INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Tato inovace předmětu Analýza dat je spolufinancována Evropským sociálním fondem a Státním rozpočtem ČR, projekt č. CZ.1.07/2.2.00/28.0014, "Interdisciplinární vzdělávání v ICT s jazykovou kompetencí".

Příprava prostředí pro digitální zkoumání

Analýza dat

Bc. Filip Pávek

Ústav informatiky
Filozoficko-přírodovědecká fakulta
Slezská univerzita v Opavě

filippavek@gmail.com

2012

Obsah prezentace

Obsah prezentace

- Co je nutné připravit před zkoumáním.
- Jaký operační systém zvolit pro zkoumání (Linux, Windows, boot CD). Jaké jsou výhody a nevýhody obou OS.
- Orientace v licencích pod kterými je SW, který budeme používat, uvolňován.
- Příprava laboratorního prostředí pro zkoumání digitálního obsahu (Linux, Windows).
- Základní představení hotových forenzních prostředí (FIRE, DEFT, CAINE, atd).
- Vývoj forenzních nástrojů na českých univerzitách (Forensic Analyzer, Operativní Forenzní Analyzátor).

Čím začít?

Nejde začít zkoumat bez přípravy.

- Než začneme zkoumat digitální obsah, tak si musíme ujasnit některé důležité body.
  - Jaké použijeme nástroje pro sběr nestálých dat a pozdější analýzu?
  - U všech nástrojů je důležité znát, jak se přesně chovají - nikdy „netestujeme“ nástroj poprvé na médiu, které je předmětem zkoumání.
  - Máme v PC, na kterém budeme provádět digitální analýzu připravené prostředí pro zkoumání?
  - Co je lepší, použít OS Linux/OS Windows/Boot live CD, jako hosta pro zkoumání?

Co musíme určit na úplném začátku

Úvodní informace

- Tato prezentace si klade dva hlavní cíle.
  1. Ukázat, jak si prostředí pro zkoumání můžeme sami připravit. Pod operačním systémem Windows i Linux. Shrneme výhody i nevýhody zkoumání pod oběma OS.
  2. Stručně představit hotová prostředí umožňující zkoumání digitálních zařízení obecně, nikoliv jen PC.

- V této části nejsou popsány všechny programy, které budeme používat při zkoumání.
- Než začneme, připomeneme si významy licencí, pod kterými jsou programy uvolňovány.

Licence: Open source

- Obecně znám, jako software distribuovaný zpravidla zdarma spolu se zdrojovým kódem.
- Aby mohl být software distribuován pod touto licencí, musí splňovat 10 podmínek stanovených společností Open Source Initiative (OSI).
- Licence umožňuje zásah do zdrojového kódu, redistribuci, užití v komerčním prostředí, atd.
- Existuje několik open source licencí, např. BSD (Berkeley Software Distribution)či GNU (General Public License).
- Většina programů, které budeme používat, jsou vydány pod některou open source licencí.
- Zobrazení a zásah do zdrojového kódu, umožňují ověřit chování aplikace či skriptu, případně provedení vlastních úprav.
- Bližší informace na: http://www.opensource.org/.

Open source (dostupnost/přenosnost/optimalizace/cena)

Open source z pohledu digitální analýzy

- Open source forenzní nástroje možňují proniknutí do problematiky všem zájemcům schopným samostudia (např. v rámci přibuzného studijního programu na VŠ).
- Poskytují možnost nejen programy spouštět a testovat s různými přepínači, ale také studovat jejich zdrojový kód. Což je užitečné chceme-li vědět, jak se přesně program chová, příp. program můžeme upravit.
- Široká možnost podpory ze stran komunit (např. rady, řešení problémů, doporučení, atd).
- Nástroje lehce dostupné na Internetu.
- Přenosnost nástrojů všude tam, kam potřebujeme (doma, v práci, ve škole, u kamaráda), mezi operačními systémy.
- Cena - ocení především všichni v bodu 1.

Freeware a Free software

Freeware a Free software není totéž!

- **Free**, na začátku obou slov vede k tomu, že jsou významy obou slov zaměňovány.

Freeware

- Distribuován zpravidla bezplatně, podmínky užívání softwaru však definovány v licenční smlouvě.
- Např. bez možnosti zásahu do zdrojového kódu, pro nekomerční užití, atd. Patří mezi proprietární software.

Free software neboli Svobodný software

- Free software není o penězích, ale o „svobodě“.
- „Free speech“ neboli svobodný projev.
- Uživatel má možnost software kopírovat, distribuovat i měnit.
- Bližší informace na: http://www.gnu.org/philosophy/free-sw.cs.html.

Zkoumáme pod OS Linux

- Výborná dostupnost Linuxových distribucí: Ubuntu, Fedora, Gentoo, Mandriva, SUSE Linux, a mnooooho dalších.
- Kterou distribuci zvolíme je čistě na nás.
- Distribuce se od sebe liší např. prostředím (GUI), obsaženým softwarem (defaulní instalace), správou balíčků, atd.
- Podstatným rozdílem je i to, jak moc jsou user friendly. Pozor, Ubuntu automaticky připojuje paměti - použít write blocker.
- Z hlediska digitálního zkoumání, nás více zajímá umístění logů, programů, konfiguračních souborů, atd. (To ale až jindy u zkoumání Linuxu).

