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".

Získání dat - tvorba obrazu

Analýza dat

Bc. Filip Pávek

Ústav informatiky
Filozoficko-přírodovědecká fakulta
Slezská univerzita v Opavě

filippavek@gmail.com

2012

Obsah prezentace

Obsah prezentace

- Různorodost datových médií, se kterými se můžeme při incidentu setkat.
- Výběr a příprava vhodných nástrojů k vytvoření forenzních kopií dat zasaženého systému.
- Metody, které můžeme při tvorbě obrazu použít (lokální, vzdálená).
- Zajištění forenzních vlastností získaných dat (integrita, autentizace).
- Tvorba duplikátu z vytvořeného obrazu.
- Neřešíme zde sběr nestálých dat z běžícího systému, pouze tvorbu obrazu z datových médií.

Obecně o sběru dat z datových médií

Sběr dat - fyzický vs. digitální svět

- Pokud si vzpomenete na úvodní přednášku, tak se právě nacházíme ve fázi „získání dat“.
  - Ve [2] autoři Carrier a Spafford porovnávají digitální a fyzické místo činu.
  - Př 1. Dojde-li k vraždě v rodiném domě je celý dům místem činu a je nesmírně důležité, aby místo bylo maximálně izolováno. Žádný pohyb nezainteresovaných osob. Pohyb vyšetřovatele a forenzních techniků musí být, co možná nejméně invazivní k okolí, aby nedošlo k poškození či ztrátě stop.
  - Př 2. Na digitálním místě činu platí totožná pravidla jako pro fyzické prostředí, jen se liší nasazené metody pro sběr stop. Myšleno ironicky: Pokud bude zkoušet zasažený server zkomat nejdříve pět techniků a teprve potom se rozhodnou přivolat specialistu (znalce), je to totéž jako když fyzickým místem činu projde zástup lidí.

Obecně o sběru dat z datových médií

Acquisition Phase je velmi důležitá!

- Nesmírně důležitá fáze, která by měla být profesionálně provedá.
- Veškeré chyby (porušení integrity, opomenutí některých stop, atd.) se neblaze promítnou do další fáze → analýzy dat (i celkových výsledků zkoumání).
- Přístup k zařízení by měl být co možná nejméně invazivní a přitom je nutné získat maximální informace (viz. níže).
- Při vytváření forenzní kopie nesmí dojít k nechtěnému zápisu na médium.
- Př. precizní fotodokumentace zařízení (kabely a propojení, vnitřek PC, atd), info o typech datových médií uvnitř PC (výrobce, rozhraní, velikost, atd), informace o konfiguraci zasaženého systému (datová média), samotná tvorba obrazů.

Obecně o sběru dat z datových médií

Live vs. Dead Acquisition [3]

- **Live Acquisition**: Data jsou získávána z kopromitovaného systému během toho, co je systém v provozu. (Útočník může zaměrně zmanipulovat sběr dat. Rootkiky.) V některých případech nelze systém vypnout a několik hodit dělat obrazy disku (např. servery, na kterých běží kriticky důležité služby pro podnik).
- **Dead Acquisition**: Sběr dat je uskutečňován bez asistence kompromitovaného systému. Př. vypnuté PC a sběr dat se uskutečňuje po nabootování Live CD.

Proč se vytváří forenzní kopie? [1]

- **Vytvoření přesné kopie originálu**. Ve fyzickém světě nejde vytvářet přesné kopie z důkazů (nůž, pistole, rozbitá láhev).

Obecně o sběru dat z datových médií

- V digitálním světě, jsme schopni vyrobit image originálu a ten dále zkoumat. Čímž se vyhneme poškození originální stopy (přip. důkazu). Při poškození použijeme další duplikát. Analýzu může tak provádět několik znalců nezávisle.
- Bitová kopie zajistí **úplnost** zdroje. Prezentace souborového systému od OS není komplexní (smazané, nealokované či přepsané soubory) (viz. níže).

Obraz (image)

- Přesná bitová kopie (bit-for-bit) zdrojového zařízení, která se ukládá na předem připravené datové médium.
- Forenzní kopie předpokládá, že výsledný obraz je naprosto totožný se zdrojovým médiem.

Obecně o sběru dat z datových médií

- Pozor na oklamání operačním systémem. Velikost musí odpovídat skutečné velikosti disku, nikoli tomu, co si operační systém myslí, že je skutečná velikost.
- Disk může obsahovat záměrně skryté sektory (viz. dále HPA, DCO)!

Datová Média

Základní charakteristika

- Velké množství nejrůznějších datových médií různých parametrů, které mohou být při incidentu předmětem tvorby obrazu.
- Je povinností znalce znát jednotlivé typy medií a jejich vlastnosti.
- První typ média, co nás dnes asi napadne je HDD (Hard Disk Drive) a SSD (Solid-State Drive). Popište základí typy rozhraní, rozměry, technické současti, princip ogranizace dat na médiu, buňky u SSD, atd.
- Flash paměťi (SSD, USB flash paměti, Memory Stick, atd.), Optická média (CD, DVD, Blue-ray, atd.).
- Různá datová média jsou v mnoha zářízeních kolem nás.

