Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-496-499

3D EDUKACIONO OKRUŽENJE ZA DIGITALNU FORENZIKU

Igor Franc, Zona Kostić
Univerzitet Singidunum, Srbija

Abstract:
Da bi se edukovali digitalni forenzičari neophodno je da postoji dobra teorijska podloga ali ono što je još važnije neophodno je razviti različite vrste laboratorijskih vežbi gde bi se studenti kroz realne slučajeve iz prakse obučavali i sticali potrebna znanja i veštine. U radu je kreiran određen broj najčešćih slučajeva iz prakse i scenarija koji su povezani kompozitno komponentnim modelom i omogućavaju studentima interaktivno učenje. Date su kvalitativna i kvantitativna evaluacija predloženog rešenja, kao i predikcije po pitanju korišćenja laboratorije i njene integracije u sisteme za učenje na daljinu.

Key words:
Digitalna forenzika,
virtuelna okruženja,
učenje na daljinu,
kompozitno komponentni model,
interaktivno učenje.

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, integrisanih virtuelnih i realnih okruženja.

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

Prvi softver koji je koristio virtuelno okruženje bio je Maze War (1974. godina) [1]. Maze je pružao korisniku osećaj da je "prisutan i da se kreće" kroz virtuelno okruženje. Podržavao je osam igrača (robota) [2]. 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 [1]. Činjenica da su računari i Internet stigli u domove ljudi, otvorila je vrata ne samo industriji igara i programerima i istraživačima društvenih virtuelnih okruženja [3].

U prelaznom periodu između dva milenijuma mnoge kompanije i investitori su bankrotirali u ranoj fazi usvajanja Internet društvenih virtuelnih okruženja [1]. Bilo je postavljeno pitanje da li 21 su društvena okruženja održiv medij ili evolutivni promašaj. Odgovor je bio uspon društvenih mreža (My Space, Facebook, Linkedln), 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 [1]. Početkom 2003. godine pojavile su se beta verzije virtuelnih okruženja (Second Life, There …) [4].

U oblasti edukacije postoji veći broj radova od kojih će samo neki biti navedeni. U radu [5] 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 [6] 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 funcionalnosti besplatne za korišćenje. U radu [7] autor je kreirao i implementirao laboratoriju za učenje u oblasti digitalne forenzike, za akviziciju digitalnih dokaza. U radu

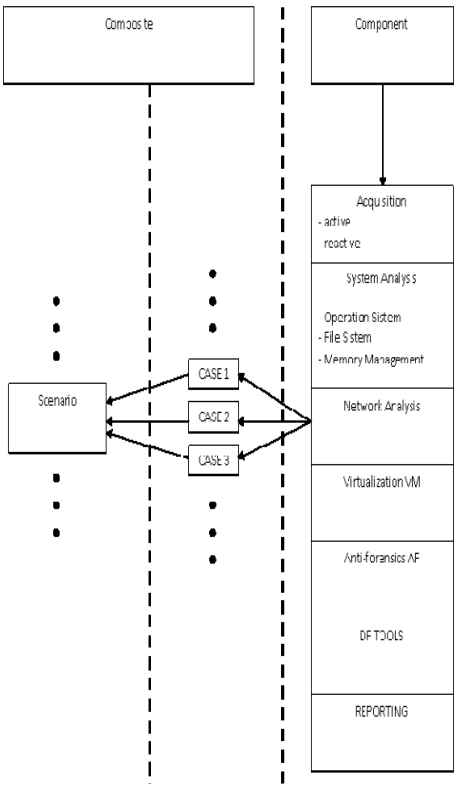
su uključene i specifikacije treninga, hardvera i softvera za pokretanje praktičnih vežbi na kursu u školi Information and Library Science (SILS) na University North Carolina. U radu [8] predstavljen je novi model za obuku digitalnih forenzičara. Predstavljena laboratorija se bazira na X3D okruženju sa VNC protokolima za pristup virtuelizovanim klijentima.

MODELOVANJE I ANALIZA

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.

Komponentno kompozitni model

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 1.1).



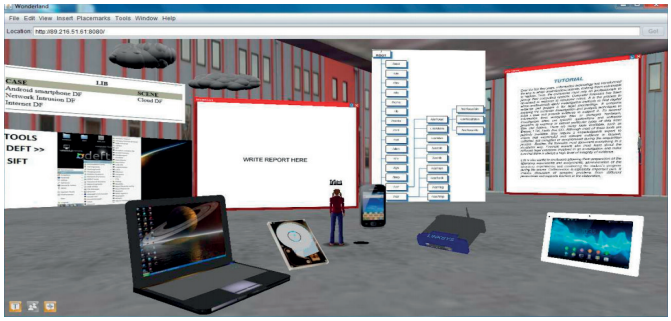
Slika 1.1 Osnovne komponente i kompozicije u digitalnoj forenzici

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.

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);
- Screen Sharer (za deljenje dela ekrana sa ostalim članovima);
- Kolaborativni Text Editor (za pisanje zajedničkog izveštaja);
- Text chat (za međusobnu tekstualnu komunikaciju među članovima);
- Voice chat (za međusobnu glasovnu komunikaciju među članovima).



Slika 1.2 Prikaz okruženja za akviziciju i analizu u Open Wonderland

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).

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.

