Osnove digitalne forenzike

Digitalni dokaz je katerikoli digitalni podatek, ki ej shranjen ali prenešen in omogoča dokaj ali zanikanje.

Računalniški sistemi :

- odprti računalniški sistemi - računalnik,
- komunikacijski sistemi - router,
- vgrajeni sistemi - projektor.

Za izvajanje forenzične preiskave ni dovolj znanje, ampak se zahteva certificiranost osebja, organizacije, laboratorija, ...

Izmmenjava dokaza :

- Prstni odtisi, e-pošta in zabeležke, zabeležke o obiskovanih straneh, komunikacijske sledi, ...
- Izmenjava dokaznega gradiva med žrtvijo in storilcem (ali prizoriščem) - Locardov princip izmenjave

Dokazi

Dokazi imajo skupne lastnosti (vsi programi te vrste) in posebne lastnosti (konkretne nastavitve)

Da je digitalni dokaz sprejemljiv na sodišču:

- mora biti pravilno obdelan (zajet)
- mora biti hranjen na forenzično pravilen način

Zato je potrebno beležiti vse akcije na prizorišču

Zagotavljanje avtentičnosti:

- vsebina mora biti nespremenjena
- vsebina mora izvirati s prizorišča (beleženje vrstnega reda posedovanja dokaza - dokazna veriga)
- dodatne informacije o rokovanju z dokazi

Celovitost dokaza

sprejeta oblika zagotavljanja cleovitosti dokaza je pospisovanje z razpršilno funkcijo MD-5, SHA

Ravnanje z dokazi

Objektivnost dokaza- vsebuje interpretacijo in predstavitev dokaza

Ponovljivost analize dokaza

Izzivi rokovanja z digitalnimi dokazi

Ostanki ali rekonstrukcija ni isto kot celotno gradivo:

- rekonstruirana datoteka ki ej bila izbrisana ni isto kot delčni le-te
- ostanki poslane e-pošte ni isto kot celotna e-pošta

Povezava med (digitalnim) dokazom in storilcem ni vedno očitna

Podatki niso večni:

- podatki o prometu na omrežju

Dokazi niso nujno brez napak:

- administrator je že poskušal rešiti pobrisano datoteko
- sistemski administrator je sremenil vsebino, da bi zavaroval sistem
- prišlo je do napake pri zajemu podatkov (nestandnardni postopek)
- pri zajemu podatkov je bil uporabljen okužen medij
- medij se je poškodoval, ...

Razvoj jezika raziskave računalniških zločinov

Na začetku ni bilo računalnikov in zakon je ščitil samo materialne dokaze

Digitalni dokazi vsebujejo:

- Računalniška forenzika
- omrežna forensika
- mobilna forenzika

- slabogramje (malware) forenzika

Pomembna razlika med preiskovanjem in analizo podatkov:

- preiskovanje vključuje zaje, ogranizacijo, ...
- analiza predstavlja dejansko obravnavo dokazov

Vloga računalnika

1. predmet (objekt) zločina -> kraja računalnika ali uničenje
2. osebek (subjekt) zločina -> zločin je bil narejen nad računalnikom
3. orodje za pripravo in/ali izvedbo zločina(instrument) -> kopiranje dokumentov
4. uporaba po svojih lastnostih v sločinu (symbol) -> ponujanje storitev ali zmožnosti storitev : dobitki na borzi, ...
5. Vir podatkov -> ostanki datotek, e-pošte, ...

Vloga računalnika -> US Department of Justice

- strojna oprema kot predmet ali rezultat zločina
- strojna oprema kot inštrument
- strojan oprema kot dokaz
- informacija kot predmet ali rezultat zločina
- informacija kot instrument
- informacija kot dokaz

Naloge izvedenca

- predstavitev dokaznega gradiva:
    - ne podleči vplivom
    - odklanjati prezgodaj postavljene teorije
    - raba znanstvene resnice za potrebe pravnega procesa
- ACM code of ethics

- IEEE code of ethics

Sprejemljivost gradiva

Pet osnovnih pravil:

1. relevantnost gradiva za primer
2. avtentičnost grradiva (zajem, sledljivost)
3. niso govorice (heresay)
4. najboljši možen dokaz
5. dokazno gradivo brez potrebe ne napeljuje na zaključke

Nalog za preiskavo

Stopnje zanesljivosti

(1) skoraj zagotovo, (2) zelo vrjetno, (3) vrjetno, (4) zelo možno, (5) možno

Računalniška zakonodaja

Zakonodaja ZDA:

- 50 zakonodaj
- zakonodaja Washington DC
- zvezna zakonodaja

Zakonodaja ES (EU)

- Irska (in Velika Britanija) ločen sistem - common law
- preostale države - civil law

Skupna zakonodaja:

- parlament EU
- Konvencija o računalniških zločinih (Convention on Cybercrime), 1. julik 2004
    - nista ratificirali Irska in VB
- Protokol o dejanjih rasizma in ksenofobije, 1. marec 2006

- GDPR, 2019

Zločini nad intergriteto računalnika

Dostop do računalnika ni dovoljen, če nam tega ne dovoli lastnik

Primeri:

- Hekerji
- Kraja podatkov
- Prestrezanje podatkov
- Vplivanje na podatke in/ali sistem (DOS / virusi)
- "napačna" ali nenamenska uporaba enote/naprave

Zločini s pomočjo računalnika

- Ponarejanje
- Goljufija
- Zloraba

Zločini povezani z vsebino podatkov

Zločini, ki zadevajo vsebino podatkov:

- otroška pornografija
- spletno zapeljevanje
- rasizem in ksenofobija

Ostali zločini

- Kršenje avtorskih pravic
- Računalniško izsiljevanje, ...

Računalnik in OS MS Windows

Zagon računalnika

Koraki b zagonu računalnika:

- Ob zagonu se sproži BIOS (Basic Input Output System)
    - Open Firmware (Mac PowerPc), EFI (Mac Intel), Open Boot PROM (Sun), ...
- Ta naredi POST (Power-On Self Test) - Battery protected, CMOS baterija
- Podatki o delovanju so shranjeni v xROM
- Včasih geslo ščiti podatke - dobiti geslo od uporabnika

Format datoteke

Datoteke imajo na začetku posebne podpise

- jpg: FF D8 FF E0 ali FF D8 FF E3
- gif: 47 49 46 38 37 61 ali 47 49 46 38 39 61
- doc: D0 CF 11 E0 A1 B1 1A E1

Datoteka je lahko gnezdena v drugi datoteki - preučimo vsebino kopirane datoteke

- poiščemo datoteko
- jo lahko označimo in prepišemo (copy-paste)
- ali uporabimo orodje **dd**

Temu postopku rečemo obrezovanje / klesanje (carving)

Druga orodja:

- scalpel, DataLifter
- EnCase, FTK (Forensic ToolKit), X-Ways

Disk:

- V mapi na disku:
    - Seznam vnosov
    - Vsakemu vnosu pripada metainformacija:

        - ime
        - datum
        - ...
- Podatki so shranjeni drugje

Izrezovanje

Na koncu dobimo samo vsebino in ne meta-podatkov iz imenika

Drugi problem je, da so lahko podatki razmetani po disku:

- rešitev: Adroit

Shramba podatkov in skrivanje

V/I enote so priključene na računalnik preko:

- vodila (IDE, ATA, SATA, SCSI, firewire)
- vmesnika (controller)

Vmesniki so lahko tudi pametni:

- SMART (Self-Monitoring, Analisys and Reporting Technology)
- hrani statistike dostopov in ostale podobne podatke
- običajno niso pomembni za forenzično raziskavo

Kako je organiziran disk?

- Plošče, sledi (cilindri), sektorji, gruče

Na prvi sledi, prvem sektorju so nadzorni podatki (MBR - master boot record)

- Velikost (geometrija), slabi bloki, particije,...

Pri SSD:

- Informacije na poziciji 0
- zelo dobro definiran format
- opis preostalega dela diska

Poenostavljena organiziranost diska z datotečnim sistemom FAT:

- disk je bločni niz, razdeljen v particije
    - Lahko skrijemo podatke v bločni niz, ki ni uporabljen v nobeni particiji
- particija ima strukturo
    - lahko podatke skrijemo v particijo, ki je ne uporablja bločni niz

Particija, volume, snopič/del

- V njej datotečni sistem
- lahko tudi brez datotečnega sistema

Načini skrivanja podatkov

Skrivanje podatkov zaradi notranje in zunanje fragmentacije:

- Skrivanje znotraj sektorja (bloka) - težko in neobičajno
- Skrivanje znotraj gruče
- skrivanje znotraj particije (particije se običajno začnejo na začetku sledi)
- skrivanje particije

Kriptiranje particije

Servisni podatki: DCO (Drive/device configuration overlay) in HPA (Host7hidden protected area)

Shramba podatkov

Ko je datoteka izbrisana, podatki ne izginejo

Tudi, ko formatiramo disk, podatki ne izginejo - lahko pogledamo z orodjem **fdisk**

Rezultat obeh operacij jepravilen datotečni sistem in polica praznih blokov

Orodja: **sleuthkit**, Norton DiskEdit

Lahko rekonstruramo datoteke na sveže formatiranem disku z uporabo EnCase

Skrivanje

Skrivanje particij

- Orodje Test Disk

Na ravni datotek:

- Skrivanje datotek: npr. MS Windows: *attrib +H in dir/AH*
- parlament.jpg -> test.exe
- sliko v predstavitev (ppt)

