Digitalni dokazi

- Kompjuterska forenzika
- Prikupljanje digitalnih dokaza
- Čuvanje digitalnih dokaza
- Spašavanje digitalnih dokaza

Kompjuterska forenzika predstavlja primenu kompjuterske istrage i tehnika analize u cilju utvrđivanja potencijalnih dokaza.

- Osnove kompjuterske forenzike
- Proces istraživanja
- Digitalni dokazi
  - Definisanje
  - Prihvatljivost na sudu

Dokazi prikupljeni iz forenzičkih ispitivanja mogu biti korisni za razne vrste istraga:

- U civilnim sporovima za razvode, zlostavljanja i diskriminaciju.
- U slučajevima gde pravna lica zahtevaju prikupljanje dokaza u pitanjima zloupotrebe službenog položaja, pronevere ili krađe intelektualne svojine.
- U slučaju seksualnog napastvovanja i fizička lica mogu zahtevati istragu.
- Osiguravajuća društva koja traže dokaze u vezi sa prevarama osiguranja, zloupotrebe smrti, prava zaposlenog i razne druge slučajeve u vezi sa premijama osiguranja.

Kompjuterska forenzika je nauka sticanja, prikupljanja, čuvanja i prezentovanja podataka koji su elektronski procesirani i uskladišteni na kompjuterskim medijima.

- Veliki broj korisnika kompjutera = veliki broj informacija
- Prikupljanje digitalnih dokaza počinje kada se informacija i/ili fizički objekt prikupe ili pohrane u očekivanju ispitivanja.
- *Podatak ili fizički objekt postaje dokaz jedino kada je prikupljen od strane ovlašćenog lica.*
- Podatak (objekat ili informacija od potencijalnog značaja koji je u vezi sa fizičkim objektom, može se pojaviti u različitim formatima)
- Digitalni dokaz (informacija od realnog značaja koja se skladišti ili prenosi u digitalnoj formi)
- Fizički objekt (objekat na kojem informacije ili podaci mogu skladištiti i/ili pomoću koga se mogu prebaciti na drugi objekat)
- Originalni digitalni dokaz (fizički objekt i podatak koji se na njemu nalazi u vreme pribavljanja ili zaplene)
- Duplikat digitalnog dokaza (precizna digitalna reprodukcija svih podataka skladištenih na originalnom fizičkom objektu)

Kompjuterska forenzika – standardi

- Originalni dokaz treba biti sačuvan u originalnom ili što približnijem stanju kao u momentu pronalaženja
- Ako je uopšte moguće, potrebno je napraviti preciznu kopiju (sliku) originala, da bi se na kopiji vršilo ispitivanje i na taj način sačuvao i zaštitio integritet originala
- Kopije podataka napravljenih u svrhu ispitivanja trebaju biti kreirane na „forenzički sterilnom“ mediju. Sterilan je onaj medij ili disk na kome prethodno nije bilo podataka, treba biti potpuno „čist“, bez virusa i defekata
- Svi dokazi moraju biti propisno označeni i dokumentovani, takođe i lanac nadležnosti mora biti očuvan

- Svaki korak forenzičkog ispitivanja mora biti detaljno dokumentovan

Kompjuterska forenzika – istraživanje

Svaki istražni postupak kojim se forenzičari bave teži da omogući:

- Prihvatljivost – postupci i metode su prihvaćeni od strane profesionalaca
- Pouzdanost – korišćenim metodama se može dokazati nalaz
- Ponovoljivost – proces može ponoviti svako, nezavisno od vremena i mesta
- Integritet – stanje dokaznog materijala je očuvano
- Uzrok i posledicu – logička povezanost između osumnjičenog, događaja i nalaza
- Dokumentaciju – beleženje ključnih stvari za svedočenje veštaka/forenzičara

Digitalni dokazi – pojam

- Dokazi se obično definišu kao sredstva kojima se optužba, za navodno počinjeno delo, utvrđuje ili odbacuje. Značaj bilo kog i kakvog dokaza leži u njegovom uticaju na sud prilikom suđenja.