Ubuntu

- Při digitální analýze budeme pracovat s distribucí Ubuntu (k dispozici je pro zájemce i Fedora).

Zkoumáme pod OS Linux

- Před instalací distribuce, můžete Ubuntu (i jiné distribuce) vyzkoušet prostřednictvím live CD (nezapomenout nastavit bootování). Instalace distribuce je triviální.

Výhody použití Linuxu

- Podpora mnoha souborových systémů (NTFS, Ext2/3, atd).
- Linux uživateli poskytuje plnou kontrolu nad operacemi.
- Velké množství šikovných a jednoduše dostupných utilit (interprety pro různé jazyky).
- Přítomnost Loopback zařízení - umožní nám připojit vytvořené obrazy (např. hda1.img1) jako bloková zařízení (běžný disk), která můžeme následně zkoumat. Více způsobů (`mount` a přepínač `loop` nebo `losetup`).

Zkoumáme pod OS Linux

- Na základě výše uvedeného můžeme konstatovat, že Linux se jeví jako ideální operační systém pro zkoumání.
- Obsahuje vše podstatné, před zkoumaním vyžaduje minimální přípravu (specifické nástroje).

Opakování základních příkazů

- Dříve než se pustíme do digitální analýzy, připomeneme si význam základních příkazů (příp. přepínačů).
- info, man, cd, find, grep, pwd, ls, cp, mv, mkdir, rm, info, mount, dd, date, ifconfig, hostname, history, chmod, chown, ...

Zkoumáme v prostředí MS Windows

- To co představovalo výhodu u Linuxu, Windows nemá.
- V základu Windows nemá interprety pro Perl, Ruby, atd. ani mnohé šikovné programy.
- Podpora pouze několika souborových systémů (NTFS, FAT, exFAT, ReFS).
- Nepodporuje loopback zařízení pro připojení obrazů.
- Nutno před zkoumáním instalovat programy i prostředí.

Cygwin

- Neexistuje pouze jediná možnost komplilace programů (VirtualBox, VMware → virtulní stroj pod Windows).
- Oficiální stránky: http://cygwin.com/install.html.
- Umožňuje simulovat Linuxové prostředí přímo v OS Windows.
- Tím lze používat nástroje napsané pro Linux (šířené jako zdrojový kód) i v prostředí Windows.

Zkoumáme pod OS MS Windows

- Cygwin nám tak zpřístupní obrovské množství forenzních nástrojů napsaných původně pro Linux, které můžeme používat při zkoumání i v prostředí Windows.
- Cygwin vyvinul Cygnus Solutions.
- Všechny programy se instalují pomocí balíčku, které se stahují přímo z Internetu. Lze balíčky odebírat i aktualizovat.

Instalace programu Cygwin

- Z oficiálních stránek výše si stáhneme instalační soubor .exe.
- Vyberte možnost „Install from Internet“ → „Next“.
- Nastavte kořenový adresář pro Cygwin (default je C:/cygwin).
- Nastavte umístění, kam budou stažený balíčky (C:/cygwin/package).
- Kontrola volby „Direct Connection“ → „Next“.

