Kriminalističke teme
Časopis za kriminalistiku, kriminologiju i sigurnosne studije
Godina XVII, Broj 1-2, 2018. str. 117-121
ISSN 1512-5505

ZIMSKA ŠKOLA "DIGITALNA FORENZIKA I INFORMACIJSKA SIGURNOST"

Prikaz

WINTER SCHOOL "DIGITAL FORENSICS AND INFORMATION SECURITY"

Review

Renata KLAČAR

Uvod

Na Fakultetu za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu, u saradnji sa Microsoft-om Bosne i Hercegovine, u periodu od 19. januara do 10. februara 2018. godine održana je zimska škola pod nazivom *„Digitalna forenzika i informacijska sigurnost".* Pored Microsoft-a Bosne i Hercegovine, partneri u realizaciji ovog projekta su Ministarstvo sigurnosti Bosne i Hercegovine, Državna agencija za istrage i zaštitu - SIPA, te Centar za edukaciju sudija i tužilaca FBiH.

U ovom akademskom programu cjeloživotnog učenja učestvovalo je više od 50 polaznika, i to stručnjaci iz IT sektora, agencija za provedbu zakona u Bosni i Hercegovini, te studenti Univerziteta u Sarajevu - Fakulteta za kriminalistiku, kriminologiju i sigurnosne studije, Elektrotehničkog fakulteta, Fakulteta političkih nauka, te sa drugih visokoškolskih ustanova. Akademsko osoblje Fakulteta za kriminalistiku, kriminologiju i sigurnosne studije i najeminentniji stručnjaci iz prakse, delegirani od strane Microsoft-a, sprovodili su intenzivnu obuku polaznika u cilju savladavanja programa iz oblasti digitalne forenzike i informacijske sigurnosti.

Treba napomenuti da ovo nije jedini program cjeloživotnog učenja koji je održan na Fakultetu za kriminalistiku, kriminologiju i sigurnosne studije – Korporativna sigurnost i zaštita, Smjernice za postupanje u slučajevima nasilja nad djecom u Bosni i Hercegovini, Upravljanje kriznim situacijama, Obrada lica mjesta krivičnog djela, Sigurnost u odgojno-obrazovnim ustanovama. Ohrabreni iskustvima iz prethodnih godina, organizatori su nastavili sa izborom izuzetno stručnih i kvalitetnih predavača, te interesantnih i aktuelnih tema. Ono što je važno napomenuti jeste da su svi ovi programi cjeloživotnog učenja realizovani i podržani od strane Ministarstva za obrazovanje, nauku i kulturu Kantona Sarajevo.

Cilj ove edukacije usmjeren je na unaprijeđenje postojećih i usvajanje novih znanja iz oblasti forenzike digitalnih uređaja i informacijske sigurnosti, a polaznici su trebali spoznati koji su to izazovi i prijetnje koje možemo očekivati u digitalnom i informacijskom okruženju, te kako se protiv njih boriti.

U okviru ove zimske škole kroz interaktivni nastavni proces obrađene su sledeće tematske cjeline: Sigurnost digitalne transformacije, Sigurnosna provjera i sigurnosna kultura u kibernetič-

kom prostoru, Forenzika mreže, Uvod u pravo informacijske sigurnosti, Sigurnost informacionih sistema, Baze podataka, Windows forenzika, Windows sigurnost i forenzika, Forenzička analiza digitalnih dokaza, Metodika istraživanja krivičnih djela iz područja cyber kriminaliteta, Nasilje nad djecom u digitalnom okruženju, Digitalna forenzika, General Data Protection Regulation, i najzad, Pravni okvir istraživanja i dokazivanja krivičnih djela u digitalnom okruženju. U nastavku ovog rada biće prikazana pojedina izlaganja predavača.

Tematska cjelina pod nazivom *„Sigurnosna provjera i sigurnosna kultura u kibernetičkom prostoru"* bila je usmjerena na pitanje sigurnosnih provjera i sigurnosne kulture u kibernetičkom prostoru. U okviru ove tematske cjeline predstavljene su savremene koncepcije poimanja termina bezbjednost i sigurnost, te su iznijeta različita stajališta u pogledu podjela sigurnosti prema vrstama, oblicima, prema subjektima i objektima zaštite, prema uzrocima i ishodištima ugroženosti, te je zaključeno da individualna, pravna i društvena sigurnost zadiru i da su sastavni dio kibernetičke sigurnosti.

