Forenzná analýza IKT

Mgr. Lukáš Hlavička
CSIRT.SK

Agenda

- Motivácia
- Proces forenznej analýzy
- Používané metódy
- Sieťová forenzná analýza
- Nástroje
- Antiforenzné počítanie - princípy

Motivácia

- Bezpečnostné incidenty, ktoré je treba vyriešiť a podľa možnosti zabrániť ich opakovaniu
- Rozvoj počítačovej kriminality
  - Prenos nepočítačovej kriminality do virtuálneho sveta

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

    (hacking, krádeže identity, softvérové pirátstvo)

Motivácia

Lockhardov princíp:

Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent.

Only human failure to find it, study and understand it, can diminish its value.

Cieľe forenznej analýzy

- Na počiatku je (najčastejšie) 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.

Využitie 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.

Využitie 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))
  - Problematické oprávnenia.

Proces forenznej analýzy

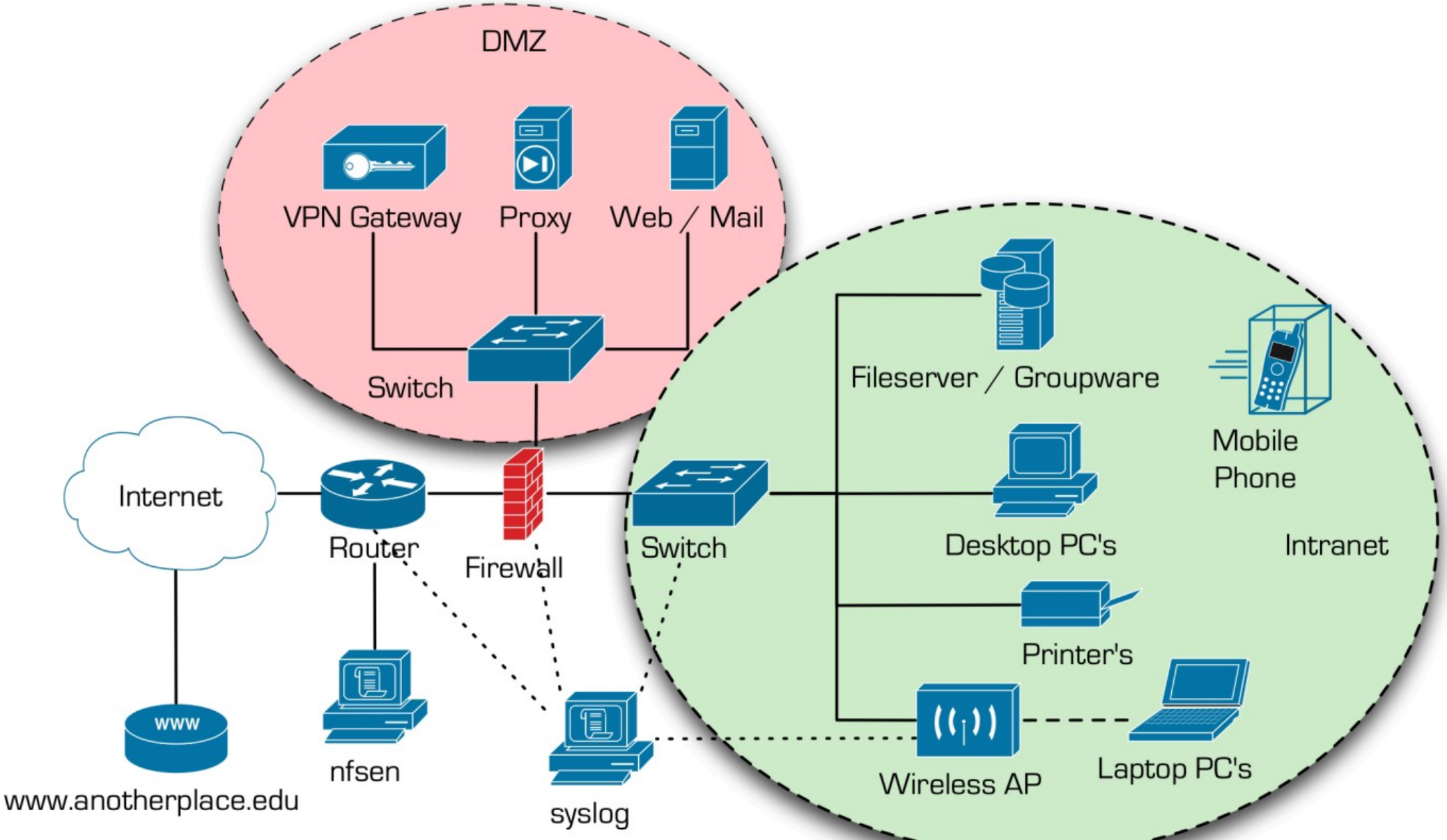
- Príprava
- Otvorenie prípadu
- **Získavanie dôkazov**
- Bezpečné uchovanie dôkazov
- **Analýza dôkazov**
- Vytvorenie hlásenia
- Uzatvorenie prípadu
- Svedectvo