Zkoumáme pod OS MS Windows

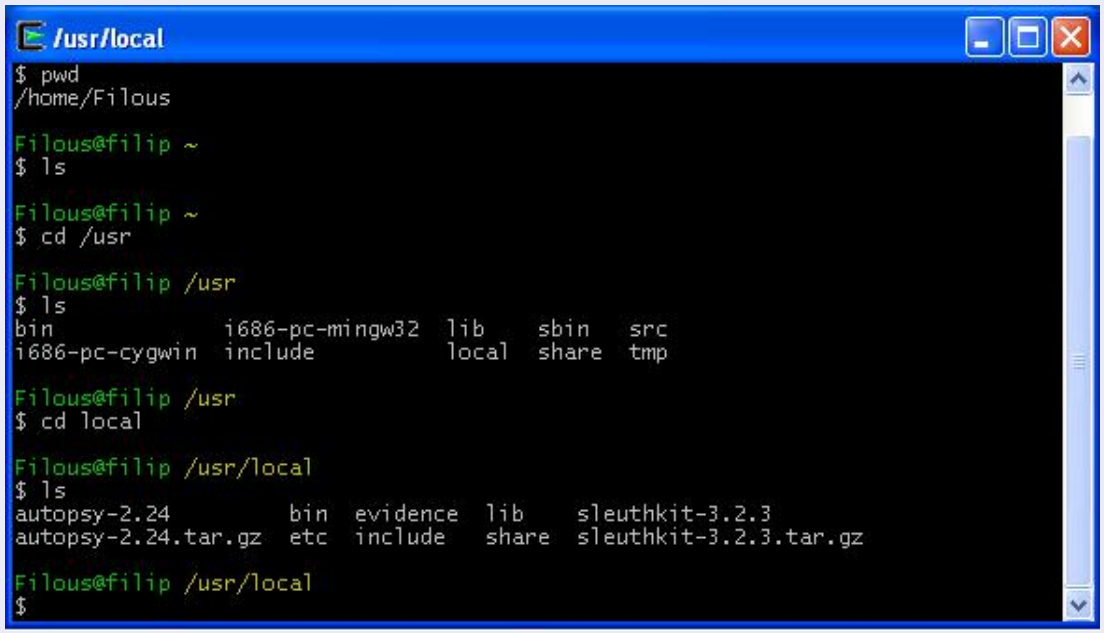
Instalace programu Cygwin

- Vyberte server pro stažení → „Next“.
- Objeví se seznam aktuálních a dostupných balíčků (některé balíčky jsou v základu již nainstalovány). Balíčky potřebujeme doinstalovat.
- Př 1: chceme-li kompilátor jazyka C klikneme na „Devel“ a vybereme „gcc:“.
- Př 1: chceme-li utilitu **make** pak ve stejném podstromě vybereme „make:“, atd.
- Potom, co jsme vybrali všechny balíčky, klikneme na „Next“ a balíčky se nainstalují. Po instalaci stačí kliknout na „Finish“ a vytvoří se zástupce na ploše.
- Hotovo → Dvojklikem na zástupce na ploše spustíme program.

Zkoumáme pod OS MS Windows

Instalace programu Cygwin

- Hotovo → Dvojklikem na zástupce na ploše spustíme Shell.
- Teď můžeme např. doinstalovávat další programy.



Zkoumáme pod OS MS Windows

Instalace balíčku

- Instalace balíčků k vytvoření plnohodnotného „Linuxového prostředí“ pro zkoumání. K instalaci použijte „Search box“.
- Seznam balíčků, které se mohou hodit na základě používání open source programů:
  - make,
  - automake,
  - cmake,
  - gcc,
  - gcc-g++,
  - python,
  - perl,
  - ruby.

Zkoumáme pod OS MS Windows

Pracujeme s obrazem

- Máme již připravené nástroje, kterými budeme získaný obraz zkoumat. Jak ale obraz souborového systému pod OS Windows připojit, abychom na něho mohli použít sílu našich nástrojů?
- Nejsme v Linuxu, takže neexistuje použití příkazu **losetup**.

