DIGITALNA FOREZNIČKA ISTRAGA U SISTEMU DOSTAVE USLUGA U OBLAKU

Mr Biljana Simić
biljanadanic037@gmail.com

Sadržaj:

- Uvod
- Sistem dostave usluga u oblaku i digitalna foreznika
- Proces sprovođenja forezničke istrage
- Dropbox
- Zaključak

UVOD

- Savremena tehnologija
  moćno oružje ili velika opasnost
- 2011. godina – hakerski napad Sony PlayStation Network
- Cloud Computing - Cloud Storage
- Izveštaj Gartnera (Kleyhans 2012. godina)
- Dropbox, Microsoft SkyDrive i Google Drive
- PC, smart telefoni, tableti
- Web browser ili posebne aplikacije

SISTEM DOSTAVE USLUGA U OBLAKU

- Oblak (*cloud)* – Internet
- Računarstvo u oblacima (*Cloud computing)*
  druga polovina 20.veka
- Dell, marta 2007, godine podnosi zahtev Američkom odeljenu za patentiranje (*United States Patent and Trademark Office)* za registraciju *cloud computing* kao zaštitnog znaka za opisivanje svojih usluga dizajna računarskih komponenti za potrebe muskulaturnih računarskih sistema
- Jul 2007. USPTO dodeljuje dozvolu a nakon mesec dana ista je povučena i zahtev kompanije Dell je zvanično odbijen

SISTEM DOSTAVE USLUGA U OBLAKU

- Raučunarstvo u oblaku predstavlja sveobuhvatni koncept iz kojeg je teško izvesti pojedinačnan element koji je najvažniji faktor za samu ideju oblaka, što je uslovilo postojanje različitih definicija ovog pojma
- Evropska unija u svom strateškom dokumnetu navodi da se: „*Cloud computing*“ može shvatiti kao čuvanje, obrađivanje i korišćenje podatka koji se nalaze na udaljenim računarima i kojima se može pristupiti preko interneta.

SISTEM DOSTAVE USLUGA U OBLAKU

KARKTERISTIKE

- Osnovne karakteristike *cloud computing-a* prema Nacionalnom institutu za standard i tehnologiju (*National Institute of Satnadards and Technology – NIST*)
  - **Pružanje usluge na zahtev korisnika** *(on-demand self-service):* omogućuje korisnicima da prilagođavaju svoje računarske mogućnosti u skladu sa trenutnim potrebama, koje uključuju snagu procesa, veličinu memorije i propusni opseg veze brze interakcije sa pružaocima usluga. Usluge se bivaju naplaćene korisnicima u zavisnosti od vremena i obima u kojem ih koriste.
  - **Širok mrežni pristup** (*broad network access*): usluge računarstva u oblaku su dostupne putem opštih Internet protokola i standarda za umrežavanje različitim klijentima, koje se mogu pokrenuti putem različitih uređaja, posebno smartfona, kompjutera, tableta i sl.

SISTEM DOSTAVE USLUGA U OBLAKU

KARAKTERISTIKE

- **Udruživanje resursa** (*resource pooling*): mogućnost spajanja resursa provajdera koji su dostupni svim korisnicima, kombinujući različite fizičke i virtuelne resurse dinamički dodeljenje prema zahtevima potrošača.
- **Brza elastičnost** (*rapid elasticity*): dinamično okupiranje i zauzimanje resursa u zavisnosti od trenutnih potreba korisnika. Naime, resursi su trenutno dostupni korisnicima i rade za njih neograničeno.
- **Izmerena usluga** (*measured service*): pomoću odgovarajućih sistema proverava se i optimizuje upotreba resursa na oblaku. Korišćenje svih funkcionalnosti se na adekvatan način može pratiti, što omogućava i pravljenje izveštaja koji su od koristi kako korisnicima tako i pružaocu usluga.

SISTEM DOSTAVE USLUGA U OBLAKU

DEFINICIJA

- Američki Nacionalni institut za standarde i tehnologiju (NIST) 2011. godine objavuje sledeću definiciju:

  „Računarski oblak je model koji omogućava svuda prisutan, pogodan mrežni pristup deljivim računarskim resursima (mrežnim, serverima, skladištu podataka, aplikacijama i servisima), koji na zahtev korisnika i uz minimalnu interakciju sa isporučiocem usluga mogu biti brzo stavljeni na raspolaganje korisniku ili otkazani”.

SISTEM DOSTAVE USLUGA U OBLAKU

KATEGORIZACIJA

- Usluge računarstva *u oblaku* mogu se kategorizovati u tri posebne grupe:
  - **Infrastruktura u vidu servisa** (*Infrastructure-as-a-Services*, *IaaS*) – model isporuke softvera u kojem su softver i povezani podaci centralno hostovnai na oblaku kojima se obično pristupa putem internet pretraživača. Može se reći da ovaj tip usluge obezbeđuje korisnicima osnovne resurse kao što su snaga procesiranja, prostor za skladištenje, mreža i sl. Pružaoci ovog vida usluge nude korisnicima virtuelne mašine, zaštitne zidove, skladišni prostor koji je dostupan preko mreže i sl. Korisnici iznajmljuju ove resurse na zahtev, pri čemu oni upravljaju samo operativnim sistemom i aplikacijama koje samostalno instaliraju.

