Forenzná analýza IKT

(Lukáš Hlavička)

Obsah

- Motivácia
- Cieľe forenznej analýzy
- Proces forenznej analýzy
- Využite forenznej analýzy
- Používané metódy.
- Bežne dostupné nástroje.
- Antiforenzné počítanie – princípy
- Antiforenzné počítanie – prípadová štúdia

Motivácia

- Bezpečnostné incidenty sú bežné.
- Rozvoj počítačovej kriminality
  - Klasické zločiny s pomocou IKT

    (vydieranie, podvody, falšovanie cenín,...)
  - Samotná počítačová kriminalita

    (hacking, krádeže identity, softwareové pirátstvo, …)
- Vysoka technologická vyspelosť počítačových zločincov → Nutná reakcia “druhej” strany.

Motivácia

Former Chief Computer Network Program Designer Arraigned for Alleged $10 Million Computer Software Bomb

Juvenile Computer Hacker Sentenced to Six Months in Detention Facility

Russian Computer Hacker Indicted in California for Breaking into Computer Systems and Extorting Victim Companies

Cieľe forenznej analýzy

Na počiatku je (najčastejšie) nejake podozrenie

- Získať dôkazy z dôkazových médií tak, aby tieto dôkazy neboli napadnuteľné napr. na súde
- Analyzovať získané dôkazy.
- Bezpečne uchovať získané dôkazy.
- Nájsť informácie podporujúce alebo vyvracajúce podozrenie.
- Prezentovať výsledky vyšetrovania (aj odborne nie zbehlým) oprávneným adresátom.

Proces forenznej analýzy

- Jedna z možných definícií FA IKT:

  "Tools and techniques to recover, preserve, and examine digital evidence on or transmitted by digital devices."

- Opakovateľný proces.
- Kroky:
  - Získavanie dôkazov
  - Uchovávanie dôkazov
  - Analýza a vyhodnocovanie dôkazov
  - Prezentácia výsledkov.

Získavanie dôkazov

- Potreba zabezpečiť:
  - Korektnosť (získané dáta sú totožné z dátami na originálnom médiu)
  - Autentickosť (získané dáta pochádzajú skutočne z analyzovaného zariadenia v danom čase)
  - Integritu (získané dáta, ktoré sa budú ďalej analyzovať nesmú byť pozmenené oproti originálu)
  - (Dôvernosť a dostupnosť)

Analýza dôkazov

- Ťažiskový krok celého procesu.
- Postup:
  - Štandardné techniky (obnova súborov z povrchu disku, file carving, …)
  - Využitie techník pre konkrétnu platformu (filesystém, operačný systém, typ zariadenia)
  - Využitie techník penetračného testovania

    POZOR NA PRÁVNE DOSLEDKY !!!
  - Využitie kapitálu ľudskej mysle. (najdôležitejšie)

Prezentácia výsledkov

- Prezentovanie výsledkov zadávateľovi forenznej analýzy:
  - Súd
  - Prokurátor
  - Vyšetrovateľ
  - Zamestnávateľ
- Poskytnutie výsledkov špecialistovi (napríklad odborníkovi druhej strany na súde)
- Výsledky musia byť opakovateľné.

Dokumentácia

- Nutnosť dokumentovať každý krok a okolnosť
- Chain of Custody – postupy a dokumentácia zaručujúce, že dôkaz ktorý sa dostane pred súd je ten istý ako bol získaný z “miesta činu”
  - Problematické zabezpečiť v mnohých prípadoch (Bežiace systémy a podobne)
  - Z hľadiska využita forenznej analýzy častokrát kritické.
- Dokumentácia musí byť tak podrobná, aby na jej základe bolo možné zopakovať proces a prísť k rovnakým výsledkom

Dokumentácia

- Dokumentácie nikdy nie je dosť z pohľadu podrobnosti a názornosti.
- Na úplnosti dokumentácie častokrát stojí celý prípad.