Datová Média

- Př. PC, čtečka elektronických knih, telefon, DVD přehrávač, televize, MP3 přehrávač, fotoaparáty, kamery, GPS navigace, aktivní síťové prvky, NAS, atd. → znalec na tuto skutečnost musí být připraven.

Je důležité vůbec odhalit potenciálního nosiče digitálních stop.

Příprava datových médií znalce

- HW vybavenost znalce. V praxi neexistuje příliš často zkoumání PC s jedním pevným diskem o velikosti 500GB. Naopak, spíše SAN, NAS, varianty RAID 0,1,3,5.
- Vzhledem k těmto okolnostem, je nezbytná dostatečná HW podpora při výjezdu k incidentu.

Datová Média

Vyčištění datového média

- Samozřejmostí je, že datová média musí být před použitím v novém zkoumání vymazána.
- K bezpečnému vymazání opět použijeme šikovnou utilitu **dd**.
  - # **dd if=/dev/zero of=/dev/hda bs=2k**
- Jako zdrojové zařízení jsou „nuly“ aplikované na celý disk.

Datová Média

Standardy rozhraní

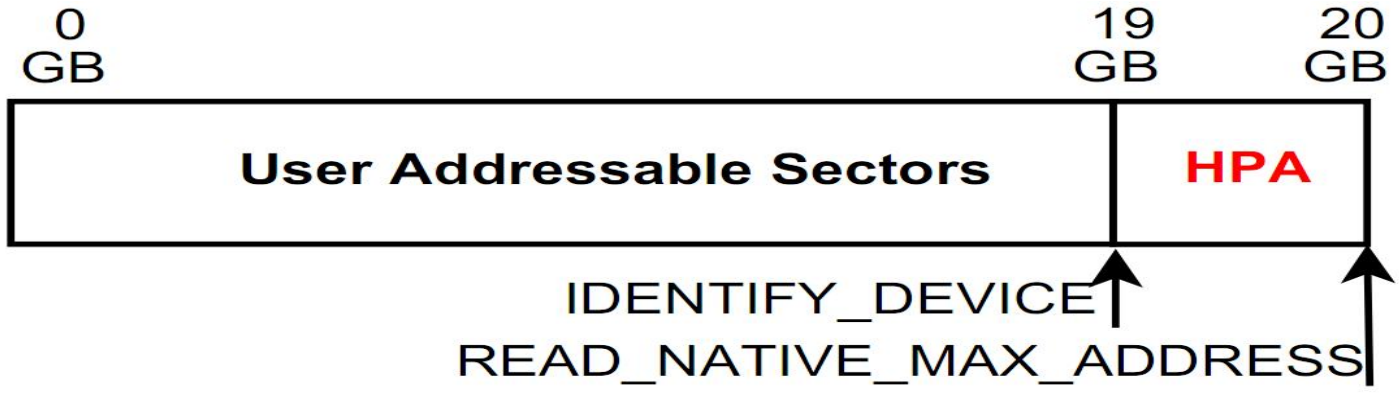
- ATA standardy pouze na pevný disk.
  - ATA 4: SMART, heslo.
  - ATA 4: 80 žilový kabel, poprve přidává HPA.
  - ATA 6: odebrána podpora CHS, přidává LBA DCO.
- SATA, SCSI, atd.

Host Protected Area [4], [5]

- Oblast, které si běžný uživatel nemusí všimnout.
- Běžná velikost 0, ale lze měnit pomocí ATA příkazů.
- Vytvořeno za účelem ukládání dat výrobců PC, kterou uživatel nemůžeme smazat běžným formátováním.
- Oblast přístupná pouze po překonfigurování pevného disku.

