INSIG2
INTEGRIRANA SIGURNOST

Digitalna forenzika
DA ili NE?

Goran Oparnica, dipl. ing.
direktor

Rovinj, 17. listopada 2012. godine

Sadržaj

- Što je to digitalna forenzika?
- Javni vs. Privatni sektor
- Primjeri iz prakse
- DF u korporativnom okruženju
  - Organizacijski aspekti
  - Pravni aspekti
  - Tehnički aspekti

Digitalna forenzika

- **Forensis [lat.] -> “pred forumom”**
  - Danas: “pred sudom”
- **Digitalna forenzika “u forenzičkom smislu”**
  - Tehničko rješenje pravnog problema
  - Javni sektor (tzv. *law enforcement* institucije)
- **Digitalna forenzika “u ne-forenzičkom smislu”**
  - Vrlo široko područje primjene
  - Privatni (*enterprise*, realni) sektor

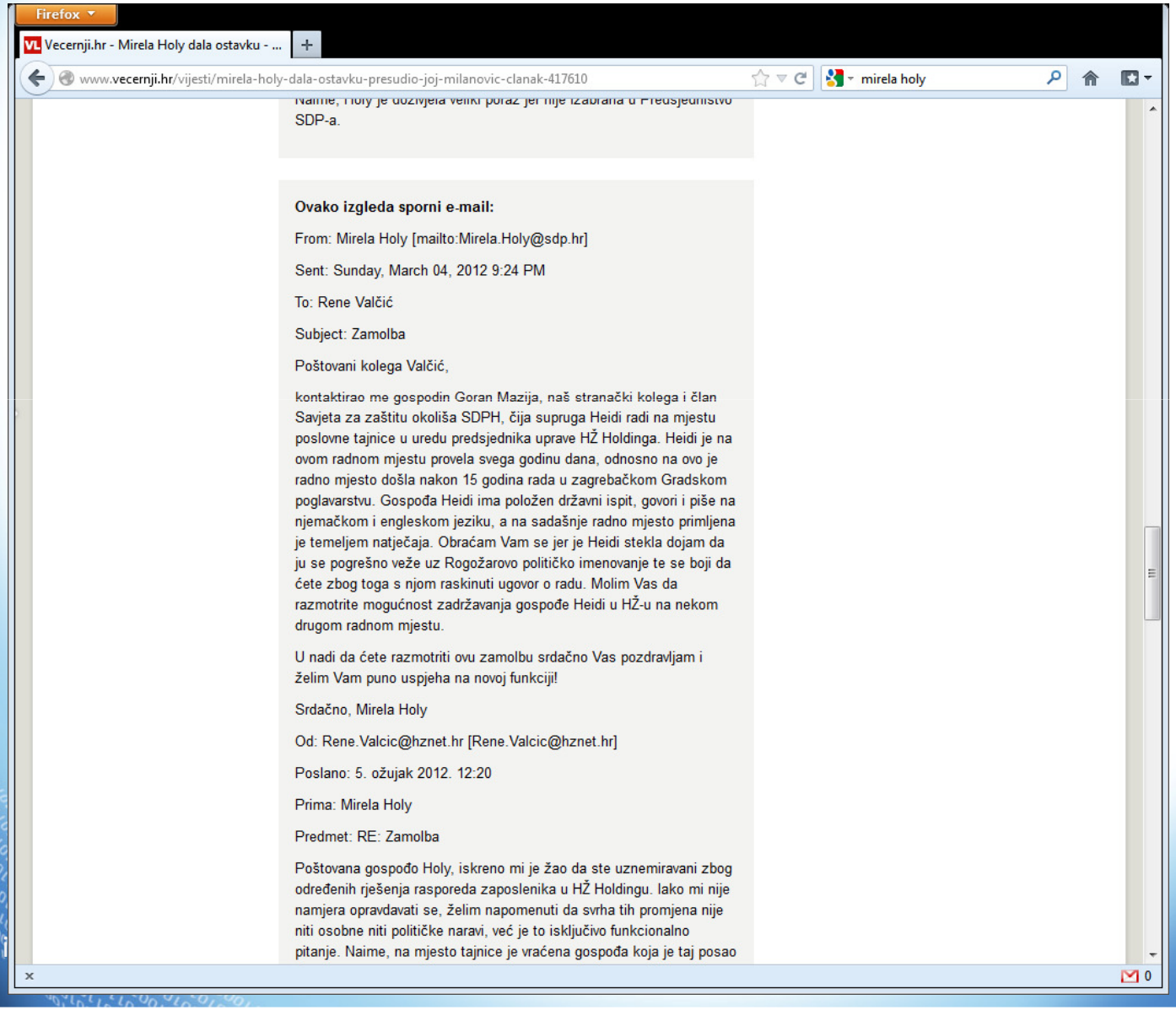
Nekoliko činjenica

- **Forenzika – sastavni dio šire istrage**
- **Koji je cilj istrage?**
  - Otkriti i/ili spriječiti neželjenu akciju
  - Pokrenuti postupak pred sudom?!
- **Poštivanje pravne procedure**
  - Radi priznavanja dokaza pred sudom
  - Radi poštovanja ljudskih prava i zaštite privatnosti
- **Poštivanje tehnološke procedure**
  - Principi digitalne forenzike
  - Metodologija digitalne forenzike

Enterprise sektor

- **Da li nam uistinu treba digitalna forenzika?!**
  - Organizacijski aspekti
  - Pravni aspekti
  - Tehnološki aspekti