U okviru osnovnih kategorija ove nastavne cjeline podcrtano je da su područja informacijske sigurnosti navedena u većini zakona o informacijskoj sigurnosti, a obuhvataju pitanja sigurnosnih provjera, sigurnosti podataka, fizičku sigurnost, sigurnost informacijskih sistema i sigurnost poslovne saradnje. Na kraju, naglašeno je da informacijska sigurnost obuhvata puno šire područje od informatičke sigurnosti koja uglavnom pokriva samo tehničke dijelove sigurnosti.

Naredna tematska cjelina *„Digitalna forenzika"* obuhvatala je obradu nekoliko povezanih pitanja, a to su digitalna forenzika, digitalni dokazi, podjela, vrste i izvori digitalnih dokaza, te pripremu i postupke prikupljanja digitalnih dokaza. U prvom djelu prezentacije navedena je definicja digitalne forenzike i digitalnog dokaza, te je istaknuto da je Federalni istražni biro *(e. Federal Bureau of Investigation, FBI)* prvi put oformio jedinicu za kompjuterske analize i tim za odgovor još davne 1984. godine. U okviru ove tematske cjeline pobrojane su i pojašnjene osnovne podjele digitalne forenzike, vrste i izvori digitalnih dokaza, pri čemu je poseban akcenat stavljen na principe digitalne forenzike – odnosno nepromjenljivost, dokumentovanje, provjerljivost, zakonitost.

Kao epilog u realizaciji nastavnog procesa pod ovom temom navedena je pažnja prilikom planiranja mjera, pri čemu je bitno voditi računa o informacijama koje su prikupljene u toku izrade kako bi se na osnovu njih mogla izvršiti procjena u kojem obliku bi se mogli pronaći digitalni dokazi i koje vrste. Nadalje, vrlo su značajne informacije o osumnjičenim radi planiranja pretresa, informacije o lokacijama, procjena ljudskih kapaciteta i potrebne opreme, te naredba za pretres pokretnih stvari. Druga faza koja je naglašena jeste prepoznavanje i obezbjeđenje lica mjesta, zatim prikupljanje predmeta koji sadrže digitalne dokaze ili samih digitalnih dokaza. Treća faza odnosila se na radnje koje se smiju poduzimati kada je uređaj upaljen, koje kada je ugašen, a četvrta faza je bila pakovanje, transport i skladištenje digitalnih dokaza.

Naredna nastavna cjelina koja se ovim prikazom prezentuje jeste *„Nasilje nad djecom u digitalnom okruženju"*. Kroz ovu tematsku cjelinu predstavljana su teorijska stajališta kao i rezultati empirijskih istraživanja koja se odnose na pitanja edukacije, prevencije u zaštiti djece od nasilja u digitalnom okruženju, te neodvojivih kriminoloških pitanja etiološke i fenomenološke dimenzije ovog problema, bez čijeg sagledavanja nije moguće voditi uspješno suprotstavljanje ovom teškom obliku pritivpravnog ponašanja. U okviru ove tematske cjeline izdvojene su osnovne informacije o međunarodnom kao i domaćem pravnom okviru kojim se propisuju kako materijalno pravne, tako i procesno pravne odredbe koje se tiču nasilja nad djecom u digitalnom okruženju.

U drugom dijelu prezentacije više se govorilo o fenomenologiji, tj. pojavnim oblicima nasilja nad djecom, pri čemu su istaknuti rezultati brojnih referentnih studija koji ukazuju da osobe koje traže svoje seksualno zadovoljstvo u djeci vrlo često imaju malo svijesti, što je često posljedica rano doživljene traume, a nerijetko su i sami kao djeca bili zlostavljani. Tako, kao najčešća protivpravna djela koje se pojavljuju kao oblik nasilja nad djecom u digitalnom okruženju su *grooming, cyberbullying, sexting, sextorsion* i *livestream*.

