

Forensic Computing



Vlasti Broucek, MSc, GradDip (IT), MACS
School of Information Systems
University of Tasmania, Australia

Vlasti.Broucek@utas.edu.au
<http://brouk.psychol.utas.edu.au/>

Program

- Definice
- Vztah mezi Forensic Computing (FC) a Computer Security (CS)
- Potřebné znalost a vědomosti
- Technické, legální a socio-politické problémy a otázky
- Expertní Systémy?

Definice

Forensic = *'used in or connected with court of law'*

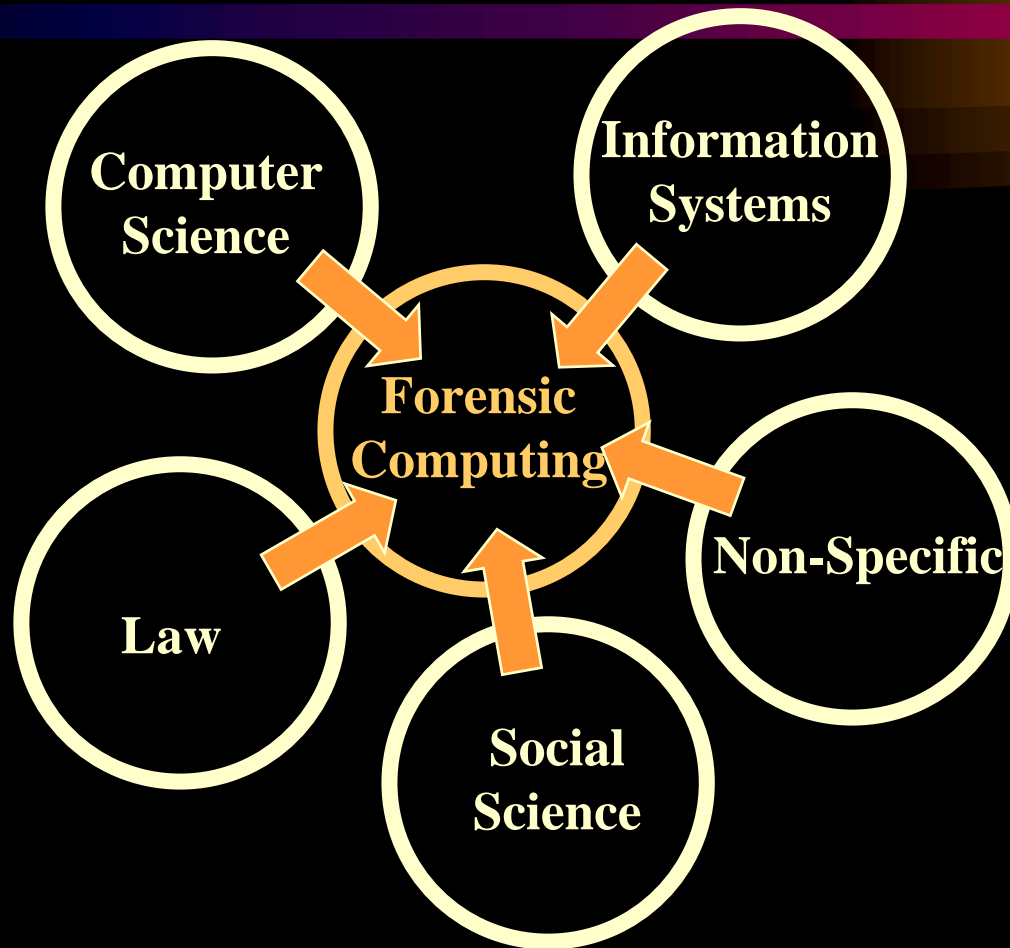
'The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable.' (McKemmish, 1999)

'Gathering and analysing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system.' (Farmer & Venema, 1999)

Definice

- Dva možné pohledy
 - technický (Farmer & Venema)
 - právní (McKemish, Sommer)
- Kde se FC uplatní
 - criminalní, ilegální a další nevhodné činnosti
- Taxonomie
 - definuje FC jako vědeckou disciplínu

Taxonomie



Vztah mezi FC a CS

- Mýt - FC je pouze jiné jméno pro CS
 - Příklad 1. - dětská pornografie
 - Příklad 2. - výhružná e-mail
- Fundamentální rozdíly
 - proč
 - kdy
 - kdo
 - pro koho

Fundamentální rozdíly

- Proč
 - CS ochraňuje systém proti napadení, zneužití atd
 - FC vyšetřuje výsledky takové činnosti
- Kdy
 - CS ideálně v reálném čase
 - FC obvykle “post mortem”