Datová Média

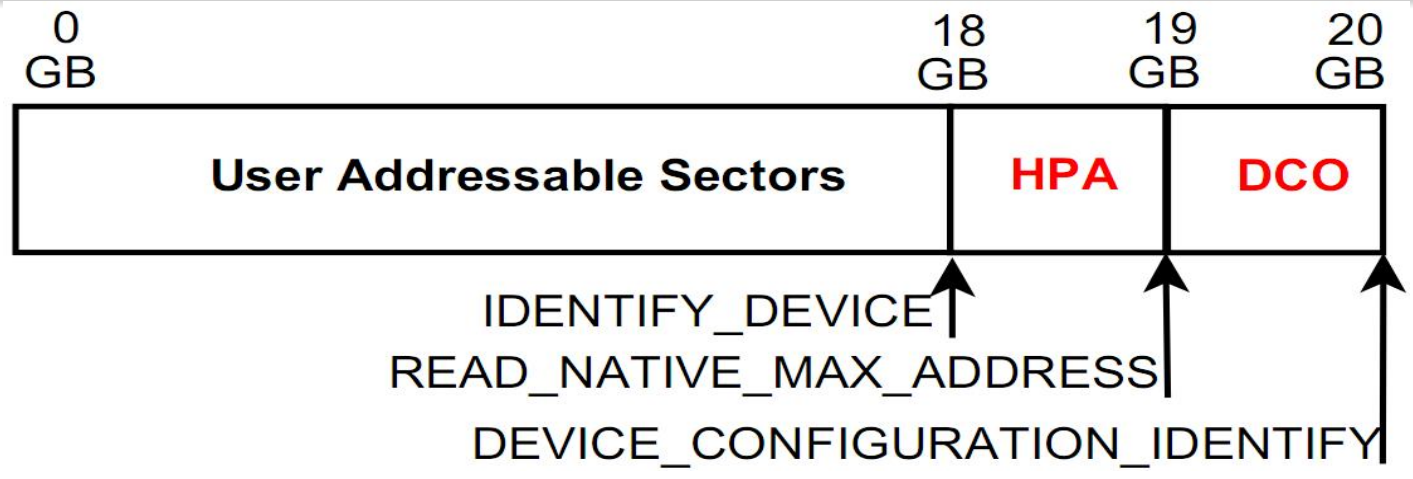
- Příkaz READ_NATIVE_MAX_ADDRESS vrátí maximální fyzickou adresu (kde disk fyzicky končí a IDENTIFY_DEVICE příkaz vrátí počet sektrorů přístupných uživateli).
- Pokud HPA existuje pak se výsledky obou příkazů liší a příkaz IDENTIFY_DEVICE prakticky vrátí začátek HPA.
- Příkazem SET_MAX_ADDRESS se vytvoří oblast, kam má uživatel přístup. Zbytek do konce fyzického disku je HPA.
- Pro odstranění HPA je nutné zadat SET_MAX_ADDRESS se skutečnou maximální velikostí disku.
- Důležité HPA rozpoznat při tvorbě obrazu. Program **hparm**.



Datová Média

Device Configuration Overlay

- Podobně jako u předchozího, opět může sloužit k ukrytí dat. Kombinace HPA a DCO je zákeřnější a měli s ní problémy i některé komerční forenzní nástroje.
- Příkazem DEVICE_CONFIGURATION_IDENTIFY zobrazíme skutečnou fyzickou velikost pevného disku. Porovnáme-li hodnotu s výstupem příkazu IDENTIFY_DEVICE můžeme detekovat DCO.
- DEVICE_CONFIGURATION_SET vytvoří DCO, naopak DEVICE_CONFIGURATION_RESET odstraní DCO.



Nástroje pro tvorbu obrazu

dd

- Jedna ze základních forenzních open source utilit.
- Součastí Unixových operačních systémů.
- Dvě základní použití dd:
  - Kopie disku/oddílu na jiný disk se stejnou geometrií např. za účelem zálohy či výměny disku.
  - Vytvoření přesné bitové kopie zdroje a její uložení do jediného souboru.

dd if=/vstupní_soubor **of=**/výstupní_soubor **volby**

- **dd if=/dev/hda1 of=/dev/hdb/imagehda1.dd**.
- Pokud se nacházíme v cílovém adresáři pak stačí:
  - **dd if=/dev/hda1 of=/imagehda1.dd**.
- Kopie může probíhat i opačně, ze souboru (obraz) na disk:
  - **dd if=imagehda1.dd of=/dev/hda1**.

Nástroje pro tvorbu obrazu

```
bs=BAJTŮ        čte a zapisuje BAJTŮ bajtů najednou (vizte též ibs=, obs=)
cbs=BAJTŮ       konvertuje BAJTŮ bajtů najednou
conv=KONVERZE   konvertuje soubor podle seznamu čárkami oddělených konverzí
count=BLOKŮ     zkopíruje pouze BLOKŮ vstupních bloků
ibs=BAJTŮ       čte BAJTŮ bajtů najednou (implicitně: 512)
if=SOUBOR       čte ze souboru SOUBOR místo ze stdin
iflag=PŘÍZNAKY  způsob čtení. PŘÍZNAKY je seznam čárkou oddělených příznaků
obs=BAJTŮ       zapisuje BAJTŮ bajtů najednou (implicitně: 512)
of=SOUBOR       zapisuje do SOUBOR místo do stdout
oflag=PŘÍZNAKY  způsob zápisu. PŘÍZNAKY je seznam čárkou oddělených příznaků
seek=BLOKŮ      přeskočí prvních BLOKŮ výstupních bloků velikosti „obs“
skip=BLOKŮ      přeskočí prvních BLOKŮ vstupních bloků velikosti „ibs“
status=noxfer   nezobrazí statistické informace o přenosu dat
```

- **bs=**(významně ovlivňuje rychlost tvorby obrazu, default 512B).
- **skip=**(využijeme při tvorbě pouze části souborového systému).
- **conv=**(**noerror** (nepřestane číst zdroj pokud dojde k např. k fyzické chybě disku), **sync** (pokud nastane fyzická chyba, zapíše nulu, vyžaduje předchozí volbu)).