Obradom ove teme, posebnu važnost dobija teza koju su iznijeli Beran i Li (2007) po kojima se online nasilje nad djecom može smatrati jednim od indirektinih oblika agresivnog postupanja koja se ne odvijaju u interakciji „licem u lice" (kao što je slučaj kod klasičnog relacijskog nasilja), već posredstvom online medija.

Poslednji segment ove tematske cjeline bio je predstavljanje sadržaja i elemenata smjernica kako prijaviti nasilje koje se dogodilo u odgojno-obrazovnim institucijama, van odgojno-obrazovnih institucija, a koje je prepoznato u njima, te kako trebaju postupiti organi starateljstva, policija, te zdravstvene ustanove. Tako, istaknuto je da se viši nivo uspješnosti kako u preventivnom tako i u represivnom smislu može ostvariti kroz saradnju škola, organa javne bezbjednosti, medija i nevladinih organizacija koje se bave zaštitom djece od nasilja putem informaciono-komunikacijskih tehnologija (IKT). U tom smislu mjere koje se preporučuju odnose se na podizanje svijesti javnosti o opasnostima i nasilju nad djecom putem ITK-a; osiguravanjem tehničke podrške za nevladine organizacije koje administriraju i upravljaju „online" linijama za prijavu i podršku u slučajevima nasilja nad djecom putem IKT-a; Motivisanjem privrednih subjekta i korporacija da podrže aktivnosti zaštite djece od nasilja putem IKT, kroz korištenje raspoloživih resursa, sponzorstva i sl.; Posebnim edukacijama, vođenim od strane specijalizovanih psihologa, izvršiti senzibilizaciju tužilaca i sudija u radu sa djecom žrtvama nasilja putem informacijskih i komunikacijskih tehnologija, te provođenjem posebnih specijalističkih i zajedničkih obuka iz oblasti nasilja nad djecom putem IKT za policijske agencije i pravosudne organe.

"Pravni okvir istraživanja i dokazivanja krivičnih djela u digitalnom okruženju" je centralna kategorija naredne tematske cjeline koja se predstavlja ovim prikazom. U okviru izlaganja iznijeti su osnovni elementi pravnog okvira istraživanja krivičnih djela u digitalnom okruženju, dok su na početku istaknuti osnovni elementi koji čine dokaz, te različita poimanja kategorije dokaza. Tako, izdvojeno je tumačenje Pavšića (2013:415), prema kojem je digitalni dokaz svaki podatak koji je kao dokaz u elektronskom (digitalnom) obliku pribavljen u skladu sa zakonom, kao i stav Protrke (2011:2) koji navodi da je to računarski podatak koji može potvrditi da je počinjeno krivično djelo ili može ukazati na povezanost između zločina i žrtve.

Kada su u pitanju digitalni dokazi i Zakon o krivičnom postupku BiH, kroz izlaganja je pojašnjeno da su "kompjuterski podaci" svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u kompjuterskom sistemu, uključujući i program koji je u stanju prouzrokovati da kompjuterski sistem izvrši određenu funkciju. Navedene su i radnje dokazivanja koje su od značaja za pribavljanje digitalnih podataka i njihovu transformaciju u digitalne dokaze, i to: privremeno oduzimanje predmeta i imovine, pretres stana, prostorija, osoba i pokretnih stvari, te vještačenje. Za kraj, naglašeno je da za krivični postupak mogu biti relevantne i neke druge posebne istražne radnje, posebno nadzor i tehničko snimanje telekomunikacija, i pristup kompjuterskim sistemima i kompjutersko sravnjenje podataka, a kao posebno važno pravilo u korištenju digitalnih dokaza u okvirima Commom Law-a izdvojeno je pravilo najboljeg dokaza *(e. Best evidence rule).*

Vježba

Tokom poslednjeg dana održavanja zimske škole „Digitalna forenzika i informacijska sigurnost" učesnicima je zadata vježba pod nazivom „Kreiranje forenzičke kopije podataka i vještačenje korištenjem programa Autopsy". Učesnici su bili podijeljeni u pet grupa koje su se sastojale od 10 osoba. Svaki tim je imao vođu koji je usmjeravao ostatak ekipe.

