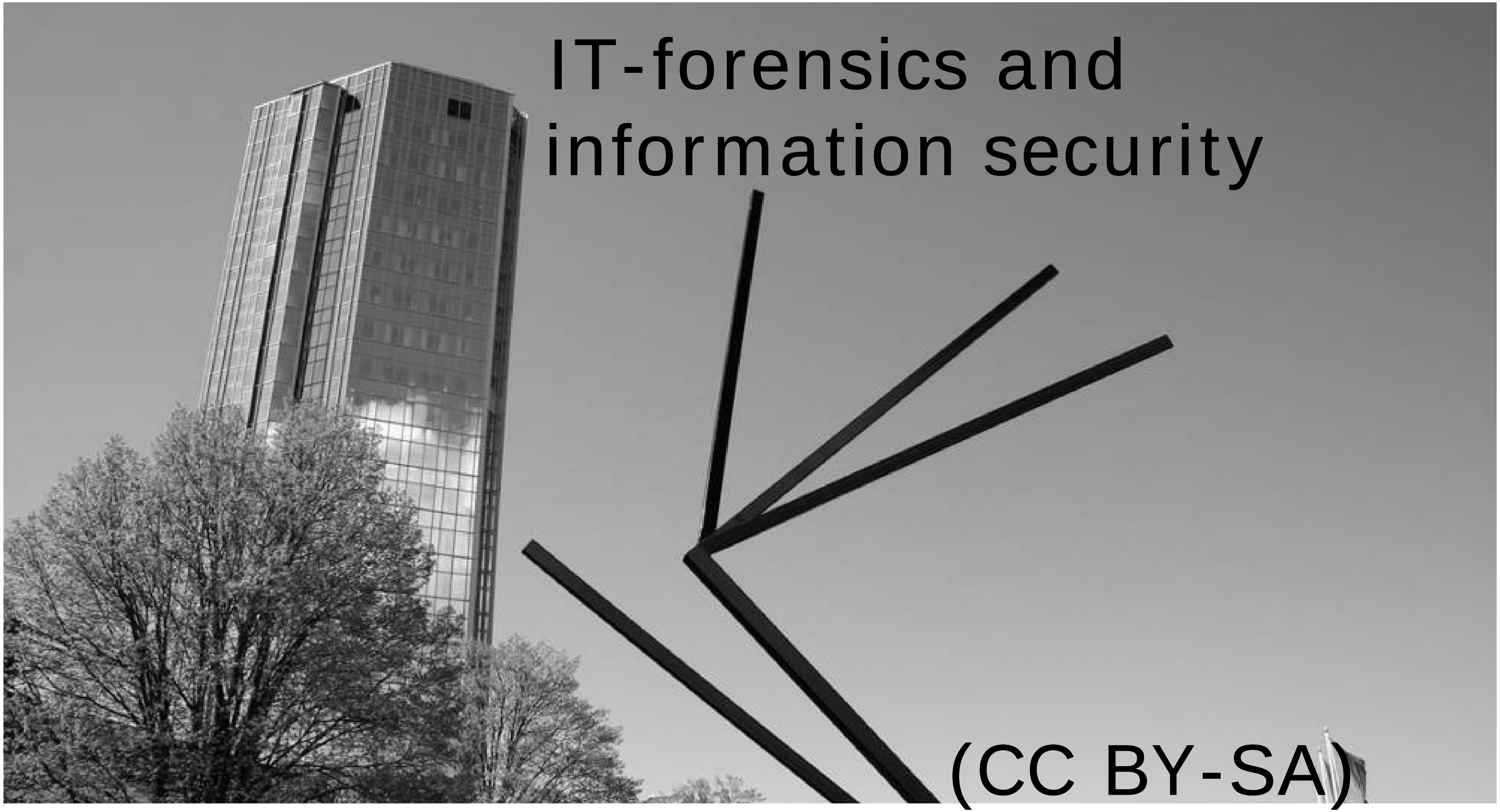


IT-forensics and information security

(CC BY-SA)

För utveckling av verksamhet, produkter och livskvalitet.

