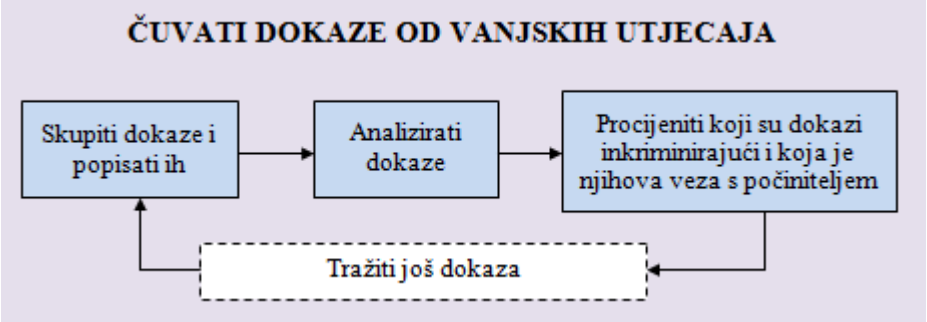
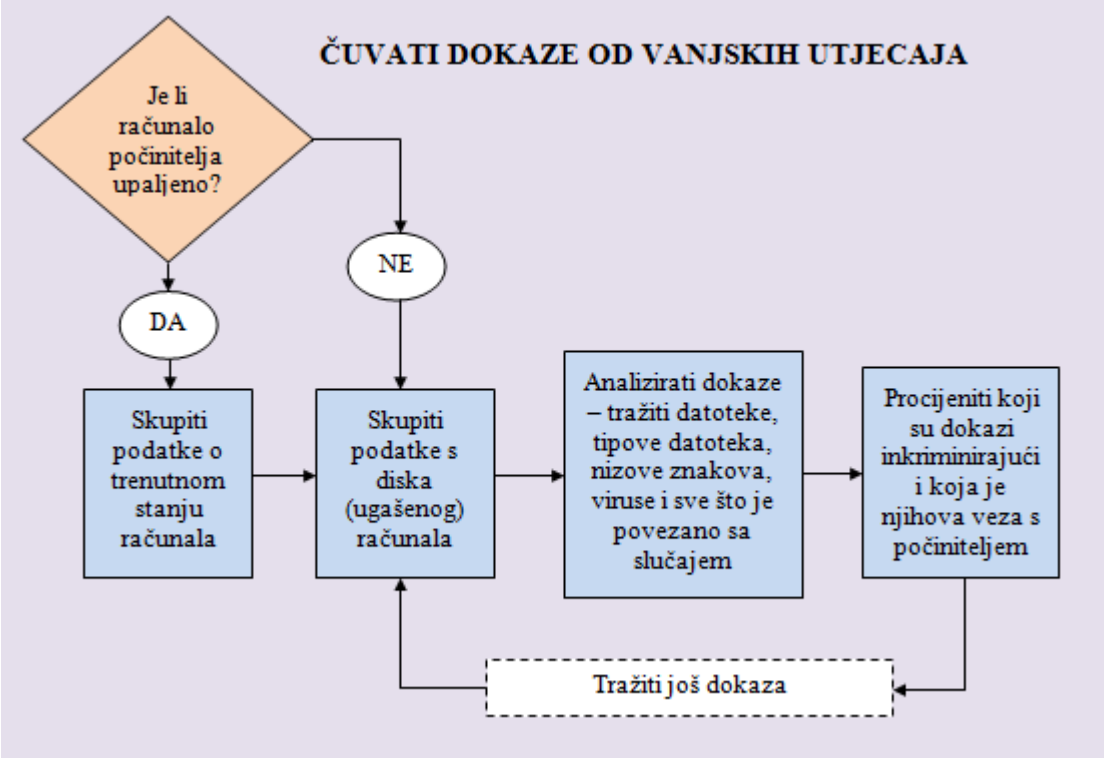
Tijek forenzičke istrage

Tijekom forenzičke istrage bitno se pridržavati određenih koraka. Oni nisu zakonski obvezujući već su oblikovani na temelju dugogodišnjeg iskustva forenzičkih istražitelja s ciljem da se smanji mogućnost previđanja bitnih detalja koji bi mogli utjecati na konačni ishod istrage. Slijedeća slika prikazuje dijagram forenzičkih postupaka. Riječ je o standardnom procesu primjenjivom u svim vrstama istraga, pa tako i u istragama računalnih zločina.



Kad se koraci forenzičkih procesa prilagode računalima, gornji dijagram dobiva novi oblik (slika ispod). Ono što je bitno kod analize računala je da se puno dokaza može skupiti dok je računalo još upaljeno. Istražitelj ima samo jednu priliku za to jer se svakom dodatnom radnjom (npr. pokretanjem neke aplikacije, otvaranjem web preglednika, ...), kao i gašenjem računala uništavaju podaci iz radne memorije računala. Računalo se stoga mora ostaviti upaljeno dok se ne kopiraju svi podaci iz radne memorije.



Koraci navedeni u gornjim dijagramima su okvirni i mogu se razlikovati od istrage do istrage.