Gesla in kriptiranje

Orodja za razbijanje in iskanje gesel:

- Password recovery tool - PRTK in Distributed Network Attack - DNA
- John the Ripper
- Cain in Abel
- Advanced Archive password Recovery

OS Windows

2 osnovna datotečna sistema: FAT (File Allocation Table) in NTFS (New Technology File System)

FAT:

- Razvit najprej za gibke diske (diskete)
- FAT12, FAT16, FAT32
- FATxx je povezan seznam indeksov gruč, v katerih je shranjena posamezna datoteka
- xx pomeni število bitov uporabljenih za indeks
- O datotekah hrani čas tvorjenja in zadnje spremembe, a le datum zadnjega dostopa

NTFS

- Sodobnejši datotečni sistem:
    - Vse je v datotekah
    - podatke o datotekah hrani v sistemski datoteki $MFT
    - imenik je samo datoteka (B drevesna struktura)

    - je dnevniški datotečni sistem (journal) in hrani transakcije nad datoteko v sistemski datoteki $logfile
- Podpira več funkcionalnosti glede datotek
    - pravica dostopa (ACL - Access Control List)
- bolje varovan, saj hrani kopije podatkov o datotečnem sistemu na večih mestih ($MFTMirr)

NTFS - $MFT

Zapis v $MFT:

- Zapis sestoji iz prilastkov (attributes)
- zapis je velik 1kB
- če je datoteka majhna, se hrani kar v zapisu
- pri brisanju samo zastavica in potem se zapis ponovno uporabi

NTFS - iskanje podatkov

Pri datoteki obstaja pojem fizične velikosti (gruče), logične velikosti (zapis v imeniku - dejanska velikost) in pojem konca datoteke (EOF)

V imeniku lahko obstajajo datoteke z enakimi imeni

NTFS - sledi datotek

- Različne operacije različno vplivajo na zabeležene čase v imeniku (tvorjenje - TV, zadnji dostop - ZD, zadnja sprememba - ZS, zapis spremenjen - VS):
    - premik datoteke v snopiču: ne vpliva nič
    - premik datoteke v drugi snopič: TV, ZD, VS
    - kopiranje datoteke (cilja datoteka): TV, ZD, VS
    - odreži in prilepi: ZD
    - primi in potegni: ZD
    - izbriši: ZD, VS
- posebnosti:

    - datoteka na palčki, lahko preko scp/...: TV > ZS
    - pri brisanju imenika, se podatki o datotekah ne spreminjajo
- Vsebina pisarniških datotek vsebuje metapodatke iz imenika
    - Shrani kot: če na isto datoteko, gre dejansko za prepis in ne za tvorjenje nove datoteke v imenik, ne pa v datoteki
- Tiskanje naprej prepiše datoteko v poseben imenik ter jo še nato natisne
    - C:\Windows\Spool\Printers, C:\WinNT\System32\Spool\Printers
    - tudi, ko tiskamo spletno vsebino
- Zapisi imajo tri dolžine:
    - AS - allocation size
    - FS - file size
    - VDL - valid data length

Kodiranje časa pri datotekah

FAT: 1.1.1980 + LLLLLLLM MMMDDDDD hhhhhmmm mmmsssss - 4 bajte velikosti

FILETIME:

- 64 bitni zapis - 8 bajtni
- vrednost = 1.1.1600 + število * 100ns

Reševanje podatkov

za reševanje izbrisanih datotek obstajajo različna orodja, ki jih lahko poganjamo na MS Windows:

- orodje SleuthKit v kombinaciji z Autopsy Browser omoggoča celo pregledovanje preko brskalnika

Iskanje izgubljenih datotek iz velike neoblikovane gmote rešujemo enako kot pri obrezovanju datotek:

- Orodje DataLifter: iščemo izgubljeno datoteko iz dveh gmot praznega prostora in enega preostalega datotečnega sistema

Če majhna datoteka prepiše veliko, lahko večino velike datoteke rekonstruiramo:

- EnCase: primer nakupovalnega vozička v CD Universe, ki se je znašel v preostanku datotečnega prostora

Zabeležke (log files)

- Operacijski sistem (odvisno od nastavitev) beleži marsikaj:
  - dostopi do virov
  - pojavljanje in brisanje vnosov
  - napake itd.
- Shranjene na %systemroot%\system32\config (c:\winnt\ ...)
  - različne zabeležke v različnih datotekah: Appevent.evt, Secevent.evt, Sysevent.evt

Register

- V OS Windows so spremenljivke okolja procesa definirane v registru
- dejansko so podatki shranjeni v datotekah (hives) v sistemskem imeniku %systemroot%\system32\config
  - ntuser.dat za vsakega uporabnika svoja datoteka
- datoteke lahko pregledujemo z Windows orodjem regedit32 (EnCase, FTK)

Omrežne sledi

- nekaj tudi iz sistemskega okolja
  - ob vzpostavitvi povezave, ...
- Večina izvira neposredno iz aplikacij
  - brskalniki, pošni agenti, ...

Brskalniki

- Zgodovina:
  - firefox-3 je hranil zgodovino v sqlite podatkovni bazi

    - internet explorer hrani zgodovino v index.dat
    - orodja so na voljo za iskanje po teh bazah: Oddesa
- lokalni predpomnilnik
- piškoti

E-pošta

- sledi so odvisne od poštnega agenta, ki ga uporabljamo
    - poslana in prejeta pošta
    - povzeti IMAP nabiralnikov
- vsebina, ki je zanimiva:
    - samo besedilo pošte
    - priponke - MIME format

Drugi programi

- Različni programi puščajo različne sledi
- Omrežno programiranje:
    - Dostop do drugih sistemov
    - dostop drugih sistemov do našega sistema
- Sistemski registri puščajo sledi v registru

Datotečni sistemi na operacijskih sistemih Unix

Operacijski sistem unix

Razvoj skozi zgodovino: System V, HP-UX, BSD, ...

kasneje so se pojavile odprtokodne različice:

- Linux: RedHat, SUSE, Ubuntu
- BSD: FreeBSD, OpenBSD, NetBSD

Standardna datotečna hierarhija

Filesystem Hierarchy Standard - FHS

delo prevzela Linux Foundation

večinoma formalizacija BSD datotečnega sistema

Korenski imenik

- /boot: statične datoteke za boot loader
- /dev: datoteke naprav
- /etc: sistemska konfiguracija specifična za gostitelja
    - /etc/opt: konfiguracija za /opt
    - /etc/X11: konfiguracija za X windows sistem
    - /etc/sgml: konfiguracija za SGML
    - /etc/xml: konfiguracija za XML
- /bin: bistvene uporabniške ukazne datoteke - za uporabo v shell
- /sbin: sistemske datoteke
- /lib: bistvene skupne knjižice in jedrni moduli
- /lib<qual>:: alternativni format bistvenih skupnih knjižnic
- /home: uporabnikov domači imenik
- /root: Home imenik root uporabnika
- /media: namestitvena točna (mounting point) za odstranljive naprave
- **/mnt**: namestitvena točka za začasno nameščen datotečni sistem
- /opt: dodatni paketi za aplikacije
- /srv: podatki o storitvenih aplikacijah (services)
- /tmp: začasne datoteke
- /usr, /var: ločene hierarhije

/usr imenik

- bsebuje datoteke, ki so namenjene samo branju
- jih uporabljajo hkrati različni sistemi
- v njem naj ne bi bilo datotek, ki so sprecifične za določen sistem
- izjema: /usr/local, ki je lokalni imenik določenega sistema

/var imenik

- vsebuje datoteke, ki se spreminjajo skozi čas:
  - poštne in tiskalniške vrste
  - beležke (logs)
  - podatkovja (podatkovne baze, ...)
  - začasne datoteke

Sistemske datoteke

Operacijski sistem je zasnovan tako, da sos sistemske datoteke človeku prijazne -> navadne besedilne datoteke:

- konfiguracijske datoteke: hosts, syslog.conf
  - običajno v imenku etc (/etc, /usr/local/etc, /opt/etc, ...)
- beležke: mail, cups, ...
  - običajno v imeniku log (/var/log, /usr/local/var/log, /op/var/log)

Beležke

V beležkah so ponavadi zapisi po RFC formatu:

- when where who: what

Datotečni sistemi

- imamo imenike in indeksna vozlišča (inode)
- inode ima podobno funkcijo kot FAT in MFT hkrati

- imenik je samo posebna oblika datoteke
    - Imamo še posebne datoteke: povezave (links), cevovode (pipe), vtič (socket)
- Najstarejši: Unix File System - UFS
- mlajša in uporabljena v sistemih linux: ext2 in ext3
    - obstaja tudi ext in ext4
- obstaja še vrsta drugih datotečnih sistemov
    - reiserFS, XFS, gfs, afs, ext4, HSM

Čas v operacijskem sistemu Unix

- čas se meri v sekundah
- hrani se kot število, ki ima začetek 1. 1. 1970 (Unix time)
    - Če je čas je shranjen kot 32- bitno število bo prišlo do preliva 19.12.2038 - Y2K38 problem
- UTC - Coordinated Universal Time: usklajena definicija časa, ki upošteva prestopna leta, prestopne sekunde, ...
    - zadnja prestopna sekunda se je zgodila 31. 6. 2016
    - usklajen čas med večimi atomskimi urami
    - eden od naslednikov GMT