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)

Odkiaľ získať dôkazy ?

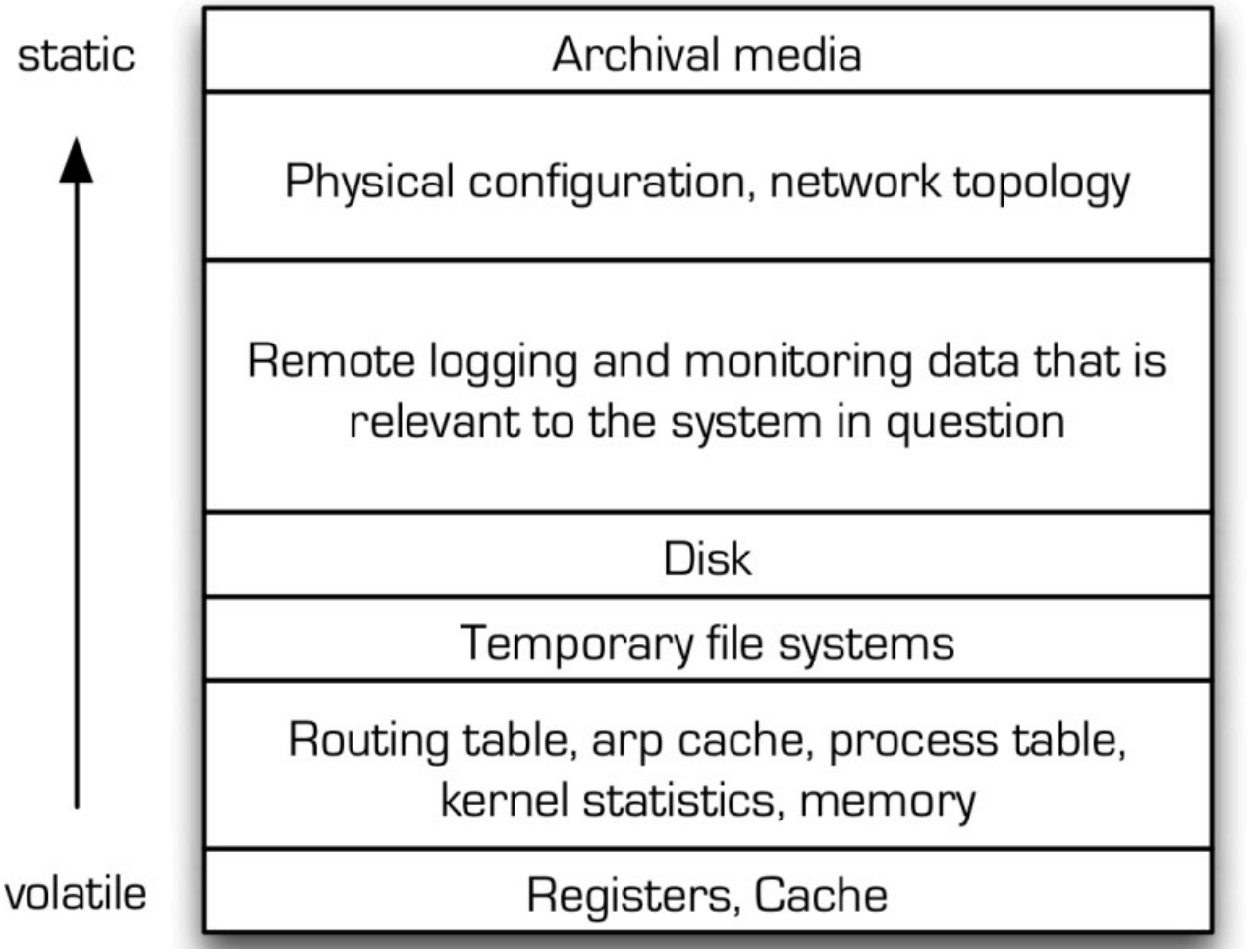


Odkiaľ získať dôkazy ?