Nástroje pro tvorbu obrazu

dcfldd/dc3dd

- Funkce příkazů je velmi totožná.
- Příkaz založen na klasické dd utilitě, stejné základní operace.
- Vytvořen v duchu forenzního získávání dat.
- Fukce navíc: hash, rozdělení výstupu, záznam průběhu činnosti.
- Instalace: **sudo get-apt dcfldd** (nebo centrum softwaru).
- Kompletní fukce: **dcfldd –help**
  - Př. **dcfldd if=/dev/hda1 of=/dev/hdb/imagehda1.dd bs=2k hash=sha1 hashlog=/dev/hdb/haslog.txt**.
- **Hash**=(md5, sha1, sha256, sha512), **hashwindow**=(př. pro každých 512KB bude vygenerována hash), **hashlog**=(kam se uloží hash, default konzole), **split**=(rozdělení výstupu do určité velikosti př. 2GB).

Nástroje pro tvorbu obrazu

dcfldd –help

```
bs=BYTES                force ibs=BYTES and obs=BYTES
cbs=BYTES               convert BYTES bytes at a time
conv=KEYWORDS           convert the file as per the comma separated keyword list
count=BLOCKS            copy only BLOCKS input blocks
ibs=BYTES               read BYTES bytes at a time
if=FILE                 read from FILE instead of stdin
obs=BYTES               write BYTES bytes at a time
of=FILE                 write to FILE instead of stdout
                         NOTE: of=FILE may be used several times to write
                               output to multiple files simultaneously
of:=COMMAND             exec and write output to process COMMAND
seek=BLOCKS             skip BLOCKS obs-sized blocks at start of output
skip=BLOCKS             skip BLOCKS ibs-sized blocks at start of input
pattern=HEX             use the specified binary pattern as input
textpattern=TEXT        use repeating TEXT as input
errlog=FILE             send error messages to FILE as well as stderr
hashwindow=BYTES        perform a hash on every BYTES amount of data
hash=NAME               either md5, sha1, sha256, sha384 or sha512
                          default algorithm is md5. To select multiple
                          algorithms to run simultaneously enter the names
                          in a comma separated list
hashlog=FILE            send MD5 hash output to FILE instead of stderr
                          if you are using multiple hash algorithms you
                          can send each to a seperate file using the
                          convention ALGORITHMlog=FILE, for example
                          md5log=FILE1, sha1log=FILE2, etc.
```

Nástroje pro tvorbu obrazu

- Přepínač **split** poskytuje hned několik možností.
- Rozdělit vytvářený obraz do více části pevné velikosti (např. 20GB obraz chceme rozdělit do čtyřech 5GB souborů).
- Nebo můžeme podobným způsobem rozdělit již hotový obraz (imagesHda.dd).
  - Př. **dcfldd if=/dev/hda1 | split -d -b 5000m - imagehda1.dd bs=2k**.
- **split -d**=(rozdělí binární vstup), **-d**=(číslování jednotlivých výstupních částí), **5000m**=(velikost částí), **„-“**=(říká, že vstupem je dd, jinak je vstupem obraz, který chceme rozdělit).
- Výsledkem budou čtyři soubory: imagehda1.dd.01 . . . imagehda1.dd.04 (přepínač -d zajistil očíslování).

Nástroje pro tvorbu obrazu

ddrescue

- Specialitou mezi různými variantami dd nástrojů je **ddrescue**. Z forenzního hlediska velmi důležitý nástroj.
- Používá jinou vnitřní logiku než dosavadní nástroje.
- Ideální v případě fyzického poškození disku - nejdříve vytvoří obraz z dat, co jsou v pořádku a následně se snaží získat data z poškozených částí disku.
- Jiný zápis než u předchozích dd.
- Oficiální stránky: http://www.gnu.org/software/ddrescue/ddrescue.html.
- Manuál: http://www.gnu.org/software/ddrescue/manual/ddrescue_manual.html.