Datotečni sistem UFS

- Definiran in uveden v BSD4.2
- Uporabljen v *BDS sistemih
- Kasneje uporabljen v Solaris OS
- Število inodov je enako številu možnih datotek
- Inodi so kreirani ob kreaciji datotečnega sistema

Imeniška datoteka

- posebna datoteka, ki sestoji iz delov imenika

- System V je imelo predoločeno velikost imenika
- korenski imenik je opisan v inode 2
- vsak imenik ima poseben vnos, ki pove kje je starš

Nadblok

- Nadblok (superblock) hrani opis konfiguracije skupine cilindrov
- raztreseno po disku - na začetku vsake skupine cilindrov
    - da se ohrani konfiguracija, če se en zapis izgubi
- orodje **dumpfs**

Datotečni sistem ext2

- Osnovna struktura podobna kot pri UFS
- Namesto skupin cilindrov, govorimo o skupinah blokov
- imeniki in indeksna vozlišča - kot pri UFS
- orodje za pregledovanje disk: Linux Disk Editor

imeniška datoteka

- posebna datoteka, ki sestoji iz delov imenika
- System V je imel predoločeno velikost imenika
- korenski imenik je opisan v inode2
- vsak imenik ima poseben vnos, ki povej, kje je starš

Nadblok (superblock)

- hrani opis konfiguracije skupine blokov
- raztreseno po disku - na začetku vsake skupine blokov
    - da se ohrani konfiguracija, če se en zapis zgubi
- orodje **dumpfs**

Datotečni sistem ext3

- Avtor Stephen Tweedie 1999 / 2000 / 2001
- Osnovna struktura enaka kot pri datotečnem sistemu ext2:
    - razdelitev na skupine blokov vključno z nadblokom (superblock)
    - imeniki in indeksna vozlišča
    - vodenje evidence o disku
- dodana je možnost hranjenja dnevniške strukture
- osnovni datotečni sistem OS Linux

Dnevniki (logs)

- V dnevnikih se hranijo zapisi o vseh spremembah v datotečnem sistemu
- Dnevniška struktura omogoča tri vrste vodenja dnevnika:
    - celovit dnevnik (journal): hrani se vse; tako metapodatke kot vsebino - najbolj varno
    - zaporedno (ordered): hranijo se samo metapodatki vendar se shranijo po uspešno opravljeni operaciji - srednje varno
    - zapiši (writeback): podobno kot zaporedni, le da se shranjujejo dnevniški zapisi hkrati z dejanskimi zapisi
- dnevnik je zaporedna datoteka
- zapisi so shranjeni pred prvo skupino blokov
- dnevniška skupina je sestavljena podobno kot bločna skupina
    - dnevniški nadblok
    - opisi transakcij
- opis transakcij vsebuje tri vrste blokov:
    - opisni blok (descriptor block): začetek transakcije
    - metapodatkovni bloki : opisi transakcije
    - zaključni blok (commit block): zaključek transakcije

    - preklicni blok (revoke block): če pride do napake in vsebuje seznam blokov v datotečnem sistemu, jih je potrebno ponovno namestiti (restavrirati)
- vsi (tudi nadblok) se prično z magično številko:
    - JFS_DESCRIPTOR_BLOCK 1
    - JFS_COMMIT_BLOCK 2
    - JFS_SUPERBLOCK_V1 3
    - JFS_SUPERBLOCK_V2 4
    - JFS_REVOKE_BLOCK 5

Forenzični viri

- za analizo slike diska uporabljamo samostoječe operacijske sisteme
- uporabljamo SleuthKit z Autopsy Forensic Browser

Osnove računalniških omrežij za potrebe forenzike

Iz zgodovine: ARPANET -> DoD- Department of Defense

TCP/IP: 1973/74

FDDI: lan network preko optike - Fiber

Koncept omrežnih slojev

- vsak sloj je neodvisen od ostalih
- nudi storitve drugim slojem in uporablja storitve drugih slojev

Referenčni modeli

Sloji referenčnega modela OSI: fizični, povezavni, mrežni, transportni, sejni, predstavitveni, aplikacijski

Referenčni model - TCP/IP

- je osnova interneta in *de facto* standard
- nima prezentacijskega in sejnega sloja
- fizični in linijski sloj je združen v t.i. "host to network layer"
- povezavna plast razdeljena na MAC in LLC (IEEE 802)
- Protokoli na slojih:
    - Aplikacijski sloj - TELNET, FTP, SMNP, SMTP, HTTP
    - Transportni sloj - TCP, UDP, ICMP
    - Mrežni sloj - IP
    - Fizični in povezavni sloj - ARPANET, paketni radio, LAN
- Vsebniki enkapsulirajo en protokol v drugega

Fizični in povezavni sloj:

- fizični: prenos signalov
- povezavni:
    - najpogostejši IEEE 802.11
    - združuje različne tehnologije - IEEE 802.3, 11, 15, 16, ...
    - razdeljen na MAC in LLC
        - MAC - *media access control*: različen med tehnologijami
        - LLC - *Link Layer control*: enak za vse tehnologije

Mrežni sloj

- IP (internet protocol - medmrežni protokol) skrbi za transparentno pošiljanje podatkov med mrežami
- dostava ni zagotovljena niti vrstni red dostave
- osnova je skupni naslovni prostor (IPv4, IPv6)
- povezava s povezavnim slojem je protokol ARP (orodje arp)

Prenosni sloj

- prenosni ali transportni sloj
- TCP in UDP osnovna protokola: povezavni in brezpovezavni način delovanja
- TCP predstavlja tok podatkov med procesoma na različnih računalnikih

Aplikacijski sloj

- standardne aplikacije: pošta, splet, novičke, IRC, ...
- nestandardne aplikacije: definira uporabnik

Nekaj osnovnih orodij

- Windows:
    - arp - za gledanje arp tabele (lahko za specifičen IP ali za vse)
    - netstat - Prikaže aktivne TCP povezave, statistike etherneta, IP usmerjevalna tabela, IPv4 statistike (skupaj z IP, ICMP, TCP in UDP protokoli), isto za IPv6
-
    - sockstat - pokaže odprte vtiče
    - netstat tudi obstaja na linux
    - ifconfig - prikaže trenutno konfiguracijo omrežnega vtičnika
    - tcpdump / pcap - prikaže TCP/IUP pakete, ki se pošiljajo po omrežju., pcap je wireshark

Nekaj smernic

1. Podatki so volatilni
2. Komunikacija:
    - Glave
    - komunikacija se zgodi
    - lažno predstavljanje
    - s kom se pogovarjamo

Profesionalna in druga orodja

- Niksun forenzična orodja

- Protokoli za upravljanje z omrežji: snmp, rmon

Protokol SNMP

- snmp v2 in v3
- nepovezavni način prenosa podatkov: UDP
- dve vrsti ukazov:
    - prenos podatkov na zahtevo
    - prenos ob dogodku
- podatki o stanju omrežja se hranijo v MDB in dnevniških zapisih

Vse je v številkah

- FQN(Fully Qualified Name) = www.fri.uni-lj.si => DNS => 212.235.188.25 = IP => se preslika v MAC prek ARP tabele
- storitev DNS preslikuje med črkovnim nizom in številko
    - namesto DNS storitve lahko uporabimo preslikovalno tabelo v datoteki /etc/hosts
- strežnik DNS storitve sprašuje druge strežnike DNS, če česa ne ve
    - datoteka /etc/namedb/named.root
- orodji *dig* in *nslookup*
- DNs storitev uporablja vrata 53
- nimamo storitve, ki bi preslikovala med imenom DNS in 53
    - imamo preslikovalno tabelo v datoteki /etc/services
- sistem poveže aplikacijo s procesom (programom) ob zagonu

In od kje pridejo številke

- svetovni dogovor o številkah
- številke hrani IANA - The Internes Assigned Numbers Authority
    - korenski DNS strežniki
    - vrata

- protokoli

Storitev WHOIS

- potrebujemo strežnik storitve whois
- pove, kdo je lastnik domene
- Ve tudi informacije o lastniku domene, ter naslov, email, državo ipd.

Mobilne naprave

Celični (mobilni) telefoni

- različne tehnologije prenosa podatkov
- včasih predvsem telefoni, danes predvsem računalniki
- bogat vir osebnih podatkov:
  - Kot telefon - komunikator:
    - zgodovina klicev (prihodnih, odhodnih, zgrešenih)
    - zgodovina sporočil SMS in MMS (prihodnih in odhodnih)
  - Kot računalnik:
    - zgodovina podatkov o mestu nahajanja
    - slike, dnevniki, koledarji, ...
    - dostopi do spletnih omrežij - skratka takorekoč vsi podatki, ki se nahajo tudi na običajnih računalnikih

Podatki na celičnem telefonu

- Primer (POCKET-DIAL M FOR MURDER):
  - *Storilec je imel v žepu telefon, ki je poklical ženin med tem, ko je moril žrtev. Na ženini strani se je sprožila zapisovalna naprava (tajnica), ki je vse skupaj posnela.*
- telefoni postajajo sodobnejši, ker vsebujejo več V/I naprav
  - merilci temperature

    - pospeškometri
    - bralniki kreditnih kartic
    - ...
    - uporaba V/I enot je neizmerna; npr. pri določeni temperaturi se sproži akcija
- Telefoni so postali celoviti vgrajeni sistemi
- viri informacij so porazdeljeni povsod

