ulazi u virtuelnu učionicu;



Slika 9.1 Izgled virtuelne učionice

- Prilazi računar (koji može biti i hardverski oštećen);
- Otvara bočnu stranu kućišta;



Slika 9.2 Model otvorenog računara u virtuelnoj učionici

- Demontira hard disk (rad sa “imidžom”);
- Prilazi forenzičkoj radnoj stanici koja je u stvari virtuelna mašina;
- Montira hard disk na radnu stanicu ali preko hard blockera (read only “imidž”) checkpoint 1;
- Pokreće forenzičku radnu stanicu (virtuelnu mašinu);
- Koristi FTK, EnCase (na virtuelnoj mašini) kako bi sa napravio “imidž” hard diska u 2 kopije checkpoint 2;



Slika 9.3 Model na kome se vidi forenzički laptop i write blocker

- Jednu kopiju čuva kao dokaz za eventualni sudski proces po svim standardima koji važe u ovoj oblasti (RFC2828 i RFC3227);
- Drugu kopiju koristi za analizu podataka uz pomoć različitih alata;
- Rezultate svog rada predstavlja u forenzičkom izveštaju koji ima propisanu formu i šalje ovlašćenom licu checkpoint 3;
- Isključuje forenzičku radnu stanicu i izlazi iz virtuelne učionice.

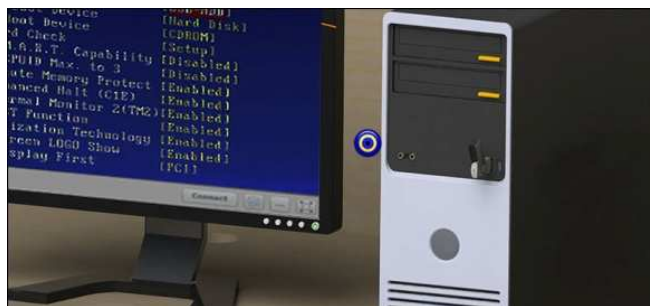
Ukupno ova aktivnost nosi 20 poena i prva tačka gde student dobija poene jeste montaža hard diska na radnu stanicu preko hard blokera gde dobija prvih 5 poena, druga tačka jeste pravljanje dva “imidža” diska uz pomoć FTK i Encase alata koja nosi 8 poena i krajnja tačka za ocenjivanje jeste popunjavanje forenzičkog izveštaja preko Web forme koja je napravljena za ovu namenu i nosi 7 poena.

Scenario 2 – akvizicija podataka (live disc)

Studenti prolaze kroz kompletan postupak akvizicije podataka sa računara korišćenjem Live diska (Helix, Spada). Simulira se postupak prilaska hardveru računara u virtuelnoj 3D učionici, zatim ubacivanje CD ili USB diska i butovanje sa njega, promenom parametara BIOS-a virtuelne mašine. Zatim studenti dobijaju mogućnost da koriste neku od specijalizovanih live distribucija i na taj način bez demontaže hard diska pristupaju određenim podacima koje mogu preneti na neki medijum ili preko računarske mreže na forenzičku radnu stanicu.

Koraci kroz koje student prolazi:

- Student kroz x3D okruženje ulazi u virtuelnu učionicu;
- Prilazi računaru i ako nije isključen isključuje računar (virtuelnu mašinu);
- Ubacuje CD ili USB disk;
- Pokreće računar (virtuelnu mašinu);
- Prilikom butovanja ulazi u BIOS (virtuelne mašine) checkpoint 1;



Slika 9.4 Model računara koji je pokrenut

- Menja parametre da se računar startuje prvo sa CD ili USB diska i izbacuje sa liste hard disk kako se ne bi eventualno zbog problema sa live diskom podigao operativni sistem i na taj način narušio integritet podataka;
- Računar se podiže sa live diska (Helix, Spada);
- Koriste se alati sa live diska da bi se prikupili potrebni podaci checkpoint 2;
- Podaci se skladište na neki disk (virtuelni disk) ili se šalju putem računarske mreže do forenzičke radne stanice gde se kasnije vrši dalja analiza podataka (FTK, EnCase);
- Rezultate svog rada predstavlja u forenzičkom izveštaju koji ima propisanu formu i šalje ovlašćenom licu checkpoint 3;
- Isključuje forenzičku radnu stanicu, računar na kome je podignut Helix i izlazi iz virtuelne učionice.