    Prednosti IaaS usluga su: potpuna kontrola i administracija virtuelnih mašina, fleksibilno i efikasno iznajmljivnaje resursa, portabilnost i dr.

    Nedostaci IaaS usluga se manifestuju u vidu: zavisnosti od mreže, rizike sigurnosti web čitača kod klijenata, ažuriranje sistema i dr.

SISTEM DOSTAVE USLUGA U OBLAKU

KATEGORIZACIJA

- **Platforma u vidu servisa** (*Platform-as-a-Services, PaaS*) – provajder pruža mrežu, servere, prostor za skladištenje kao i usluge, dok korisnik kreira softver i razvija samu konfiguraciju. PaaS je najpribližniji tradicionalnim računarskim sistemima za koje se mogu razvijati aplikacije koje će se izvršavati na njima i koje će koristiti krajnji korisnici usluga.

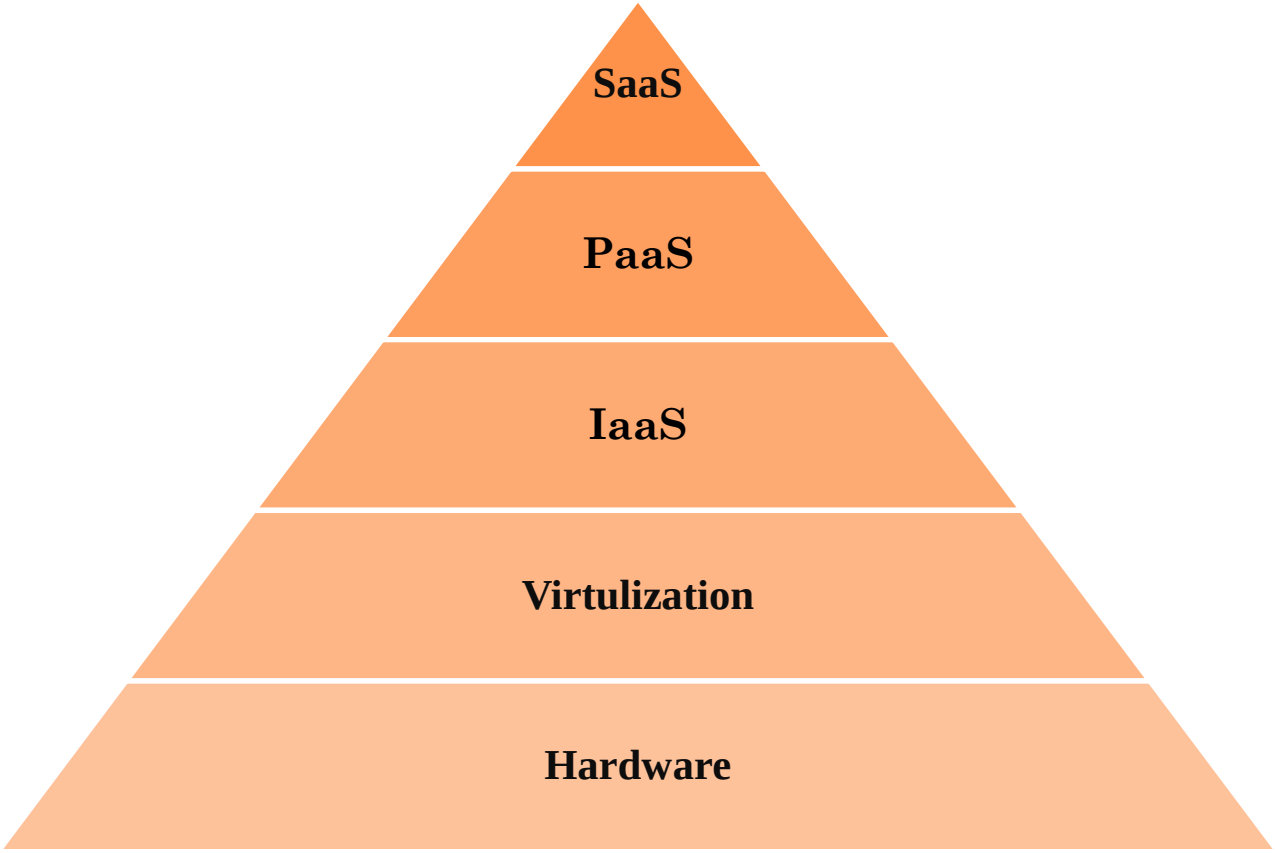
  Sporna pitanja u vezi korišćenja PaaS se manifestuju u vidu rizika i sigurnosti veb čitača kod klijenata, zavisnost od mreže, pitanja izolacije nasuprot efikasnosti i sl.

- **Softver u vidu servisa** (*Software-as-a-Services, SaaS*) – provajder nudi računare i druge resurse na zahtev, dok korisnici obezbeđuju instalaciju i infrastrukturu operativnih sistema.

  Osnovni nedostatak ovog modela se manifestuje u vidu zaštite podataka zbog čega se komunikacioni kanal između korisnika i provajdera najčešće kriptuje SSL/TLS vezom

SISTEM DOSTAVE USLUGA U OBLAKU

HIJERARHIJSKA ORGANIZACIJA OBLAKA *CLOUD-A*



SISTEM DOSTAVE USLUGA U OBLAKU FOREZNIČKO ISTRAŽIVANJE

- Prikupljanje digitalnih dokaza iz *oblaka* može dovesti do složenih tehničkih i unakrsnih pravnih izazova
- Korišćenje sistema za skladištenje podataka u oblaku može ubrzati proces foreznike i fokusirati istragu na relevantne podatke ranije u istrazi
- Digitalna foreznika predstavlja jedini pouzdani alat za istragu računarskog kriminala, akviziciju i analizu digitalnih podataka i pripremu i prezentaciju digitalnih dokaza pred sudom.