Forenzika mobilnih naprav

- naprave imaojo sposobnejše operacijske sisteme:
    - Android
    - iPhone
    - Blackberry
    - Windows Mobile
- in starejše operacijske sisteme (SYMBIAN, ...)
- naprave so po definiciji omrežne naprave
    - GPRS, CDMA, UMTS, ...
    - IEEE 802.11
    - IEEE 802.15 (Bluetooth)
    - infrardeča komunikacija
    - ...
- dostop do naprave lahko uniči ali spremeni dokazno gradivo
- Podatki so običajno hranjeni v pomnilniških medijih
    - ki jih ni moč brisati, ampak prepisati
    - zaradi omejenega števila zapisovanj zapisovalni algoritmi razpršijo podatke po mediju
    - zato lahko pridobimo precej podatkov, za katere izgleda, kot da so izbrisani

- Zajem podatkov iz naprav:
  - običajno preko podatkovnega kabla
    - potrebno poznavanje protokola
  - včasih je potreben neposreden zajem iz pomnilniškega medija
    - neposredno branje iz čipa
- Naprave sestoje iz dveh delov:
  - naprave kot takšne
  - SIM kartice
- naprava ima enoličen identifikator IMEI(International Mobile Equipment Identity)
- Sim kartice so računalniki:
  - CPU, ROM, RAM
- Vsebujejo ICC-ID(Integrated circuit Card Identifier)
  - MCC (Mobile country code)
  - MNC (Mobile network code)
  - serijsko številko kartice

Podatki o in na napravi

- Na napravi - odvisno od tipa naprave:
  - osnovni telefon
  - pametni telefon
- kje se še nahajajo podatki
  - uporabnikov računalnik
  - operater
  - SIM kartica
- na napravi so lahko shranjeni vsaj

    - naslovi
    - prejeti, oddani in zgrešeni klici
    - prejeti in oddani SMS

SMS kot dokazno gradivo

- Celovita informacija: kdaj poslano / prejeto od koga in vsebina
- ni podatka, kdaj je prvič prebrano
- vpogled možen z orodjem BitPim

Slikovno gradivo

- Pametni telefoni imajo kamero
- slikovno gradivo v EXIF zapisu (običajno)
    - Podatki o napravi, resoluciji, času posnetka, napravi, **geolokaciji**

Dostop do medmrežnih storitev

- mobilne naprave omogočajo dostop do spleta
    - pogosto uporabnik na njih hrani gesla
    - obstaja zgodovina dostopov
    - zebeležke zadnjih dostopov
    - ...
- mobilne naprave omogočajo branje pošte
    - gesla za dostop do nabiralnikov
    - zadnje prejete / poslane pošiljke
    - ...
- druge aplikacije in njihovi podatki
- Na iPhonu so podatki shranjeni v SQLite bazi.

Geografski podatki

- hrani se zgodovina prehodov med baznimi postajami
- GPS naprave lahko hranijo natančne koordinate
- Slike lahko hranijo podatke o tem kdaj in kje so bile posnete - EXIF format

Drugi podatki

- koledar, zapiski, ...

Napadi na mobilne naprave

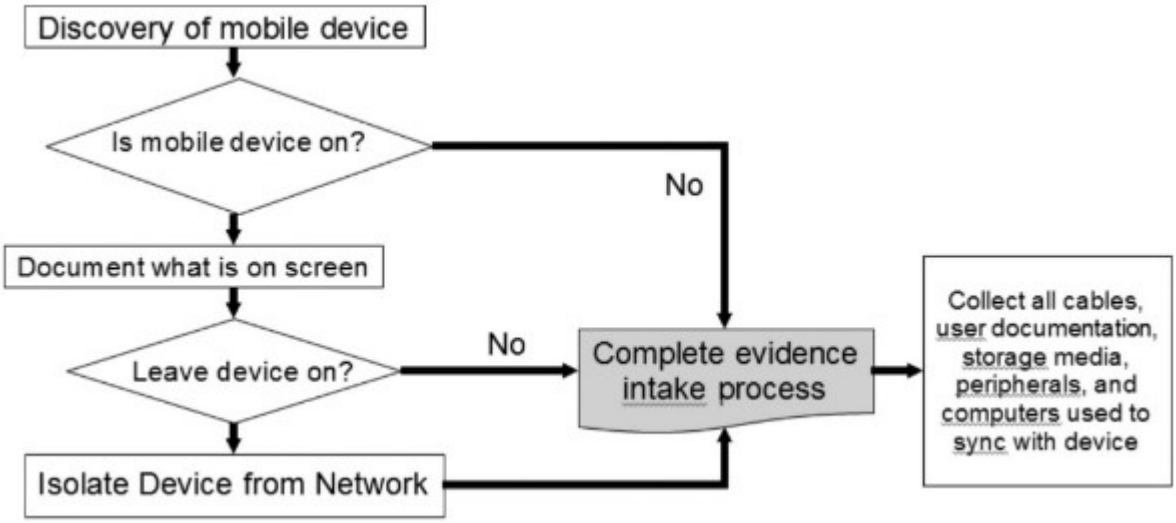
- napadalec naloži svojo kodo na napravo
    - preko omrežja
    - uporabnik naloži aplikacijo, ki sicer izgleda uporabna in prijazna
- aplikacija pobira gesla, ...
    - omogoči dostop napadalcu do bančnih računov
    - glej MobileSpy

Misli širše

- dodatni podatki:
    - uporabnikov računalnik
    - operater: klicni center in bazne postaje
- naprave, o katerih uporabnik nekaj ve (tranzitivnost)

Rokovanje z napravo

- naprava se lahko brezžično poveže s svetom
- napravo je treba onemogočiti:
    - umakniti napajanje
    - drugi načini



- Umakniti pomnilniške module
    - pomnilniški moduli so vedno manjši
- običajno FAT datotečni sistem
    - iPhone: APFS, Android: Linux zasnova
- sicer običajni postopki (podpis, dnevnik, ...)

Pridobivanje podatkov

- različni načini dostopa pri različnih modelih
    - nima vsaka naprava USB vodila
- primeri:
    - preko uporabniškega vmesnika
    - preko komunikacijskih vrat
    - notranjega vodila (Nokia F-BUS, Flash BUS)
    - preko JTAG (Joint Test Action Group) vmesnika
    - preko neposrednega dostopa do čipa
- Nekatere naprave omogočajo agentni dostop
    - ko se naprava zažene, se naloži naš agent, ki prevzame nadzor nad napravo (iPhone)

- včasih lahko prekinemo nalaganje programja in vsilimo našo kodo kot nadaljnje nalaganje
- proizvajalci nudijo programje za arhiviranje podatkov, ki omogoča tudi dostop do izbrisanih in ostalih podatkov
- Naprava, ki je delno uničena, morda še vedno dovolj deluje

Orodja za mobilne naprave

- katerokoli orodje omogoča predvsem dostop do pomnilnika naprave
- pri disku je dostop relativno varen, kar sam po sebi ne more spreminjati vsebine
- pri mobilni napravi to ni nujno res
- posebej pri tujih aplikacijah
- XRY, Cellebrite UFED, Logicube CellDEK,
- Programska oprema za analizo: iXAMMOBILedit!, Forensic, Twister Flasher

Preiskava - datotečni sistem

- odvisno od naprave
    - posebni
    - vgrajeni v sisteme Qualcomm (BREW - Binary Runtime Environment for Wireless)
    - FAT, ext2, ext3, HSFX, APFS, ...
- Na voljo različna orodja: BitPim, Forensic Toolkit - iPhone

Neceloviti podatki

- četudi nimamo vseh podatkov, lahko iz logičnih podatkov rekonstruiramo delno izbrisane podatke
- če je običajen datotečni sistem (FAT, ext2, ext3, APFS, ...) že znana orodja
    - EnCase
- V primeru sestavljenih datotek (MMS, docx, ...) lahko najdemo dele podatkov
- skladiščni medij je SSD

- podatki, ki so v shrambi a niso strukturirani
    - delno zbrisani podatki
    - podatki v zbrisanih blokih, ki so razpršeni po enoti

Oblika datoteke SMIL

- Synchronised Multimedia Integration Language
    - del w3c standarda
    - različice 1, 2 in 3
- vključuje SVG predmete
- omogoča:
    - animacijo, vključevanje drugih slik, modularizacijo,...