Ukupno ova aktivnost nosi 20 poena i prva tačka gde student dobija poene jeste ulazak u BIOS virtuelne mašine i promena parametara butovanja gde dobija prvih 5 poena, druga tačka jeste prikupljanje podataka uz pomoć alata Helix live distribucije koja nosi 8 poena i krajnja tačka za ocenjivanje jeste popunjavanje forenzičkog izveštaja preko Web forme koja je napravljena za ovu namenu i nosi 7 poena.

Scenario 3 – akvizicija podataka (network, local, remote)

Studenti prolaze kroz kompletan postupak akvizicije podataka sa računara koji radi i ne sme se isključiti jer se određeni podaci mogu nalaziti u RAM memoriji ili na nekim drugim mestima i

isključivanjem računara došlo bi do gubitka takvih podataka. Takođe je moguć i scenario u realnom radnom okruženju da računar obavlja neki posao koji se ne sme prekidati jer bi to nanelo veliku štetu kompaniji (Web server, server baze podataka, e-commerce). Studenti putem mreže pristupaju računaru koji radi, odnosno virtuelnoj mašini u ovom slučaju i koriste određene komande kako bi prikupili podatke putem mreže i preneli ih na forenzičku radnu stanicu.

Koraci kroz koje student prolazi:

- Student kroz x3D okruženje ulazi u virtuelnu učionicu;
- Prilazi forenzičkoj radnoj stanici (virtuelna mašina) i ukoliko računar nije uključen uključuje ga;
- Podešava komandom nc da forenzička radna stanica “izigrava” server koji na određenom portu očekuje podatke od računara koji će se ispitivati checkpoint 1;



Slika 9.5 Model forenzičke radne stanice u virtuelnom okruženju

- Sa forenzičke radne stanice udaljenim pristupom prilazi računaru koji će se ispitivati i koji je uključen i ne sme se isključivati zbog eventualnog gubitka podataka u RAM memoriji ili nekim privremenim fajlovima;
- Pokreće određene komande (sysinternals) i to određenim redosledom za prikupljanje podataka (RFC 3227 part 2.1 Order of Volatility) kako bi podatke sa tog računara putem mreže uz pomoć komande nc preneo na forenzičku radnu stanicu (postoje dve opcije, jedna je localna da se komande pokreću na samom računaru koji je predmet ispitivanja i da se sa njega šalju putem mreže do forenzičke radne stanice preko nc-a, a druga je udaljena gde se komande startuju na forenzičkoj radnoj stanici ali tako da se izvršavaju

ne na radnoj stanici već na računaru koji se ispituje i onda se podaci putem mreže prosleđuju do forenzičke radne stanice koja je prethodno konfigurisana i čeka podatke na određenom portu uz pomoć nc-a checkpoint 2;

- Posle prenosa podataka na forenzičku radnu stanicu sprovodi se postupak analize prikupljenih podataka (FTK, EnCase);
- Rezultate svog rada predstavlja u forenzičkom izveštaju koji ima propisanu formu i šalje ovlašćenom licu checkpoint 3;
- Isključuje forenzičku radnu stanicu i izlazi iz virtuelne učionice.

Ukupno ova aktivnost nosi 20 poena i prva tačka gde student dobija poene jeste podešavanje komandom nc.exe svoje virtuelne mašine da osluškuje određeni port za prenos podataka gde dobija prvih 5 poena, druga tačka jeste prenos podataka preko nc.exe sa kompromitovanog računara i analiza prikupljenih podataka koja nosi 8 poena i krajnja tačka za ocenjivanje jeste popunjavanje forenzičkog izveštaja preko Web forme koja je napravljena za ovu namenu i nosi 7 poena.

Na kraju kada student prođe sva tri scenarija polaže završni ispit na sistemu Mtutor gde se automatski ocenjuje nivo znanja. Kreiran je određen broj testova iz sledećih oblasti: hardverska akvizicija podataka – 7 poena, softverska akvizicija podataka (FTK, Encase, DEFT, SIFT, BACKTRACK) – 7 poena, akvizicija podataka kroz računarsku mrežu – 8 poena, analiza prikupljenih podataka – 8 poena, pisanje forenzičkog izveštaja – 5 poena, poznavanje forenzičkih standarda – 5 poena što ukupno nosi 40 poena.

Izvršena je kvalitativna i kvantitativna evaluacija predloženog rešenja za edukaciju. Kvalitativna evaluacija uključuje broj studenata koji su ispitivani i diskutovali sa predavačima. Cilj ispitivanja je bio da se sazna šta studenti prihvataju kao dobar alat za edukaciju i kako oni ocenjuju efikasnost ovog predloga. Većina anketiranih studenata na pitanje šta im se najviše sviđa istakla je intefejis DF-lab-a koji je intuitivan i lak za korišćenje.