Locards kontamineringsprincip

Locards kontamineringsprincip

Locards kontamineringsprincip

Exempel

- Du träffar på en påslagen dator.
  - Ska du ta med den påslagen?
  - Ska du stänga ner den via operativsystemet?

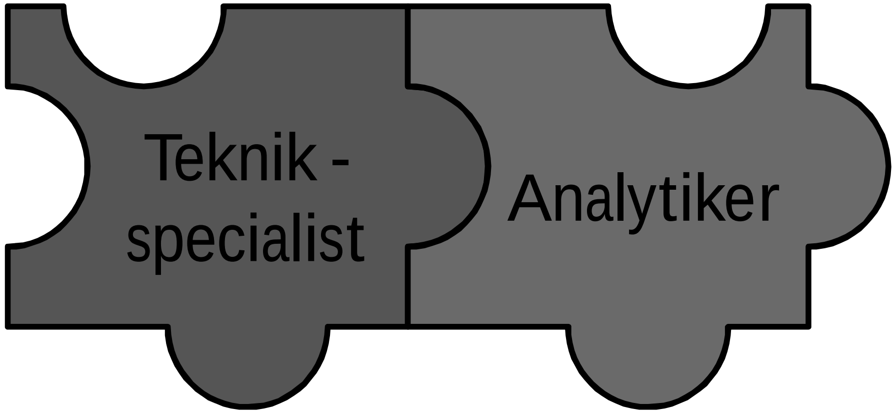
- Båda metoderna kontaminerar.