Integrita dat

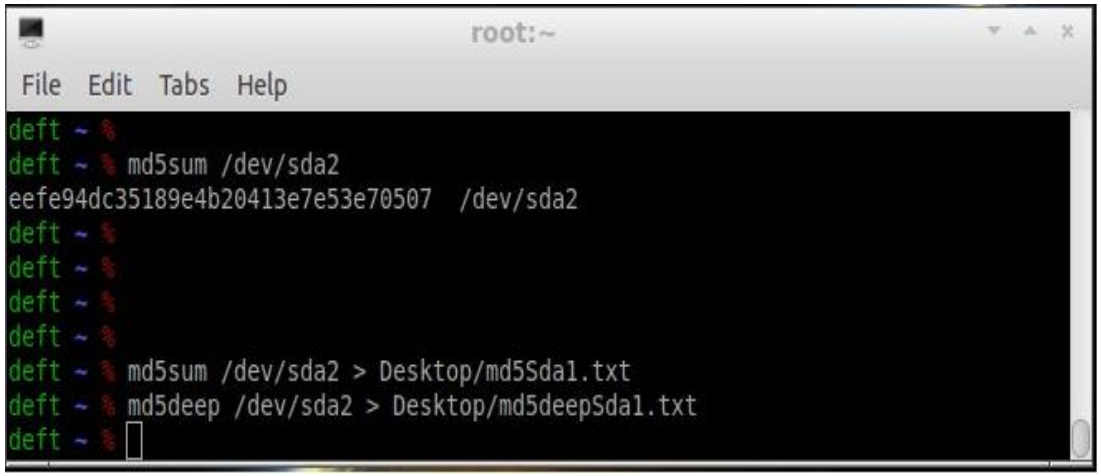
Integrita dat

- V průběhu forezního zkoumání je kladen veliký požadavek na zajištění integrity dat.
- Při vytváření dat a později při analýze je nesmírně nutné, aby nedošlo ke změně na datech.
- To lze zajistit vypočtením kontrolního součtu z dat (př. MD5, SHA-1, SHA-2, SHA512).
- Nejprve vypočteme kontrolní součet z kompromitovaného média, vytvoříme obraz a následně vypočteme znovu kontrolní součet pro obraz. Oba součty se musí shodovat! Problém u disků z fyzickým poškozením.
- I minimální změna na datech způsobí, že se oba součty nebudou shodovat.

Nástroje

Integrita dat

- Při tvorbě obrazu můžeme, jako parametr zvolit výpočet hash funkce.
- Kontrolní součet si můžeme nechat vypsat do Terminálu nebo přesměrovat např. na bezpečné uložiště znalce.
- Obě možnosti jsou níže vidět. Vytvořeno ve forenzním prostředí DEFT.
- Jaký je rozdíl, použiju-li při přesměrování „>“ a „>>“.



Metody tvorby obrazu

Metody pro tvorbu obrazu

- V podstě existují 3 postupy, jak při tvorbě forezní kopie datového média postupovat:
- **Lokální metoda 1**: Pevný disk je z kompromitovaného systému vyjmut a připojen k forezní stanici znalce.
- **Lokální metoda 2**: Forenzní obraz je vytvořen na kompromitovaném systému.
- **Vzdálená metoda**: Vytvoření forenzní kopie přes počítačovou síť.

Metody tvorby obrazu

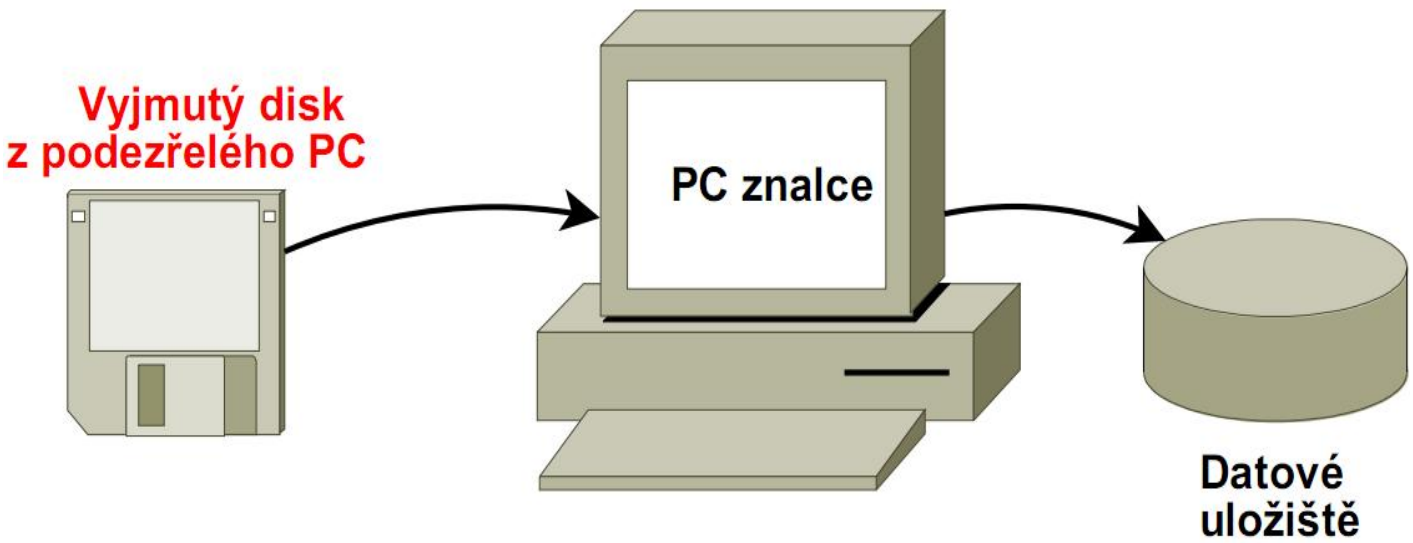
Sběr informací ze systému [3]