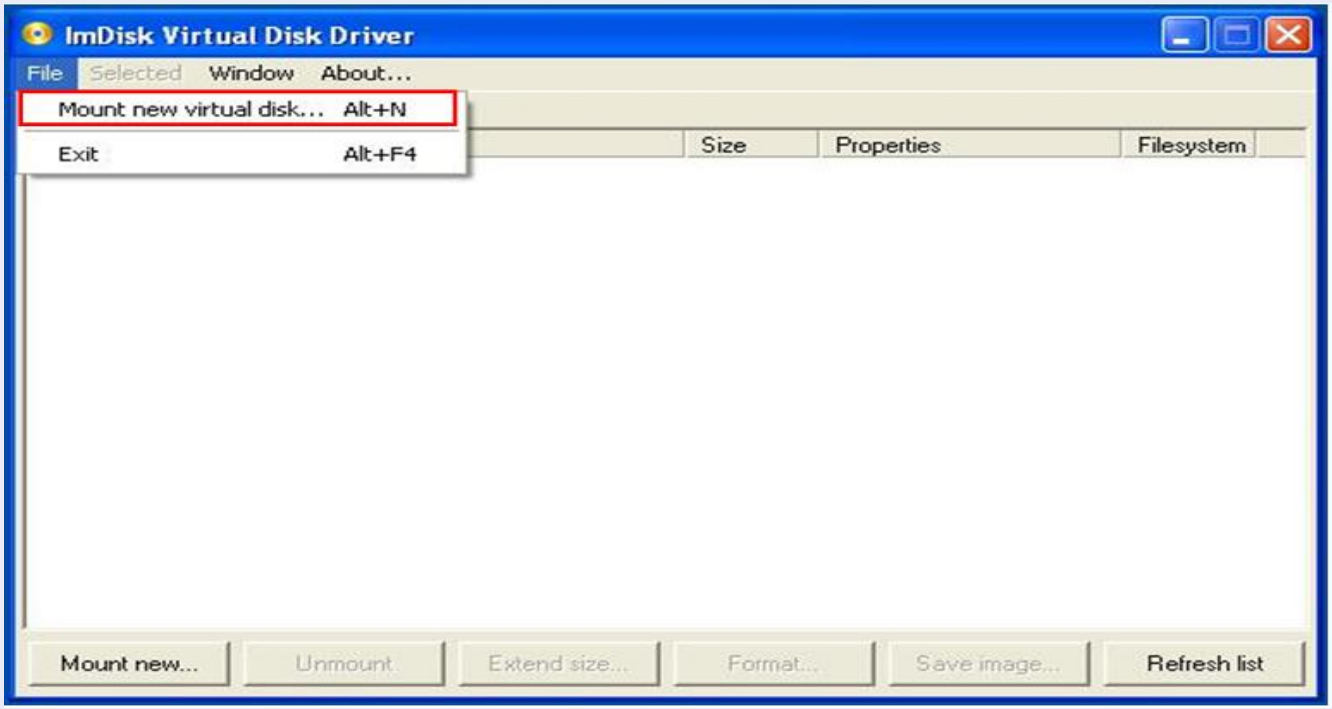
Instalace programu ImDisk

- Odkaz: http://www.ltr-data.se/opencode.html/#ImDisk.
- Jedná se o open source program, který napsal Olof Laregkvist.
- Začneme, že ze zdroje výše stáhneme instalační .exe soubor.
- Instalace je rychlá a intuitivní. V „Ovládacích panelech“ se vytvoří spouštěcí ikona.

Zkoumáme pod OS MS Windows

Instalace programu ImDisk

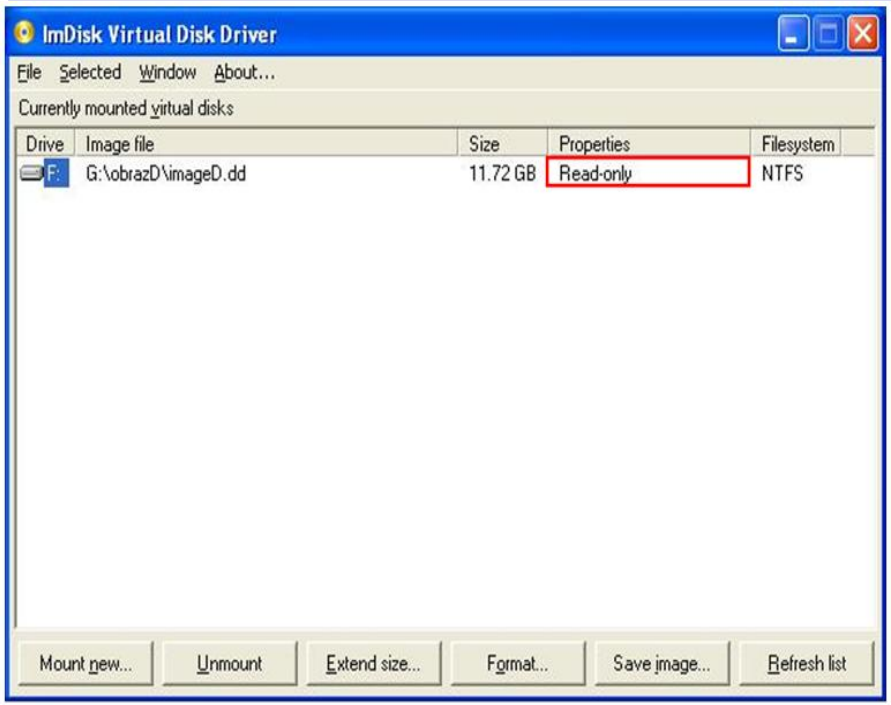
- Dvojklikem spustíme aplikace a otevře se níže zobrazené hlavní okno.
- Chceme připojit disk na zkoumání. „File“ → „Mount new virtual disk...“