DIGITALNA FOREZNIKA PODELA

- Sa aspekta **predmeta forezničke istrage,** digitalnu forezniku možemo podeliti na:
  - forezniku računarskih sistema,
  - forezniku mobilnih uređaja,
  - forezniku baze podataka i
  - Internet ili kibernetičku forezniku

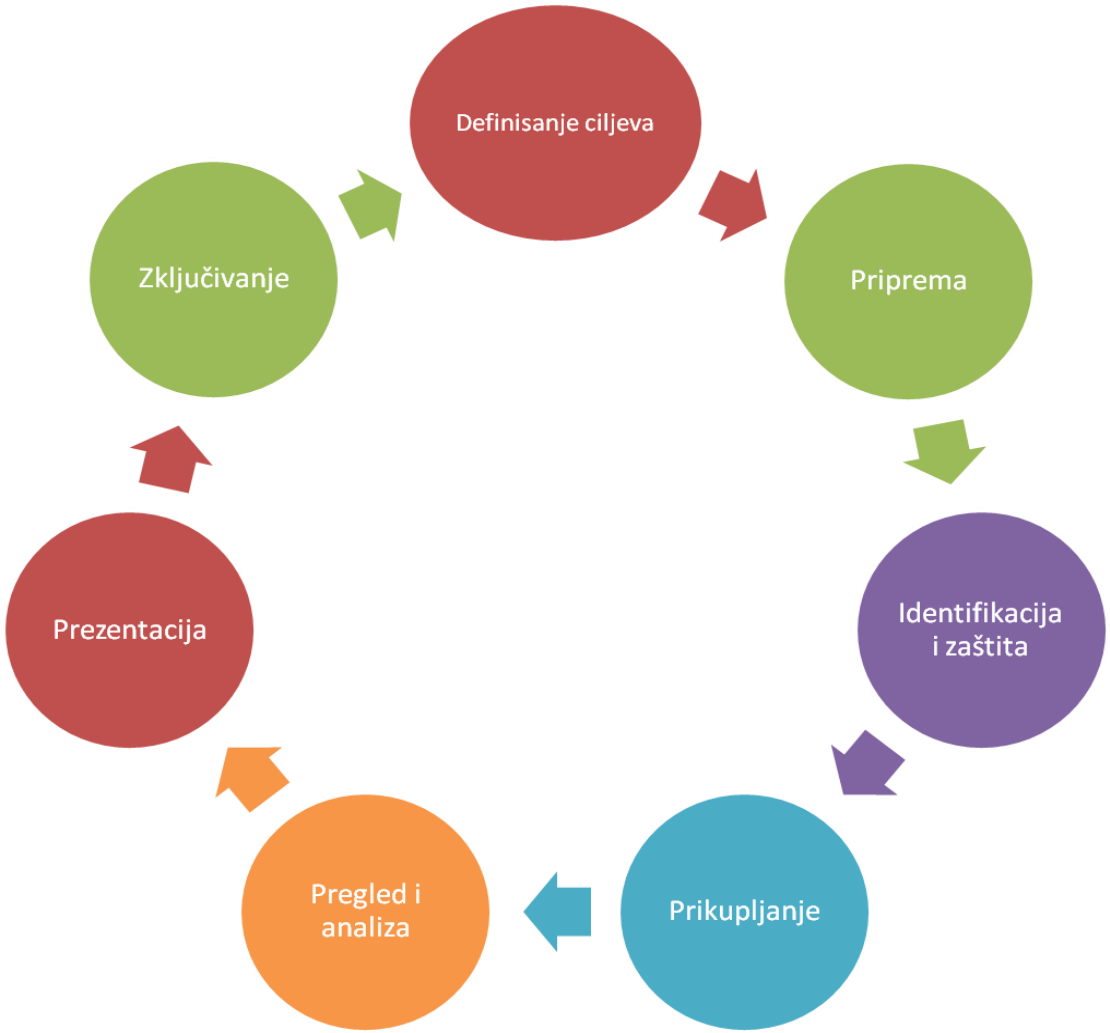
DIGITALNA FOREZNIKA

MODELI DIGITALNE FOREZNIKE U OKVIRU SISTEMA DOSTAVE USLUGA *U OBLAKU*

- McKemmish, identifikuje četiri faze digitalne forezničke istrage:
  - identifikacija digitalnih dokaza,
  - čuvanje digitalnih dokaza,
  - analiza digitalnih dokaza i
  - prezentacija digitalnih dokaza

- Proces digitalne foreznike potrebno je posmatrati kao fleksibilan proces sa mogućnošću povratka na prethodne korake tokom analize.
- Okvir forezničke istrage treba da omogući otkrivanje novih informacija, na taj način da istražitelj može da se vrati na prethodne korake ukoliko otkrije novo skladištenje podataka

DIGITALNA FOREZNIKA
OKVIR ZA SPROVOĐENJE FOREZNIČKE ISTRAGE U *CLOUD STORAGE* SISTEMU



DIGITALNA FOREZNIKA
OKVIR ZA SPROVOĐENJE FOREZNIČKE ISTRAGE U *CLOUD STORAGE* SISTEMU

- **Definisanje ciljeva**

  Taylor, Haggerti, Gresti i Lamb „važno da se svrha digitalne forezničke istrage jasno definiše, tako da se na osnovu definisane svrhe, može doneti odluka o celokupnom obimu istražnog postupka.“

  Forenzički istražitelji treba da razumeju šta, gde, kada, ko, zašto i kako, u toku sprovođenja istražnog postupka uz jasno definisanje granica istrage.