- Informace o konfiguraci zasaženého systému, začneme tím, že odpojíme pevné disky (HDD či SSD).
- Spustíme zasažený systém a zkontrolujeme nastavení BIOSu. (nastavený čas/datum, pořadí bootování, atd) a vypneme PC.
- Vložíme forenzní live CD do mechaniky a provedeme druhý boot. Přitom ověříme funkčnost systému nabootovat prověřený systém znalce a vypneme PC.
- Teprve nyní připojíme datové nosiče (HDD a SSD) a znovu necháme nabootovat náš systém. Získáme informace o konfiguraci datových médií (velikost, LBA, atd).
- Vypneme PC (odpojit disky).

Forenzní kopii vytvoříme ideálně na bezpečném systému.

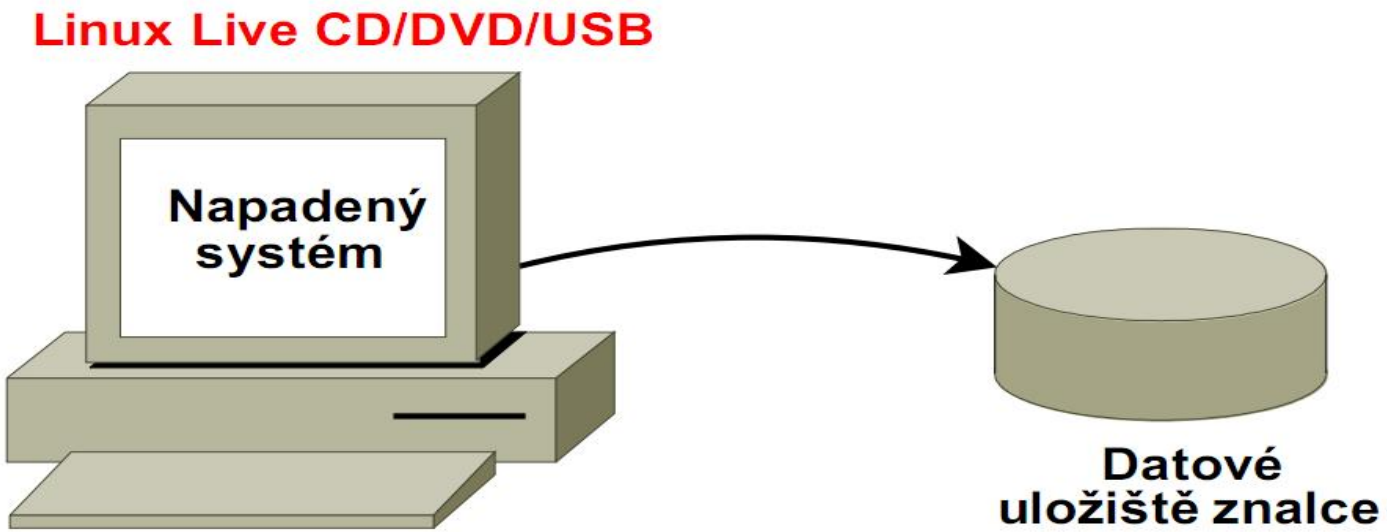
Lokální metoda 1

- Znalec vyjme disk z kompromitovaného PC a připojí ho ke své stanici.
- Jedná se o ideální případ. Použít write blocker.
- Př. jak může vypadat příkaz pro vytvoření kopie:
  - # **dd if=/dev/hda1 of=/dev/hdb/imagehda1.dd bs=2k**