IT-forensikern

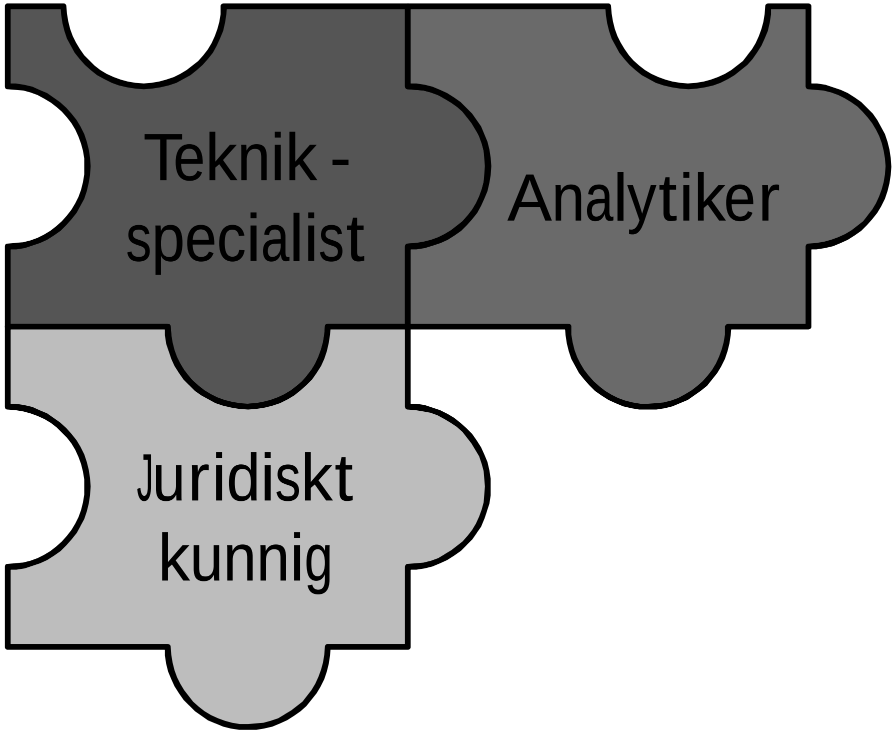
IT-forensikern

Teknik -
specialist

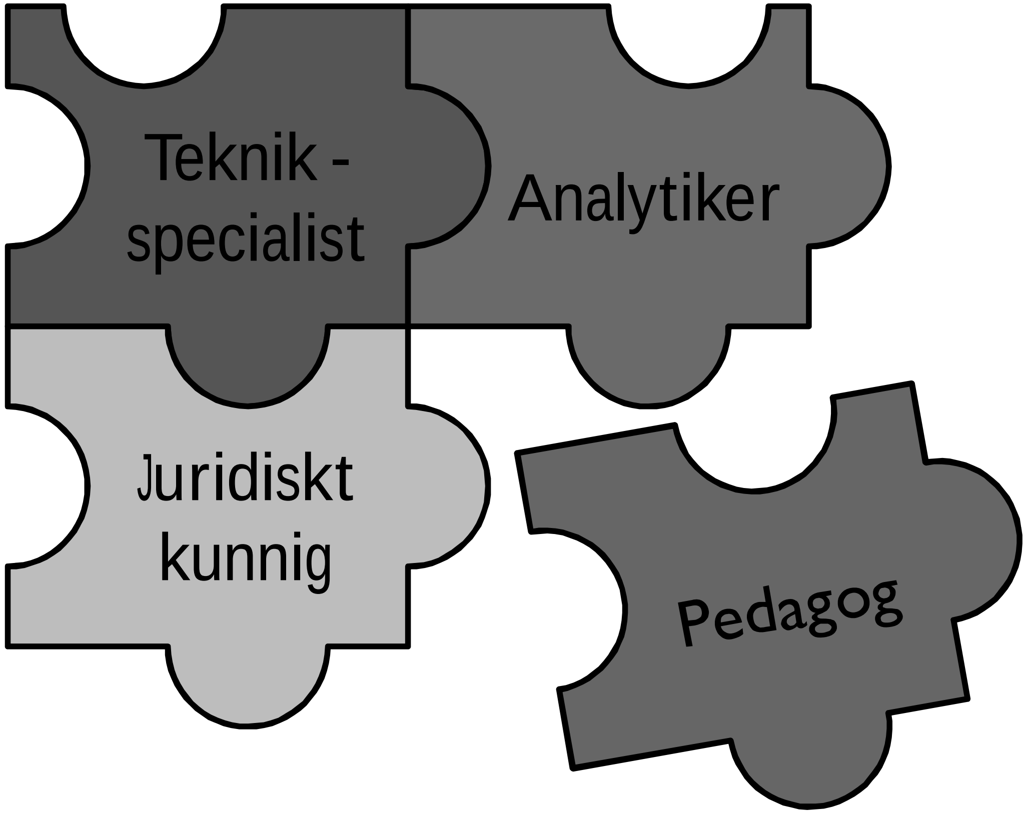
IT-forensikern



IT-forensikern



IT-forensikern


Teknik - specialist

Analytiker

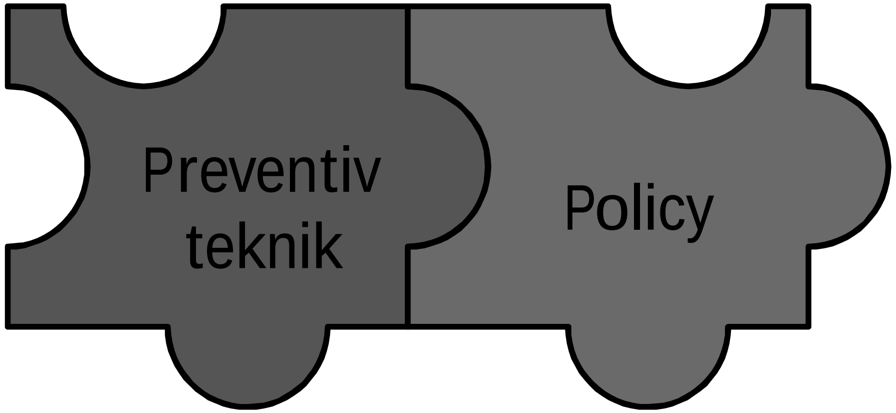
Juridiskt kunnig

Pedagog

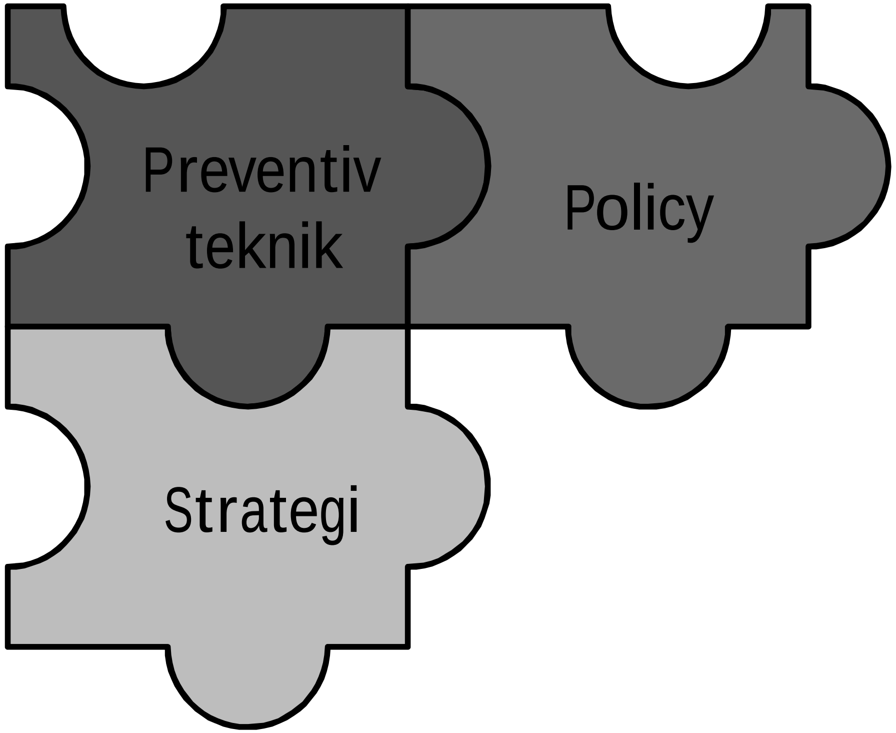
IT-forensiska uppdrag

IT-forensiska uppdrag

IT-forensiska uppdrag



IT-forensiska uppdrag

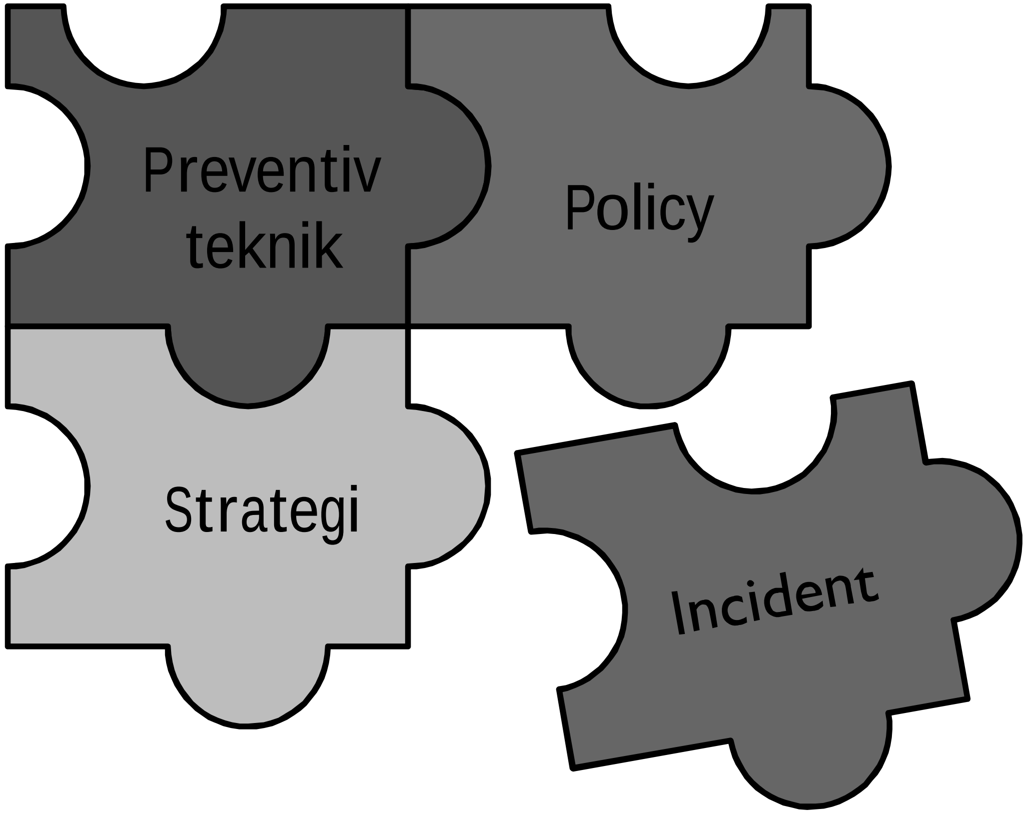


Preventiv teknik

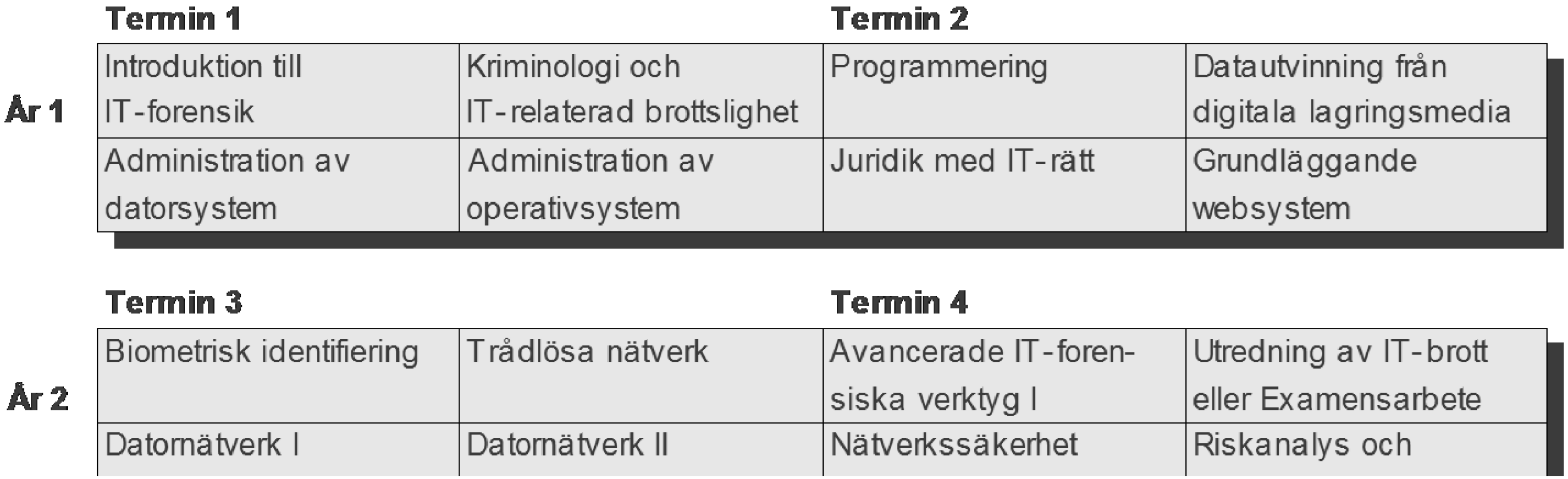
Policy

Strategi

IT-forensiska uppdrag



IT-forensik och informationssäkerhet, 120/180 hp



	Termin 1		Termin 2	
År 1	Introduktion till IT-forensik	Kriminologi och IT-relaterad brottslighet	Programmering	Datautvinning från digitala lagringsmedia
	Administration av datorsystem	Administration av operativsystem	Juridik med IT-rätt	Grundläggande websystem
	Termin 3		Termin 4	