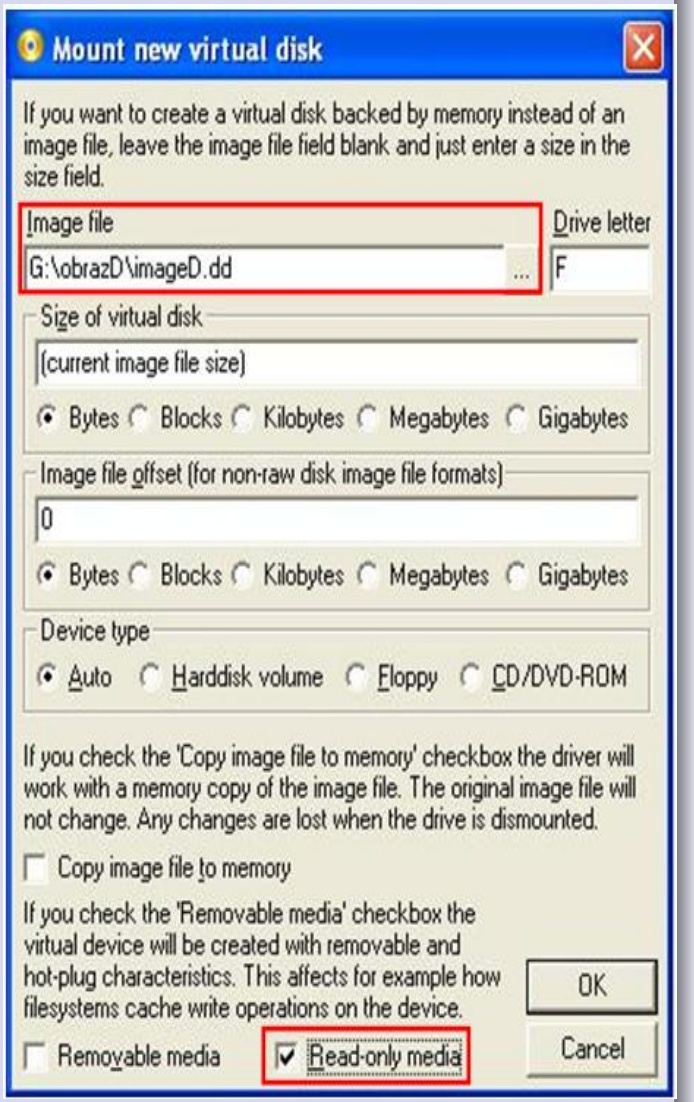


Zkoumáme pod OS MS Windows

Instalace programu ImDisk

- Do pole označeného „Image file“ načteme náš vytvořený obraz.
- Pro naše digitální zkoumání je nesmírně důležité zaškrtávátko „Read-only media“.

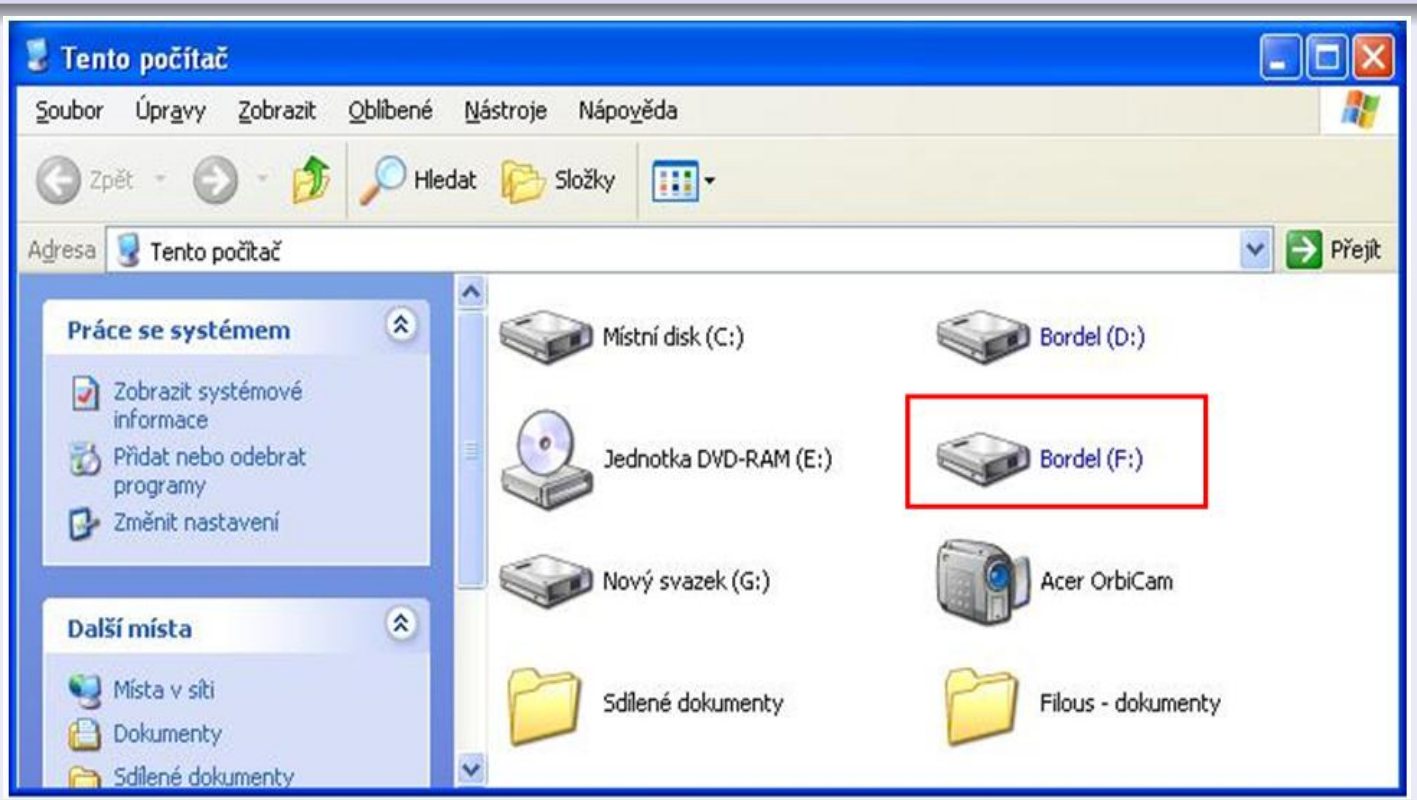




Zkoumáme pod OS MS Windows

Instalace programu ImDisk

- Výše uvedenými kroky jsme připojily obraz, který nyní můžeme zkoumat.
- Níže můžete vidět, že se svazek objeví stejně, jako kterékoli běžně připojené zařízení.



Zkoumáme pod OS MS Windows

Souborové systémy

- Další, co zbývá vyřešit jsou pro Windows neznáme typy souborových systémů.
- S NTFS a FAT si nevystačíme, potřebujeme podporu Ext2/3, HFS a HFS+.