U slučaju kompjuterskog kriminala, dokaz se može definisati kao:

- **digitalni dokaz** (informacija od značaja za kriminalni slučaj koja se skladišti ili prenosi u digitalnom obliku)
- **fizički medij** (na kome se digitalne informacije skladište ili kroz koji se prenose ili odašilju)
- **objekti** (informacije od značaja za kriminalni slučaj koje su povezane sa fizičkim medijima)

Postoje tri kategorije dokaza:

- fizički dokaz (sastoji se od opipljivih dokaza koji se mogu videti, čuti ili opipati)
- dokaz direktnog svedočenja (svedočenje svedoka koji može dati određeni broj činjenica na bazi ličnog iskustva i čulnog doživljaja)
- posredni dokaz (nije baziran na ličnom opažaju već na bazi znanja činjenica koje podržavaju indirektni zaključak ali ga ne definišu konačno)

Američki zakoni koji su u znatnoj prednosti u odnosu na Evropske u ovoj sferi, koriste „pravilo najboljeg dokaza“ (best-evidence rule).

Originalni dokument mora biti prezentovan osim ako je uništen ili otpada zbog drugih izuzetaka.

„Federalni zakon o dokazima“ (Federal Rule of Evidence) prepoznaje različitost digitalnih od ostalih pisanih dokaza.

Pravilo 1001-3 koje se odnosi na ovo pitanje kaže: **„Ukoliko je podatak pohranjen u kompjuteru ili sličnom uređaju, svaki štampani izveštaj ili bilo kakva forma izlaza koja se može videti, prikazana tako da precizno predstavi podatke, je original.“**

Digitalni dokazi – prihvatljivost

Dokaz mora biti:

- **„kompetentan“** (odnosno pouzdan tj. kredibilan)
- **„relevantan“** (sa težnjom da dokazuje činjenice u vezi sa slučajem)
- **„materijalan“** (podupire pitanje u vezi sa slučajem)

- Da bi bio prihvatljiv u SAD, dokazni materijal mora biti pribavljen legalnim putem. To podrazumeva pribavljanje i zaplenu u skladu sa zakonima, uključujući tu i ustave, kako država članica, tako i SAD.
- Ukoliko je dokazni materijal pribavljen prilikom nezakonite pretrage, iako dokazuje krivicu, smatra se „kompromitovanim“ i kao takav se odbacuje.

Test relevantnosti

„bilo koji dokaz sa tendencijom da potkrepi postojanje bilo koje činjenice čije će utvrđivanje biti manje ili više verovatno nego što bi bilo bez tog dokaza“

Frye-ov standard

nalaže da je naučna metoda ili tehnika pre svega opšte prihvaćena u stručnim krugovima pre nego što se njen rezultat može prihvatiti kao dokaz

Prikupljanje digitalnih dokaza

- Veoma je važno da bude određena jedna osoba na licu mesta koja će imati apsolutni autoritet u određivanju načina na koji će se osigurati mesto zločina odnosno lice mesta, kao i načina na koji će se pretraga sprovesti i kako će se rukovati dokazima.
- Jednako je važno da svaki od članova tima razume sopstvenu ulogu i da doprinese timskom radu.
- Timski rad je neophodan i ključan za uspeh prikupljanja dokaza.

Nakon dolaska policije na mesto zločina, u procesu prikupljanja digitalnih dokaza učestvuje više lica:

Prikupljanje digitalnih dokaza – uloge

Prvi pristigli na lice mesta

- Identifikovanje mesta zločina
- Zaštita mesta zločina
- Čuvanje privremenih ili osetljivih dokaza

Istražitelj

- Uspostavljanje lanca komande
- Sprovođenje pretrage na mestu zločina
- Očuvanje integriteta dokaza

Tehničar za mesto zločina

- Očuvanje osetljivih dokaza i dupliciranje diskova
- Gašenje sistema i priprema za transport
- Obeležavanje i evidentiranje dokaza
- Pakovanje dokaza
- Transport dokaza
- Procesiranje dokaza

Procedura zaplene kompjutera na licu mesta (kompjuter je uključen)

- Fotografisanje monitora
- Očuvanje osetljivih dokaza
- Pravljenje kopije diska pre zaplene kompjutera
- Provera integritet kopije
- Ugasiti kompjuter shodno operativnom sistemu
- Fotografisanje povezivanja kompjutera
- Odvajanje kablova od kućišta sa preciznim beleženjem svih elemenata
- Upotreba antistatičke narukvice na zglobu ruke (ili druge metode uzemljenja) da bi se izbegla potencijalna šteta
- Smeštanje svih elektronskih uređaja u antistatičke kesice

