Kompjuterska forenzika i forenzički alati

- **Zakon o informacionoj bezbednosti RS**
  - **Zakon o elektronskom dokumentu**

Forenzika

- Pojam „forenzika“ je nastao od latinske reči „forensi“ što znači „na otvorenom prostoru“ a dolazi od reči „forum“.
- Kasnije, kada je ta reč počela de se koristi u engleskom jeziku njeno značenje je ograničeno na „oblast pravnokrivične istrage“.

Digitalna forenzika

- Digitalna forenzika je nauka koja ima za cilj prikupljanje, čuvanje, pronalaženje, analizu i dokumentovanje digitalnih dokaza odnosno podataka koji su skladišteni, obrađivani ili prenošeni u digitalnom obliku.
- Vrste:

✓računarska forenzika,

✓forenzika mobilnih uređaja,

✓mrežna forenzika i

✓forenzika baze podataka

- Digitalna forenzika ima široku primenu i nije ograničena samo na policijsko-sudske i vojno-obaveštajne aktivnosti.
- Bankarski sektor, osiguravajuća društva i kompanije raznih profila imaju potrebu i moraju biti izuzetno oprezni sa podacima kojima raspolažu jer je mnogim kompanijama nanesena nemerljiva šteta zbog industrijske špijunaže i generalne zloupotrebe IT sistema

Kompjuterska forenzika

- Kompjuterska forenzika je grana digitalne forenzike koja se odnosi na pronalaženje dokaza u kompjuterima i na drugim digitalnim medijima.
- Kompjuterska forenzika je disciplina koja ima za cilj da prikupi, sačuva i prezentuje podatke koji su dobijeni sa medija za čuvanje podataka (Hard Disk, CD ROM, DVD,ROM, Floppy Disk Drive, USB Driver…).
- Kombinujući elemente prava i kompjuterske nauke sakuplja i analizira podatke koji se dalje koriste kao dokazi na sudu. Koristi slične tehnike koje se podrazumevaju prilikom spasavanja podataka sa dodatkom smernica za primenu u pravnom postupku.

- Internet kao globalna mreža koja povezuje milijarde kompjutera je značajno izmenila značenje kompjuterske forenzike, tako da se sada više govori o cyber forenzici, koja predstavlja širi pojam.
- Mesto izvršenja zločina više nije samo prostorija u kojoj se nalazio kompjuter u vreme izvršenja, tradicionalna forenzička analiza koja se sprovodila u laboratorijama i gde se pregledavala zaplenjena oprema više nije dovoljna, a digitalin dokazi se mogu nalaziti bilo gde u svetu, što utiče na povećanje složenosti samog procesa prikupljanja dokaza.
- Svi upadi u tuđe mreže, zloupotrebe tuđih podataka, pregledavanje i distribucija zabranjenih sadržaja, kao i ostale nedozvoljene radnje se dešavaju on-line, u realnom vremenu i da bi se počinioci uhvatili na delu prvo njihove aktivnosti moraju biti praćene, a da se ne povredi pravo na privatnost.

Da bi se videle aktivnosti na računaru vrši se pregled:

- ✓ **Radne memorije**
- ✓ **Sistemskih registra**
- ✓ **Skrivenih fajlova i datoteka**
- ✓ **Liste poslednjih dokumenata**
- ✓ **Za pregledavanje on-line aktivnosti proveravaju se:**
- ✓ **Kolačići**
- ✓ **Obeleživači**
- ✓ **Istorija**
- ✓ **Cache**
- ✓ **Privremeni internet fajlovi**
- ✓ **Informacije vezane za IP adresu kompjutera i vreme kojeje provedeno na Internetu se mogu dobiti od lokalnog ISPprovajdera.**

Forenzički alati

- Alati (hardver i softver) koji se koriste za istragu su alati za detekciju podataka, alati za analizu prikupljenih podataka, alati za proveru autentičnosti itd. Postoji veliki broj različitih softverskih alata koji se mogu preuzeti besplatno sa Interneta.

Software

- Danas se koristi kao najnapredniji sigurnosni alat, a kao standard su ga prihvatile većina vodećih kompanija I organizacija u oblasti digitalne forenzike. Omogućava I olakšava sudskim veštacima i IT stručnjacima istraživanje slučajeva, akviziciju i analizu dokaznog materijala

Podela forenzičkih alata

- **Prema načinu inplementacije**:

❖ Hardverske alate

❖Programske (softverske) alate

- **Prema oblasti upotrebe**:

❖ Alate za forenziku računarske mreže

❖Alate za forenziku računarskog sistema

❖Alate za analizu drugih digitalnih uređaja

❖ Alate za forenziku softvera

- **Prema tipu koda**:
  - Programske alate otvorenog koda
  - Licencirane programske alate
- **Prema platformi na kojoj ra**de:
  - Alate koji rade na Windows platformi
  - Alate koji rade na linuksu i drugim platformama
- **Prema fazi procesa koji obavljaju u forenzičkoj istrazi**:
  - Alate za pravljenje sterilnih medijuma
  - Alate za pravljenje fizičke kopije čvrstog diska
  - Alate za oporavak podataka
  - Alate za dešifrovanje podataka
  - Alate za analizzu digitalnog materijala
  - Alate za dokumentovanje

- Izbor alata za digitalnu forenzičku istragu predstavlja izazov i nedovoljno je istražena tema u oblasti digitalne forenzike.
- Izbor alata koji će biti korišćen za konkretnu digitalnu forenzičku istragu u velikoj meri utiče na ishod u sudnici.
- Iako je cilj uvek jasan – dobijanje validnih digitalnih dokaza prihvatljivih na sudu, praksa pokazuje da do toga nije nimalo lako doći.
- Digitalni dokaz treba da potkrepi dokaze iznete u sudnici, da dokaže krivicu ili oslobodi osumnjičenog. Mora biti pouzdan i doprinositi istrazi.
- Ono što je potrebno da bi se neki forenzički alat koristio u istrazi, je da bude sertifikovan i priznat od državnih sudskih organa.
- Izbor alata je najznačajniji za adekvatnu I pravno valjanu forenzičku istragu.

HVALA VAM NA PAŽNJI!