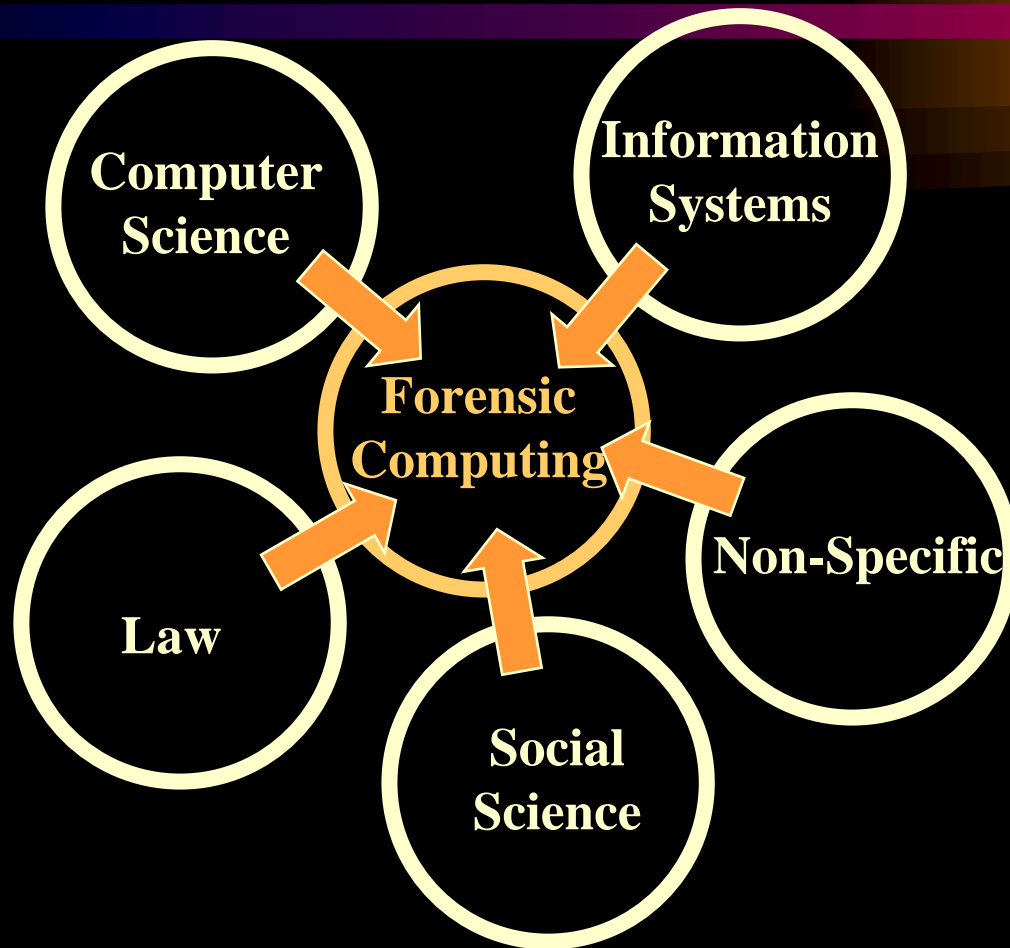
Fundamentální rozdíly

- Kdo
 - obvykle počítačový odborník
 - může být také, ale mnohdy ne
- Pro koho
 - když presentováno, tak odborníkům
 - obvykle (a hlavně v případě soudní evidence) presentováno laikům

Fundamentální rozdíly

- Fundamentální problém
 - CS systémy mohou být obejity systémovými administrátory (root v UNIX)
 - Integrita a časová následnost evidence je absolutně nezbytná v FC!!!

Taxonomie



Znalosti a vědomosti

- Počítačové systémy
 - computer security
 - operační systémy a aplikační software
 - systémové programování a programovací jazyky
- Právo
 - specializované počítačové
 - kriminální, civilní a tzv. “soft”

Znalosti a vědomosti

- Informační Systémy
 - strategický management
 - policies
 - vzdělávání uživatelů
- Sociální vědy
- A další...

Problémy

- Počítačové systémy a security
 - Technická řešení nejsou vhodná pro právní proces
 - Intrusion Detection Systems
 - rychlost, spolehlivost, legálnost...
 - Příklad: Útok na Rome Labs
 - Christy a Sommer
 - Nepřipravenost administrátorů
 - Příklad: CodeRed Worm

Problémy

- Právo
 - různé zákony
 - vhodnost electronicke evidence jako právní důkaz “per se”
 - rozdíl mezi vědeckým důkazem a právním důkazem
 - přípustnost
 - váha

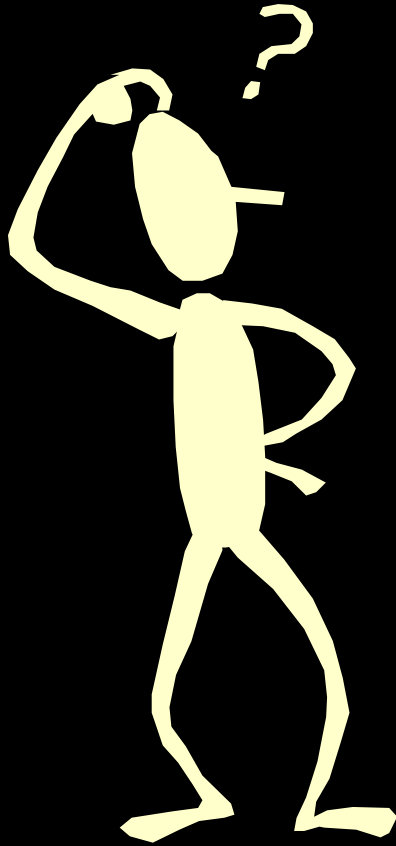
Problémy

- Informační systémy
 - rozhodnutí managementu
 - “pull the plug?”: Mitnick versus Microsoft koncem 2000
 - policies
 - výchova uživatelů
 - Příklad: používání “volných e-mail systémů”
 - Příklad: e-mail a virusy, falešné virusy (hoaxy)

Problémy

- Sociální vědy
 - ochrana soukromí
 - PGP, KeyEscrow, Carnivore
 - European Convention on CyberCrime 2001
 - Příklad: ruský špión v USA
 - Neobvyklé formy obhajoby
 - Příklad: Kelman (UK, hacking addiction)

FC a Expertní Systémy



- Vhodnost?
- Jak a kde?
 - vyšetřovatel
 - soudní expert
- Problémy
 - různé jurisdictions
 - různé systémy (UNIX, MS)