Efikasnost laboratorije je merena poređenjem konačnih rezultata studenata koji su pristupali vežbanjima kroz DF-lab i realnom okruženju (fizičkoj laboratoriji). Rezultati završog ispita su

upoređeni. Ispitivanje je izvršeno u kontrolisanom okruženju i obuhvatalo je ukupno 40 studenata (20 studenata koji su koristili klasično fizičko okruženje i 20 koji su koristili virtuelno okruženje - VE).

	Kontrolna grupa (fizičko okruženje)	Eksperimentalna grupa (VE)
Broj studenata	20	20
Prosečni rez (points)	71.55	79.35
Standardna devijacija	17.73	15.20
Varijansa	314.35	232.04

Tabela 9.1 Statistička analiza rezultata

Rezultati završnog ispita analizirani su statistički korišćenjem T-testa. Kontrolna grupa je napravljena od studenata koji su koristili fizičko okruženje. Eksperimentalnu grupu su činili studenti koji su koristili virtuelno okruženje. Prosečni rezultat kontrolne grupe je 71.55, standardna devijacija je 17.73 a varijansa je 314.35. Za eksperimentalnu grupu prosečan rezultat je 79.35, standardna devijacija je 15.20 a varijansa je 232.04. Iz analize tabele sa rezultatima i odgovarajućim vrednostima u T-test tabeli može da se izvede zaključak da rezultati nisu statistički značajni što je bio i očekivan rezultat.

10 Zaključak i smernice za budući rad

U ovom radu dizajniran je i realizovan model 3D edukacionog okruženja za digitalnu forenziku sastavljeno od virtuelnih učionica i laboratorija koje obezbeđuju interaktivnost između učesnika, kao i specifičan pedagoški pristup baziran na povratnim informacijama učesnika u procesu obrazovanja, koji se koristi kao pomoćno sredstvo za edukaciju u oblasti digitalne forenzike.

U radu su prvo definisani osnovni principi i prikazana prethodna istraživanja i alati za digitalnu forenziku, virtuelna okruženja, vizualizaciju i virtuelizaciju. Opisana je primena 3D virtuelnih okruženja u edukaciji, predstavljena su i upoređena postojeća virtuelna okruženja i izabrano je odgovarajuće rešenje za realizaciju. Opisane su ontologije visokoškolske obrazovne institucije i digitalne forenzike.

Definisani su i analizirani model 3D virtuelnog okruženja, elementi, ontologije i hardverska platforma na kojoj je okruženje realizovano. Prikazana je forenzička laboratorija (biblioteke forenzičkih scenarija i slučajeva). Na osnovu sugestija i komentara studenata pojedinačno za svaki semestar, kao i prethodno stečenog iskustva kreiran je kompleksni virtuelni edukacioni model koji se lako može primeniti u različitim oblastima. Realizovan je softverski paket za različita anketiranja studenata. Na osnovu povratnih informacija učesnika u procesu obrazovanja dinamički se kreiraju: grafički interfejs, sadržaj, tutorijal, komunikacije, brzina rada i kurikulumi. Predstavljani su silabusi za osnovne, master i doktorske studije kao i dinamički kurikulumi.

Budući rad uključuje uvođenje DF-lab u redovnu nastavu i automatizaciju svih koraka uvođenjem veštačke inteligencije i generalizacije, standardizacije i dobijanja opšteg modela koji će biti primenljiv u različitim oblastima. Cilj je razvoj okruženja za samoučenje i samotestiranje koje pruža mogućnost praćenja studentskih profila i statistike korišćenja okruženja i generisanje zaključaka i pravila za prilagođavanje silabusa i kurikuluma. Verujemo da će u budućnosti obrazovne institucije prihvatiti virtuelna okruženja na svim nivoima obrazovanja i ovaj rad predstavlja pokušaj prezentovanja ovog pristupa u edukaciji digitalnih forenzičara.