Primjer iz prakse



Primjer iz prakse

- **Virginia prescription monitoring program home web page**
  - "I have your shit! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh :(For $10 million, I will gladly send along the password.„
- **Utvrđeno:**
  - Podaci su zaista obrisani, stoga je i postojao napad
  - DF nije pronašla tragove downloada podataka
- **Ništa se nije dogodilo**

Enterprise sektor

- **Da li nam uistinu treba digitalna forenzika?!**
  - Organizacijski aspekti
  - Pravni aspekti
  - Tehnološki aspekti
- **DA!**
  - Za interne istrage (IP theft, industrijska špijunaža i sl.)
  - Za IT sigurnost u širem smislu
    - Incident response

Organizacijski aspekti

- **Nadzor zaposlenika u realnom vremenu?**
  - Etički, pravni, kulturni, org, tech i sl. aspekti
- **Uspostaviti organizaciju za DF**
  - Tko će vršiti istragu?
  - Kojima alatima?
  - Kojim procedurama?
  - In-house ili outsourcing istrage?
- **Tko zna da je istraga u toku?**
- **Što sa rezultatima istrage?**
  - Što s irelevantnim podacima?
- **Definirati pravni okvir za istragu**

Pravni aspekti

- **Europska konvencija o ljudskim pravima:**
  - Article 8 / § 1: Everyone has the right to respect for his private and family life, his home and his correspondence.
- **Europski sud za ljudska prava:**
  - Halford vs. UK (1997)
    - Court decision: The applicant (Mrs. Halford was Assistant Chief Constable with the Merseyside police) in the present case had been given no warning that her calls would be liable to monitoring, therefore, according to the Court, she had a reasonable expectation as to the privacy of calls made from her work telephone.
  - Copland vs. UK (2007)
    - Court decision: the Court considers that the collection and storage of personal information relating to the applicant's telephone (Mrs. Copland worked in Carmarthenshire College, a statutory body administered by the State), as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8 of European Convention on Human Rights.

Pravni aspekti

Pravno zaposlenika na privatnost

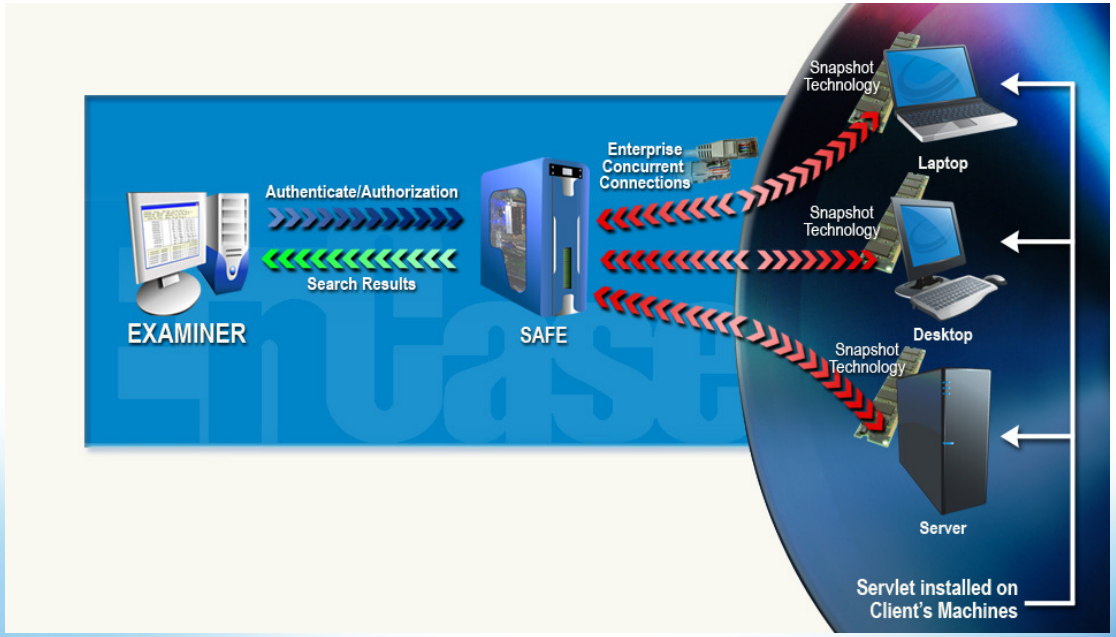
vs.

Pravo poslodavca na zaštitu IP

Sukob dva ustavna prava

Tehnički aspekti

- **Tradicionalna DF istraga**
  - Odredi odredišne uređaje
  - Bit stream image medija (RAM + disk)
  - Pokušaj naći ono što želiš (dugotrajan proces)
- **DF istrage putem mreže**



Tehnički aspekti

- **Mrežna DF infrastruktura**
  - Osnova za učinkoviti incident response

Usporedba unaprijed definiranih profila računala

… daljnje filtriranje sa poznatim izvršnim kodom

Uzimanje kopije sumnjivog koda iz memorije

… te analiza što kod stvarno može napraviti

Zaključak

- **Digitalna forenzika – definitivno DA**
- **Interne istrage**
  - IP theft, curenje informacija, ind. špijunaža i sl.
- **Incident response**
  - Utvrditi incident, trijaža, kontroliranje, oporavak
- **Preduvjeti**
  - Pravni
  - Organizacijski
  - Tehnički

Pitanja