År 2	Biometrisk identifiering	Trådlösa nätverk	Avancerade IT-forensiska verktyg I	Utredning av IT-brott eller Examensarbete
	Datornätverk I	Datornätverk II	Nätverkssäkerhet	Riskanalys och

Methods

- Blended learning
- Flipped classroom
- Peer interaction
- Hands on, lab intensive

Administration of Computer Systems

- Computer fundamentals
  - Computer components
  - Installing OS
  - Configuring/ hardening
  - Troubleshooting
- Based on ”Cisco IT Essentials”
- Practical test
- Report
- Presentation

Administration of Operating Systems

- Linux fundamentals
- Set up a typical linux environment, LAMP, mail server, DNS
- Practical test

Digital Storage Data Extraction

- Basics of evidence handling
- Basics of data extraction from different media types
- Understanding of how to prevent data extraction
- Understanding of limitations
- Capability to make ”back of the envelope” calculations

Advanced IT-Forensic Tools 1

- How to work with typical IT-forensic suites
  - Data extraction
  - Search, Mining, Recover, Windows specifics...
- Focus on EnCase / EnCE certification
- Practical hands on ”live” case with role play
  - Student selling exam drafts
  - Missing person scenario
  - Illegal surveilance

Advanced IT-Forensic Tools 2

- Focus on embedded systems
  - How to hack a modern car
  - Border scan protocol (JTAG)
  - Identifying data manipulation
  - Data extraction & mining
- Seminars, reading scientific papers
- Paper
- Workshop/ mini conference

Advanced IT-Forensic Tools 3

- Project based training
- Standard cases
- Two teams, alternating red/blue operation
  - Create a case
  - Swap cases
  - Try to analyze
  - Report
- Increasing difficulty

SCADA

- Industrial systems
- Embedded systems
- Security/ safety/ reliability
- Real hands on project, risk analysis, modelling the problem, creating a solution, reporting.