  Obim sprovođenja forezničke istrage podrazumeva definisanje aktera, sve podatke ili dokaze koji su već oduzeti, termine ključnih reči, sve vremenske okvire pristupa sistemu dostave usluga u oblaku, kao i druge relevatne informacije.

  Na samom početku istražnog postupka, forenzički istražitelji opseg istraživanja definišu samo generički, s’tim da u će se u toku same istrage definisati ključna pitanja.

DIGITALNA FOREZNIKA
OKVIR ZA SPROVOĐENJE FOREZNIČKE ISTRAGE U *CLOUD STORAGE* SISTEMU

- **Priprema**

  Može obuhvatiti pored nabavke opreme i obuku IT stručnjaka koji su uključeni u proces istrage.

  - U skladu sa ACPO principom stručnjak koji sprovodi postupak istrage pre svega mora posedovati odgovarajuću kompetentnost za sprovođenje istrage, što se može postići sprovođenjem odgovarajuće obuke pre obavljanja samog ispitivanja.

  Faza pripreme podrazumeva i manipulaciju sa preuzetim informacijama radi razumevanja određenog pitanja ili aspekta istrage.

  - Na primer istražitelji mogu prikupljene podatke i informacije testirati u kontrolisanom okruženju kako bi se odredili ishodi, koji se zatim mogu primeniti u toku istrage u cilju dobijanja odgovora na određena pitanja, ili samom razumevanju prisustva podatka i informacija kao i u postupku formiranja hipoteze.

DIGITALNA FOREZNIKA
OKVIR ZA SPROVOĐENJE FOREZNIČKE ISTRAGE U *CLOUD STORAGE* SISTEMU

- **Identifikacija i zaštita izvora prikupljenih dokaza**

  - identifikacija izvora podataka u najvećem broju slučajeva otpočeće sa tradicionalnim uređajima koji su podvrgnuti forezničkoj analizi (PC računara i mobilnih uređaja).

  - faza identifikacije podrazumeva i lociranje usluge skladištenja u oblaku (kako elektronski tako i fizički) u cilju određivanja pružaoca usluge skladištenja podataka u oblaku.

  - nakon obezbeđivanja podataka o korisničkom imenu i datumu i vremenu pristupa, od pružaoca usluga skladištenja podataka u oblaku zahteva se saradnja u skladu sa relevantnim pravnim propisima, pre svega radi identifikacije i čuvanje izdvojenih podatka i omogućavanje pristupa istim forezničarima.

  Ovde je potrebno napomenuti da kompeksnost identifikacije i očuvanja podataka koji se nalaze u oblaku posebno dobija na značaju imajući u vidu da internetska priroda servisa u oblaku, omogućava osumnjičenima da se prijave i brišu podatke u realnom vremenu dok sa druge strane istražitelji čekaju dostavu istih od strane pružaoca usluge.

DIGITALNA FOREZNIKA
OKVIR ZA SPROVOĐENJE FOREZNIČKE ISTRAGE U *CLOUD STORAGE* SISTEMU

- **Prikupljanje podataka (kolekcija)**

  Uobičajna praksa prikupljanja dokaza sa tradicionalnih PC računara, se sastojala najčešće od uklanjanja hard diska, priključivanje uređaja na forezнички blok, odnosno blokiranje korišćenja forezničkog softvera na računaru za prikupljanje napona diska.

  Prikupljanje podataka u okviru sistema dostave usluga u oblaku je znatno složenija u smislu lokacije i tehnologije. U ovom slučaju javlja se i problem pravne prirode jer su provajderi, pružaoci usluga najčešće locirani u drugim pravnim jurisdikcijama što zahteva primenu instrumenata uzajamne pravne pomoći ili drugih sporazuma koji obezbeđuju razmenu podataka između dva nezavisna entiteta.

DIGITALNA FOREZNIKA
OKVIR ZA SPROVOĐENJE FOREZNIČKE ISTRAGE U *CLOUD STORAGE* SISTEMU

- **Pregled i analiza**

  Analiza forezničkih podataka se preduzima u cilju lociranja informacija i testnih hipoteza u odnosu na postavljene parametre istraživanja.

  Može da se zasniva na nizu različitih procesa, koristeći različite softvere i hardvere za prikupljanje odgovora na pitanja koja se odnose na obih istraživanja.

  - *Ukoliko se tokom ispitivanja otkriju i drugi izvori podataka, istražitelji će započeti ponovo sa fazom pripreme za novoidentifikovane podatke. Analiza se pri tome nastavlja sa već prikupljenim podacima, a novootkriveni podaci biće analizirani kada budu i dostupni.*

DIGITALNA FOREZNIKA
OKVIR ZA SPROVOĐENJE FOREZNIČKE ISTRAGE U *CLOUD STORAGE* SISTEMU

- **Prezentacija**

  Pojašnjenje prikupljenih informacija na način koji je razumljiv pravosuđu i drugim donosiocima odluka, što podrazumeva da oni svi podaci i informacije moraju biti prikupljeni na zakonski prihvatljiv način.