11 Literatura

- [1] Ibáñez-Martínez, J., Delgado-Mata, C., & Aylett, R. (2006, April 2). Virtual Environments: A Multi-disciplinary Field. *Upgrade - The European Journal for the Informatics Professional* , VII (2), pp. 2-5.
- [2] Schroeder, R. (1996). Possible Worlds: The Social Dynamic of Virtual Reality Technologies. *Westview Press* .
- [3] Schroeder, R. (2006). Being There and the Future of Connected Presence. *Journal of Teleoperators and Virtual Environments* , 15 (4), pp. 438-454.
- [4] Schroeder, R. (2008, July). Defining Virtual Worlds and Virtual Environments. *Journal of Virtual Worlds Research* , Vol.1 (No.1).
- [5] Castronova, E. (2001). Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier. *The Gruter Institute Working Papers on Law, Economics, and Evolutionary Biology* , 2 (1).
- [6] Prentice, S. (2008). Virtual Worlds - What to Expect in 2009. *Virtual Worlds Forum 08*. London.
- [7] Bartle, R. A. (2003). *Designing Virtual Worlds*. Indianapolis: New Riders.
- [8] Damer, B. (1998). *Avatars!* Berkeley: Peachpit Press.
- [9] Perlin, K. (2000). Creating Emotive Responsive Characters Within Virtual Worlds. In J. C. Heudin (Ed.), *VW 2000, LNAI 1834* (pp. 99-106). Berlin Heidelberg: Springer-Verlag.
- [10] Robertson, G., Card, S., & Mackinlay, J. (1993). Nonimmersive virtual reality. *Computer*, 26(2), 81-83.
- [11] Kauff, P., Schäfer, R., & Schreer, O. (2000, September). Tele-immersion in shared presence conference systems. *International Broadcasting Convention*, Amsterdam.
- [12] Dalgarno, B. J. (2004). Characteristics of 3D environments and potential contributions to spatial learning. Unpublished doctoral dissertation, University of Wollongong, Faculty of Education.
- [13] Ko, C. C., & Cheng, C. D. (2009, July). Interactive Web-based virtual reality with java 3D. In (p. 4-5). Hershey, PA: IGI Global.
- [14] Beier, K. (2004). Virtual reality: A short introduction.
- [15] Horne, M., & Hamza, N. (2006). Integration of virtual reality within the built environment curriculum. *ITcon Vol. 11*(2006).
- [16] Lascara, C., Wheless, G., Cox, D., Patterson, R., Levy, S., Johnson, A. E., et al. (1999). Teleimmersive virtual environments for collaborative knowledge discovery. *Advanced Simulation Technologies Conference*, San Diego, CA.
- [17] Park, K. S., Kapoor, A., Scharver, C., & Leigh, J. (2000, June 19-20). Exploiting multiple perspectives in tele-immersion. In *Proceedings of the 4th international immersive projection technology workshop*. Ames, Iowa, US.

- [18] Kjeldskov, J. (2001). Interaction: Full and partial immersive virtual reality displays. In In proceedings of iris24 (p. 587-600).
- [19] Bar-Zeev, A. (2009, March 23). Retrieved June 1, 2009, from RealityPrime: The [unofficial] History of Virtual Worlds
- [20] Bell, M. W. (2007). *Definition of Virtual Worlds*. Retrieved August 7, 2009
- [21] Capin, T. K., Pandzic, I. S., Magnenat-Thalmann, N., & Thalmann, D. (1999). *Avatars in Networked Virtual Environments*. Chichester: John Wiley & Sons Ltd.
- [22] Sutherland, I. E. (1968). A head-mounted three-dimensional display. *Proceedings of the Fall Joint Computer Conference*, (pp. 757-764).
- [23] Antunes, R., Fonseca, B., Martins, P., & Morgado, L. (2006). Use of 3-D virtual environments to support the learning of programming. *FORMATEX*, (pp. 689-673).
- [24] Damer, B. (2008, July). Meeting in the Ether - A brief history of virtual worlds as a medium for user-created events. *Journal of Virtual Worlds Research* (Vol.1, No.1).
- [25] Koster, R. (2000, March 4). *Raph Koster's Website*. Retrieved June 2, 2009, from Online World Timeline
- [26] *DigiBarn computer museum*. (2004, November 7). Retrieved June 2, 2009, from DigiBarn Events: Maze War 30 Year Retrospective
- [27] Kennelly, A. (2006, September 8). *Articlesbase - Free Online Articles Directory*. Retrieved June 7, 2009, from Massive Multiplayer Online Role-Playing Games
- [28] Morningstar, C., & Randall Farmer, F. (1991). The Lessons of Lucasfilm's Habitat. In M. Benedikt (Ed.), *Cyberspace: First Steps*. Cambridge: MIT Press.
- [29] Kent, S. L. (2003, September 23). *GameSpy.com*. Retrieved June 9, 2009, from Gaming's Homepage
- [30] Koster, R. (2005). *Theory of Fun*. Arizona: Paralyph Press.
- [31] *The Contact Consortium*. (1996). Retrieved 13 June, 2009, from About the Contact Consortium and its Member Services
- [32] *VLearn3D*. (2001). Retrieved June 17, 2009, from VLearn3D – About
- [33] Damer, B., Gold, S., de Bruin, J., & de Bruin, D. J. (2000). Conferences and Trade Shows in Inhabited Virtual Worlds: A Case Study of Avatars98 & 99. In J. C. Heudin (Ed.), *VW 2000, LNAI 1834* (pp. 1-11). Berlin Heidelberg: Springer-Verlag.
- [34] Bainbridge, E. G. (2007). *Avatarplanet*. Retrieved August 7, 2009, from History of virtual worlds
- [35] Kluge, S., & Riley, L. (2008). Teaching in Virtual Worlds: Opportunities and Challenges. *Issues in Informing Science and Information Technology* (5), pp. 127-135.