4 osnovna principa

1. **Minimizirati gubitak podataka**
   Sustav ni u kojem slučaju ne može ostati nepromijenjen u procesu skupljanja podataka. Cilj dobrog istražitelja je da minimizira gubitak i maksimizira količinu prikupljenih podataka.

2. **Bilježiti sve o svemu**
   Istražitelj mora snimati, slikati, zapisivati i bilježiti apsolutno sve svoje postupke i pronađene podatke.

3. **Analizirati sve prikupljene podatke**
   Nakon što je utvrđeno da je stvarno došlo do incidenta, istražitelj treba početi duplicirati sve podatke, počevši od onih najsklonijih izmjenama koji će se izgubiti gašenjem računala.

4. **Izvjestiti o nalazima**
   Izvještaj treba biti jasan i precizan te sadržavati nalaze, zaključke i postupke koji su doveli do zaključka. Izvještaj bi trebao biti jasan i ljudima koji nisu stručnjaci u tom području.

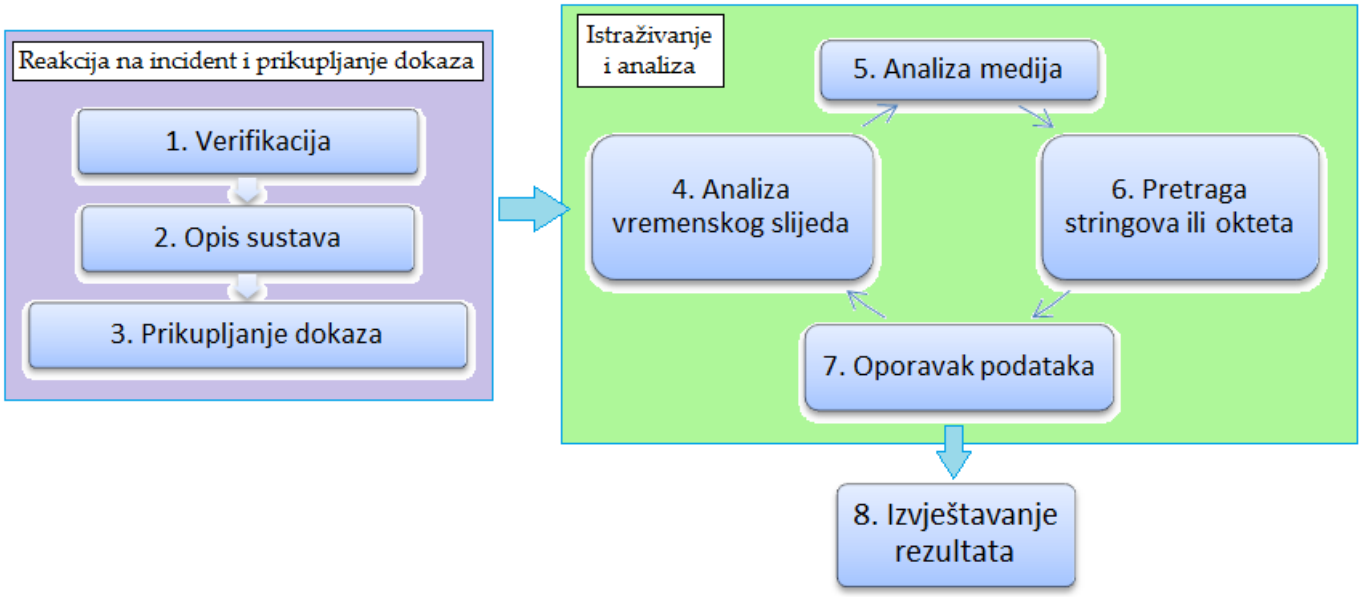
Alati forenzičke istrage

Prilikom pristupa računalu koje je predmet istrage, svaki računalni forenzičar bi trebao sa sobom imati barem osnovni alat koji će mu pomoći u skupljanju dokaza. Tu se ubrajaju:

- forenzički programi s raznim funkcijama,
- digitalna kamera,
- USB uređaj od barem 4 GB memorije za pohranjivanje manjih komada dokaza,
- tvrdi disk (500 GB je dovoljno za većinu slučajeva) za pohranjivanje dokazne kopije cijelog diska,
- računalo za analizu (laptop), s uvjetom da ne sadrži bilo kakve maliciozne programe kako ne bi ugrozilo dokaze (čak i ako se dokazi nisu oštetili, činjenica da je forenzičko računalo bilo ranjivo može rezultirati odbacivanjem dokaza na sudu),
- bilježnica i kemijska olovka za uzimanje bilješki o mjestu zločina i stanju računala ,
- program za pregledavanje preuzete slike sustava (eng. *mounting*),
- *Antivirus/Antispyware/Rootkit detector* programi na forenzičkom računalu.

Metodologija računalne forenzike

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.



- **REAGIRANJE NA INCIDENT I PRIKUPLJANJE DOKAZA**
  U ovom koraku se preuzima računalo i skupljaju promjenjivi (eng. *volatile*) i nepromjenjivi podaci.

  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.

- **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.

- **IZVJEŠTAVANJE REZULTATA**
  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.