- **Zaključivanje**

  Poslednji korak koji je važan kako bi se sasvim sigurno potvrdilo da je na sva sporna pitanja odgovoreno u istražnom postupku, da je sprovedeni postupak bio odgovarajući u odnosu na okolnosti, da su identifikovane sve mogućnosti za analizi i da se sprovedeni proces može preporučiti kao efikasan i relevantan i za druge slične istražne postupke.

POSTUPAK ZA DIGITALNU FOREZNIKU SISTEMA DOSTAVE USLUGE U OBLAKU

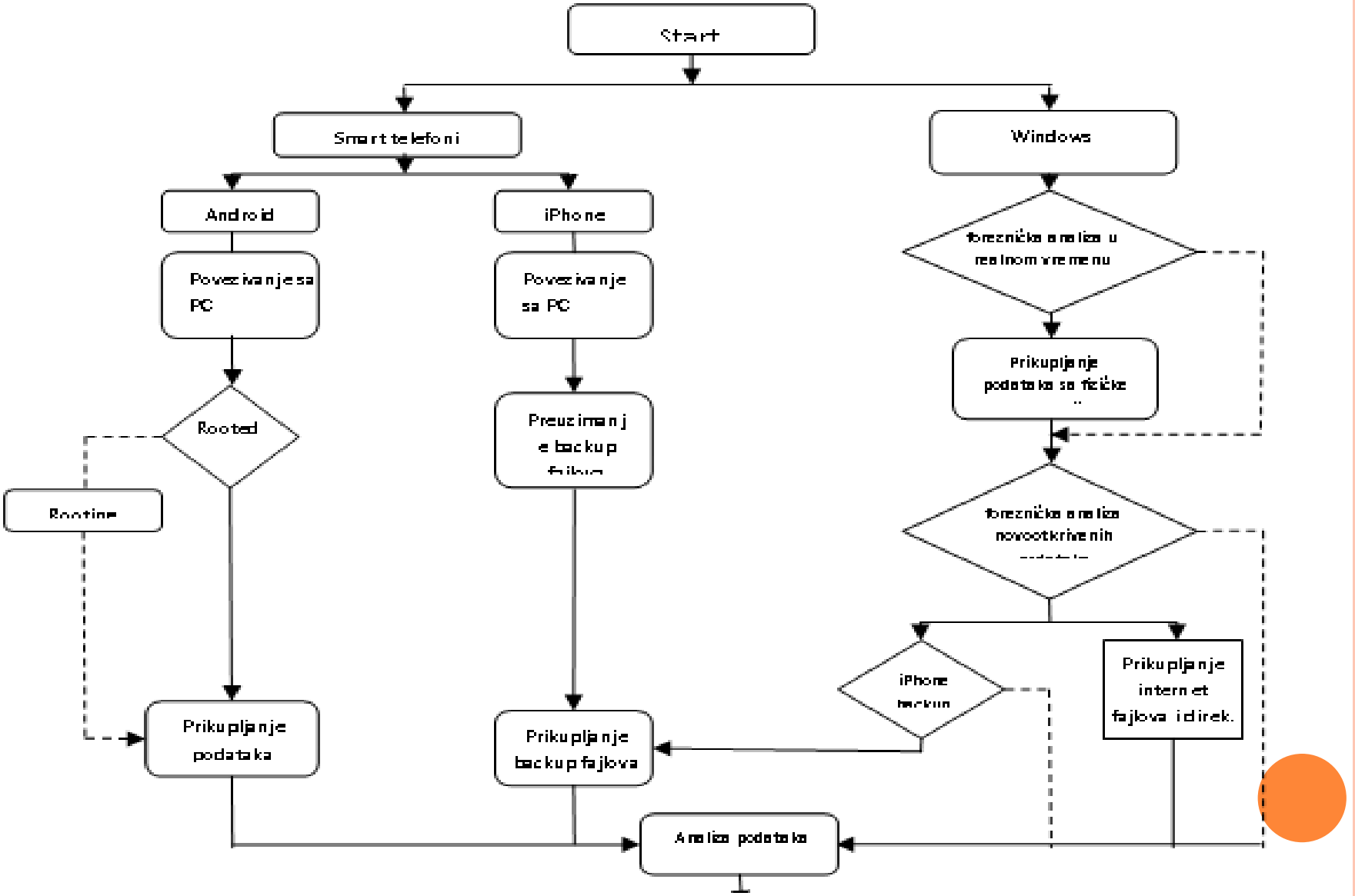
- **Prezentacija**

  Pojašnjenje prikupljenih informacija na način koji je razumljiv pravosuđu i drugim donosiocima odluka, što podrazumeva da oni svi podaci i informacije moraju biti prikupljeni na zakonski prihvatljiv način.