Čuvanje digitalnih dokaza

Neki podaci su „privremeni", tj. za razliku od podataka smeštenih na disku oni će se izgubiti nakon gašenja napajanja.
Podaci na hard disku se lako mogu oštetiti, uništiti ili promeniti (namerno ili slučajno bez razlike).
Prvi korak u rukovanju takvim digitalnim dokazima je zaštita od bilo kakve manipulacije ili nesreće.
Najbolji način je pravljenje kompletne „bitstream" kopije diska ili medija na kojoj se nalaze dokazi ili potencijalni dokazi.

Privremeni dokazi

- Podaci koji se čuvaju u privremenim lokacijama (RAM, keš memorija, kao i memorija prisutna na video karicama, ruterima...) nazivaju se privremeni pošto zavise od prisustva struje u očuvanju sadržaja.
- Prikupljanje ove vrste podataka predstavlja značajan izazov pre svega zato što se samim pristupom menja stanje sistema (samim tim i stanje sistemske memorije).

Kreiranje precizne kopije diska

- Za forenzičare je najbitnije očuvanje redosleda i rasporeda svih podataka zato je neophodno korišćenje „bitstream" kopije.
- Ovakva kopija je identična originalu, i fizički i logički.

Postoji nekoliko načina kreiranja precizne kopije diska na nivou bitova:

- Uklanjanje diska iz kompjutera osumnjičenog i priključivanje istog na radnu stanicu forenzičara i pravljenje kopije
- Priključivanje drugog diska na kompjuter osumnjičenog i pravljenje kopije
- Upotreba samostalnih mašina za kloniranje
- Pomoću mrežne konekcije/interneta/USB priključka

Čuvanje digitalnih dokaza – aplikacije

Postoji veliki broj aplikacija koje su razvijene specijalno za upotrebu dupliciranja diskova za potrebe digitalnih dokaza i analiziranja tog materijala. Najpoznatiji je svakako Encase.

Ovaj program se ističke veoma intuitivnim grafičkim okruženjem, kao i podrškom za veliki broj platformi i fajl sistema. Takođe odlikuje se i brzinom u pretraživanju i analiziranju datoteka kao i ugrađenoj mogućnosti bitstream kopiranja.

- *SafeBack*

Jedan od prvih alata koji je razvijen za ovu namenu. Od 1990 se koristi u laboratorijama američkog FBI i IRS-a. On nema mogućnost analiziranja podataka, kao ni grafički interfejs.

- *AccessData*

Kao jedan od pionira na ovom polju AccessData predstavlja nezaobilazni alat za svakog forenzičara. Pre svega ova kompanija predstavlja lidera na polju razbijanja šifara. Takođe najpotpuniji set aplikacija koji se nalazi u UTK (Ultimate Toolkit) omogućava spašavanje dokaza, kloniranje, uništavanje podataka, pregled registara.

Možda i najznačajnije od svega, ovaj paket odlikuje i sjajan sistem izveštaja.

Specifične situacije

Faktor uticaja okruženja

Podaci koji su smešteni kao namagnetisanje na nekom mediju mogu biti uništeni ili oštećeni:

- ✓ izlaganjem magnetnom ili elektromagnetnom polju
- ✓ izlaganjem toploti
- ✓ statičkim elektricitetom
- ✓ mehaničkim putem (udar)

Očuvanje vremenskog žiga

Vremenski žig sadrži vreme i datum pristupa, kreiranja ili modifikovanja datoteka. Ovi podaci se mogu pokazati kao ključni u nekom sudskom postupku.

Pristup datoteci menja ovaj žig, zato je neophodno beleženje vremena svake datoteke ukoliko se ne može raditi na kopiji.

Spašavanje digitalnih dokaza

- Prikupljanje obrisanih podataka
- Pronalaženje skrivenih podataka
- Zaštićena zona diska
- Razbijanje šifara

Prikupljanje obrisanih podataka

- Mnogi korisnici kompjutera, uključujući tu i kriminalce, misle da kada jednom obrišu datoteku ona nestaje sa hard diska.
- Brisanje datoteke uz pomoć alata operativnog sistema, jednostavno uklanja pokazivač na tu datoteku iz tabele sadržaja diska.