Instalace programu Ext2Fsd

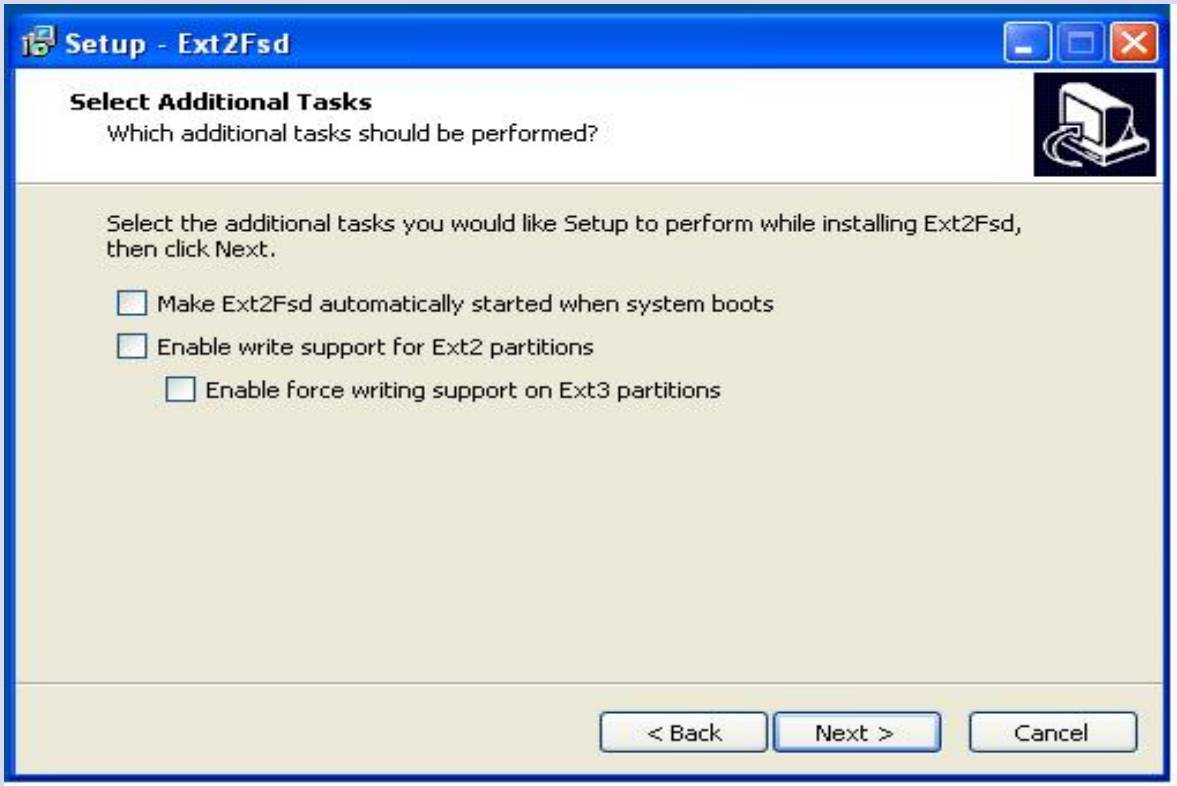
- Odkaz: http://www.ext2fsd.com/.
- Ext2Fsd je ovladač pro operační system Windows (XP, Vista i Win7).
- Jedná se o free software (GPL2), který umožní číst/zapisovat souborové systémy Ext2/3.
- Instalační soubor stáhneme z odkazu výše.

Zkoumáme pod OS MS Windows

Souborové systémy

Instalace programu Ext2Fsd

- Instalace je intuitivní, jen je vhodné nezaškrnout volbu „Enable write support for ..“ (v závislosti na použití).

