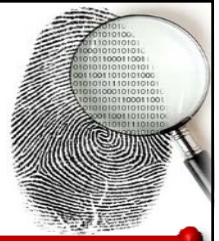

Računalna forenzika
Predrag Pale

Što je forenzika?



- otkrivanje tragova
- određivanje **redoslijeda** digitalnih tragova
- dodjeljivanje **vremena, mjesta i osobe** pronađenom tragu

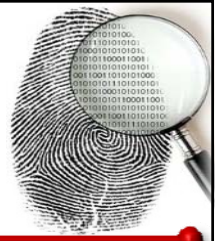
- u cilju:
  - **otkrivanja** ne očitog
    - Ono što nije vidljivo na **prvi pogled**
    - Ono što nije vidljivo **laiku**
  - **pronalaženja** nečeg što je izgubljeno
  - **pomoći u istrazi** bilo koje vrste

Po čemu se razlikuje digitalna forenzika?

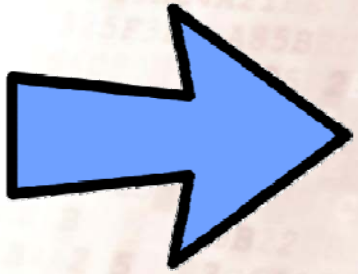
- Tragovi su **isključivo digitalni**
  - ne postoje **materijalni tragovi**
- **promjena u binarnom zapisu podataka**
  - Ne ostavlja **dodatne tragove**
- stoga, moguće je promijeniti binarne podatke
  - a da se pritom **ne može detektirati**
  - sa sigurnošću
  - **tko je i kada to učinio**

Stoga ne možemo govoriti o digitalnim dokazima već samo o digitalnim tragovima

Digitalna forenzika obuhvaća



- **analizu** digitalnih
  - informacija
  - sklopovlja
  - sustava
  - komunikacija

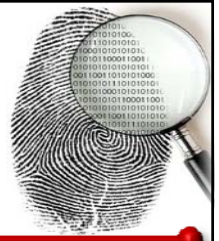


- **otrkiva**
  - sadržaj
  - događaje
  - algoritme
  - značajke sklopovlja

Područja računalne forenzike ...

- … i područja s kojima se u praksi često dotiče
  - računalna forenzika
    - otkrivanje sadržaja na računalu
    - otkrivanje prošlih događaja na računalu
  - forenzika digitalnog sadržaja
    - otkrivanje izmjena u digitalnom sadržaju
  - kriptografija
    - otkrivanje informacija
  - steganografija
    - otkrivanje namjerno skrivenih informacija
  - reverzni inženjering (eng. reverse engineering)
    - računalnih aplikacija
      - otkrivanje što i kako aplikacije rade
    - sklopovlje
      - otkrivanje što i kako sklopovlje (digitalno i analogno) radi

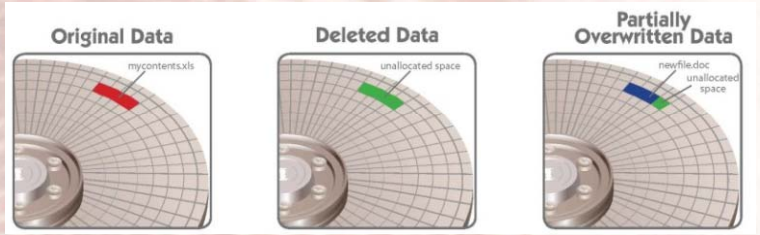
Računalna forenzika



- pronalaženje **datoteka s podacima** na digitalnim medijima
- Pronalaženje **nevidljivog sadržaja** u datotekama
- identifikacija **procesa**
  - i njegovih parametara
- identifikacija **komunikacije** s drugim računalima
  - kao i sadržaja
- analiza **sadržaja e-mail** poruka
- analiza **dnevnika aktivnosti**

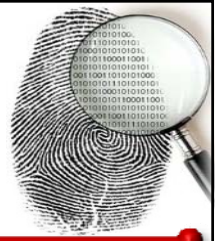
Pronalaženje podataka na digitalnim medijima