Preiskava - ostali podatki

- vleiko pametnih telefonov hrani svoje podatke v podatkovni bazi
    - SQLite - Android, iPhone, Palm, ...
    - cemail.vol - Windows Mobile

Preiskava - format podatkov

- večinoma standardni formati
- SMS sporočila:
    - 7-bitni standatd; GSM 03.38: 160 znakov
    - 16-bitni UCS-2 (Universal Character Set, UTF-16): 70 znakov
- Debeli in tanki konec - odvisno od procesorja
    - Motorola - debeli konec
- debeli in tanki košček (nibble)
    - številka 12036452774 se shrani kot 2130462577F4 (F je polnilo)

Preiskava - SIM kartica

- SIM (Subscriber Identity Module)
- naprava je last uporabnika, SIM kartica je last operaterja
    - ki dovoli uporabniku shranjevanje določenih podatkov nanjo
- podrobna definicija v: ETSI(European Telecommunications Standards Institute) : GSM, Global mobile Communications, GSM 11.11, 1995

SIM kartica

- preprosta notranja struktura
- sestoji iz datotek, od katerih ima vsaka svojo dvo-bajtno identifikacijsko kodo
- prvi bajt označuje tip datoteke:
    - 3F - glavna datoteka (Master File), MF
    - 7F - namenska datoteka (Dedicated File), DF
    - 2F - delna datoteka MF
    - 6F - delna datoteka DF
- nekatere datoteke so definirane v standardu
    - 3F00:7F10 (DFTELECOM, dedicated file: zapisi o uporabi storitev (npr. poslana SMS sporočila, klicane številke)
    - 3F00:2FE2 (EFICCID, elementary file): hrani ICC-ID (integrated Circuid Card ID)
    - 3F00:7F20:6F07 EFIMSI: hrani IMSI (International Mobile Subscriber Identity)
    - 7F20:6F7E (EFLOCI): kako se je kartica premikala med operaterji
    - 7F20:6F53 (EFLOCIGPRS): GPRS usmerjevalno področje
- Orodja za pregledovanje SIM kartic:
    - TULP2G: Nethernalds Forensic Institute
    - orodje ni posodabljano, a za branje SIM kartic je vredu

SIM kartica in varnost

- Kartica je zaščitena s PIN (personal Identification number) kodo

- če se prevečkrat zmotimo (ni možno pregledovanje), se kartica zaklene
- za odklepanje potrebujemo PUK (PIN unlock key) kodo
    - pogosto jo ima operater

Izvajanje digitalne preiskave

- (digitalna) preiskava se izvaja po točno določenih korakih
- koraki so definirani v priročnikih, navodilih

Koraki v digitalni preiskavi

1. *priprava*: priprava načrta preiskave
2. *pregled/identifikacija*: kaj je potrebno zajeti in kako
3. *shranjevanje*: forenzična korektnost zajetega gradiva
4. *raziskava (examination)*: in *analiza*: zajeto gradivo se ustrezno pripravi za analizo, ki temelji na ustreznih znanstvenih metodah
5. *predstavitev gradiva*: izsledke preiskave se ustrezno namenu predstavi (sodišče, v podjetju, vojska, ...)

Poznamo več vrst zaporedij kriminalnih preiskav: Casey 2004, DFRWS 2001, NIJ 2001, NIJ 2004, Cohen 2009

Procesni modeli preiskave - fizični model

- Klasičen pristop (Carrier, 2003)
    1. Zavarovanje kraja zločina - Zavarujemo vhode in izhode in preprečimo fizične spremembe na dokazih
    2. Raziskava kraja zločina - Ob sprehodu skozi kraj identificiramo očitne in krhke fizične dokaze
    3. Dokumentacija kraja zločina - Fotografije, skeči, zemlejvidi dokazov in kraja zločina
    4. Pregled kraja zločina in zbiranje - poglobljeno iskanje fizičnih dokazov

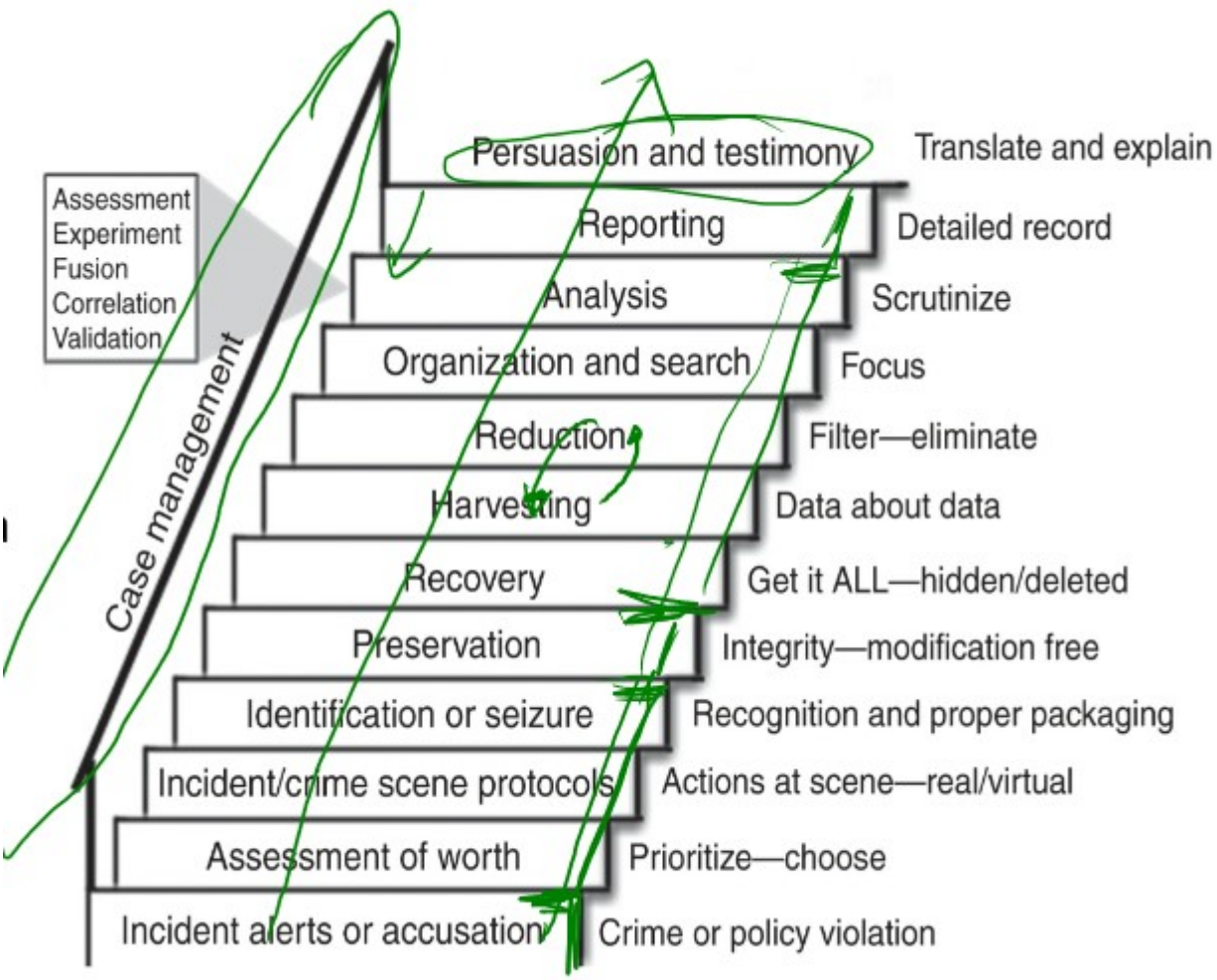
5. Rekonstrukcija kraja zločina - Razvijemo teorije glede na analizi dokazov in testiranja dokazov

- Digitalni pristop (Carrier, 2003):

1. Zavarovanje kraja zločina -Preprečimo spreminjanje morebitnih digitalnih dokazov, vključno z izoliranjem omrežja, zbiranjem volatilnih dokazov in kopiranjem digitalnega okolja
2. Raziskava kraja zločina - Identifikacija očitnih dokazov z raziskovanjem digitalnih dokazov (ponavadi v laboratoriju)
3. Dokumentacija kraja zločina - Fotografije digitalnih naprav in posamezni opisi digitalnih naprav
4. Pregled kraja zločina in zbiranje - Analiza sistema za neočitne digitalne naprave
5. Rekonstrukcija kraja zločina - Razvijemo teorije glede na analizi dokazov in testiranja dokazov

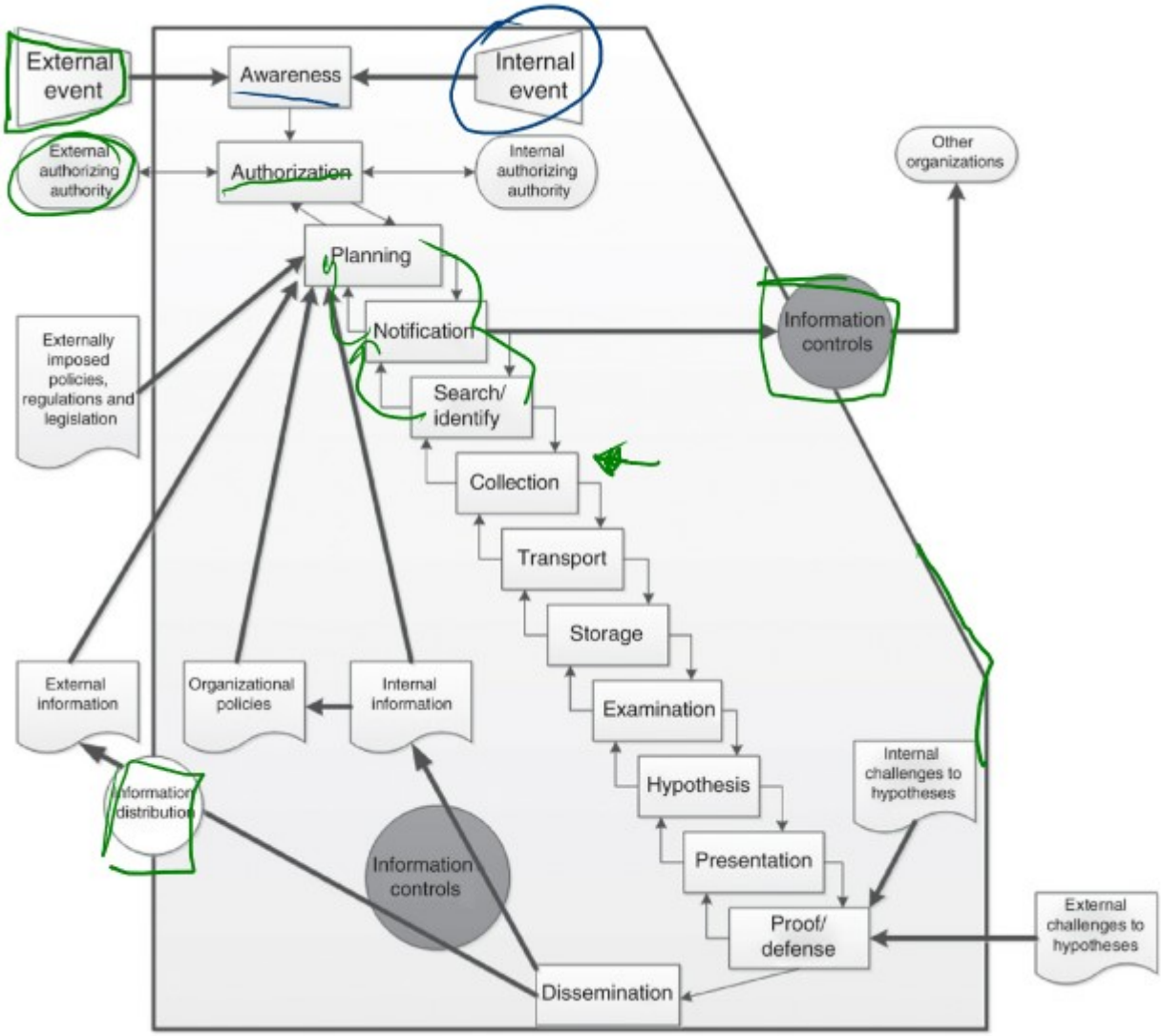
Procesni modeli preiskave - stopničasti model