- [36] Calongne, C. M. (2008, September/October). Educational Frontiers: Learning in a Virtuel World. *EDUCAUSE Review* , 43 (5).
- [37] In-Cheol, K. (2006). 3D Interactive Computer Games as a Pedagogical Tool. In Z. Hongbin, P. Zhigeng, T. Hal, A. C. Addison, & M. Forte (Ed.), *VSM 2006, LNCS 4270* (pp. 536-544). Berlin Heidelberg: Springer-Verlag.
- [38] Maher, M. L., Skow, B., Cicognani, A. (1999). Designing the virtuel campus. *Design Studies*, 20(4), 319 – 342.
- [39] Boulos, M. N. K., Hetherington, L., Wheeler, S. (2007). Second life: an overview of the potential of 3-d virtuel worlds in medical and health education. *Health Information & Libraries Journal*, 24(4), 233–245.
- [40] Dickey, M. D. (2005). Three-dimensional virtuel worlds and distance learn- ing: two case studies of active worlds as a medium for distance education. *British Journal of Educational Technology*, 36(3), 439-451.
- [41] Berge, Z. L. (2008, May–June). Multi-user virtuel environments for education and training? a critical review of second life. *Educational Technology Magazine: The Magazine for Managers of Change in Education*, 48(3), 27–31.
- [42] Chittaro, L., Ranon, R. (2007). Web3D technologies in learning, education and training: motivations, issues, opportunities. *Computers & Education*, 49, 3–18.
- [43] Moore, P. (1995). Learning and teaching in virtuel worlds: Implications of virtuel reality for education. *Australian Journal of Educational Technology*, 11, 91–102.
- [44] Dalgarno, B., Hedberg, J. (2001). 3D learning environments in tertiary education. In *Ascilite'01: Meeting at the crossroads* (pp. 33–36). Melbourne, Victoria.
- [45] Ang, K. H., Wang, Q. (2006, December). A case study of engaging primary school students in learning science by using active worlds. In (pp. 5–14). Sydney, Australia.
- [46] Sanders, R., McKeown, L. (2007). Promoting reflection through action learning in a 3D virtuel world. *International Journal of Social Sciences*, 2(1), 50–56.
- [47] Holmberg, K., Huvila, I. (2008, October). Learning together apart: Distance education in a virtuel world. *First Monday*, 13(10).
- [48] Milosavljević M., Grubor G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum 2009, ISBN: 978-86-7912-171-4
- [49] National Policing Improvement Agency, *Core Skills in Data Recovery & Analysis Reference Book V2.01*, Bradford, UK, maj 2007.
- [50] Whitcomb C M., *A Historical perspective of Digital Evidence: A Forensic Scientist s View*, *International Journal of Digital Evidence*, , vol.1, issue 1, 2002.

