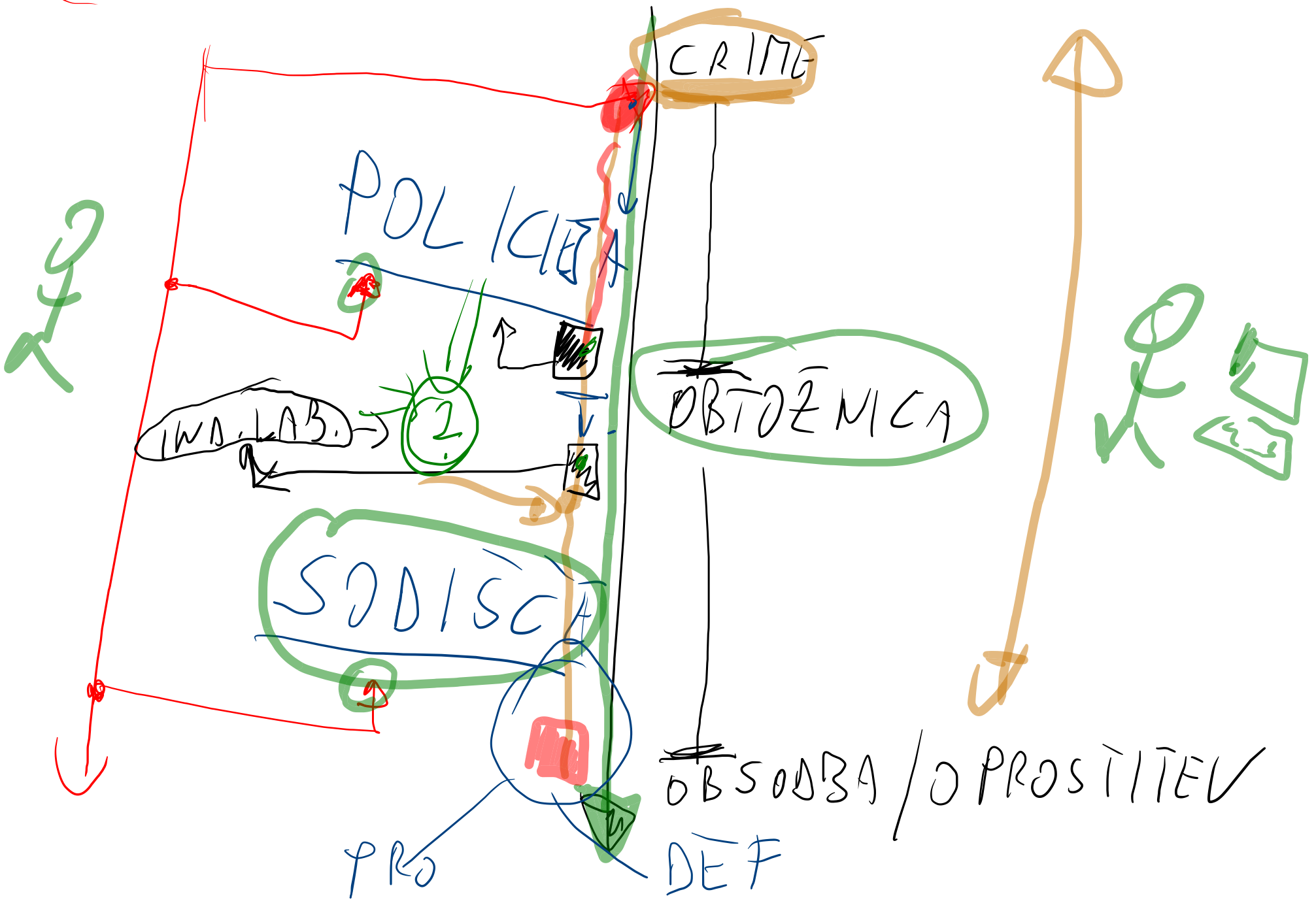
Digitalna forenzika

Andrej Brodnik

forenzika

time



Razvoj jezika raziskave računalniških zločinov

poglavje 2

- na začetku ni bilo računalnikov in zakon je ščitil samo materialne dokaze
- digitalni dokazi vključujejo:
  - računalniška (datotečna) forenzika
  - omrežna forenzika
  - mobilna forenzika
  - slabogramje (*malware*) forenzika
- pomembna razlika med preiskovanjem in analizo podatkov
  - preiskovanje vključuje zajem, organizacijo, ...
  - analiza predstavlja dejansko obravnavo dokazov