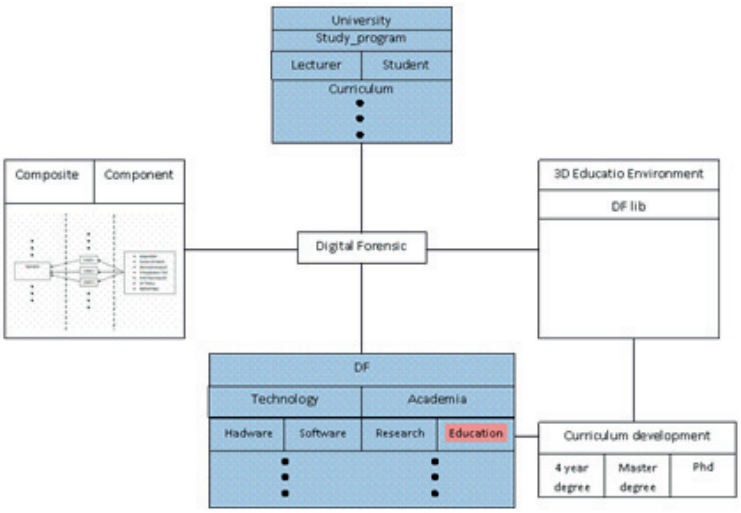
Protokoli koji se koriste u virtuelnoj laboratoriji su RDP 8.0 i VNC. RDP (Remote Desktop Protocol) je protokol koji se koristi za daljinski pristup desktopu virtuelnog računara i omogućava sigurnu tj. šifrovanu komunikaciju. Aktuelna verzija je 8.0 i ona je podržana od strane MS Windows 8 i Windows 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.

REALIZACIJA

U radu je dat nov pristup u edukaciji u oblasti digitalne forenzike (slika 1.3):

- 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 1.3 Arhitektura DF modela

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 poslati na server, podeljen po korisnicima ili grupama);
- Alati za navigaciju (sinhronizacija kontrole nad objektima koje istovremeno može da upotrebi nekoliko korisnika);
- Multimedijski alati (video striming, URL navigacija, snimanje video i audio zapisa unutar okruženja).

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.

Forenzička laboratorija

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.

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.

Dinamički kurikulumi

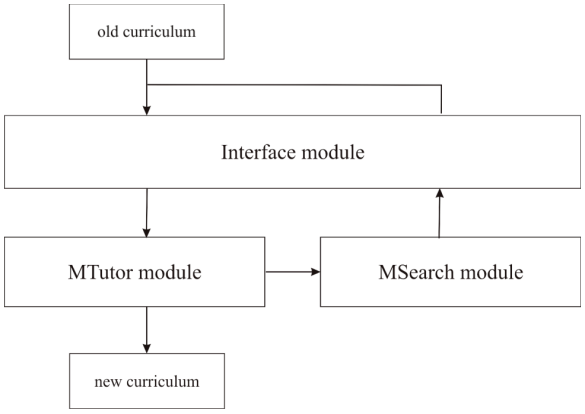
Kurikulum se definiše kao sadržaj određenog kursa ili kao program učenja u smislu znanja i veština, tj. kurikulum određuju glavne metode podučavanja, učenja i procene znanja. Kurikulum takođe indicira resurse učenja potrebne za efikasno održavanje predmeta (kursa). Silabus opisuje sadržaj određenog studijskog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

Na Univerzitetu Singidunum u okviru virtuelnog univerziteta razvijaju se kurikulumi koristeći odereñeni pedagoški pristup baziran na studentskim profilima i edukacionim materijalima koji su dobijeni korišćenjem specijalnog modula uzimajući u obzir prethodna iskustva u učenju [9].

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 edukaciji računarskih nauka.

Softverski sistem virtuelni univerzitet sastoji se od tri softverska modula (slika 1.4)

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



Slika 1.4 Softverski sistem virtuelni univerzitet [9]

PROCENA ZNANJA I ANALIZA POSTIGNUTIH REZULTATA

Originalni rezultati primene DF-lab dati su u radu [8]. 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.

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).

Tabela 1.1 Statistička analiza rezultata

	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

Rezultati završnog ispita analizirani su statistički korišćenjem T-testa. Kontrolna grupa je napravljena od studenata koji su koristili fizičko okruženje. Eksperimenatalnu grupu su činili studenti koji su koristili virtuelno okruženje. Prosečni rezultat kontrolne grupe je 71.55, standardna devijacija je 79.35 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.

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.

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.

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.

LITERATURA

[1] Damer, B. (2008, July). Meeting in the Ether - A brief history of virtuel worlds as a medium for usercreated

[2] Koster, R. (2000, March 4). Raph Koster's Website. Retrieved June 2, 2009, from Online World Timeline

[3] Bartle, R. A. (2003). Designing Virtuel Worlds. Indianapolis: New Riders.

[4] Bainbridge, E. G. (2007). Avatarplanet. Retrieved August 7, 2009, from History of virtuel worlds

[5] Crellin, Jonathan and Karatzouni, Sevasti (2009) Simulation in digital forensic education. In: Third International Conference on Cybercrime Forensic Education and Training (CFET3) (BCS SIG)

[6] 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

[7] 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

[8] Igor Franc, Zona Kostić, Aleksandar Jevremović, Ranko Popović, „DF-lab Digital forensic virtuel loboratory for collaborative distance learning", Metalurgia International 2013 SPECIAL ISSUE vol. 8- 2013 ISSN 1582 – 2214, pp. 102-107

[9] Z. Kostić, A. Jevremović, I. Branović, D. Marković, R. Popović, 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