  - Water supply/ waste water handeling/ water power plant
  - Note: half a year after the students analyzed risks with water supply there was a major lye discharge in the drinking water system.

Thesis work

- 20 weeks – C level
- 10 weeks – B level

Optimizing using Triage

(CC BY 2.0) U.S. Army

OSS vs. proprietary solutions

Copy left.

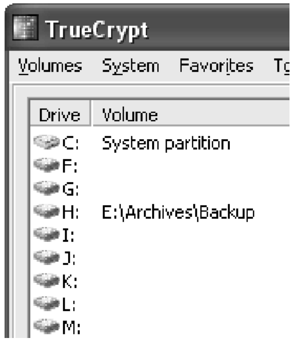
Copy right.

Portabel UPS

RAM contamination during data extraction

(CC BY-SA 2.0) Daniel Dionne

Identification of TrueCrypt-containers



Drive	Volume
C:	System partition
F:	
G:	
H:	E:\Archives\Backup
I:	
J:	
K:	
L:	
M:	

Wardriving

- Mapping of three major cities
- Focus on the WPS bug (121231)
- Image not related

Pen-test of medium sized ISP

Collaboration

- Program comity
- Thesis topics
- Thesis supervision
- Project topics
- Guest lectures

UT-EXPO

- 30/5 - 1/6

mattias.wecksten@hh.se