- Pevné disky, flash disky, CD, DVD
  - Je potrebné vytvoriť bitový obraz HDD
- Operačná pamäť
  - Pri zapnutom zariadení
  - Je potrebné čo najmenej meniť jej obsah
- Sieť
  - Vzdialené zariadenia

Ktoré dôkazy získavať prvé ?

- Taken from http://www.faqs.org/rfcs/rfc3227.html: Guidelines for Evidence Collection and Archiving



Používané metódy (pre pracovnú stanicu alebo server)

- 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(pre pracovnú stanicu alebo server)

- 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 (pre pracovnú stanicu alebo server)

- 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 (pre pracovnú stanicu alebo server pripojený do siete)

- Používané metódy vychádzajú z niekoľkých faktov (?):
  - Zariadenia, ktorými prechádzajú rámce, resp. pakety si často ukladajú logy, ktoré uchovávajú relatívne dlho.
  - Zariadenia, ktoré poskytujú služby si často ukladajú logy, ktoré uchovávajú relatívne dlho.
- Dát sa je takmer nemožné 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
    - 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
Požiadavky (najmä pre súd)

- Opakovateľnosť
  - Vyšetrovanie (a každú jednu metódu) môže zopakovať expert na základe dokumentácie
- Akceptovanosť
  - Daná metóda musí byť akceptovaná ako správna.
- Spoľahlivosť
  - Metóda musí vedieť dokázať, že jej výsledky sú správne.
  - Súvisí s akceptovanosťou.

Používané metódy
Požiadavky (najmä pre súd)

- Integrita
  - Dôkazy nie sú pri procese FA zmenené.
  - Ak sú → Potreba odhadnúť veľkosť zmeny a akceptovateľne ju zdôvodniť.
- Dokumentácia
- Logická súvislosť
  - Ako súvisí zistenie s prípadom ?
  - Aká je relevancia zistenia ?

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

- Sanitácia médií:
  - Príprava médií na forenzné použite.
  - Týka sa prepisovateľných médií.
  - Štandardy DOD 5220-M a Nist 800-88
- DOD 5220-M
  - Popisuje bezpečné vymazanie média.
  - V súčasnosti zastaralý → Nist 800-88
  - Algoritmus:
    - Prepíš dáta náhodným bytom.
    - Prepíš dáta komplementom bytu
    - Prepíš dáta náhodným reťazcom

Používané metódy
Získavanie dôkazov

- DOD 5220-M Implementácia v Linuxe

```
# prepísanie zariadenia bytom 0x53
cat /dev/zero | tr '\000' '\123' | dd of=/dev/zariadenie
# prepísanie zariadenia bytom 0xAC
cat /dev/zero | tr '\000' '\254' | dd of=/dev/zariadenie
# prepísanie zariadenia náhodnými dátam pomocou generátoru /dev/urandom
dd if=/dev/urandom of=/dev/zariadenie
```

- Aby bolo možné médium ďalej používať:

```
dd if=/dev/zero of=/dev/zariadenie
```

