FEL ČVUT

Forenzní analyzátor pro operativní analýzu

Róbert Lórencz, Tomáš Zahradnický, Jiří Buček

19. května 2008

Základní pojmy

Forenzní analýzou myslíme užití vědecky odvozených metod ke sběru, zhodnocení, identifikaci, analýze, interpretaci, dokumentaci a prezentaci digitálních důkazů ze zdrojů digitálních dat s cílem rekonstrukce událostí shledaných zločinnými nebo k odhalení neautorizovaných akcí, které působí rušivě na plánovaný běh operací.

Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.

Proces forenzní analýzy

1. **Zajištění objektů dat ke zkoumání**

   Zajištěné objekty jsou odborně zduplikovány a originály uloženy a zapečetěny.

2. **Analýza objektů dat ke zkoumání**

   Fáze zkoumání a shromažďování digitálních stop prováděná buď soudním znalcem, anebo kriminalistickým expertem, obojí v součinnosti s vyšetřovatelem.

3. **Report — výstup požadovaných informací**

   Report obsahuje soupis digitálních stop, které jsou relevantní k případu, a které soudní znalec zahrne do svého posudku.

Kdo provádí forenzní analýzu

soudní znalec — jmenován MSp ČR, expertní osoba, poskytuje výstup forenzní analýzy — znalecký posudek.

- znalců je nedostatek

kriminalistický expert — vysoce vyškolená osoba, která je s to pracovat s forenzními analyzátory.

- expertů je nedostatek
- velmi nákladné školit další experty

⇒ Znalců i expertů je nedostatek, a proto je potřeba, aby mohl počáteční analýzu provádět přímo vyšetřovatel, nebo jím pověřená osoba.

Forenzní analyzátory

- Hardwarové
  - \+ získávání dat z HDD na analogové úrovni
  - \+ zkoumání roztříštěných CD/DVD a zničených médií
  - – vysoce nákladné a časově náročné
  - – vyžadují vysoce vyškolený personál
- Softwarové
  - \+ získávání dat na softwarové úrovni
  - \+ není zdaleka tak nákladné
  - – vyžadují vysoce vyškolený personál?

  enCase Forensic Edition
  iLook Investigator
  Autopsy/SleuthKit

Jak probíhá operativní analýza

1. Operativec pracuje na kopii dat
   - ta může mít formu CD/DVD, disk image, fyzického disku, nebo být na síti
   - obdrží ji od znalce nebo experta
   - dostane k ní hash originálních dat

   $\Rightarrow$ není nutné chránit proti zápisu

2. S daty se provede:
   - vyhledání relevantních souborů (digitálních stop)
   - sestavení reportu, který obsahuje
     - jména souborů a jejich umístění
     - hashe souborů
     - datum, atd.
3. Předání znalci k sestavení posudku

- Otevřený zdrojový kód
- Spustitelné CD (Linux), ale i možnost spustit z CD (Windows)
- V češtině
- Minimum interakce s příkazovou řádkou
- Automatická filtrace uživatelských souborů
- Vyhledávaní v souborech určitého typu podle klíčových slov
- Prohledávaní archivů (poštovní DBX/PST)
- Vykopírování vybraných souborů na paměťové médium
- Sestavuje zprávu (report)
- Analýza smazaných souborů

Forma OFA v češtině

- Nutnost vyloučit vliv

  software nainstalovaného v počítači
  počítačové sítě

  $\Rightarrow$ Linuxové bootovací CD (Knoppix)
  $\Rightarrow$ Windows aplikace spustitelná z CD

- Qt 4.4
- Pro low level technologie COM bez vazeb na Qt
- Sada prohlížečů

- Vše česky!

Automatická filtrace a vyhledávaní v souborech

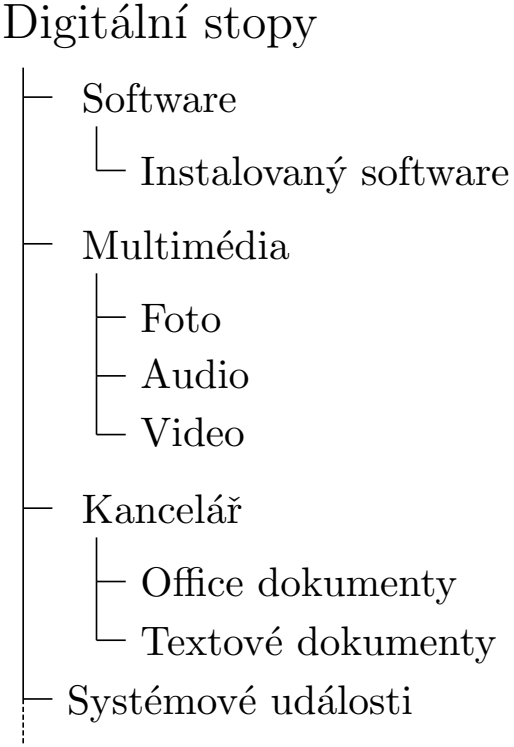
Hledat lze:

- v adresářové struktuře
- ve stromu digitálních stop

A to podle (i současně):

- koncovky
- skutečného typu souboru
- obsahu souboru
- dalších atributů (velikost, datum, . . .)

Strom digitálních stop



Prohledávaní archivů a pošty

- Archivy se tváří jako složky
- Vyžadují scratch space pro rozbalení:
  - ramdisk
  - externí paměťové médium

- Poštovní soubory (nejčastěji Outlook DBX/PST) lze chápat jako archivy a zařadit poštu do stromu digitálních stop.