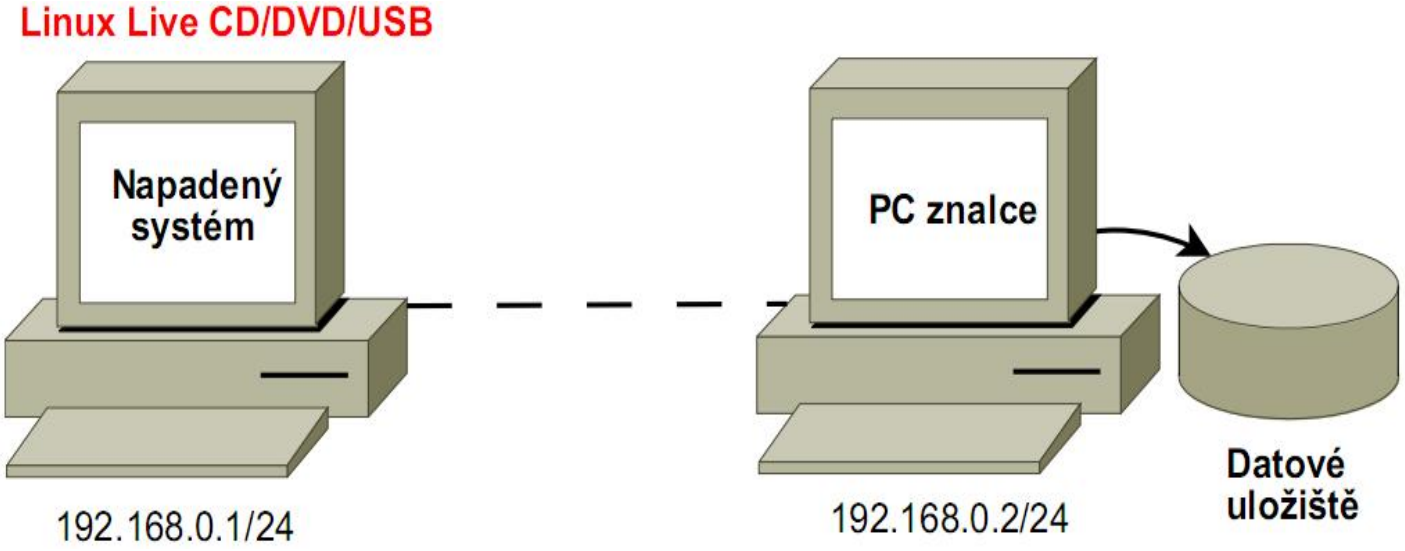
Lokální metoda 2

- Není tak ideální jako předchozí metoda. Je nutné dodržet postup výše.
- 100% ujištění, že se v mechanice nachází forenzní Live CD, které je schopné bezpečně nabootovat.
  - # **dcfldd if=/dev/hda1 of=/dev/hdb/image.dd bs=2k hashlog=/dev/hdb/hash.txt**

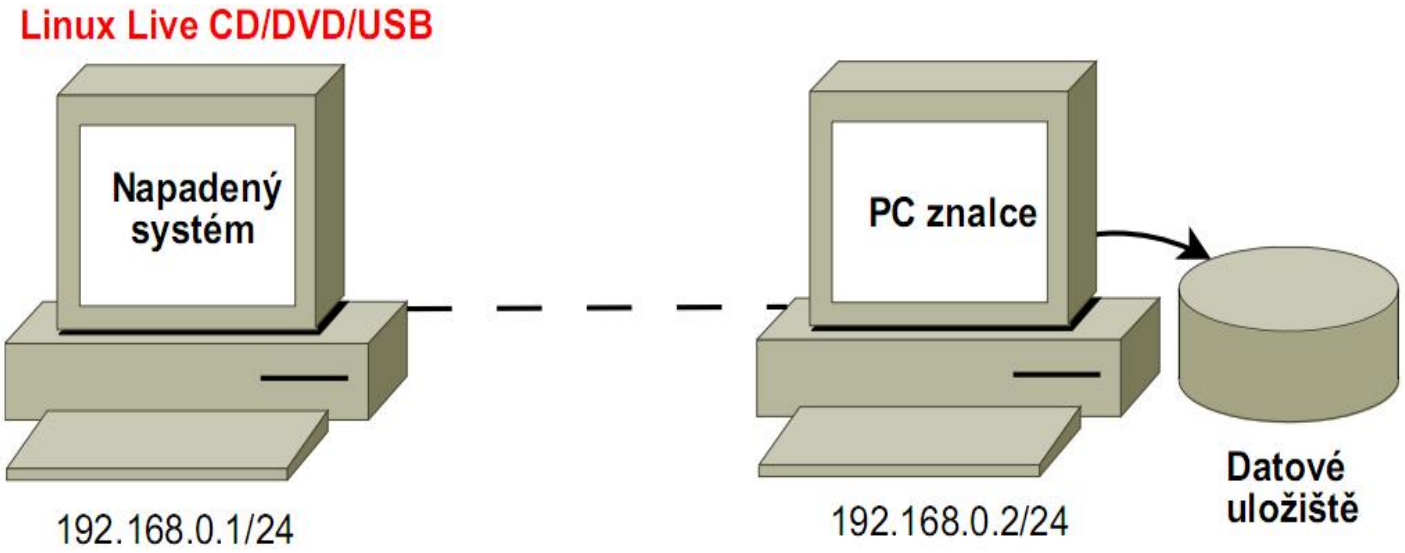


Vzdálená metoda

- Existuje několik příkladů, kdy použít vzdálenou metodu přístupu k podezřelému systému. Př. nemáme fyzický přístup k zařízení, interface/rozhraní.
- Používáme-li podnikovou síť, je důležité myslet na bezpečnost přenášených dat. Př. odposlechnutí provozu. Šifrování přenášených dat.
- HW omezení síťových prvků - časově náročná metoda.