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

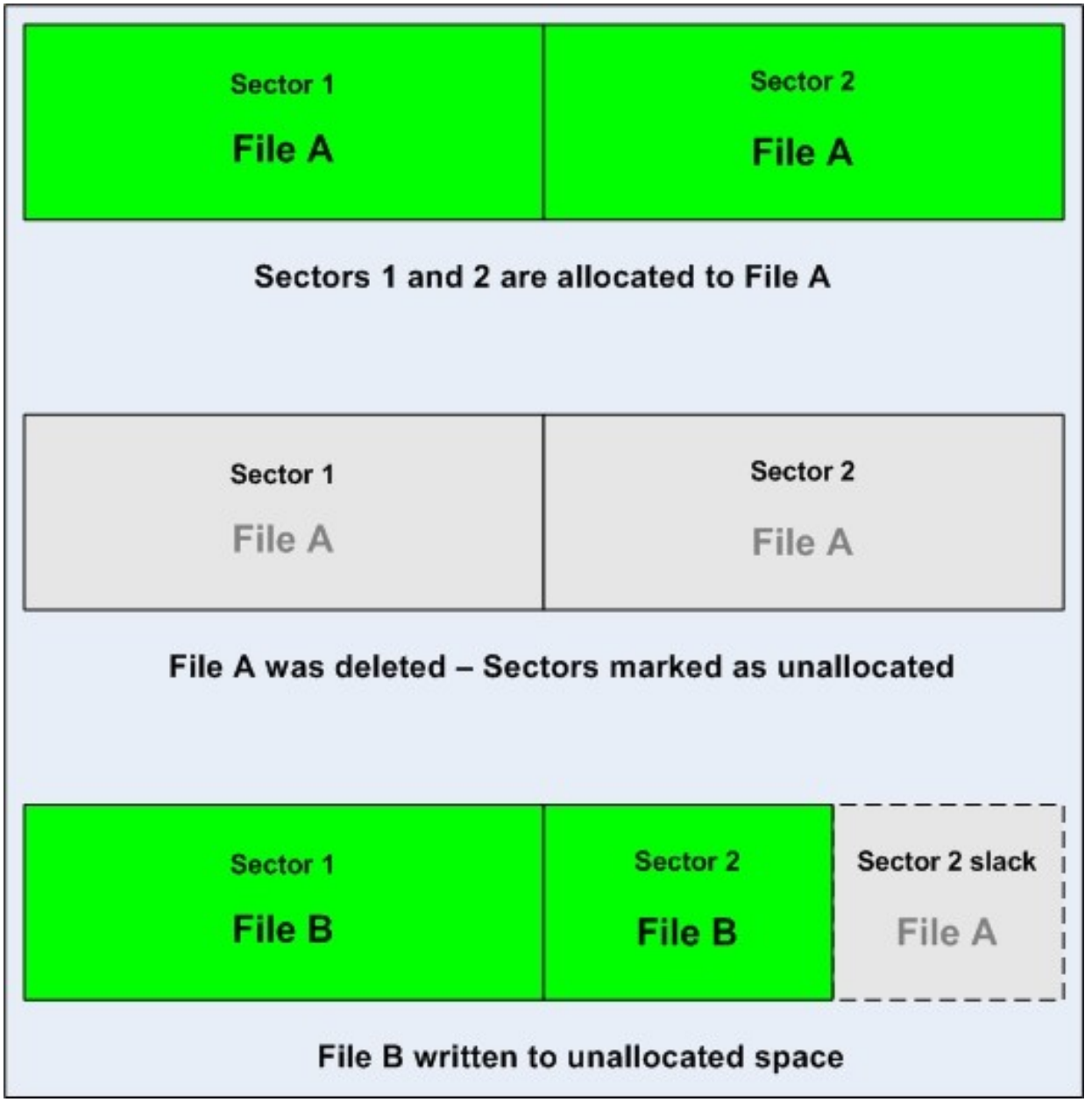
Používané metódy
Analýza dôkazov

- 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

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 hlavičiek a pätičiek

Vymazávanie vo FS

FAT . Súbor vo FAT filesystéme pozostáva z troch častí:

- Záznam vo File Allocation Table: obsahuje postupnosť clusterov, ktoré obsahujú konkrétny súbor.
- Záznam v adresári: obsahuje meno súboru a cluster v ktorom súbor začína(je to zároveň aj odkaz do FAT tabuľky).
- Clustre na médiu obsahujúce obsah súboru.

Pri zmazaní súboru je zodpovedajúci záznam v adresári označený znakom 0xE5 a uvolnením zodpovedajúceho záznamu vo FAT tabuľke.

NTFS Súbor v NTFS filesystéme pozostáva z dvoch častí:

- Záznam v tabuľke Master File Table (MFT).
- Clustre na médiu obsahujúce obsah súboru.

Pri zmazaní súboru sa vymaže záznam z tabuľky MFT.

Vymazávanie vo FS

ext2 Súbor v ext2 filesystéme pozostáva z:

- i-node.
- Dátové bloky obsahujúce obsah súboru.
- Záznam v inode bitmape, že daný inode sa používa.
- Zázanmy v block bitmape, že dané bloky sa používajú.