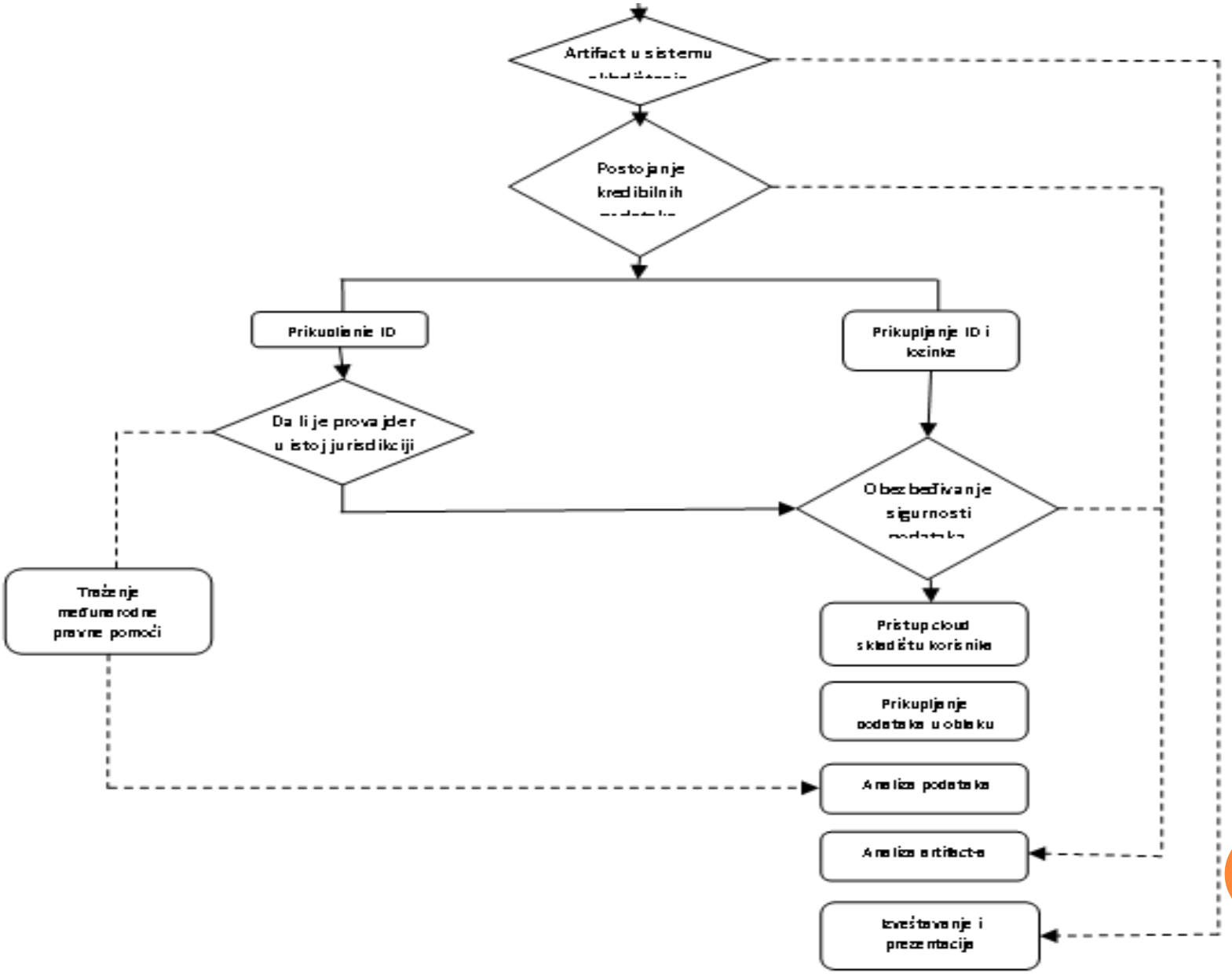
- **Zaključivanje**

  Poslednji korak koji je važan kako bi se sasvim sigurno potvrdilo da je na sva sporna pitanja odgovoreno u istražnom postupku, da je sprovedeni postupak bio odgovarajući u odnosu na okolnosti, da su identifikovane sve mogućnosti za analizi i da se sprovedeni proces može preporučiti kao efikasan i relevantan i za druge slične istražne postupke.

PROCES SPROVOĐENJA FOREZNIČKE ISTRAGE



PROCES SPROVOĐENJA FOREZNIČKE ISTRAGE



POSTUPAK ZA DIGITALNU FOREZNIKU SISTEMA DOSTAVE USLUGE U OBLAKU

Značajni faktori koji utiču na izbor elemenata koji su prioritetni za istraživanje

- **Log fajlovi u web pretraživaču**

  Analiza datoteka koje su ostavljene u pozadini kada se koriste InternetExplorer i Firefox kao najčešći korišćeni web pretraživači širom sveta, dok su slični tragovi dostupni i u drugim web pretraživačima kao što su Chrome i Safari. Datoteke dnevnika web čitača se nalaze i čuvaju u direktorijumu profila i sastoje se od keša, istorije kolačića i datoteka za preuzimanje.