Pronalaženje skrivenih podataka

- *Shadow* podaci, predstavljaju jednu od opcija prilikom istraživanja, a nastaju kao razlika u pozicioniranju (vertikalnom i horizontalnom) magnetnih glava.
- *Steganografija* podrazumeva skrivanje datoteka unutar drugih datoteka.
- *Alternativni tokovi podataka* predstavljaju još jedan od mogućih izvora informacija u okviru kompjuterske forenzike. Ovaj pojam se odnosi na NTFS fajl sistem koji podržava ovu mogućnost.

Zaštićena zona diska

Zašto je postojanje ove zone bitno forenzičarima?

- Postoje dve realne opasnosti:
  Prva je zaključavanje diska i postavljanje stepena zaštite na maksimum.
  - Druga opasnost leži u podešavanju SET_MAX_LBA.

Uništavanje podataka

- Prepisivanje diska
- *Demagnetizacija*
- *Fizičko uništavanje diska*
  - *Pulverizacija (pretvaranje pločica u prah)*
  - *Paljenje (paljenje pločica do pepela)*
  - *Peskiranje (pomoću peska odstranjivanje površine pločice)*
  - *Kiselina (potapanjem pločice u rastvor ili koncentrat kiseline)*

Elektronsko poslovanje

- **Elektronsko poslovanje** je **kupovina i prodaja informacija**, **proizvoda** i **usluga putem računarske mreže**, podrška za bilo koju vrstu transakcija putem digitalne infrastrukture i elektronska realizacija poslovanja.
- Elektronsko poslovanje je takav oblik poslovnih aktivnosti i transakcija koje se **odvijaju u računarskim mrežama uz korišćenje odgovarajućih protokola** nastalih u standardnim procesima.
- Elektronsko poslovanje se može obavljati u okviru:
  - **Zatvorenih mreža** (npr. Bankarske mreže); i
  - **Otvorenih mreža** (Internet).
- Najveći obim elektronskog poslovanja se odvija putem interneta te će se i ova prezentacija odnositi na ovaj tip poslovanja.

Vrste elektronskog poslovanja

- **B2C** (business to consumers) – predstavlja model elektronskog poslovanja kompanije sa krajnjim potrošačima – kompanija preko web strane nudi robe i usluge krajnjim potrošačima.
- **B2B** (business to business) – predstavlja model elektronskog poslovanja između privrednih subjekata u okviru svoje delatnosti.
- **C2C** (consumers to consumers) - – predstavlja model elektronskog poslovanja između potrošača odnosno fizičkih lica (i pravnih lica van njihove osnovne delatnosti). U okviru ovog tipa poslovanja kompanije se javljaju kao posrednici tj. nude aplikacijske usluge putem kojih se obavlja poslovanje. Primjer ovog tipa poslovanja su intgernet aukcije (npr. eBAY).

Regulisanje Elektronskog poslovanja

- Na Elektronsko poslovanje se najpre primenjuju propisi koji se inače odnose na samu delatnost koja se obavlja putem elektronskog poslovanja.
  - Primer: ukoliko želite da se bavite prodajom farmaceutskih proizvoda putem interneta neophodno je da ispunite sve propisane uslove i pribavite sve potrebne dozvole za obavljanje ove delatnosti (otvaranje Apoteke).
- Dodatno, na elektronsko poslovanje se primenjuju posebni propisi koji regulišu ovaj vid obavljanja poslovne aktivnosti.

Pravni okvir Elektronskog poslovanja u Republici Srbiji

- Zakon o elektronskoj trgovini
    - Službeni glasnik RS br. 41/09
- Zakon o elektronskom potpisu
    - Službeni glasnik RS br. 135/04
- Zakon o elektronskom dokumentu
    - Službeni glasnik RS br. 51/09
- I drugi koji mestimično spominju Internet i elektronsko poslovanje.

Predmet Zakona o elektronskoj trgovini

- Zakon o elektronskoj trgovini uređuje:
    - način pružanja **usluga informacionog društva**;
    - obaveze **informisanja korisnika** usluga;
    - **komercijalne poruke**;
    - pravila u vezi sa **zaključenjem ugovora** u elektronskom obliku;
    - **odgovornost pružaoca usluga** informacionog društva; i
    - nadzor i prekršaje.