- Casey in Palmer 2004
- odvetniki in preiskovalci delujejo skupaj
- ni enosmeren tok, ampak se lahko vračamo na prejšnje faze



Procesni modeli preisakve - model toka podatkov

- O Cairdhuain, 2004
- celovit proces od zavarovanja do sodišča
- celotna veriga dogodkov



Procesni modeli preiskave - (pod)fazni model

- Beebe in Clark, 2005
- proces je razdeljen na faze, od katerih ima vsaka točno določene cilje / namen
- osnovne faze so (prim. nazaj):
    1. priprava
    2. odziv na prijavo
    3. zbiranje gradiva
    4. analiza gradiva (podatkov)
    5. predstavitev izsledkov

6. zaključek primera

- primer: cilji analize datotečnega sistema
    1. zmanjšanje količine podatkov za analizo
    2. ocena znanja osumljenca
    3. pridobitev izbrisanih datotek
    4. iskanje relevantnih skritih podatkov
    5. ugotovitev zaporedja dejavnosti z datoteko
    6. pridobitev relevantnih ASCII podatkov
    7. pridobitev relevantnih ne-ASCII podatkov
    8. ocena spletne (e-pošta, brskanje) dejavnosti
    9. pridobitev relevantne e-pošte s priponkami
    10. pridobitev relevantnih drugih podatkov (koledar, adresar, zaznamki, ...)
    11. iskanje natisnjenih podatkov
    12. identifikacija relevantnega programja
    13. iskanje dokazil o neavtoriziranih dostopih (malware)
    14. rekonstrukcija omrežnih dogodkov

Procesni modeli preiskave - model vlog in odgovornosti

- leong, 2006
- FORZA - vsak udečeženec ima določeno vlogo v procesu

Table 2 – A high-level view of the FORZA framework

	Why (motivation)	What (data)	How (function)	Where (network)	Who (people)	When (time)
Case leader (contextual investigation layer)	Investigation objectives	Event nature	Requested initial investigation	Investigation geography	Initial participants	Investigation timeline
System owner (if any) (contextual layer)	Business objectives	Business and event nature	Business and system process model	Business geography	Organization and participants relationship	Business and incident timeline
Legal advisor (legal advisory layer)	Legal objectives	Legal background and preliminary issues	Legal procedures for further investigation	Legal geography	Legal entities and participants	Legal timeframe
Security/system architect/ auditor (conceptual security layer)	System/Security control objectives	System information and security control model	Security mechanisms	Security domain and network infrastructure	Users and security entity model	Security timing and sequencing
Digital forensics specialists (technical preparation layer)	Forensics investigation strategy objectives	Forensics data model	Forensics strategy design	Forensics data geography	Forensics entity model	Hypothetical forensics event timeline
Forensics investigators/system administrator/operator (data acquisition layer)	Forensics acquisition objectives	On-site forensics data observation	Forensics acquisition/ seizure procedures	Site network forensics data acquisition	Participants interviewing and hearing	Forensics acquisition timeline
Forensics investigators/ forensics analysts (data analysis layer)	Forensics examination objectives	Event data reconstruction	Forensics analysis procedures	Network address extraction and analysis	Entity and evidence relationship analysis	Event timeline reconstruction
Legal prosecutor (legal presentation layer)	Legal presentation objectives	Legal presentation attributes	Legal presentation procedures	Legal jurisdiction location	Entities in litigation procedures	Timeline of the entire event for presentation

Zbiranje podatkov

- začetna točka je obtožba ali bovestilo o dogodku
- sledi avtorizacija za izvedbo preiskave
    - avtorizacija na podlagi napotila
    - (sodni) nalog za preiskavo
- triaža primera - odločitev ali so dokazi zadovoljivi
- prenašanje in delo z dokaznim gradivom - dnevniški zapisi
- preverjanje zaseženega gradiva
- vodenje primera - vključuje ostale udeležence

Metodologija dela v digitalni preiskavi

- delo mora sloneti na znanstvenih metodah
    - oblikovanje in preverjanje hipotez
- koraki:
    - priprava na digitalno preiskavo
    - pregled mesta zločina
    - shranjevanje podatkov

    - raziskovanje podatkov
    - analiza
    - poročanje in pričanje

Znanstveni pristop

1. opazovanje (*brskalnik se je sesul in takoj za tem se je pognal antivirusni program*)
2. oblikovanje hipotez
3. predpostavka, kje so dokazi za potrditev hipotez
4. preverjanje hipotez
5. zaključek

Primer: zaposleni je obtožen kraje podatkov ob tem, ko je zapustil službo

Priprava na digitalno preiskavo

1. *opazovanje*: število sistemov, kakšni so sistemi, ...
2. *oblikovanje hipotez*: sistemi uporabljajo ATA in SATA diskovna vodila
3. *preverjanje hipotez*: pregledovanje računalnikov
4. *zaključek*: načrt kako natančno zajeti podatke vključno s potrebno opremo in postopki

- Šele po po zaključku lahko pričnemo z zbiranjem samega gradiva - *ad hoc* postopki niso zaželjeni

Pregled mesta zločina

1. *opazovanje*: pregled mesta zločina
2. *oblikovanje hipotez*: nenavadnosti - zakaj nekaj manjka ali je nekaj prisotno; omejevanmje količine gradiva
3. *predpostavka, kje so dokazi za potrditev hipotez*: hipoteza o pomembnosti podatka in nato predpostavka, kje se nahajajo dokazi
4. *preverjanje hipotez*: preverjanje hipoteze o relevantnosti podatka in njegovem mestu nahanja

5. *zaključek*: zbiranje dokaznega gradiva se izvede

Shranjevanje podatkov

- odvisno od oblike podatkov
    - primer: e-pošta je shranjena na strežniku vključno s 30 dnevnim arhivom
- spet po znanstvenem pristopu

Raziskovanje podatkov

- običanje faze:
    - pregled in triaža podatkov
    - predhodno raziskovanje
    - temeljito raziskovanje
- faze se seveda lahko ponovijo na istih podatkih
- vključuje: pripravo na raziskavo, ogled, forenzično raziskavo, pridobivanje podatkov, izločanje zanimivih podatkov, temeljita raziskava
- Primer:
    1. *opazovanje*: trdi disk vsebuje obilico dokumentov, ki so zanimivi za raziskavo
    2. *oblikovanje hipotez*: dokumenti so v .doc obliki
    3. *predpostavka, kje so dokazi za potrditev hipotez*: če pridobimo vse .doc datoteke, bomo pridobili vse gradivo
    4. *preverjanje hipotez*: pridobimo sicer vse .doc datoteke, a najdemo še .pdf in .tiff
    5. *zaključek*: ko pridobivamo vse dokumente smo naredili zadovoljivo in celovito raziskavo

Analiza

- dejansko znanstveno utemeljen odgovor na vprašanja $\left(k^5 z^1\right)$

: kdo, kaj, kje, kdaj, kako, zakaj

- upoštevamo, da imajo podatki vsebinsko in kontekstualno vrednost

1. *opazovanje*: osumljenec je bil zabeležen na kameri pri dvigu gotovine na avtomatu v bližini mesta zločina neposredno po zločinu. Zločinec je kmalu po zločinu dvignil denar z žrtvinega računa.
2. *oblikovanje hipotez:*
3. *predpostavka za potrditev hipotez:*
4. *preverjanje hipotez:*
5. *zaključek:*

Poročanje in pričanje

- sodišče običajno ni izkušeno o strokovni materiji
- poročanje mora biti natančno in verodostojno ter transparentno
    - pri opisu postopkov
    - pri posredovanju zaključkov

Delo na mestu digitalnega zločina

- digitani so dokazi, zločin je lahko povsem fizičen
- obstajajo priročniki, ki opisujejo postopke za delo na mestu zločina (ali za prikrito opazovanje)

Osnovni princip

1. z nobenim dejanjem se naj ne spreminjajo ali neposredno dostopa do podatkov na napravi
2. če že dostopamo, potem moramo biti sposobni razumeti in predvideti posledice le-tega
3. obstajati mora zapis o vseh dejavnostih, ki jih mora biti tretja stran sposobna preveriti
4. vodja preiskave je odgovoren, da se zakon in ta pravila spoštujejo

- primer: vključevanje naprave, ...