Využite forenznej analýzy

- Súdne vyšetrovanie
  - Usvedčiť páchateľov
  - Dokázať nevinu nevinných
  - Musí byť vykonávané podľa prísnych pravidiel aby boli dôkazy prijateľné pre organy činne v trestnom konaní (najmä sud)
  - Ošetrené súdnym poriadkom a zákonom o znalcoch a zákonom o policajnom zbore.
  - Relatívne jasné čo môžem a čo nie.
- Tajné služby, armáda, etc.

Využite forenznej analýzy

- Incident response
  - Riešenie a vyšetrovanie bezpečnostných incidentov
  - Môže sa transformovať na súdne vyšetrovanie
  - Ošetrené zmluvou, zákonom o ochrane osobných údajov, zákonom o utajovaných skutočnostiach, prípadne smernicami a politikami používania informačných zdrojov.
  - Častokrát nejasné čo môžem a čo nie.
- Iné (napríklad rozvody (USA))

Využite forenznej analýzy Príklady udalostí spúštajúcich vyšetrovanie

- Systémový administrátor zistí neobvyklú aktivitu na sieti alebo dostane upozornenia z IDS.
- Oprávár počítačov nájde na opravovanom počítači nelegálnu pornografiu a alarmuje políciu.
- Na mieste vraždy je nájdený počítač.
- Zamestnankyňa podá žalobu na šéfa kvôli sexuálnemu obťažovaniu prostredníctvom E-mailu
- ...

Používané metódy - úvod

- Používané metódy vychádzajú z niekoľkých faktov (?):
  - Vymazané dáta nie sú vymazané bezpečné

    (častokrát možná obnova + kedy prišlo k zmazaniu)
  - Zo systému možno obnoviť veľkú časť informácií o tom ako bol počítač používaný
  - Formátovanie disku v skutočnosti veľa dát nezmaže.
  - Informácie o navštívených stránkach www (aj informácie na nich zobrazené) je v mnohých prípadoch možné relatívne ľahko získať

Používané metódy - úvod

- Používané metódy vychádzajú z niekoľkých faktov (?):
  - Správne použitie šifrovania je zložité
    (dáta sú nepoužiteľné pokiaľ sa nedešifrujú)
  - Správne použite steganografie je ešte zložitejšie
    (nepriame náznaky – nainštalovaný stego SW)
  - Odinštalovať správne aplikácie je ťažké
  - Volatilné dáta zostávajú v systéme relatívne dlho (dokonca aj po reštartoch systému)
  - Anti-forenzné a privacy nástroje sú častokrát nefunkčné a nerobia to čo sľubujú

Používané metódy - úvod

- Používané metódy vychádzajú z niekoľkých faktov (?):
  - Častokrát nestačí ani fyzická likvidácia

    (niekedy je aj tak možné obnoviť dáta)

- Dát sa je veľmi ťažké zbaviť

Používané metódy - úvod

- Typy forenznej analýzy
  - Live (In Vivo)
    - Zariadenie je aktívne
    - Často Ad Hoc riešenie
    - Práca Online.
    - Stav systému sa mení aj bez činností súvisiacich s FA aj pri ich vykonávaní → Problem s Chain of Custody
    - Nemožnosť dôverovať aplikáciám a binárkam na danom systéme.
    - Zlatá baňa informácií – pamäť RAM
    - Vysoké požiadavky na expertízu a skúsenosti

Používané metódy - úvod

- Typy forenznej analýzy:
  - Post Mortem
    - Zariadenie nie je aktívne.
    - analýza “iba” média.
    - Stav dát sa nemení.
    - Práca Offline
    - “Jednoduchšie vykonateľná”

      (ale je možné získať menšie množstvo dôkazov)

Používané metódy

- Rôzne stupne volatility dát
  - Cache procesora
  - RAM
  - Swap
  - Pevné disky a USB pamäťové médiá
  - CD/DVD..
- Volatilnejšie dáta treba získať skôr.
- Snaha extrahovať dôkazy.

