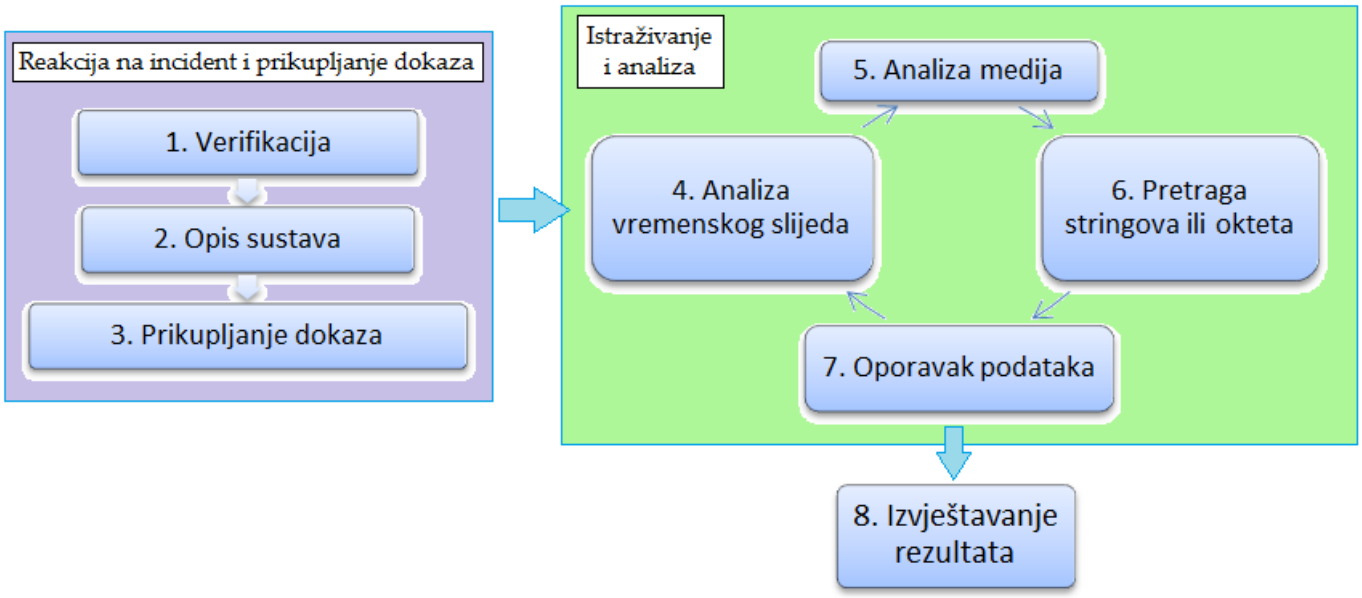
Osnove forenzike računala

Računalna forenzika je više od analize blokova podataka. Riječ je o efektivnom skupljanju, analizi i izvještavanju o korištenim postupcima i nalazima. Iskusni istražitelj zna da je svaki korak bitan kako bi njegov slučaj imao željeni kraj.

1. **REAKCIJA NA INCIDENT I PRIKUPLJANJE DOKAZA**
   U ovom koraku se preuzima računalo i skupljaju promjenjivi (eng. *volatile*) i nepromjenjivi podaci.
2. **ISTRAŽIVANJE I ANALIZA**
   U ovom koraku istražitelj pregledava skupljene podatke i analizira ih kako bi dobio jasnu sliku o tome što se dogodilo. Pri analizi se koriste alati i tehnike za oporavak podataka, otkrivajući dijelove slagalice i vremenski slijed događaja.
3. **IZVJEŠTAVANJE O REZULTATIMA**
   Izvještavanje je najvažniji korak od svih jer su bez njega ostali koraci uzalud utrošeno vrijeme. Bez detaljnog izvještaja o korištenim alatima, tehnikama te o pronađenim dokazima, ništa otkriveno se ne može koristiti na sudu.

Metodologija forenzičke istrage



1. **VERIFIKACIJA**
   Prvi korak istrage je utvrđivanje da je uistinu došlo do incidenta kojeg treba istražiti.
2. **OPIS SUSTAVA**
   Način na koji istražitelj opiše sustav će utjecati na daljnju istragu. Ako je riječ o kritičnom poslužitelju, možda se neće moći isključiti iz mreže. Ako je riječ o radnoj stanici, potrebno je odrediti za što se koristila. Predviđanje vrste informacija koje se mogu naći na sustavu će pomoći prilikom daljnjeg skupljanja i analize podataka.
   - Općenito opisati sustav koji se analizira.
   - Gdje je nađen sustav?
   - Za što se koristi(o)?
   - Kako je konfiguriran (operacijski sustav, mreža)?

- Ostali podaci koji bi mogli biti važni za slučaj.

3. **PRIKUPLJANJE DOKAZA**
   Dokazima se smatra sve što se može pronaći na istraživanom sustavu. To mogu biti podaci o procesima, mrežnim vezama, dnevničke datoteke (eng. *log files*) i podaci o korisniku.
   - Uzeti forenzičku sliku sustava (eng. *image*).
   - Skupiti važne podatke.
   - Skupiti promjenjive podatke - procesi, memorija, mrežne veze.