Avtorizacija za preiskavo

- raziskavo delamo po navodilu ali naročanju

    - sodišče, tožilstvo, vodja oddelka, ...
- navodilo ali naročilo mora natančno opredeljevati, kaj raziskujemo in katere podatke smemo zbrati
- primer:
    - preverite, ali je oseba A poslala e-pošto osebi B
    - to navodilo dovoljuje samo zbiranje podatkov o poslani pošti in ne zbiranje vsebine te pošte
    - podobno pri klicih (telefonskih, VoIP, ...)
- sodišče (naredvodejalec) mora / naj bi skrbel za to, da se pri zbiranju podatkov ščiti zasebnost
- osumljenec ni kriv, dokler ni pravnomočno obsojen
    - in še tedaj se mora spoštovati njegova zasebnost

Priprava na delo na mestu digitalnega zločina

- pripravimo načrt dela na mestu zločina
- priprava je izredno pomembna, saj le ustrezna priprava lahko **zaščiti dokazno gradivo**
- **ACPO priporočila**
    - upoštevanje tehničnega znanja osumljenca
    - vključevanje ustreznih orodij in metod
    - upoštevanje ranljivosti podatkov: brezžične in omrežne naprave, delujoče naprave (računalniki), ...

Ogled mesta digitalnega zločina

- digitalni dokazi se lahko najdejo an različnih mestih - pomembna sistematičnost ogleda
- V/I enote, priročniki za strojno in programsko opremo, ...
- izklop naprav
- zapis o izklopu naprave
- natančen popis naprav in njihova vloga

- gesla za dostop in enkripcijo
- zapisovanje posegov v skladu z načrtom

Zavarovanje mesta digitalnega zločina

- nadzor dostopov na mesto zločina:
    - videokamere ipd: ugasniti sistem, da se ohranijo podatki
    - (brezžična) omrežna: ugasniti oziroma odklopiti, da ne pride do nehotenega ali drugega dostopa
- zamrznitev mesta zločina
    - dokaze prepišemo z ustreznimi napravami ter jih podpišemo in shranimo
    - zavarovanje oddaljenih podatkov
    - zavarovanje nedigitalnih dokazov (prstni ali drugi biološki dokazi)
- priprava **načrta** za zavarovanje podatkov
- oddaljeno zavarovanje

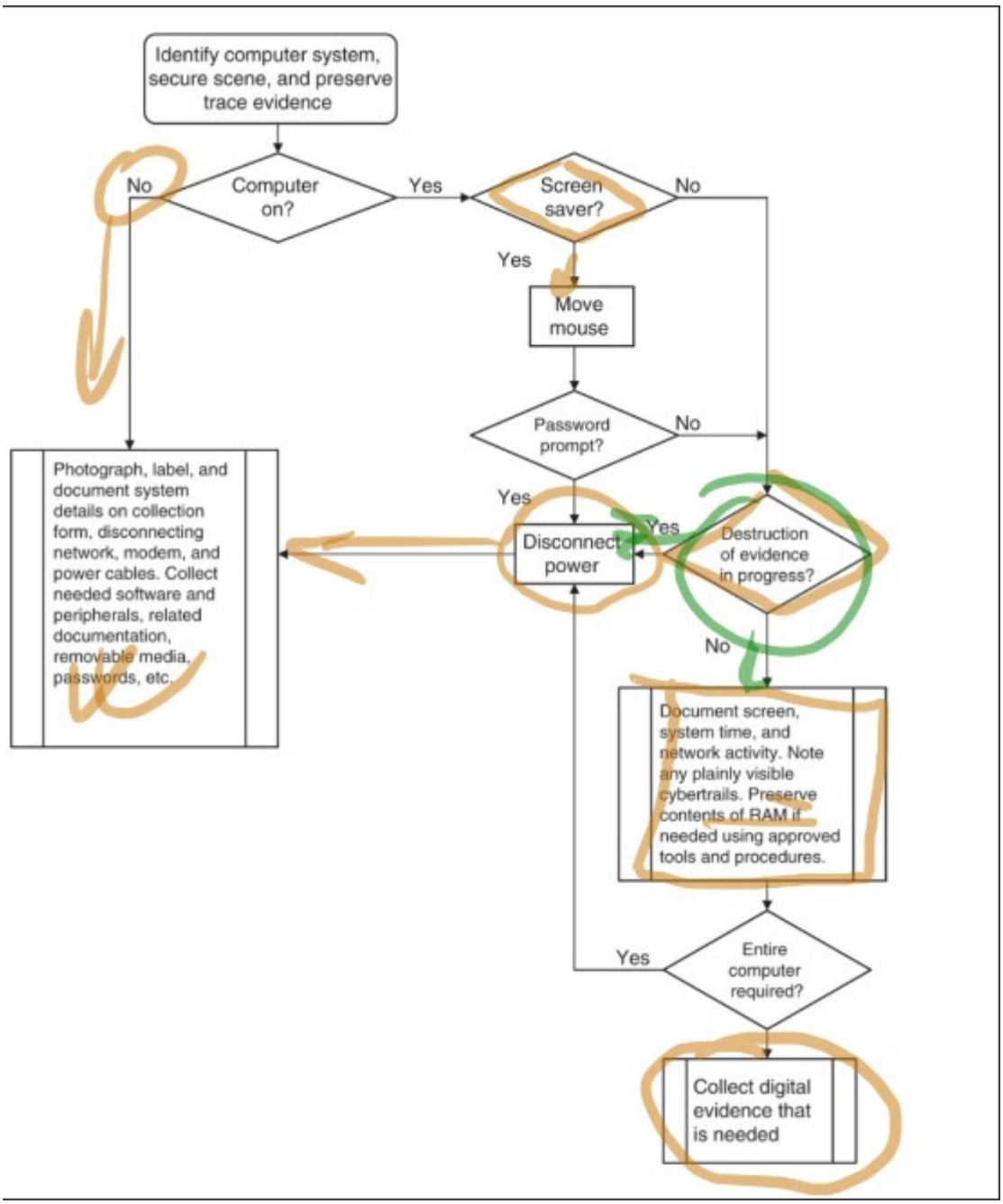
Kaj pa pri delujočih napravah?

- običajno težko ohranimo vsebino glavnega pomnilnika (RAM)
- vendar:
    - trenutno izvajajoči procesi povedo kaj o vdoru v sistem
    - zakriptirani datotečni sistem je priklopljen in gelo vnešeno
    - odklenjeni dostopi do oddaljenih mest oz. storitev
    - ...
- na delujočih napravah uporabimo običajna forenzična orodja (FTK)
- drugo načelo ACPO!!

Zaustavitev sistema:

- odklop elektrike - kje?

- odstranitev ohišja in ogled notranjosti
    - manjkajoči deli, ...
- odklop napajanja na diskih
- pri vseh posegih se zavedajmo sestaljenosti položaja:
    - odklop računalnika lahko sproži eksploziv
- **VEDNO OCENIMO TEHNIČNE SPOSOBNOSTI STORILCA**



Izzivi

Windows datotečni sistemi

Opišite uporabo orodja dd za skrivanje datotek v drugih

Primarna vloga ukaza dd je pretvorba in kopiranje datotek. Lahko jo uporabljamo za skrivanje datotek v drugih datotekah. Primer:

dd zastavice:

- bs (block size) - povečamo, če je podatkov veliko in želimo večjo hitrost
- if (input file) - vhodna datoteka
- of (output file) - izhodna datoteka
- seek n (skip) - preskoči n blokov
- count - pove, koliko blokov naj kopiramo.
- conv (convert) - spremeni datoteko glede na comma seperated symbol list

```
$ cat catpic

 ^ ^
>'.'<
(U U)
$ wc -c # need this later to extract image
18 catpic

$ cat diskimage
Lorem ipsum dolor sit amet, consectetur adipiscing elit,
sed do eiusmod tempor incididunt ut labore et dolore
magna aliqua. Ut enim ad minim veniam, quis nostrud
exercitation ullamco laboris nisi ut aliquip ex ea
```

Nato sliko umestimo v diskimage z odmikom 100

```
$ dd if=catpic of=diskimage bs=1 seek=100 conv=notrunc
18+0 records in
18+0 records out
18 Bytes (18B) copied, 8.5e-05 seconds, 212 kB/s
```

Da pogledamo, če je slika znotraj diskimage, jo ekstrahiramo

```
$ cat diskimage
Lorem ipsum dolor sit amet, consectetur adipiscing elit,
sed do eiusmod tempor incididunt ut labore
 ^ ^
>'.'<
(U U)
iqua. Ut enim ad minim veniam, quis nostrud
exercitation ullamco laboris nisi ut aliquip ex ea

$dd if=diskimage bs=1 skip=100 count=18 2>/dev/null

 ^ ^
>'.'<
(U U)
```

Uporaba orodja dd za razkosane datoteke

Porobno kot v zgornjem primeru, le da moramo veliko datoteko razkosati. To naredimo z ukazom *split*:

```
split myfile # če je datoteka dolga 3000 vrstic,
# bodo izhodne datoteke xaa, xab in xac dolge vsaka 1000 vrstic.


split -l 500 myfile seg # Izhod tega bo 6 500-vrstic dolgih datotek:
# sega, segb, segc, segd, sege, segf


split -b 40k myfile seg # Če je datoteka dolga 160KB, bo vsaka datoteka
# sega, segb, segc, segd dolga 40KB
```

Poiščite orodje anadisk in poglejte, kaj zna in zmore početi

Anadisk je orodje za analizo disket. Uporablja se pri forenzični analizi disket.