Používané metódy

- Digitálne dôkazy:
  - Ľubovolná digitálna informácia nachádzajúca sa na dôkazovom médiu:
    - Súbory
      - Aktívne, Zmazané, Fragmenty ..
      - Špecialne Logy a systémové informácie
    - Metainformácie o súboroch
      - Dátumy vytvorenia, zmeny, vlastník súboru …
    - Obsah pamäte RAM
    - Slack Space
    - Swap súbor/partícia
  - Doplnené nedigitálnymi dôkazmi.

Používané metódy
Získavanie dôkazov

- Rozdiel podľa toho, či je zariadenie aktívne.
- Live (zariadenie aktívne):
  - Identifikácia podstatných informácií
  - Kópia vybratých informácií sa presunie na predpripravené médium.
  - Rozhodnutie, či sa zariadenie vypne.
- Post Mortem (zariadenie neaktívne):
  - Bitová kópia dôkazových médií
  - Využívanie blokovačov zápisu
  - Opatrenia v prípade bootovania na sledovanom zariadení
  -

Používané metódy
Získavanie dôkazov

- Zabezpečenie integrity médií:
  - Kontrola hashových odtlačkov kópie a originálu
- Pri HDD kontrola HPA, DCO
- Implementácia v Linuxe(bitová kópia +integrita):

```
dd if=/dev/zariadenie of=SNzal1.iso bs=1M
md5sum /dev/zariadenie ; md5sum SNzal1.iso
```

- Alebo:

```
dcfldd md5log=SNmd5.txt bs=1M if=/dev/zariadenie of=SNzal1.iso of=SNzal2.iso
```

HPA a DCO

- Skryté partície na disku
- Nevidí ich ani operačný systém ani BIOS
- Využívané výrobcami a distribútormi počítačov:
  - Škálovanie diskov
  - Ukladanie počiatočnej konfigurácie počítača a utilít.
- Majú s nimi problémy aj niektoré forenzné nástroje.

Live získavanie dát

- Mám prístup PC a administrátorské práva ?
- Získanie prístupu k zariadeniu.
  - Techniky penetračného testovania.
  - OWASP, ISAAF, OSSTM
  - Backtrack, Metasploit, … :)
- Vytvorenie obrazu pamäte
  - Priamo zo systému (nutné administrátorské privilégiá)
  - Cold Boot Attack
  - Hot Boot Attack

Live získavanie dát

- Využívanie bežiaceho systému na analýzu
  - Čokoľvek môže byť kompromitované
  - Mať k dispozícii dôveryhodné binárky
  - Poznať stretegický význam zariadenia a služieb bežiacich na ňom

Používané metódy
Uchovávanie dôkazov

- Originálne dôkazové materialy sú umiestnené na bezpečnom mieste (napríklad trezor)
- Pracuje sa vždy iba s kópiou dôkazového média.

Používané metódy
Analýza dôkazov

- Neexistuje konkrétny algoritmus (príliš veľké množstvo formátov, dát, diametrálne odlišných prípadov)
- Analýza dôkazov sa skladá z troch častí:
  - "Veda": využitie technických možností na analýzu, vychádzajúcich z poznatkov o práci zariadenia.
  - "Umenie": skladanie častí mozajky do celkového obrazu prípadu.
  - Skúsenosti

