

# Forenzički postupci

Predrag Pale



# Zašto su važni forenzički postupci?



- forenzika često pokušava **rekonstruirati** i objasniti događaje
  - njihove **sudionike**
  - **uzroke**
  - **posljedice**
- **pojedinačni** forenzički postupci
  - u najboljem slučaju mogu dati samo **dijelove slagalice**
- za **cijelu priču**
  - ih trebamo **sastaviti u pravom slijedu**
  - **interpretirati** u širem kontekstu
- zato nam treba **definirani postupak**



# Naglasak predavanja

---



- policijska (sudska) forenzika
  - ima svoje **propisane postupke**
  - zakonom **definirani djelokrug**
- u ovom predmetu bavimo se **općenitom** forenzikom
  - primjenjivom **u industriji**
- stoga **nije zasnovana** na zakonom propisanim postupcima



# Forenzički postupak

---



- **izviđanje** sustava
- **planiranje** prikupljanja dokaznog materijala
- **prikupljanje** dokaznog materijala
- **pohrana** i čuvanje
- **analiza** materijala
- **izvještavanje**



# Izviđanje sustava



- o čemu se radi – što istražujemo
  - havarija, napad, problemi , sumnja...
- definirati opseg sustava – što ćemo sve promatrati
  - računalo/uređaj, cluster, sustav, podaci, organizacija, javnost ...
- pobrojiti komponente
  - poslužitelji, radne stanice, prijenosnici, telefoni, ostala oprema povezana s IKT komponentama
- intervjuirati (su)dionike
  - operatori, rukovoditelji, uprava, korisnici, partneri ...
- prikupiti dokumentaciju
  - nacrti komunikacijskog sustava
  - logičke sheme informacijskog sustava





# Prije prikupljanja dokaznog materijala

- prikupiti **što više** informacija
  - o onome što istražujemo
- **pasivno** prikupljanje
- **intervjui**
  - korisnika
  - operatera
  - nadležnih
  - svih uključenih
- saznajte
  - koji se mrežni resursi koriste
  - koji komunikacijski servisi
    - mail serveri
    - društvene mreže
    - ...



# Planiranje prikupljanja dokaznog materijala



- identificirati **ciljani** uređaj/program/podatke
- ako to nije moguće **pobrojiti**:
  - računala: poslužitelji, korisnička
  - ručni uređaji
  - komunikacijska oprema
  - ostalo
- identificirati **ciljane uređaje**
- identificirati **ciljane podatke**
- odrediti koja se mogu **ugasiti**
- definirati **redoslijed** izuzimanja dokaznog materijala
- osigurati **legitimnost** postupka, nadležnost, potporu



# Prikupljanje dokaznog materijala



- **maknuti sve** osobe iz prostora osim forenzičara
- **ne dirajte ništa**
- **fotografirati** scenu
  - **zabilježiti** (i pismeno) sve što se čini važno
- fotografirati i dokumentirati kako je što bilo **spojeno**
- **uzeti uređaje**
- uzeti i **kabele**, ako su posebni
  - **napajanja**
- uzeti **medije**
- ne zaboraviti i **tiskane** dokumente
  - rukom pisane podsjetnike itd...
- dobro **fizički zaštитiti** predmet
  - za **prijevoz**
  - i za **skladištenje**
  - **dajte upute** za prijevoz
- svaki predmet jednoznačno **označiti**
  - i sam **predmet**
  - i **ambalažu**
- **izraditi** potrebnu **dokumentaciju** o preuzimanju potrebnog dokaznog materijala
  - i dobiti potrebne **potpise**



# Izuzimanje uređaja



- upaljene uređaje **ne gasite**
  - ugašene **ne palite**
- komunikacijske uređaje s uključenom bežičnom komunikacijom staviti u **Faradayeve vrećice**
- pogledajte na i oko uređaja
  - **uzmite sve napravice koje bi mogle biti dijelom uređaja**
- ako morate i želite ugasiti uređaj
  - prvo fotografirajte **ekran**
  - **popišite** aktivne aplikacije, posjećene stranice, ...
    - ako je sigurno!!!
  - snimite **RAM**
  - prijenosnima izvadite **bateriju**
- kad rastavljate kabele
  - označite ih, napravite skicu
  - i fotografirajte





# Pohrana i čuvanje

- pohrana i čuvanje moraju biti **u skladu sa zakonom**
- **voditi posebnu evidenciju** pohranjenog materijala
- sve što se može, treba **kopirati**
  - da se analize **ne rade** na dokaznom materijalu
- **pristup** pohranjenom dokaznom materijalu mora biti **pod strogom kontrolom**
  - kao i bilješkama analize i kasnije izvještajima
  - voditi **evidenciju pristupa** pohranjenom materijalu
- posebno voditi računa o dijelovima koji se mogu rastaviti
  - da svaki odvojiv dio bude **posebno označen i zaveden**



# Analiza materijala



- pribaviti **nalog** za analizu
  - **što tražimo?**
- **obaviti** forenzičku analizu
  - ali **na kopijama** podataka
- **voditi** precizan **dnevnik**
  - **što smo istraživali**
  - **zašto**
  - **tko je to radio**
  - **kako, čime**
  - **što je našao**
    - **podaci**
    - **zaključci**
- **pripremiti podatke** za izvještaj



# Dnevnik analize



- pitanje ili hipoteza
- na čemu (kojem materijalu) će se raditi analiza
- kojom metodom
- kojim alatima
- kada (od – do)
- rezultati
- zaključak
- idući korak - prijedlog

- Istraga
- Forenzičar
- Datum
- Mjesto
- ID analize
- ....



# Izvještavanje



- **kome** sve ide izvještaj i koja su njihova **pitanja**
- napisati **odvojeno** za svakog
  - iz dokumentacije koja je prikupljena i
  - dobivenih nalaza
- **Važno! Forenzičar nije sud i ne utvrđuje odgovornost**
  - već samo **činjenice** te daje njihovu stručnu **interpretaciju**
  - u idealnom slučaju forenzičar **samo odgovara** na pitanja
- voditi računa o **stupnju povjerljivosti**
  - označiti izvještaj na odgovarajući način
- pripremiti se za **usmeno iznošenje** nalaza te za
  - pitanja
  - protuargumente

Voditi **detaljne bilješke**  
o danim **odgovorima!**



# Struktura izvještaja



- Opis slučaja
- Širi zadatak
  - nalog
- Mišljenje
  - odgovor na pitanje 1
  - odgovor na pitanje 2
  - ...
  - odgovor na pitanje N
- Obrazloženje mišljenja
  - po pitanju
  - kratko
- Nalaz
  - rezultati analiza
  - po pitanju
- Forenzički tim
  - opis kompetencija
- Metode rada
- Prilozi



# Završetak



- kad je **sigurno** da se više neće raditi istraža
  - **vratiti** sav dokazni materijal
  - **pohraniti** svu dokumentaciju
    - evidencije
    - zapisnike
    - dnevničke
    - izvještaje





RacFor.zesoi.fer.hr  
RacFor@zesoi.fer.hr