Usluge informacionog društva

- ***Usluga informacionog društva*** je usluga koja se pruža:
    - na daljinu
    - uz naknadu;
    - putem elektronske opreme za obradu i skladištenje podataka; i
    - na lični zahtev korisnika usluga.
- **Usluge informacionog društva** su pre svega **usluge koje se pružaju putem interneta** a naročito:
    - prodaja robe i usluga putem Interneta;
    - nuđenje podataka i reklamiranje putem Interneta,
    - elektronski pretraživači, kao i omogućavanje traženja podataka i usluga koje se prenose elektronskom mrežom,
    - obezbeđivanje pristupa mreži ili skladištenje podataka korisnika usluga.

Način pružanja usluga informacionog društva

- Pružanje usluga informacionog društva je slobodno odnosno nije potrebna posebna dozvola ili odobrenje.
- Pružalac usluga mora, pre nego što otpočne da obavlja delatnost pružanja tih usluga, da bude registrovan pri Agenciji za privredne registre.
- *Pružalac usluga **sa sedištem u Republici Srbiji*** dužan je da postupa i pruža usluge u skladu sa zakonima i propisima donetim na osnovu zakona Republike Srbije. (član 4. stav 1.)
- *Pružalac usluga informacionog društva* je pravno lice ili preduzetnik koji pruža usluge informacionog društva (član 3. stav 1. tačka 4.)
- *Pružalac usluga* mora, pre nego što otpočne da obavlja delatnost pružanja tih usluga, da bude registrovan u Registar privrednih subjekata u skladu sa zakonom kojim se uređuje registracija privrednih subjekata. (član 5. stav 3.)
- Prethodna odredba ne odnosi se na pružaoca usluga koji ima **svojstvo stranog lica** u smislu zakona kojim se uređuje spoljnotrgovinsko poslovanje. (član 5. stav 4.)
- Pružalac usluga dužan je da korisnicima usluga na web stranici pruži sledeće informacije:

- naziv; sedište, email i ostale podatke o pružaocu usluga na osnovu kojih korisnik usluga može sa njim brzo i nesmetano da ostvari komunikaciju;
- matični broj, Pib i PDV broj
- podatke o upisu u Registar; pojedinosti o nadležnom organu, ako delatnost pružaoca usluga podleže službenom nadzoru a u pogledu posebno regulisnih delatnosti, odnosno profesija:
    - profesionalno ili slično strukovno udruženje kod koga je pružalac usluga registrovan;
    - profesionalni naziv i država koja ga je odobrila;
    - uputstva o profesionalnim pravilima u državi u kojoj se obavlja delatnost i mestu njihove dostupnosti;

- Ukoliko pružalac usluga **navodi cene**, one moraju biti **jasno i nedvosmisleno naznačene**, a posebno mora naznačiti da li su u te cene uključeni troškovi dostave, ostali manipulativni troškovi, porez i drugi troškovi koji na njih utiču.

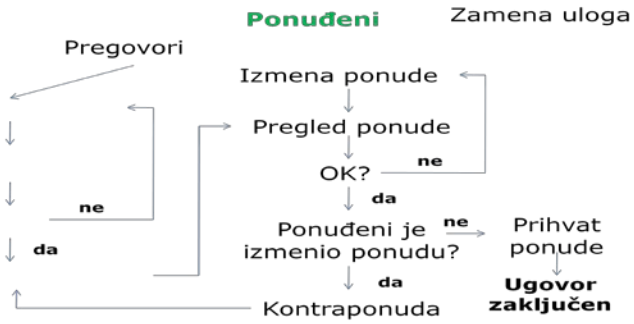
Komercijalne poruke

- Ukoliko vrši reklamiranje putem interneta, pružalac usluga dužan je da obezbedi:
    - da je komercijalnu poruku moguće kao takvu jasno identifikovati u trenutku kada je korisnik usluga primi;
    - da je lice u čije ime je komercijalna poruka sačinjena moguće jasno identifikovati;
    - da svaki promotivni poziv za stavljanje ponude iz komercijalne poruke (uključujući popuste i poklone) mora kao takav biti jasno identifikovan;
    - da uslovi koji moraju biti ispunjeni za stavljanje ponude iz komercijalne poruke moraju biti lako dostupni, kao i da su predočeni na jasan i nedvosmislen način.
- Korišćenje elektronske pošte u svrhu slanja netražene komercijalne poruke (SPAM), dozvoljeno je samo uz prethodni pristanak lica kome je takva vrsta poruke namenjena, u skladu sa zakonom.