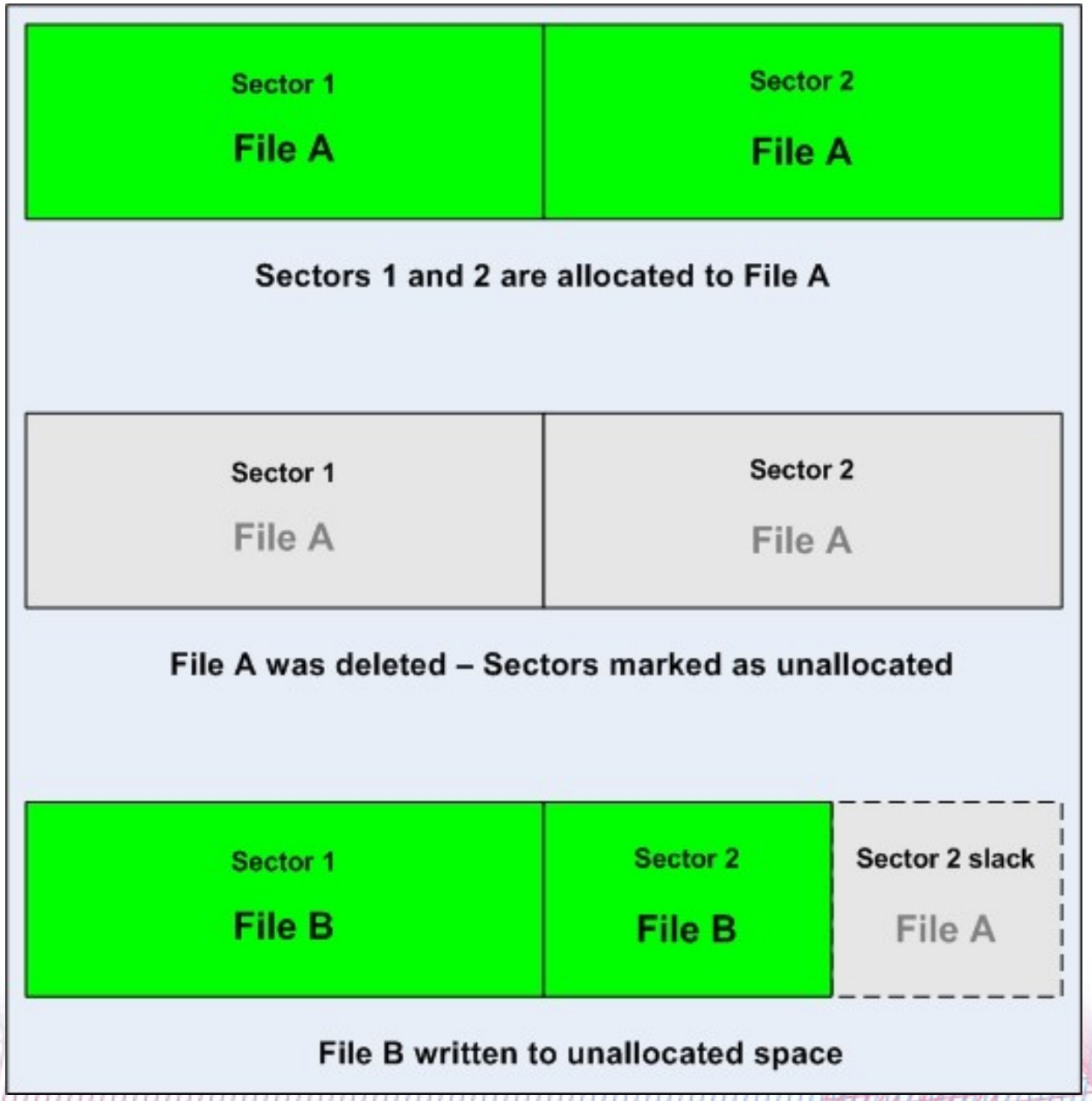
Používané metódy
Analýza dôkazov

- Framework na forenznú analýzu:
  - Získanie prístupu k zariadeniu
  - Obnova zmazaných dát a súborov
  - Sledovanie aktivity užívateľov
    - IM
    - Emaily
    - Navštívené stránky
    - Posledné otvorené súbory,
    - …
  - Vyhľadanie a pokus o dešifrovanie šifrovaných súborov

Používané metódy
Analýza dôkazov

- Framework na forenznú analýzu:
  - Preskúmanie swap, slackSpace, hibernačných a dočasných súborov.
  - Vyhľadávanie podľa kľúčových slov.
  - Kategorizácia informácií a ich redukcia
  - Prehliadanie informačných zdrojov.
    - Databáza Registry, logy, databaza SQL etc.