Zmazanie súboru prebieha iným spôsobom ako v hore uvedených file systémoch. V inode je ako jedna z položiek uvedená hodnota *link count*. Táto hodnota označuje počet miest, ktoré vo filesystéme odkazujú na daný súbor. Pri zmazaní jedného miesta vo filesystéme systém zavolá operáciu *unlink* na inode, ktorý dané miesto reprezentuje. Operácia *unlink* zníži položku *link count* o 1. Ak je po ukončení *unlink* hodnota *link count* rovná nule, systém nastaví dátove bloky priradené k danému inode ako nepoužívané (ak nie je práve otvorený)[34].

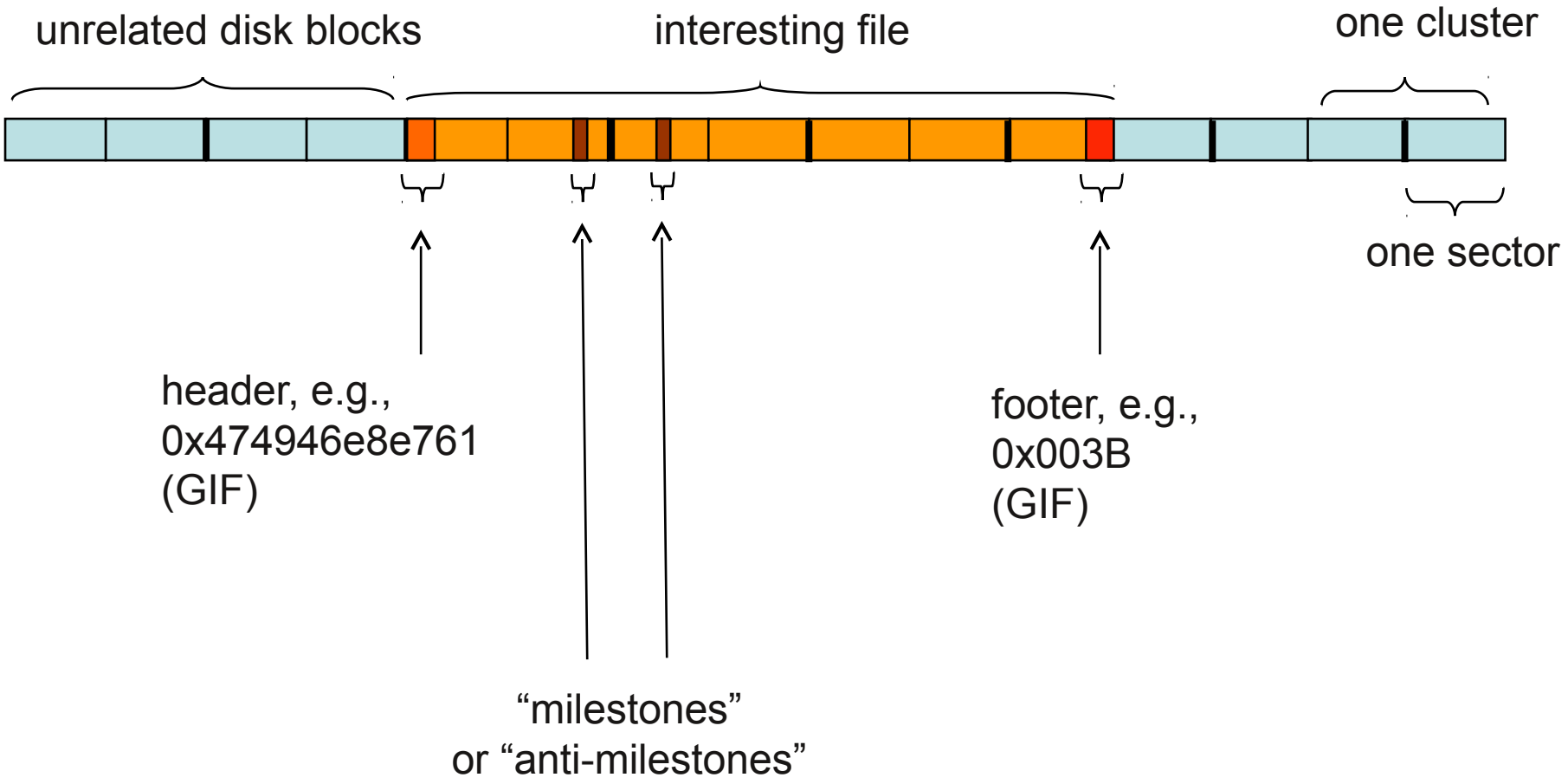
Obnova zmazaných dát a súborov

- 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.