U okviru ove vježbe bilo je potrebno izvršiti 8 koraka kako bi vježba bila uspješno završena. Prvi korak se odnosio na instaliranje programa FKT Imager i programa Autopsy koji omogućava efikasnu analizu hard drajva i pametnih telefona. Svaki tim je morao spojiti USB na laptop, te izbrisati fajl koji se nalazio na njemu. Korištenjem programa FTK Imager bilo je potrebno kreirati forenzičku kopiju (tip EO1) USB stika, a nakon kreiranja forenzičke kopije otvoriti TXT fajl koji je kreirao FTK Imager. Sledeći korak je bio pokretanje Autopsy programa, te učitavanje kreirane forenzičke kopije. Učesnici su morali izvršiti analizu dostupnih podataka i zabilježiti detalje koje su smatrali bitnim, poput datuma pristupa, naziva dokumenta i sl. Na kraju, svaki tim je morao prezentovati rezultate vježbe. Na ovaj način učesnici, koji i nisu najbolje upoznati sa IT svijetom, su utvrdili da se fajl, koji je obrisan sa USB stika, može ponovo povratiti i učiniti vidljivim.

Vježba pokazala uspješnom, jer su svi timovi bez problema obavili zadatak. Iz ovoga se može zaključiti da se polaznici zimske škole mogli praktično primjeniti sve ono što su naučili tokom predavanja.

Zaključak

S obzirom na digitalizaciju i modernizaciju tehnologije, ključno je stalno unaprijeđivanje kadrova. Nemoguće je usavršavati spoznaje o nekoj pojavi, a pri tome da se o istoj ne razmjenjuju iskustva, diskutuje, promišlja. Jedan od izvora saznanja jesu svakako programi cjeloživotnog učenja, kursevi, edukacije.

Program cjeloživotnog učenja „Digitalna forenzika i informacijska sigurnost" je uspješno implementirao zadatke i ciljeve, te postavio kvalitetan temelj za dalji razvoj novih oblika svrhovite edukacije u naučnim okvirima ove forenzičke discipline. O tome najbolje govori anketa koju su popunili učesnici ovog programa. Anketa je bila percipirana na način da sadrži pitanja koja su se odnosila na ocjenu predavača, tj. njihovog prezentovanja, programa, te cijele organizacije.

Jedno od postavljenih pitanja je bilo da li su polaznici zadovoljni organizacijom rada zimske škole. 58,1% učesnika je dalo ocjenu 5, 32,6% ocjenu 4, a 9,3% ocjenu 3. Također, na pitanje da li su sadržaji modula cjeloživotnog učenja adekvatno odabrani i da li odražavaju potrebe polaznika, 44,2% je odgovorilo pozitivno i dalo ocjenu 5, 41,9% ocejenu 4, a 14% ocjenu 3.

Naravno, učesnicima je ostavljeno prostora i za sugestije kako bi ovakva vrsta programa bila još uspješnija. Naime, polaznici su skrenuli pažnju da se više vremena trebalo izdvojiti na pravni okvir, jer upravo većina njih dolazi iz IT sektora, te nisu najbolje upućeni u regulisanje krivičnih djela počinjenih u digitalnom svijetu. Isto tako, istaknuto je da je potrebno više praktičnih vježbi.

Za kraj važno je pomenuti i izjavu James Comey-a, bivšeg direktora FBI-a, koja ukazuje od kolikog značaja su znanja iz oblasti digitalne forenzike i informacijske sigurnosti: „Postoje samo dvije vrste kompanija na svijetu - one koje su hakovane i one koje još to ne znaju."

Podaci o autoru

Renata Klačar, diplomirala na Fakultetu za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu i magistrirala na Pravnom fakultetu Univerziteta u Sarajevu. Dobitnica Povelje za najboljeg studenta prvog ciklusa pomenutog fakulteta. Učestvovala u organizaciji Evropske kriminološke konferencije koja je održana u Sarajevu. Također, pristustvovala edukaciji iz područja upravljanja kriznim situacijama, te područja digitalne forenzike i informacijske sigurnosti. Trenutno stažira na Fakultetu za kriminalistiku, kriminologiju i sigurnosne studije.
E-mail: renataklacar@fkn.unsa.ba.