- [51] Franc I., Grubor G., „METHODICAL DATA COLLECTING FOR FORENSIC ANALYSIS PURPOSE FROM LIVE SYSTEMS", Conference ZITEH, Belgrade 2010
- [52] Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, Syngress 2011 Elsevier ISBN: 978-1-59749-586-8
- [53] Smith F. C., Gurley R. B., A Guide to Forensic Testimony – The art and Practice of Presenting testimony as an Expert Technical Witness, Addison – Wesley, Boston SAD, 2002.
- [54] Franc I., Grubor G., „THE DIGITAL FORENSIC INVESTIGATION MODELS EVOLUTION", Conference ZITEH, Belgrade 2010
- [55] Nance, K., Bishop, M. i Hay, *Virtual Machine Introspection: Observation or Interference*, IEEE [55]
- [56] Security & Privacy, Volume 6 Issue 5, pp. 32-37, Sept.-Okt. 2008. Carrier, B., *File System Forensic Analysis*, Addison-Wesley, Boston, MA, 2005.
- [57] Wei Shi ; Lee, G. ; Hinchley, J. ; Corriveau, J.P. ; Kapralos, B. ; Hogue, A., Using a Virtual Learning Environment with Highly Interactive Elements in Second Life to Engage Millennial Students, e-Education, e-Business, e-Management, and e-Learning, 2010. IC4E '10. International Conference, 2010
- [58] Boulos, M.N.K.; Hetherington, L. & Wheeler, S. Second Life: an overview of the potential of 3-D virtual worlds in medical and health education. *Health Information & Libraries Journal* 2007, 24(4), pp. 233–245.
- [59] Kemp, J. , Livingstone, D. Putting a Second Life “Metaverse” Skin on Learning Management Systems, in proceedings of the Second Life Education Workshop at SLCC, San Francisco, August 2006, pp.13-18.
- [60] Santos, F.R. Guetl, C. Bailey, P.H. Harward, V.J. Dynamic virtual environment for multiple physics experiments in higher education, *Education Engineering (EDUCON)*, 2010 IEEE, pp. 731-736
- [61] Blair, J., Fuhua Lin, An Approach for Integrating 3D Virtual Worlds with Multiagent Systems, *Advanced Information Networking and Applications (WAINA)*, 2011 IEEE Workshops of International Conference, pp. 580-585
- [62] Ranaweera, R. Spatial Media Group, Univ. of Aizu, Aizu-Wakamatsu, Japan Frishkopf, M.; Cohen, Michael, *Folkways in Wonderland: A Cyberworld Laboratory for Ethnomusicology*, *Cyberworlds (CW)*, 2011 International Conference, 106-112
- [63] Judy F. Chena, Clyde A. Wardenb, David Wen-Shung Taic, Farn-Shing Chend, Chich-Yang Chaod, Level of abstraction and feelings of presence in virtual space: Business English negotiation in Open Wonderland, Elsevier, *Computers & Education* Volume 57, Issue 3, November 2011, Pages 2126–2134
- [64] Callaghan V, Shen L, Gardner M, Shen R, Wang M (2010) A Mixed Reality Approach to Hybrid Learning in Mixed Culture Environments, in *Handbook of Research on Hybrid Learning Models: Advanced Tools, Technologies, and Applications*, 260-283 pp, IGI Global

- [65] Gardner M, Adela G-G, Scott J, Horan B, Callaghan V, Immersive education spaces using open wonderland: from pedagogy through to practice, Chapter 13 in “Multi-User Virtuel Environments for the Classroom: Practical Approaches to Teaching in Virtuel Worlds” edited by G. Vincenti & J Braman, Published by Information Science Reference (an imprint of IGI Global), Hershey PA, USA, 2011 ISBN 978-1-60960-545-2
- [66] R. Sassen, WonderSchool: Open Wonderland and Collaboration using Alice, Presented at the 2nd European Immersive Education Summit – 26-27 November 2012, Paris, France.
- [67] Rainer Poisel, Erich Malzer, and Simon Tjoa, Evidence and Cloud Computing: The Virtuel Machine Introspection Approach, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2012 volume: 4, number: 1, pp. 135-152
- [68] Dominik Birk, Christoph Wegener, Technical Issues of Forensic Investigations in Cloud Computing Environments, Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop, ISBN: 978-1-4673-1242-4, pp. 1-10
- [69] Denis Reilly, Chris Wren, Tom Berry, Cloud Computing: Pros and Cons for Computer Forensic Investigations, International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, March 2011
- [70] Mell P., Grance T., The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 (Draft), National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.
- [71] Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie , Advances in Digital Forensics VII, 7th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 31 – February 2, 2011
- [72] Shams Zawoad, Ragib Hasan, Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems (arXiv preprint arXiv:1302.6312)
- [73] Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, Shuo Chen, Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System, TSINGHUA SCIENCE AND TECHNOLOGY Volume 18, Number 1, February 2013, ISSN 1007-0214 05/12 pp 40-50
- [74] Jeff Lessard, Gary C. Kessler, Android Forensics: Simplifying Cell Phone Examinations, SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL VOL. 4, NO.1, SEPTEMBER 2010, ISSN# 1941-6164
- [75] Archit Goel, Anurag Tyagi, Ankit Agarwal, Smartphone Forensic Investigation Process Model, International Journal of Computer Science & Security (IJCSS), Volume (6) : Issue (5) : 2012, pp. 322-341
- [76] Brian Carrier, Open Source Digital Forensics Tools: The Legal Argument, @stake’s Center of Excellence – Incident Management & Forensics, Research Report, 2002
- [77] Brian Carrier, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, International Journal of Digital Evidence, Winter 2003, Volume 1, Issue 4