POSTUPAK ZA DIGITALNU FOREZNIKU SISTEMA DOSTAVE USLUGE U OBLAKU

Verzija operativnog sistema	Podaci	Putanje
Windows 2000 XP	Keš	%Profile%\Local Settings\Temporary Internet Files\Content.IE5\index.dat
		%Profile%\Local Settings\Temporary Internet Files\Content.IE5\<Random>\<All of the files>\
	Istorija	%Profile%\Local Settings\History\History.IE5\index.dat
		%Profile%\Local Settings\History\History.IE5\index.dat
	Kolačići	%Profile%\Cookies\index.dat
		%Profile%\Cookies\<All of the text files>\
	Preuzimanja	Nije vidljiva
Windows Vista 7	Keš	%Profile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
		%Profile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\<Random>\<All of the files>\
	Istorija	%Profile%\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
		%Profile%\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
	Kolačići	%Profile%\AppData\Local\Microsoft\Windows\Cookies\index.dat
		%Profile%\AppData\Local\Microsoft\Windows\Cookies\<All of the text files>\
	Preuzimanja	%Profile%\AppData\Local\Microsoft\Windows\IEDownloadHistory\index.dat (From IE 9, samo za Windows 7)

Značajni fajlovi i putanje (Internet Explorer)

POSTUPAK ZA DIGITALNU FOREZNIKU SISTEMA DOSTAVE USLUGE U OBLAKU

Verzija operativnog sistema	Podaci	Putanje
Mac OS x lion	Keš	/Users/<user name>/Library/Caches/Firefox/Profiles/xxxxxxx.default/Cache/CACHE_MAP
	Istorija	/Users/<user name>/Library/Application Support/Firefox/Profiles/xxxxxx.default/places.sqlite
	Kolačići	/Users/<user name>/Library/Application Support/Firefox/Profiles/xxxxxx.default/cookies.sqlite
	Sesije	/Users/<user name>/Library/Application Support/Firefox/Profiles/xxxxxx.default/session.store.js

Značajni fajlovi i putanje (Firefox)

POSTUPAK ZA DIGITALNU FOREZNIKU SISTEMA DOSTAVE USLUGE U OBLAKU

Datoteke koje se nalaze u keš memoriji obuhvataju datoteke sa slikama, tekstualne datoteke, ikone, HTML i KSML datoteke, URL-ove kojima je vršeno preuzimanje, vreme preuzimanja kao i veličinu preuzetih podataka. Istorija web pretraživača nudi podatke o URL adresa koje je korisnik posetio, naslove Veb stranica, vreme i broj poseta stranice.

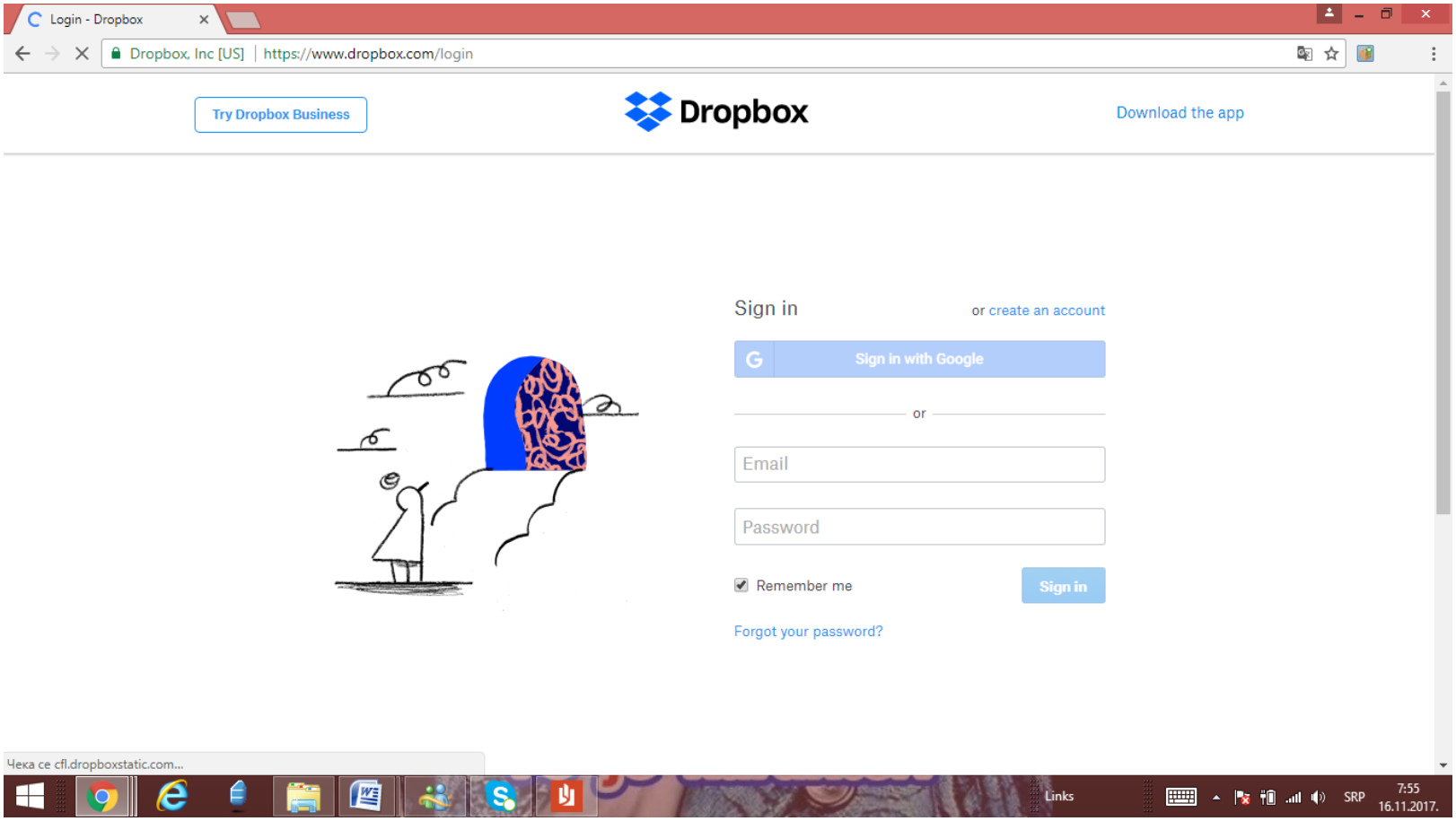
Datoteke cookie (kolačića) čuvaju informacije o hostovima, modifikaciju kolačića, istek vremena, imena i vrednosti i preuzimanja – delovi preuzetih fajlova, preuzetih URL, veličina fajlova, vreme preuzimanja i status. Ove datoteke web browser-a omogućuju forezničkim istražiteljima podatke o korisničkim aktivnostima, među kojima su i pristup ili prijavljivanje na sisteme za dostavu usluga u oblaku.