- datoteke mogu biti oštećene i obrisane zbog
  - **kvarovi** u računalu i/ili mediju
  - **kvarovi** kod **operacijskih sustava** ili aplikacija
  - **greške** prilikom rukovanja aplikacijama i/ili sklopovljem
  - **zlođudnih** aplikacija
  - **korisnika** koji namjerno izazovu kvar



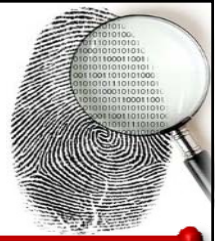
- računalna **forenzika nastoji**
  - **utvrditi** jesu li datoteke uopće postojale
  - **rekonstruirati sadržaj** datoteke ili barem njene dijelove
  - **prepoznati vrstu** sadržaja za daljnju obradu

Pronalaženje nevidljivog sadržaja u datotekama

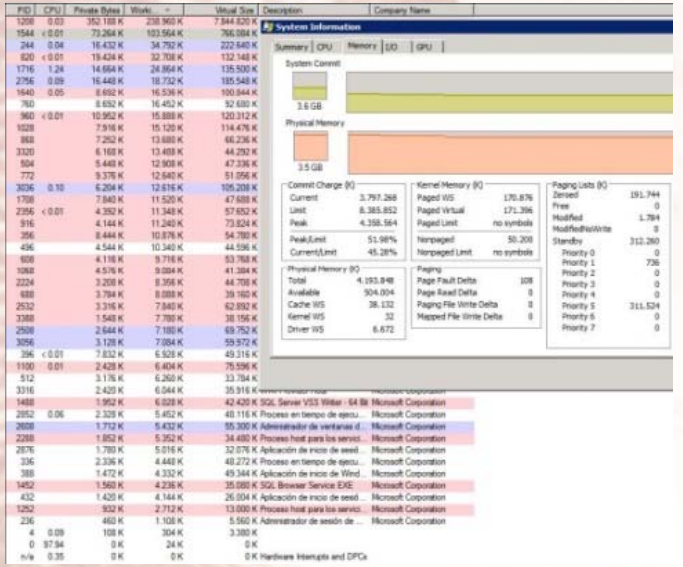


- osim **vidljivog**, namijenjenog sadržaja, podatkovne datoteke sadrže
  - **metapodatke** koji opisuju datoteke i njihov sadržaj
  - **privremene podatke** stvorene tijekom uređivanja datoteke
  - **sadržaj zaostao** od starijih datoteka koje su prethodno boravile na istom mjestu na mediju
- **forenzika** pokušava
  - **pronaći** takve podatke
  - i **prikazati** ih na koristan način