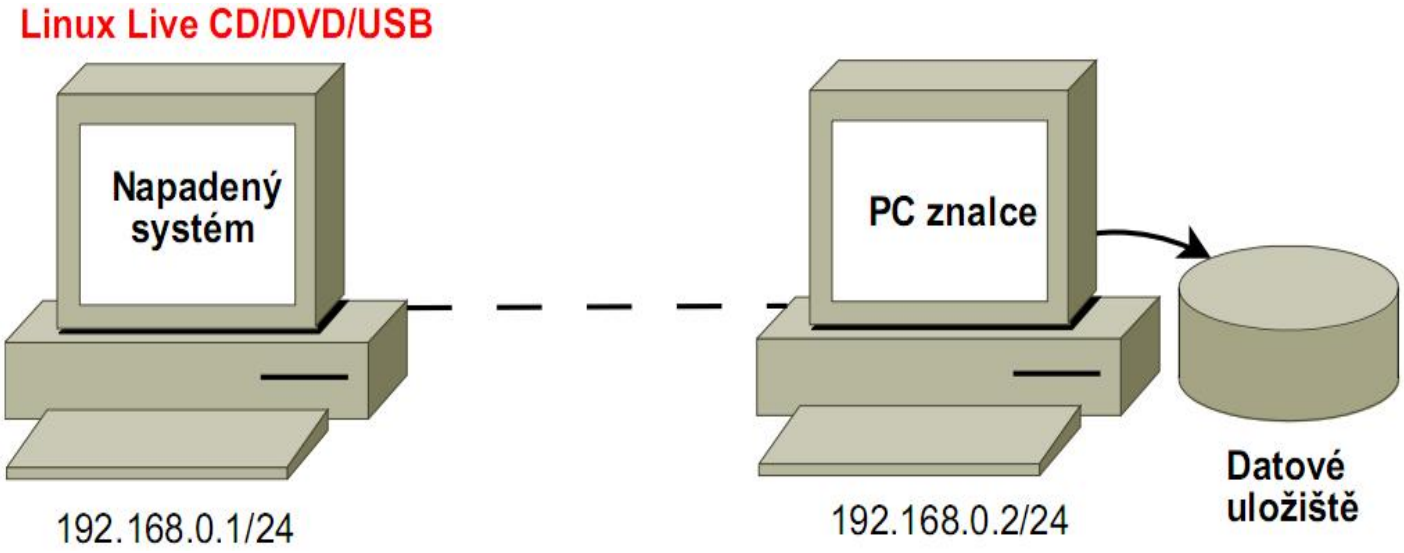


Vzdálená metoda



- Na kompromitovaném systému spustíme Live CD a na obou PC nastavíme IP adresu → ověříme konektivitu.
- Na PC znalce nastavíme port, na kterém bude naslouchat pro data a místo, kam se má náš obraz uložit:
  - # **nc -l -p 3000 | dd of=/mnt/images/imagehda1.dd**
- Přenos použije programu netcat, **-l** (listennig mode), **-p** (port 3000), obraz se uloží do souboru „imagehda1.dd“.

Vzdálená metoda



- Na kompromitovaném systému přesměrujeme výstup programu netcat na port 3000 a adresu 192.168.0.2
  - # **dd if=/dev/hda1 bs=2k | nc 192.168.0.2 3000**
- Zdrojem programu dd je oddíl 1, ale výstup je poslán programu netcat.

Použitá Literatura

[1] Altheide, C., Carvey, H. *Digital Forensic With Open Source Tools.*
Syngress, 2011. 264 s. ISBN 978–1–59749–586–8.
[2] Carrier, B., Spafford, H. E. *Getting Physical With The Digital Investigation Process* [online]. CERIAS Tech Report 2003-29, Pardue University.
[3] *Forenzní zkoumání digitálních důkazů: Příručka vyšetřovatele* [online]. Risk Analysis Consultants, s.r.o.
[4] Carrier, B. *File System Forensic Analysis.*
Pearson Education, 2005. 569 s. ISBN 0–321–26817–2.
[5] Gupta, R. M., Hoeschele, D. M., Rogers, K. M. *Hidden Disk Areas: HPA and DCO* [online]. International Journal of Digital Evidence. Fall 2006, Volume 5, Issue 1. Pardue University.

Děkuji za pozornost!