Najčešće korišćeni web browser na globalnom nivou na windows sistemu je Internet Explorer, dok je na sistemu Mac najpoznatiji web pretraživač Firefox, dok su slični tragovi prisutni i u drugim web pregledačima, poput Chrome i Safari.

DROPBOX

- Jedna od najpopularnijih usluga skladištenja podataka u oblaku koje se koriste u svetu.
- Karakteristično za ovaj sistem usluga je da kada god korisnik doda datoteku u folder za sihronizaciju, uređuje ili briše datoteku, dropbox automatski sihronizuje datoteku sa svojom web lokacijom.
- Pristup je omogućen pomoću Windows sistema, Mac sistema i iPhona i Android smart telefona, unosom korisničkog imena i šifre.

DROPBOX


Login - Dropbox
Dropbox, Inc [US] | https://www.dropbox.com/login
Try Dropbox Business
Dropbox
Download the app
Sign in
or create an account
Sign in with Google
or
Email
Password
Remember me
Sign in
Forgot your password?
Чека се cfl.dropboxstatic.com...
Links
SRP
7:55
16.11.2017.

DROPBOX

- **Artefact-i iz Windows-a**

  Kao rezultat različitih analiza studija slučaja, utvrđeno je da ukoliko korisnik koristi Windows operativni sistem za pristup Dropbox servisu, u procesu forezničke istrage može se utvrditi korisničko ime Dropbox-a, URL-ovi koji su korišćeni u mrežnom saobraćaju, podaci o link datotekama, istorija pregledača kao i informacije koje se nadograđuju iz memorijskih datoteka. U situaciji kada se utvrdi da se na Dropbox računu korisnika nalaze potencijalni dokazi koji su relevantni za dalju istragu može se pokrenuti pravni postupak za obezbeđivanje i čuvanje podataka.

DROPBOX

- **Artifact-i iz browsera**

  Uočeno je da Dropbox zadržava evidenciju o računaru koji se koristi za pristup i sihronizaciju sa nalogom, uključujući i IP broj. Ove informacije su važne u forezničkoj istrazi kako bi se utvrdilo da li je određeni računar sihronizovan sa Dropbox nalogom. Sve podatke u vidu istorije vremena za datoteke i kompjutersku sihronizaciju, kao i prethodne vrezije datoteke trebaju biti identifikovani i očuvani kroz pravni postupak kako bi se osigurala dostupnost podataka istrazi.

  Na osnovu navedenog, može se zaklučiti da je u samom postupku forezničke istrage moguće utvrditi korisničko ime, lozinku, metod pristupa, imena datoteka, sadržaj i datume i vremena pristupa kada se Dropbox koristi za čuvanje, pristup ili preuzimanje podataka iz skladišta koje se nalazi u oblaku.

DROPBOX

- **Artefact-i iz iPhone**

  Rezultat više sprovedenih studija slučaja je pokazao da se prilikom traženja dokaza o korišćenju iPhone ili smart telefona za pristup Dropbox sistemu izdvajaju nekoliko ostataka podataka. U situacijama kada je korišćen iOS pretraživač za pristup Dropbox sistemu, tragovi pristupa se nalaze u histori.plist, dok se sama šifra koja je korišćena za pristup veoma teško može odrediti.

ZAKLJUČAK

- **Digitalna foreznika** predstavlja visoko specijalizovano i interdisciplinarno područje, koje zahteva razumevanje osnovnih tehničkih, regulatornih, pravno noramtivnih i drugih aspekata, kao i poznavanje trendova u korišćenju digitalnih sistema za prenos, čuvanje i modifikaciju podataka.

  Ključni izazovi sa kojima se suočavaju forezničari nalaze se u konstantnoj evoluciji sajber kriminala, brzom menjanju tehnološkog okruženja, kao i stalno povećanje sistema za skladištenje podataka u oblaku.
- Moguće je identifikovati podatke i obezbediti dokazni materijal u slučaju forezničke istrage sistema dostave usluga u oblaku na Windows računarskim sistemima i na Apple iPhone 3G.
- Tragove u vidu podataka je moguće identifikovati i kada su preduzete anti-forenzički procesi koji podrazumevaju brisanje fajlova i čišćenje pregledanja i istorije podataka o datotekama.
- Korisničko ime i lozinka se mogu naći na različitim lokacijama, a istorija pretraživanja pruža niz informacija od interesa za samu forezničku istragu.

HVALA NA PAŽNJI