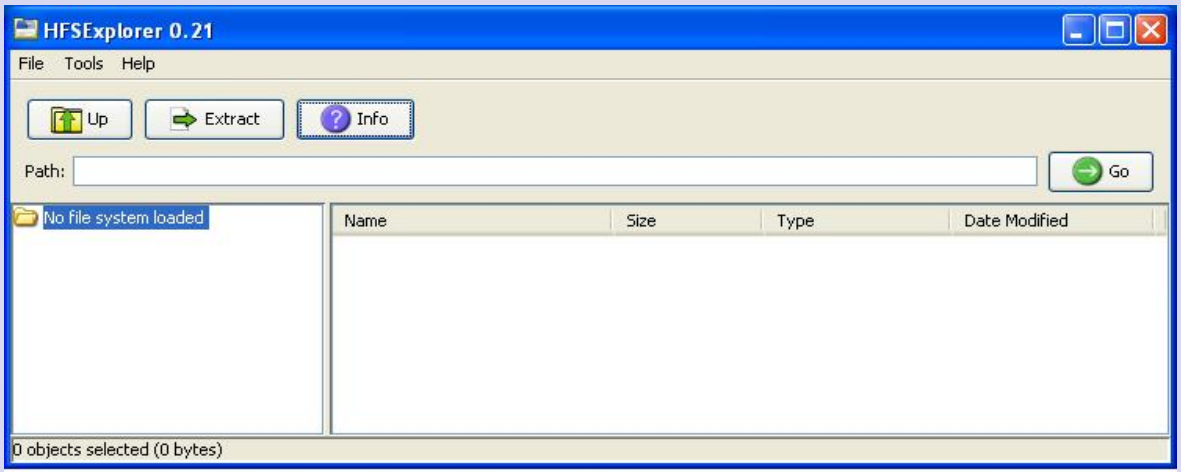


Zkoumáme pod OS MS Windows

Souborové systémy

Instalace programu HFS Explorer

- Odkaz: http://www.catacombae.org/hfsx.html.
- HFS Explorer je aplikace umožňující práci se souborovými systémy OS MAC (HFS, HFS+, HFSX).
- Aplikace uvolněna pod licencí GPL3 a vyžaduje prostředí Java.



Linux Live CD/DVD

Live CD/DVD

- Plně funkční operační systém založený na některé Linuxové distribuci (Ubuntu, RedHat, Knoppix, Slax, atd.)
- Volně ke stažení ze stránek příslušné distribuce.
- Výhoda spočívá ve velikosti, vejde se na CD/DVD/USB.
- Stáhnout ISO obraz, vypálit jako image.
- Při startu PC - proběhne POST - přechod do SETUP (dle výrobce BIOSU, F2, delete, atd).
- V BIOSU nastavíme pořadí bootování, jak nám vyhovuje (dle zařízení).
- Použití - seznámení s konkrétní distribucí, diagnostika PC nebo jako záchrané CD při nefunkčnosti systému (např. záloha dat).

Linux Live CD/DVD

Live CD/DVD

- Z forenzního pohledu je zajímavé snad jen to, že sytém je načten z onoho CD/DVD a nesáhne tak disk (pozor).
- Zkoumaný systém může být zmanipulovaný (záměrné smazání disku, přepsání Slack-space, atd).
- No automount vlastnost (SW write blocker) Pozor, dle distribuce.
- Před nabootováním bezpečného systému se přesto vždy doporučuje disky odpojit (viz. detaily později).
- Výhoda Linuxových distribucí spočívá v tom, že již v základu obsahují mnoho nástrojů používaných při zkoumání (dd, grep, md5sum, sha1sum, xxd, atd).
- Př. „forensic sound“ live linuxové distribuce je BackTrack verze 4 a 5.

Prostředí pro zkoumání digitálního obsahu

- Na všech níže uvedených prostředích najdete nesčetné množství open source či freeware forenzních (bezpečnostních) nástrojů.

C.A.I.N.E - Computer Aided Investigative Environment

- Stránky projektu: http://www.caine-live.net/index.html
- CAINE je vyloženě open source projekt italské výroby postavený na Ubuntu 10.04.
- Aktuální verze prostředí CAINE (WinTaylor) je 2.5.1.
- Kompletní prostředí pro forenzní zkoumání od fáze sběru až po závěrečý report jsou v jednom GUI.
- Pokud live CD necháme nabootovat máme plně funkční operační systém CAINE.
- WinTaylor je GUI pro CAINE vytvořené pro OS Windows. Ideální pro live analýzu (Incident Response).