Identifikacija procesa

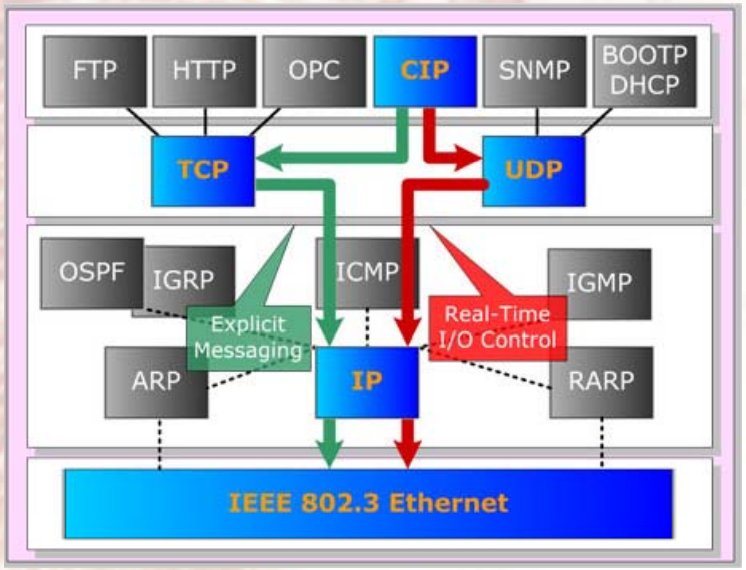


- **Svu aktivnost** u računalu izvode **procesi**
- **analizom** aktivnosti procesa moguće je **utvrditi**
  - **tko, što i kada** nešto radi
  - uključujući **skrivene programe**
    - koje nadziru aktivnost korisnika
    - ili zloćudni programi koji su infiltrirali (‘inficirali’) računalo
- forenzika pokušava
  - **identificirati** procese
  - njihove **aktivnosti**
  - **podatke** koje koriste
  - otkriti druge sustave s kojima **komunicira**



Otkrivanje komunikacije s drugim računalom

- Računala izmjenjuju podatke s **drugim računalima**
  - bilo **na eksplicitan zahtjev** korisnika (ili skrivene aplikacije)
    - SMTP, SSH, HTTP, FTP, …
  - ili **automatski**, kao dio tehničkog (pod)sustava
    - DNS, DHCP, ARP, …
- forenzika pokušava
  - **identificirati** računala s kojima se komunicira
  - otkriti **tokove** razmjene informacija
  - pronaći **ključne podatke**
    - adrese
    - ključevi
    - vremena

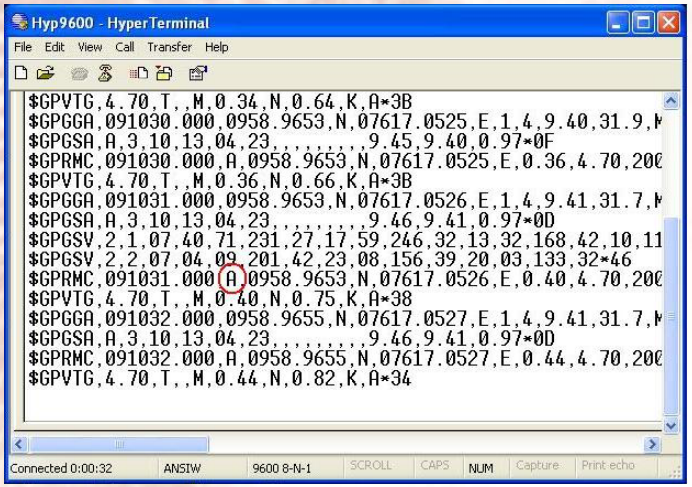


Analiza sadržaja e-mail poruka

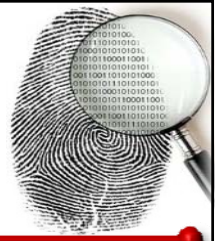
- **Pošiljatelj** e-mail poruke može biti **krivotvoren**
  - forenzika pokušava otkriti
    - (ako je moguće) **stvarnog pošiljatelja**
    - ili barem **IP adresu** od koje je poruka poslana
      I točno vrijeme **kada** je poslana
- **privitci** mogu biti **izmijenjeni**
  - forenzika pokušava
    - otkriti **stvarnu vrstu** sadržaja
    - **rekonstruirati** sadržaj

Analiza dnevnika aktivnosti

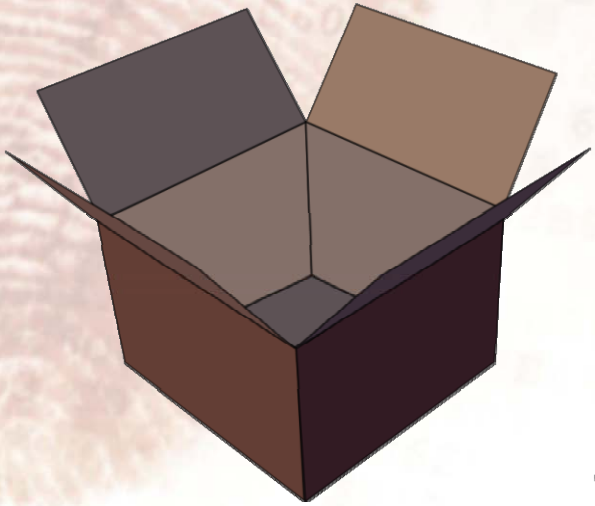
- **Prilikom rada** računala
  - **operacijski sustav i** aplikacije
  - snimaju aktivnosti u **dnevniku (engl. log)**
  - u raznim datotekama
- Forenzika analizira dnevnik kako bi
  - utvrdtila **tko je radio što i kada**
- Kolegij će analizirati dnevnike na
  - Windows OS-u
  - Linux OS-u