- [78] Vishal R. Ambhire, Dr. B.B. Meshram, Digital Forensic Tools, IOSR Journal of Engineering, ISSN: 2250-3021, Mar. 2012, Vol. 2(3) pp: 392-398
- [79] Derek Bem, Ewa Huebner, Computer Forensic Analysis in a Virtuel Environment, International Journal of Digital Evidence, Fall 2007, Volume 6, Issue 2
- [80] Julia Narvaez, Chiraag Aval, Barbara Endicott-Popovsky, Christian Seifert, Ashish K. Malviya, Douglas Nordwall, Assessment of Virtuelization as a Sensor Technique Comparison of detection capabilities of honeypots deployed in virtuel environments versus physical machines, 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, ISSN 978-0-7695-4052-8/10, pp 61-65
- [81] Sina Manavi, Sadra Mohammadalian, Nur Izura Udzir, Azizol Abdullah, Secure Model for Virtuelization Layer in Cloud Infrastructure, International Journal of Cyber-Security and Digital Forensics (IJCSDF) pp. 32-40, The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012)
- [82] Sasa Mrdovic, Alvin Huseinovic, Ernedin Zajko, Combining Static and Live Digital Forensic Analysis in Virtuel Environment, Information, Communication and Automation Technologies, 2009. ICAT 2009. XXII International Symposium, ISSN 978-1-4244-4221-8/09
- [83] Smita V. Khengar, G. H. R. C. E. Nagpur, and Rajiv V. Dharaskar, Digital Forensic Investigation for Virtuel Machines, International Journal of Modeling and Optimization, Vol. 2, No. 6, December 2012, pp. 663-666
- [84] Mamoun Alazab, Sitalakshmi Venkatraman, Paul Watters, EFFECTIVE DIGITAL FORENSIC ANALYSIS OF THE NTFS DISK IMAGE, Special Issue on ICIT 2009 Conference - Applied Computing, UbiCC Journal – Volume 4 No. 3, pp. 551-558
- [85] Sindhu. K. K, Shweta Tripathi, Dr.B.B. Meshram, Digital Forensic investigation on File System And Database Tampering, IOSR Journal of Engineering (IOSRJEN), ISSN : 2250-3021, Vol. 2 Issue 2, Feb.2012, pp.214-221
- [86] Mousa Al Falayleh (2012) BUILDING A DIGITAL FORENSIC LABORATORY FOR AN EDUCATIONAL INSTITUTE. In: The International Conference on Computing, Networking and Digital Technologies (ICCNDT2012)
- [87] Kara Nance, Helen Armstrong, Colin Armstrong (2010) Digital Forensics: Defining an Education Agenda. In: 43rd Hawaii International Conference on System Sciences
- [88] Crellin, Jonathan and Karatzouni, Sevasti (2009) Simulation in digital forensic education. In: Third International Conference on Cybercrime Forensic Education and Training (CFET3) (BCS SIG)
- [89] Crellin, Jonathan, Adda, Mo, Duke-Williams, Emma and Chandler, Jane (2011) Simulation in computer forensics teaching: the student experience. In: Researching Learning in Immersive Virtuel Environments 2011