Prostředí pro zkoumání digitálního obsahu

WinTaylor

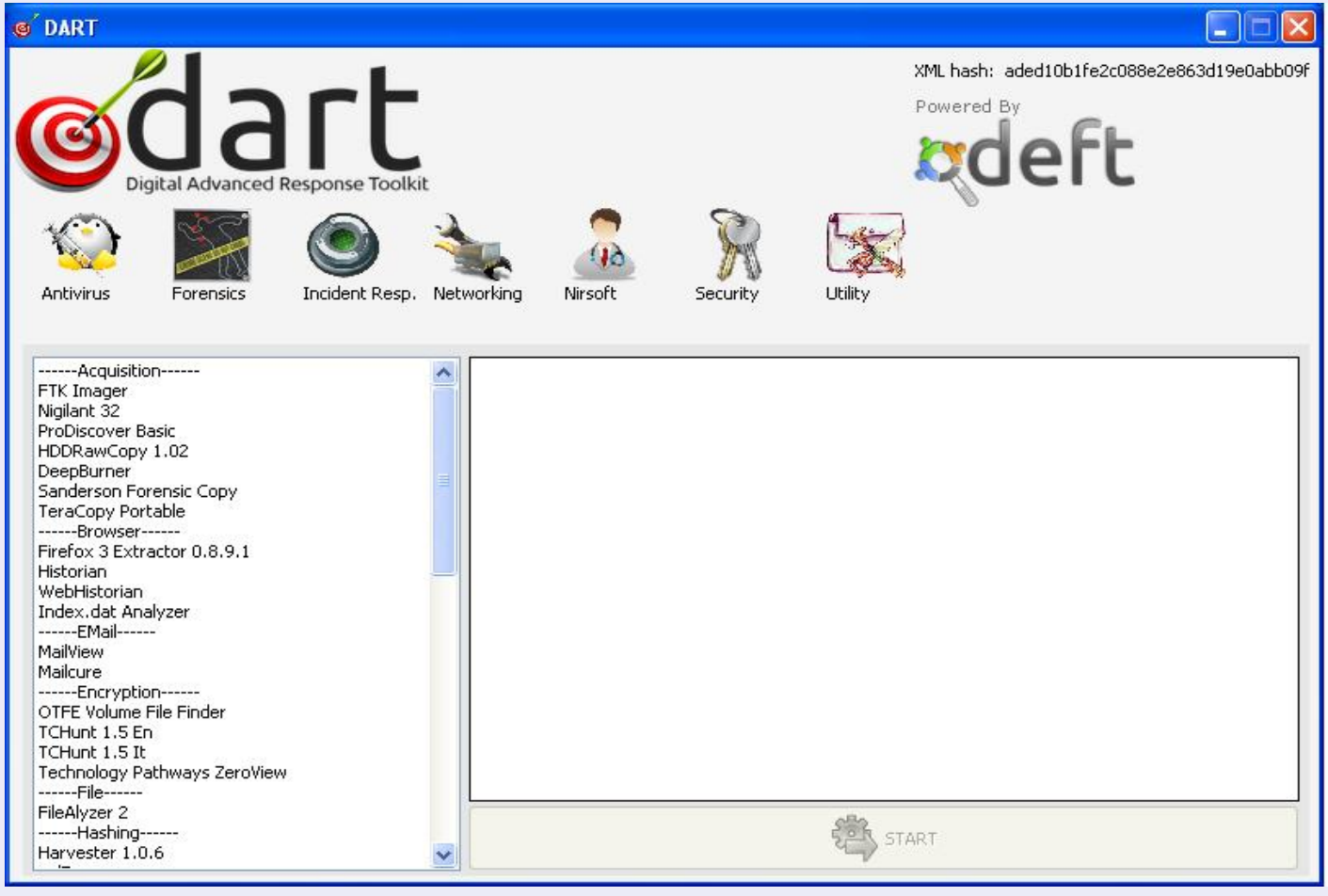
Prostředí pro zkoumání digitálního obsahu

DEFT - Digital Evidence & Forensic Toolkit

- Stránky projektu: http://www.deftlinux.net/
- DEFT v7 je další italský projekt postavený na distribuci Lubuntu 11.10.
- Live CD představuje kompletní forenzní prostředí ke zkoumání PC, sítí, mobilních zařízení, atd.
- Dříve DEFT Extra v1.0, nyní DART v1.0 (Digital Advanced Response Toolkit) GUI vytvořený pro sběr nestálých dat při live forensic nebo (Incident Response) .

Prostředí pro zkoumání digitálního obsahu

DART



Prostředí pro zkoumání digitálního obsahu

- Nebylo cílem představit všechna hotová forenzní prostředí.
- V průběhu dalších hodin si některá prostředí přestavíme více do detailů.
- Příklady dalších forenzních prostředí.
  - FCCU (Federal Computer Crime Unit) Forensic Boot CD: http://www.lnx4n6.be/index.php#.
  - Forensic and Incident Response Environment (FIRE): http://fire.dmzs.com/.
  - Helix 3 (omezená verze, nutná registrace): https://www.e-fense.com/store/index.php?_a=viewProd\&productId=11
  - BackTrack Forensic v4 a v5: http://www.backtrack-linux.org/wiki/index.php/Forensics_Boot
  - Operativní Forenzní Analyzátor, FIT-ČVUT: http://service.felk.cvut.cz/anc/ofa/index.html.

Prostředí pro zkoumání digitálního obsahu

Forenzní nástroje a univerzity v ČR

- Slyšeli jste o forenzních nástrojích vyvinutých na českých univerzitách?

Forensic Analyzer

- Stránky projektu již nejsou udržovány a projekt se již nerozvíjí.
- Open source uvolněný pod licencí GPL2, použitelný pod Os Windows i Lnux.
- Umožňuje provádět analýzu smazaných dat, slack space, obnovovat části smazaných souborů.
- Skládá se ze dvou částí. Klient (Forensic Analyzer) a server (Forensic Analyzer Probe) bootovatelné CD.

Prostředí pro zkoumání digitálního obsahu

Forenzní nástroje a univerzity v ČR

Operativní Forenzní Analyzátor

- Stránky projektu: http://service.felk.cvut.cz/anc/ofa/index.html.
- Vyvíjen na FIT-ČVUT pro účely policie ČR.
- Vytvořen pro zkoumání digitálního obsahu v první vlně.
- Určen pro uživatele, kteří nejsou specialisté v oblasti digitálního zkoumání (GUI, jenoduchost, rychlost,). Více informací na oficiálních stránkách.

Použitá Literatura

[1] Altheide, C., Carvey, H. *Digital Forensic With Open Source Tools.*
Syngress, 2011. 264 s. ISBN 978–1–59749–586–8.

Děkuji za pozornost!