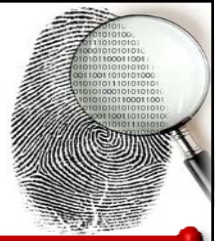
Kolegij se neće baviti



- otkrivanje je li **fotografija** mijenjana
- otkrivanje je li **audio** datoteka lažirana
- otkrivanje **tihih** dijelova **audio** datoteka
- dešifriranje **šifriranih** poruka
- **reverzni inženjering** aplikacija
- otkrivanje **algoritama**



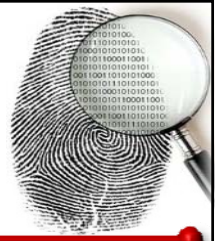
Kolegij se neće baviti ...



- **Tehnikama napada** na računalne sustave:
  - računala
  - komunikacija
  - ljudi
  - informacija

- **Tehnike zaštite** protiv napada

Metode rada tijekom semestra



- Domaće zadaće
  - **kao priprema za svako predavanje**

- Predavanja
  - pružaju **teorijsko znanje** iz pojedinih tema
    - objašnjavaju kako nešto radi

- Laboratorijske vježbe
  - pomaže u **savladavanju** sadržaja
  - olakšati stjecanje **vještina**
  - bilo u laboratoriju ili **kod kuće**

- Projekt
  - **proučavanje** specifične (pod)teme
  - **prezentacija** područja s kojima se u praksi često dotiče

Preduvjeti

- Kontinuirani rad – cijeli tjedan
  - **Priprema** za predavanje – do 1 sat
  - **Prisustvovanje** u svakom predavanju – 2 sata
  - **Rad** na laboratorijskim vježbama – do 2 sata
  - **Rad** na projektu – do 2 sata
- treba vam osobno računalo

- instalirati virtualno računalo

- instalirati operacijski sustav:
  - Windows – XP je OK
  - Linux

- koristiti dokuwiki kolegija
  - upload svih rezultata svoga rada
  - komentirati rad drugih studenata

Bodovanje

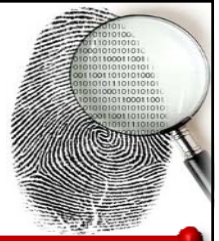
- Sve aktivnosti
  - se **boduju**
  - imaju **rokove**
  - i vaš uspjeh (rezultat)
    - se **automatski** boduje
    - kroz ispunjavanje važnih **zadatak**
    - **on-line** kroz stranicu predmeta

Aktivnost	Bodova
Predavanja	5
Domaće zadaće	10
Vježbe	30
Projekt	20
Ispit	35

- Ocjene
  - **Za prolaz potrebno je**
  - **barem 50%** bodova
  - u **svakoj** aktivnosti

Bodovi	Ocjena
60	Dovoljan (2)
70	Dobar (3)
80	Vrlo dobar (4)
90	Odličan (5)

Važno !!!



- Koristite svoju FER e-mail adresu

  Ime.Prezime@FER.hr

- Pretplatite se za sve obavijesti na kolegiju
  - http://www.fer.unizg.hr/predmet/racfor
  - Sve tipove:
    - Anketa
    - Forum
    - Obavijesti
    - Repozitorij

I u svakom slučaju,
Obavezno se zabavljajte !!! ☺

- Pratite upute u e-mail porukama i one na stranicama kolegija
  - bez odgode
- Ukoliko trebate komunicirati s nastavnicima:

  RacFor@zesoi.fer.hr


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