Vloga računalnika

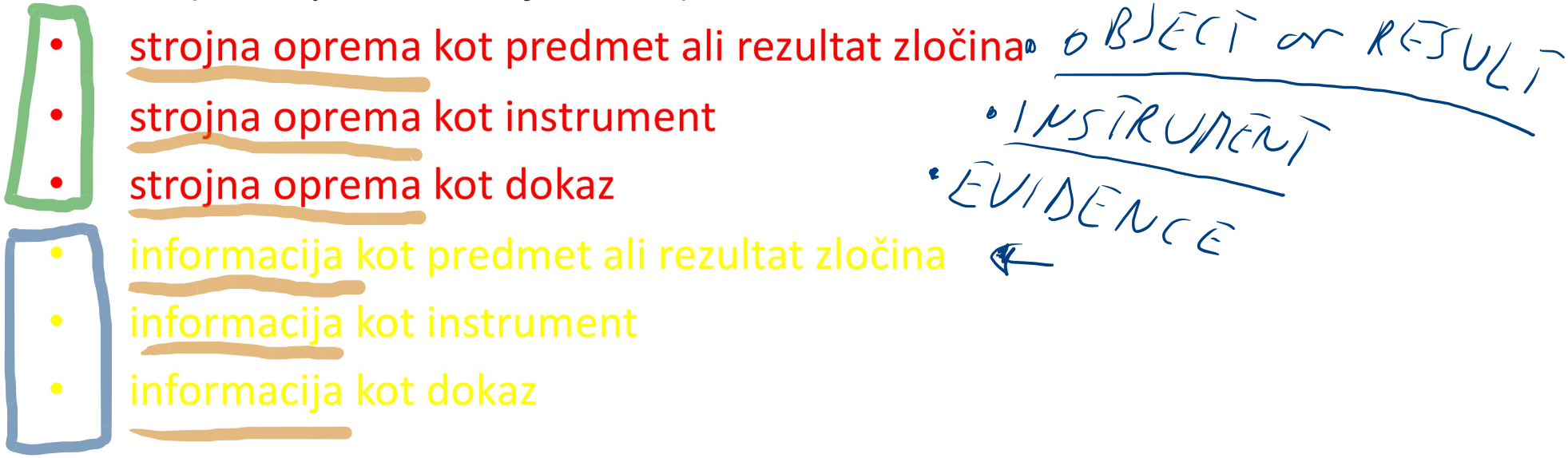
Po Parkerju, 1976, 1983, 1998:

1. predmet (objekt) zločina
   - kraja računalnika ali uničenje
2. osebek (subjekt) zločina – zločin je bil narejen nad računalnikom
   - okužba računalnika
3. orodje za pripravo in/ali izvedbo zločina
   - kopiranje dokumentov
4. uporaba po svojih lastnostih v zločinu (*symbol*)
   - ponujanje storitev ali zmožnosti računalniških storitev: dobitki na borzi, ...
- vir podatkov(!!) – ostanki datotek, e-pošte, ...

Vloga računalnika

USDOJ (*US Department of Justice*), 1994, 1998:

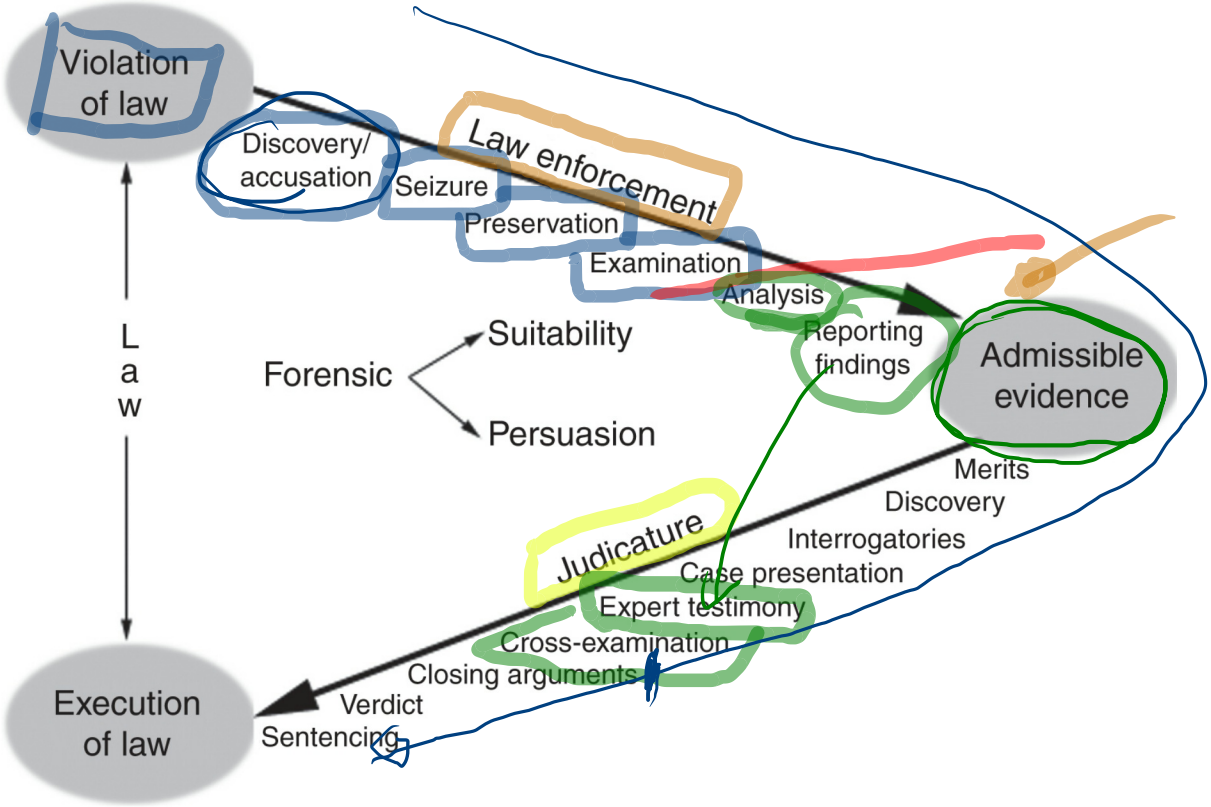
- strojna oprema kot predmet ali rezultat zločina
- strojna oprema kot instrument
- strojna oprema kot dokaz
- informacija kot predmet ali rezultat zločina
- informacija kot instrument
- informacija kot dokaz