Prohlížení souborů

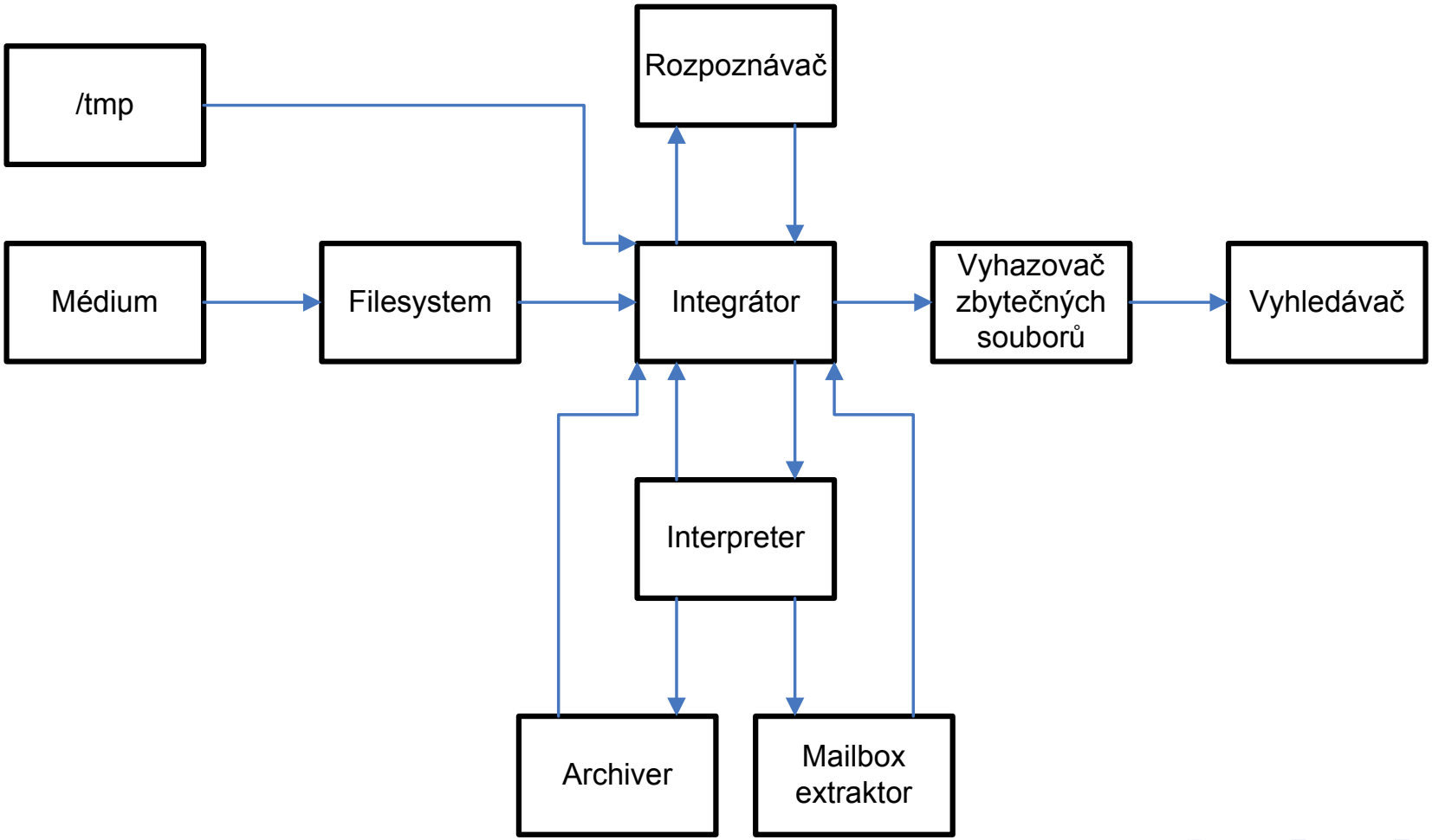
- Požadavek na velké množství formátů souborů
- Použití Open Source projektů
  - GhostScript
  - MPlayer
  - OpenOffice?
- Různá složitost implementace
  - Bitmapy – jednoduché (libjpeg, libpng, libtiff...)
  - Vektorové obrázky – složitější (CorelDraw!?)
  - Office – může být značně složité
- Některé formáty se nepodaří prohlížet interně

  $\Rightarrow$ Odkaz na externí aplikaci

Vykopírování souborů a reportu na paměťové médium

- Výběr souborů lze vykopírovat na paměťové médium spolu s reportem
- Proces probíhá takto:
  1. Zvolí se disk, na který se bude exportovat
     - dojde k přimountování zvoleného disku
  2. Zvolí se mód exportu
     - jestli zachovávat adresářovou strukturu
     - anebo flat level s automatickým vyřešením možných konfliktů
  3. Zvolí se složka, do které se bude exportovat
     - proběhne export souborů
     - dojde u uložení reportu v csv/tdt
     - zvolený disk se odmountuje

Struktura FS části OFA



Závěr

- Vyvíjený OFA je určen pro nasazení v „první vlně“
- Multiplatformní aplikace
- Jednoduché ovládání, v češtině
- Open Source

Otázky a odpovědi[1]

Tomáš Zahradnický
zahradt@fel.cvut.cz

[1]Výzkum projektu „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky“ je podporován grantem Ministerstva vnitra ČR, VD20072010B13.