Pravila u vezi sa zaključenjem ugovora u elektronskom obliku

- Ugovor može biti zaključen elektronskim putem, odnosno u elektronskoj formi.
- Ponuda i prihvat ponude mogu se dati elektronskim putem, odnosno u elektronskoj formi.
- Kada se elektronska poruka, odnosno elektronska forma koristi prilikom zaključenja ugovora, takvom ugovoru se ne može osporiti punovažnost samo zbog toga što je sačinjen u elektronskoj formi.
- Kada se kao pretpostavka punovažnosti i nastanka ugovora zahteva potpis lica, smatra se da taj uslov zadovoljava elektronska poruka potpisana kvalifikovanim elektronskim potpisom, u skladu sa zakonom kojim se uređuje elektronski potpis.

Proces zaključenja ugovora



Pravila u vezi sa zaključenjem ugovora u elektronskom obliku

- Pružalac usluga dužan je da obezbedi da tekst ugovora i odredbe opštih uslova poslovanja koje su sastavni deo ugovora zaključenih u elektronskoj formi budu dostupni korisnicima usluga.

- Pružalac usluga dužan je da, bez odlaganja, elektronskim putem, posebnom elektronskom porukom, potvrdi prijem elektronske poruke koja sadrži ponudu ili prihvat ponude za zaključenje ugovora.
- Ugovor u elektronskoj formi smatra se zaključenim onog časa kada ponuđač primi elektronsku poruku koja sadrži izjavu ponuđenog da prihvata ponudu.
- Ponuda i prihvat ponude, kao i druge izjave volje učinjene elektronskim putem, smatraju se primljenim kada im lice kome su upućene može pristupiti.

Odgovornost pružaoca usluga informacionog društva

Pružalac usluga koji skladišti podatke pružene od strane korisnika usluga, na zahtev korisnika usluga, **nije odgovoran za sadržaj skladištenog podatka**, ako:

1. **nije znao niti je mogao znati** za nedopušteno delovanje korisnika usluga ili za sadržaj podatka;
2. **odmah nakon saznanja** da se radi o nedopuštenom delovanju ili podatku ukloni ili onemogući pristup tom podatku.

Pružalac usluga koji posredstvom **elektronskog upućivanja** omogući pristup podacima drugog pružaoca usluga, **nije odgovoran za te informacije**, ako:

1. **nije znao niti je mogao znati** za nedopušteno delovanje korisnika usluga ili za sadržaj podataka u tim informacijama;
2. **odmah nakon saznanja** da se radi o nedopuštenom delovanju ili podatku ukloni ili onemogući pristup podacima.

Elektronski potpis

- **Elektronski potpis** - skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika
- Elektronski potpis vrši se upotrebom **Elektronskog sertifikata** - elektronska potvrda kojom se potvrđuje veza podataka za proveru elektronskog potpisa i identiteta potpisnika
- Kako se elektronski potpisuje:
    - **tajni ključ**
    - **javni ključ**
    - **uparivanje** da dati javni ključ predstavlja kriptografski par sa tajnim ključem kojim je poruka elektronski potpisana

- **Elektronski sertifikat** predstavlja mehanizam za pouzdano pridruživanje između identiteta određenog korisnika i njegovog javnog ključa za primenu asimetričnog kriptografskog algoritma tj. implicira da je sertifikaciono telo (izdavalac elektronskog sertifikata), kao "treća strana od poverenja", proverila da dati javni ključ pripada definisanom korisniku i da svojim potpisom sertifikuje da je to istinito.
- **Kvalifikovani elektronski potpis** - elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata i onemogućava naknadno poricanje odgovornosti za njihov sadržaj.
- **Kvalifikovani elektronski potpis** se kreira primenom sredstva za kreiranje kvalifikovanog elektronskog potpisa (SSCD – Secure Signature Creation Device) i koji se proverava putem kvalifikovanog elektronskog sertifikata potpisnika. Ovaj potpis je pravno ekvivalentan svojeručnom potpisu u skladu sa Zakonom o elektronskom potpisu.

