

Open Source IT Forensics

avagy

Nyílt forráskódú programok felhasználása
az informatikai igazságügyi szakértésben



Illési Zsolt, CISA, CISM,
informatikai igazságügyi szakértő
a ZMNE doktorandusza
illesi.zsolt@proteus.hu

Témák

- Számítógépek igazságügyi szakértői vizsgálatának szükségessége
- Nyílt forráskódú programok és vizsgálati módszerek
- Merre tovább?



Számítógép és bűnözés

A számítógép lehet:

- célpont
- megvalósítási/ elkövetési tárgy/környezet
- elkövetést/ megvalósítást megkönnyítő eszköz
- elkövetés szimbóluma
- elkövetés „tanúja”



Általános krimináltechnikai alapelvek

- **Locard Exchange Principle:** minden érintkezés nyomot hagy → „digitális” nyom
- **Occam borotvája:** valamennyi bizonyíték alapján a legegyszerűbb magyarázat a legvalószínűbb
- **Daubert kritériumok:** gyakorlatban is ellenőrzött (tesztelt) elmélet, előzetes bírálat alapján tudományban elismert módon publikált, ismert hibaarány, a szakemberek tekintélyes közössége által elismert



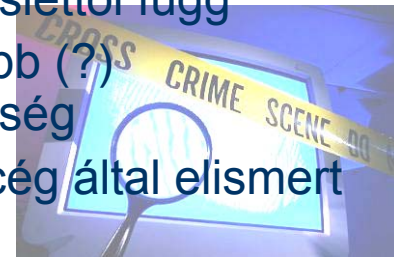
„Nyílt” vs „zárt”

- „Nyílt” rendszerek

- forráskód megismerhető (fehér doboz)
- hibái „ismertek”
- funkciók több programban, esetleg hiányosak
- fejlesztés esetleges (de rendszerint stabil)
- bonyolultabb (?) kezelhetőség
- fejlesztői közösség által elismert
- forráskód/funkció szabadon módosítható

- „Zárt” rendszerek

- forráskód nem megismerhető (fekete doboz)
- hibák „marketingje” ismert
- funkciók ~zártak (egy-egy problémakörre)
- fejlesztés a fizetőképes piaci kereslettől függ
- egyszerűbb (?) kezelhetőség
- fejlesztő cég által elismert
- forráskód/funkció nem módosítható



Nyílt „forráskódú” vizsgálati módszerek

- Ajánlások
 - U.S. Department of Justice: Forensics Examination of Digital Evidence: A guide for Law Enforcement (2004. április)
- Sourceforge.net: Open Source Computer Forensics Manual (2003.07.15)
- <http://www.opensourceforensics.org/>
 - eszközök (windos és linux)
 - eljárások
 - teszt/példa
 - kutatási dokumentumok



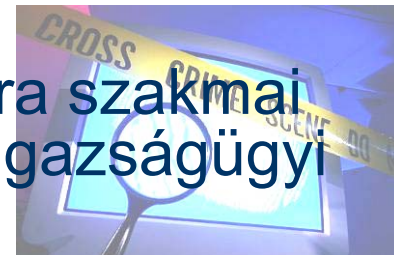
Nyílt forráskódú rendszer: Helix₃

- Live (Knoppix) Linux CD (2008.09.15)
- Releváns segédprogramok gyűjteménye (windows és linux)
- felhasználói kézikönyv (2006.03.07)



A magyar valóság

- Nincs protokoll az alábbi területekre
 - digitális nyomrögzítés
 - rögzített adatnyom kezelés
 - informatikai eszköz és adatnyom elemzés/értékelés
- Nincs bevált és széles körben alkalmazott vizsgálati „szoftver park”
- Nincs pénz, paripa fegyver...
- A bírósági ítéletek nem kutathatók
- De! 2008: Igazságügyi Szakértői Kamara szakmai kezdeményezésre az első informatikai igazságügyi szeminárium



Összefoglalás

A nyílt forráskódú eszközök

- alkalmasak krimináltechnikai vizsgálatok lefolytatására
- ~teljesítik a Daubert kritériumokat (a zárt kódúak nem)
- továbbfejlesztése, hazai adoptációja és széleskörű (jogalkotó, jogalkalmazó, szakértő) szakmai kooperáció szükséges
 - a jogalkotó, jogalkalmazó (hatóság/bíróság), szakértők
 - értelmezésének (mi a probléma, mit kell kérdezni, milyen formában kell válaszolni stb.)
 - gyakorlatának egységesítéséhez
 - funkcionalitás és kezelhetőség javítása érdekében
 - eljárási, módszertani ajánlások (pl. hazai és EU jog) kidolgozására

Az ítéleteket jutathatóvá kell tenni