Digitalni dokaz na sodišču

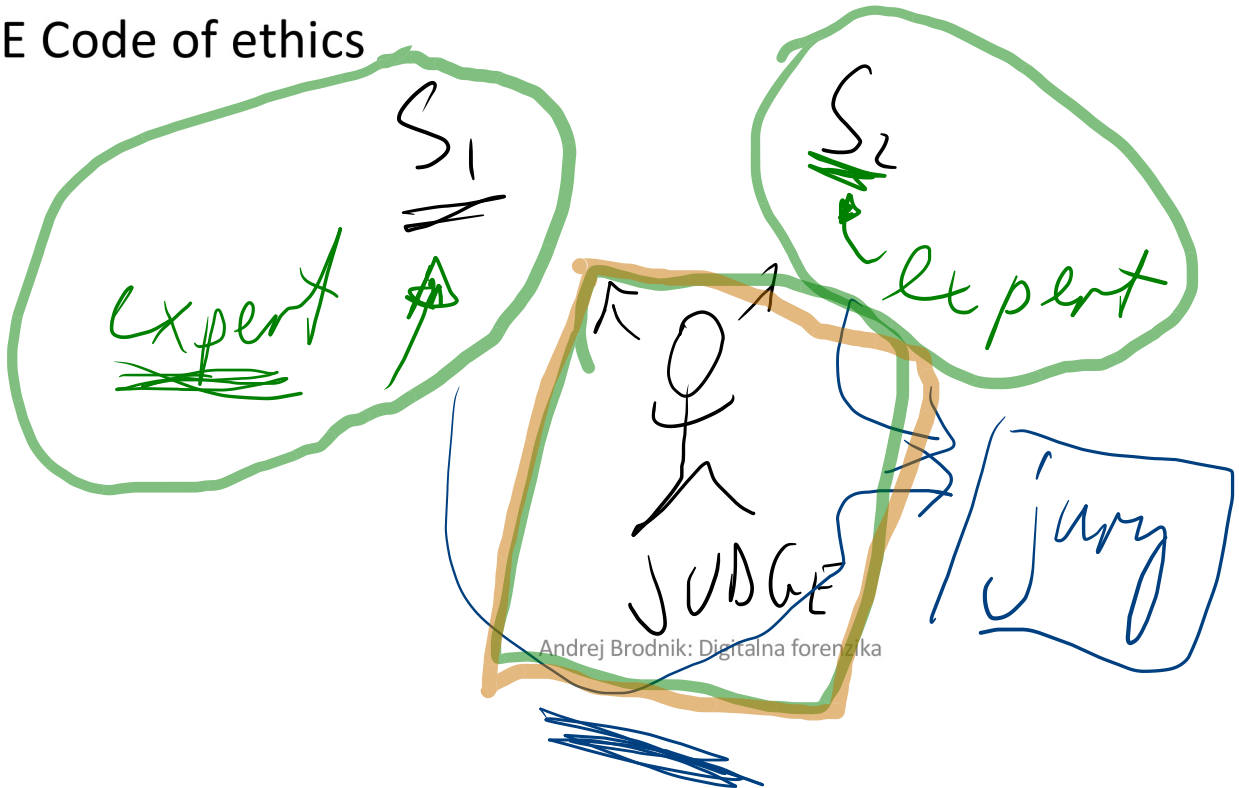
poglavje 3

digitalni dokaz na sodišču



Naloge izvedenca

- predstavitev dokaznega gradiva:
  - ne podleči vplivom
  - odklanjati prezgodaj postavljanje teorije
  - raba znanstvene resnice za potrebe pravnega procesa
- ACM Code of ethics
- IEEE Code of ethics



Sprejemljivost gradiva

- pet osnovnih pravil:
  1. relevantnost gradiva za primer → RELEVANCE
  2. avtentičnost gradiva *(zajem, sledljivost, ...)* → AUTHENTICITY
  3. niso govorice *(dokaz sam niso govorice, če ni govorec prisoten)* HEAR-SAY
  4. najboljši možen dokaz *(original in kopija)* → BEST POSSIBLE
  5. dokazno gradivo brez potrebe ne napeljuje na zaključke
- nalog za preiskavo

LEAD TO CONCLUSION

Stopnje zanesljivosti

- v beležkah imamo zapis:

```
2009-04-03 02:28:10 W3SVC1 10.10.10.50 GET
  /images/snakeoil13.jpg-80-192.168.1.1
  Mozilla/4.0+(compatible;+MSIE+6.0;Windows+NT+5.1) 200
  0 0
```

- kaj sklepamo iz njega?
- stopnje zanesljivosti:
  - (1) skoraj zagotovo; (2) zelo verjetno; (3) verjetno; (4) zelo možno; (5) možno
  - statistična verjetnost

Računalniška zakonodaja

poglavje 4

- zakonodaja ZDA
  - 50 zakonodaj
  - zakonodaja Washingon DC
  - zvezna zakonodaja

Računalniška zakonodaja

poglavje 5

- zakonodaja ES (*EU*)
  - Irska (in Velika Britanija) ločen sistem – *common law*
  - preostale države – *civil law*
- skupna zakonodaja:
  - parlament EU
  - Konvencija o računalniških zločinih (*Convention on Cybercrime*), 1. julij 2004
    - nista ratificirali Irska (in Velika Britanija)
  - Protokol o dejanjih rasizma in ksenofobije, 1. marec 2006
  - GDPR, 2019

Zločini nad integriteto računalnika

- Dostop do računalnika ni dovoljen, če nam tega ne dovoli lastnik
- Primeri:
  - hekerji
  - kraja podatkov
  - prestrezanje podatkov
  - vplivanje na podatke in/ali sisteme (DOS, virusi)
  - ››napačna‹‹ ali nenamenska uporaba enote/naprave

Zločini s pomočjo računalnika

- ponarejanje
- goljufija
- zloraba

Zločini povezani z vsebino podatkov

- Zločini, ki zadevajo vsebino podatkov
  - otroška pornografija
  - spletno zapeljevanje
  - rasizem in ksenofobija

Ostali zločini

- kršenje avtorskih pravic
- računalniško izsiljevanje
- …