Slack Space


Sector 1
File A
Sector 2
File A
Sectors 1 and 2 are allocated to File A
Sector 1
File A
Sector 2
File A
File A was deleted – Sectors marked as unallocated
Sector 1
File B
Sector 2
File B
Sector 2 slack
File A
File B written to unallocated space

Databáza Registry

- Zlatá baňa na informácie
- Viacero súborov (Windows XP)
  - NTUSER.dat
  - System, Software, SAM,...
- Obsahuje
  - Spustené aplikácie od inštalácie Windows (UsserAssist)
  - Používateľské mená
  - Informácie o nainštalovaných súboroch
  - Informácie o pripojených externých médiách (USB)
  - Naposledy otvorené súbory

Získanie prístupu k zariadeniu

- Live analýza (popísané vyššie)+
  - Dôležité najmä ak je disk šifrovaný
  - Možnosť obísť Full disk encryption
- Post mortem analýza
  - Často nie je potrebné vykonať tento krok (iba ak je potrebné nabootovať systém)
  - Využitie Rainbow table útoky (Windows)
  - Nastavenie administrátorského hesla

Obnova zmazaných dát a súborov

- Obnova súborov z Koša
- Obnova súborov prostredníctvom čŕt filesystému
  - DOS / Windows: FAT, FAT16, FAT32, NTFS
  - Unix: ext2, ext3, Reiser, JFS, …
  - Mac: MFS, HFS, HFS+
- Obnova súborov z povrchu disku na základe