- [90] Christopher A. Lee, Kam Woods, Digital Acquisition Learning Laboratory: A White Paper, School of Information and Library Science University of North Carolina at Chapel Hill November 2011
- [91] Paul Stephens, Abhaya Induruwa, Cybercrime Investigation Training and Specialist Education for the European Union, Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), ISBN: 0-7695-2941-0/07 pp. 28-37
- [92] Gary C. Kessler, Don Haggerty, Pedagogy and Overview of a Graduate Program in Digital Investigation Management, Hawaii International Conference on System Sciences, Proceedings of the 41st Annual 2008, ISSN: 1530-1605, pp. 481
- [93] Frederick B. Cohen, P, A Ph.D. Curriculum for Digital Forensics, System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference, ISBN: 978-0-7695-3450-3/09, pp. 1-8
- [94] Eddie Soon Eu Hui, Asst. Prof. Roberts Hedley, Dr. Daniela Leva, Interactive 3D Forensic Visualisation: Virtuel Interactive Prototype, Computer Graphics, Imaging and Visualisation (CGIV 2007), ISBN: 0-7695-2928-3/07, pp. 148-153
- [95] Jeffrey S. Marean; Mike Losavio, JD; Dr. Ibrahim Imam, A Research Configuration for a Digital Network Forensic Lab, Third International Workshop on Systematic Approaches to Digital Forensic Engineering 2008, ISBN: 978-0-7695-3171-7/08, pp. 141-142
- [96] Ben Martini, Kim-Kwang Raymond Choo, An integrated conceptual digital forensic framework for Cloud computing, Elsevier, Digital Investigation, Volume 9, issue 2 (November, 2012), p. 71-80, ISSN: 1742-2876
- [97] Dominik Birk, Christoph Wegener, Technical Issues of Forensic Investigations in Cloud Computing Environments, Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop, ISBN: 978-1-4673-1242-4, pp. 1-10
- [98] Ashley Brinson, Abigail Robinson, Marcus Rogers, A cyber forensics ontology: Creating a new approach to studying cyber forensics, Digital Investigation, Volume 3, issue (September, 2006), p. 37-43, ISSN: 1742-2876
- [99] Damir Kahvedzic, Tahar Kechadi, DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge, Digital Investigation, Volume 6, issue (September, 2009), p. S23-S33, ISSN: 1742-2876
- [100] Jingshan Huang, Alec Yasinsac, Knowledge Sharing and Reuse in Digital Forensics, Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop, ISBN: 978-0-7695-4052-8, pp. 73-78
- [101] Digital Forensic Certification Board. (2009). DFCB KSA Domains. Retrieved November 2, 2009, from Digital Forensic Certification Board: http://www.ncfs.org/dfcb/DFCB_Final_KSAs-submiited-3-15-2009.pdf

- [102] Beebe, N.L. & Clark, J.G. (2006). Digital forensics curriculum development: Identification of knowledge domains learning objectives and core concepts. Proceedings of the Twelfth Americas Conference on Information Systems, Acapulco, Mexico.
- [103] Kathleen Strzempka, The Development of a Standard Digital Forensics Master's Curriculum, Purdue University, College of Technology Masters Theses 2010
- [104] Igor Franc, Zona Kostić, Aleksandar Jevremović, Ranko Popović, „DF-lab Digital forensic virtual laboratory for collaborative distance learning“, Metalurgia International 2013 SPECIAL ISSUE vol. 8-2013 ISSN 1582 – 2214, pp. 102-107
- [105] Igor Franc, Gojko Grubor, Angelina Njeguš „The use of ethical hacking in active forensic investigation“, Metalurgia International SPECIAL ISSUE vol. 8-2013 ISSN 1582 – 2214 , pp. 265-270
- [106] I. Branovic, D. Markovic, R. Popovic, V. Tomasevic, D. Zivkovic, Development of modular virtual lab for introductory computing courses, 2013 IEEE Global Engineering Education Conference (EDUCON), pp. 1027–1031, Berlin, Germany, 2013.
- [107] Hong-Rong Yang, Ming Xu and Ning Zheng, “An Improved Method for Ranking of Search Results Based on User Interest”, IFIP International Conference on Network and Parallel Computing, 2008, pp. 132-138
- [108] Hoss A.M, Carver D.L, “Weaving ontologies to support digital forensic analysis”, IEEE International Conference on Intelligence and Security Informatics, 2009, pp. 203-205
- [109] Mannes A and Golbeck J, ” Ontology Building: A Terrorism Specialist's Perspective”, IEEE Aerospace Conference, 2007, pp. 1-5
- [110] Gruber, T. A translation approach to portable ontology specifications, Knowledge Acquisition, An International Journal of Knowledge Acquisition for Knowledge-Based Systems, Volume 5, Number 2, pp. 199-220, 1993.
- [111] Guarino, N. Formal Ontology and Information System [Conference] // Proceeding of FOIS98. - Trento-Italy : IOS Press - Amsterdam , 1998. - pp. 3-15.
- [112] Pretorius, J. Ontologies-Intruduction and Overview [Journal]. - 2004. Protege Project [Online] // <http://protege.stanford.edu/>. - jun 12, 2013. - <http://protege.stanford.edu/>.
- [113] Z. Kostic, A. Jevremovic, I. Branovic, D. Markovic, R. Popovic, Dynamic Composition of Curriculum for Computer Science Courses, ICIW 2012: The Seventh International Conference on Internet and Web Applications and Services, Stuttgart, pp. 238-243