Elektronski dokument

- **Elektronski dokument** - jeste skup podataka sastavljen od slova, brojeva, simbola, grafičkih, zvučnih i video zapisa sadržanih u bilo kom aktu
- **Uslov postojanja** - da je elektronski izrađen ili digitalizovan, poslat, primljen, sačuvan ili arhiviran na elektronskom, magnetnom, optičkom ili drugom mediju

- **Digitalizacija** - prenošenje dokumenata iz drugih oblika u elektronski oblik
- **Vremenski žig** - zvanično vreme pridruženo elektronskom dokumentu kojim se potvrđuje sadržaj elektronskog dokumenta u to vreme

Žigovi, internet i sukob zakona

ŽIG – pravni pojam

Žig je **pravo** kojim se **štiti znak** koji u prometu **služi za razlikovanje robe**, odnosno **usluga** jednog fizičkog ili pravnog lica **od iste ili slične robe**, odnosno usluga drugog fizičkog ili pravnog lica.

Koji znak može biti predmet zaštite?

Znak koji se može grafički predstaviti.

Primeri:

- reči, slova
- brojevi
- slogan
- slike, crtež
- rasporeda boja i trodimenzionalnih oblika
- kombinacija navedenih znakova

Kako steći pravo na ŽIG?

- Zavod za intelektualnu svojinu Republike Srbije vodi Registar prijava za priznanje žigova i Registar žigova koji su javne knjige.
- Zainteresovana lica mogu da razgledaju Registre bez plaćanja posebnih taksa. www.zis.gov.rs
- Žig se stiče registracijom odnosno momentom upisa priznatog prava u Registar žigova i traje deset godina od sticanja podnošenja prijave.

Prava nosioca žiga

- Nosilac žiga:
  - **ima** isključivo **pravo da** znak zaštićen žigom **koristi** za obeležavanje robe, odnosno usluga ; i
  - **ima pravo da** drugim licima **zabrani** da isti ili sličan znak neovlašćeno koriste za obeležavanje iste ili slične robe, odnosno usluga, **ako taj znak može da izazove zabunu u prometu.**

Ograničenja žiga

TRŽIŠNO:

- Nosilac žiga ne može zabraniti drugom licu da isti ili sličan znak koristi za obilježavanje robe, odnosno usluga druge vrste, osim ako je u pitanju čuveni žig.

VREMENSKO:

- Nosilac žiga ne može da zabrani drugom licu da pod istim ili sličnim znakom stavlja u promet svoju robu, odnosno usluge, ako taj znak predstavlja njegovu firmu ili naziv koji je na savjestan način stečen prije priznatog datuma prvenstva žiga.

TERITORIJALNO:

- Nosilac žiga ne može da zabrani drugom licu da pod istim ili sličnim znakom stavlja u promet svoju robu na tržištu na kome žig nije registrovan/zaštićen.

Kako pravo intelektualne svojine vidi svet:

Princip teritorijalnosti: Nosilac žiga uživa prava koja je stekao registracijom žiga u okviru teritorije države prema čijim propisima je stekao samo pravo.

Šta nosilac prava može da zahteva tužbom?

- U slučaju povrede žiga ili prava iz prijave žiga, tužilac može tužbom da zahtijeva:
    1) utvrđenje povrede prava;
    2) prestanak povrede prava;
    3) uništenje ili preinačenje predmeta kojima je izvršena povreda prava;
    4) uništenje ili preinačenje alata i opreme uz pomoć kojih su proizvedeni predmeti kojima je izvršena povreda prava, ako je to neophodno za zaštitu prava;
    5) naknadu imovinske štete i opravdanih troškova postupka;
    6) objavljivanje presude o trošku tuženog;
    7) davanje podataka o trećim licima koja su učestvovala u povredi prava.

Budućnost rešenja problema

- Moguća rešenja:
    - Napuštanje principa teritorijalnosti u žigovnom pravu (pravu intelektualne svojine) ili
    - Uvođenje principa teritorijalnosti na Internet-u