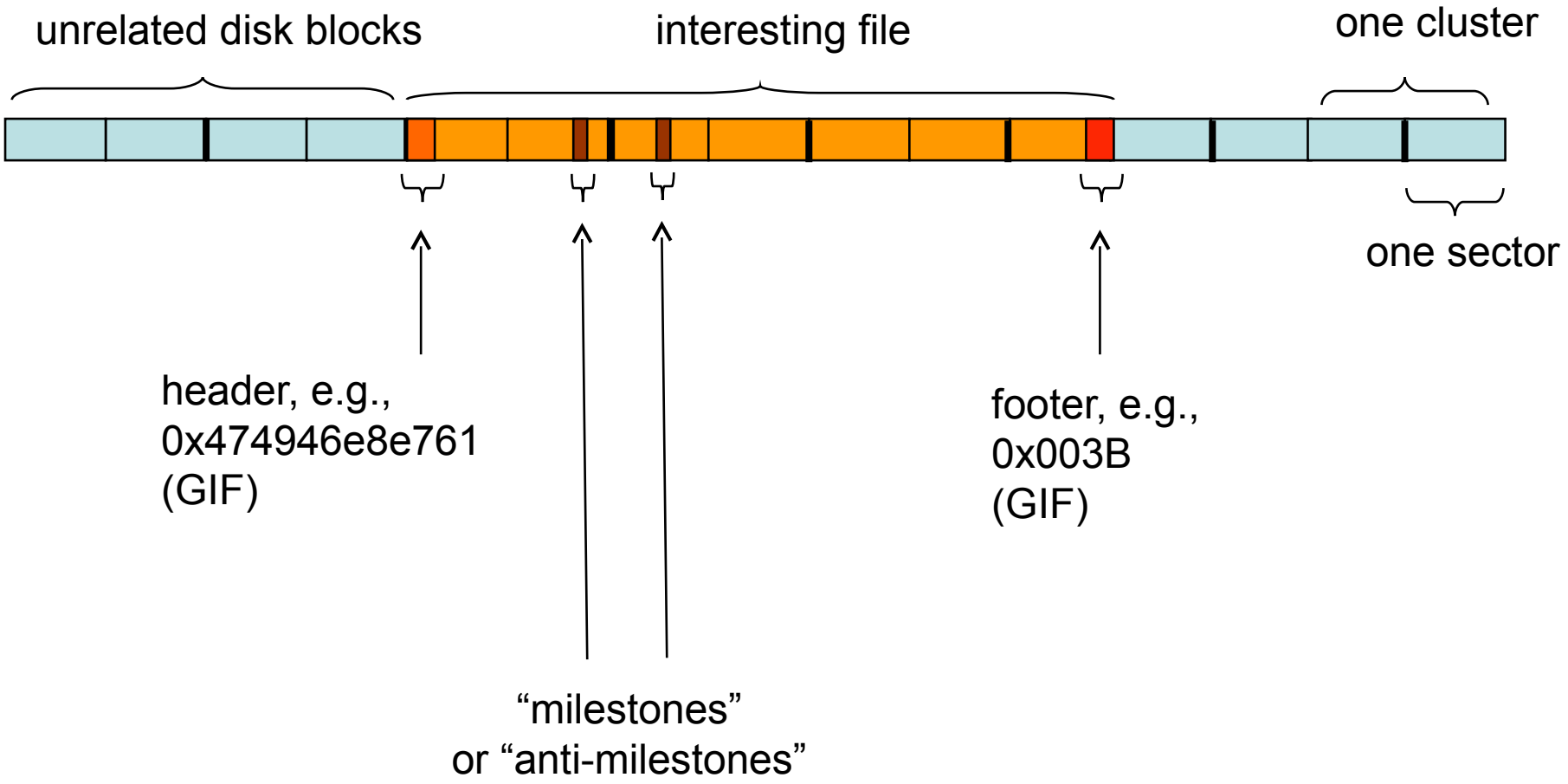
Obnova zmazaných dát a súborov

- Žiadny z filesystémov nepremazáva priamo časti disku, ktoré obsahujú dáta
  - Toto je možné použiť na obnovu.
  - Automatizované nástroje
    - DiskDigger (Windows)
    - Photorec (Linux/Unix)
    - FATWalker, NTFSWalker (Windows)

File Carving

- Obnova súborov z povrchu disku na základe jeho štruktúry.
- Väčšina typov súborov má rozoznateľnú štruktúru
  - Štandardizovanú hlavičku a pätičku
  - Prípadne ďalšie znaky
- Možnosť vyhľadávať priamo na disku pomocou grep a sed.
- Existujú špecializované nástroje
  - Foremost (linux/unix)
  - Disk Digger (Windows)

File Carving: Basic Idea



File Carving

- Problematický ak je súbor fragmentovaný.
- Existencia špecializovaných nástrojov riešiaci problém fragmentovaných súborov (SMARTCarving)

Ďalšie často používané techniky

- Obnova partícií
- Extrakcia kryptografických kľúčov z pamäte
- Obnova súborov z pamäte RAM
- Vytváranie slovníkov hashových odtlačkov.
- Odchytávanie packetov a rámcov (sniffing)
- ...

Dostupné nástroje.

- Komerčné nástroje:
  - Encase
  - FTK
  - SMART Linux
- Open Source nástroje
  - dd, strings, grep, find.....
  - Autopsy
  - PyFlag
  - Wireshark
  - XPlico

Antiforenzné počítanie - princípy

- Útoky na proces Forenznej analýzy
  - Vymazávanie dát.
    - Pozor na bezpečné vymazanie.
  - Znemožnenie prístupu k dátam.
    - Šifrovanie. Pozor na správne použitie.
  - Skrývanie dát
    - Steganografia. Najlepšie vytvoriť vlastný algoritmus.
  - Skrývanie aktivity užívateľa na sieti a na zariadení
    - Vymazávanie logov.
  - Znehodnotenie dôkazov

Antiforenzné počítanie – prípadová štúdia

- Full Disk Encryption
  - Spoľahlivý software (najlepšie open source)
    - Truecrypt,DiskCryptor
    - Niektore distribúcie Linuxu majú integrovanú podporu (Alternative CD Ubuntu, Fedora)
  - Dostatočne dobré heslo.
    - Problém so slabými heslami
  - Podpora Plausible Deniability

Antiforenzné počítanie – prípadová štúdia

- Anonymizéry.
  - Nástroje, ktoré sa snažia maskovať cieľ aj zdroj
  - Tor
- Korektné vymazávanie údajov
  - Ak je potreba niečo dobre zmazať je potrebné vymazať aj volné miesto, swap a slackspace.
- Skrývanie aktivity na zariadení.
- Čo možno najviac dát uchovávať iba v pamäti
  - RAMdisky

Ďakujem za pozornosť
Priestor pre Vaše otázky.