Omogoča:

- Varnostni pregled disket za nepravilnosti pri shranjevanju
- Dupliciranje disket, ki so ne-standardne ali imajo nepravilnosti pri shranjevanju
- Urejevanje disket na fizičnem sektoprskem nivoju

- Iskanje podatkov na disketi v tradicionalnih ali ne-tradicionalnih mestih
- Formatiranje disket na ne-tradicionalne načine, da se ponazori skrivanje datotek.

Kakšna je struktura MBR?

MBR ali master boot record je poseben tip zagonskega sektorja na začetku particioniranega medija za shranjevanje. Hrani informacije, kako so diskovni sektorji ali bloki porazdeljeni v particije. Vsaka particija vsebuje podatkovni sistem. MBR tudi shranjuje executable kodo, ki deluje kot nalagalnik za operacijski sistem. Ta MBR koda se imenuje tudi Boot Loader ali zagonski nalagalnik.

Struktura MBR omogoča največje naslovnljivi prostor 2TiB ~2 TB. Uporablja 32-bitno aritmetiko in sektorje velike 512-Bytov.

Preverite konfiguracijo vašega diska

Na Linux komanda:

```
df -H # H naredi izhod human-readable
```

Na windows:

1. Windows key + R
2. MSINFO32
3. Components > Storage > Devices (standardne informacije) / Disks (napredne informacije)

Notri so vse informacije o disku.

Sami poglejte, kako izgleda FAT na vašem disku. Poglejte še posebej tiste gruče, ki so prazne - niso del nobenega datotečnega sistema

Primer sestave 16- bitnega FAT sistema (FAT16)

Example of FAT12 table start with several cluster chains

Offset	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F
+0000	F0	FF	FF	03	40	00	05	60	00	07	80	00	FF	AF	00	14
+0010	C0	00	0D	E0	00	0F	00	01	11	F0	FF	00	F0	FF	15	60
+0020	01	19	70	FF	F7	AF	01	FF	0F	00	00	70	FF	00	00	00

- FAT ID / endianness marker (in reserved cluster #0), with 0xF0 indicating a volume on a non-partitioned superfloppy drive (must be 0xF8 for partitioned disks)
- End of chain indicator / maintenance flags (in reserved cluster #1)
- Second chain (7 clusters) for a non-fragmented file (here: #2, #3, #4, #5, #6, #7, #8)
- Third chain (7 clusters) for a fragmented, possibly grown file (here: #9, #A, #14, #15, #16, #19, #1A)
- Fourth chain (7 clusters) for a non-fragmented, possibly truncated file (here: #B, #C, #D, #E, #F, #10, #11)
- Empty clusters (here: #12, #1B, #1C, #1E, #1F)
- Fifth chain (1 cluster) for a sub-directory (here: #13)
- Bad clusters (3 clusters) (here: #17, #18, #1D)

Poiščite v svojem NTFS sistemu gruče, ki so prazne (neuporabljene) in nato poglejte njihovo vsebino

Katere gruče sestavljajo vašo datoteko? Poiščite zaseden a uporabljen del vaše datoteke (na akterih gručah) in kaj je v njem?

Datoteka je en podatek v datotečnem sistemu, ki ga lahko uporabniki uporabljajo in urejajo. Mora imeti unikatno ime v svojem imeniku. Sestavljena je iz enega ali večih tokov bajtov, ki vsebujejo relevantne podatke plus lastnosti (attributes/properties) - čas urejanja, kreiranja. Vsaka gruča v datoteki ima svojo virtualno številko gruče (VCN - virtual cluster number), ki je relativna odmiku od začetka datoteke. Te gruče so samo relativne.

Kaj se zgodi, če naredimo 1000 datotek, jih nato 1000 pobrišemo in delamo naprej?

Prostor, ki so ga datoteke rezervirale, bo še vedno zapisan na disku, izbrisali se bodo samo logična sposobnost dostopa do teh podatkov. Gruče, ki so bile rezervirane za te datoteke bodo sedaj zopet na voljo.

Najdite datoteko, ki ima čas tvorjenja večji od časa zadnje spremembe

To se lahko zgodi z datotekami, ki smo jih kopirali. Ko kopiramo datoteko, je čas kreiranja enak času modificiranja, trenutni datum pa postane čas kreiranja.

kaj lahko rečete, če ima nakdo takšno datoteko na sistemu in ima čas zadnjega dostopa enak času tvorjenja?

Da je bila datoteka samo kopirana, ni pa bila odprta.

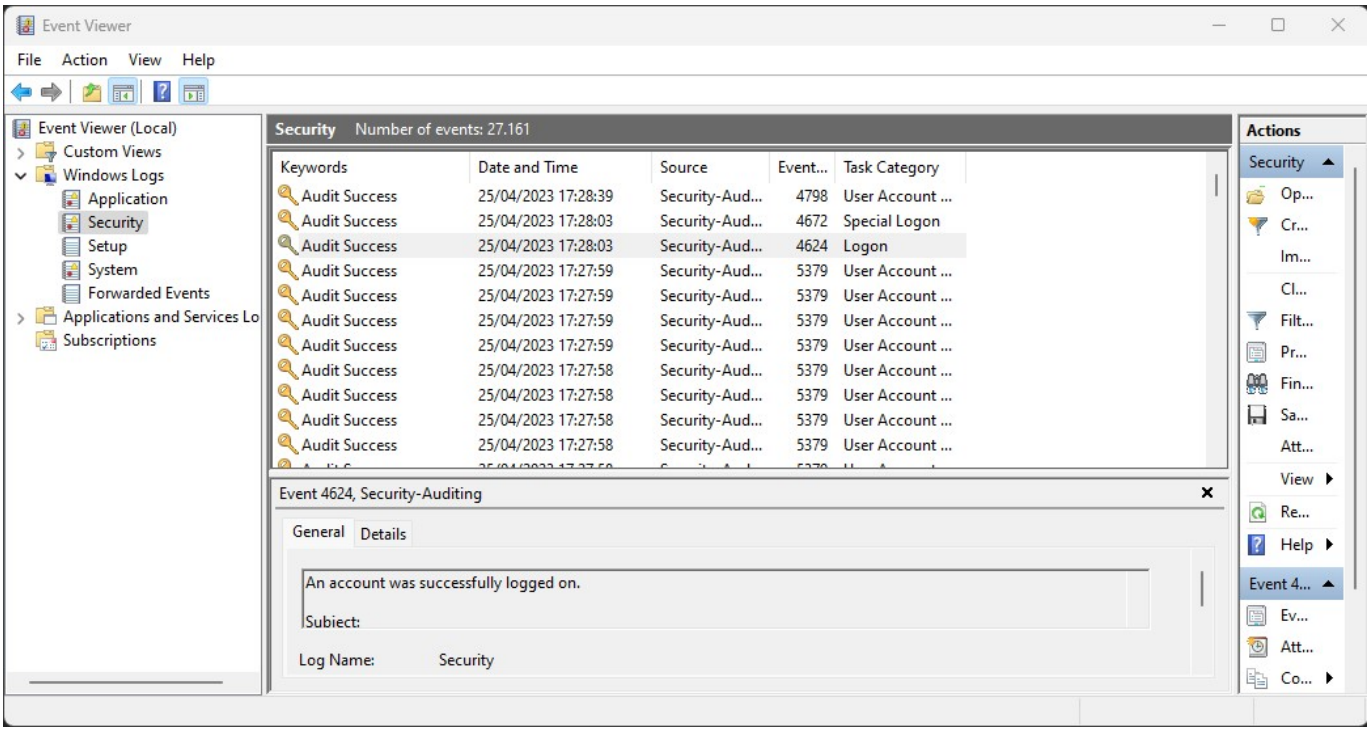
Kaj je to EMF način tiskanja? Kaj se v tem primeru shrani v datoteki tiskalniške vrste (spool)?

EMF ali Enhanced Medafile sestavljajo navodila za klice GDI funkcij. GDI funkcije tiskalni procesor, da renderira slike ki jih lahko tiskamo. EMF je neodvisna od sistema, in je lahko hitrejša od RAW podatkov.

Namestite Sleuthkit in AutopsyBrowser in poiščite izgubljene datoteke.

Preverite format evt datoteke in poglejte, kdaj ste se prijavili v sistem

EVT datoteka je Windowsova datoteka za ogled dnevnika dogodkov. V start napišemo "Event viewer"



Preverite forenzično vrednost podatkov v registru

Lahko preverimo:

- Transakcijske zabeležke registrarja (.LOG) - dejanski entryji v registrarju
- Transakcijski register transakcijskih dnevnikov (.TxR) - task scheduler
- Izbrisani vnosi v registerske "panje" - hives
- Varnostne kopije sistemskih panjev (REGBACK)

- Panji, ki so varnostno kopirani z System Restore.

Poiščite kakšne ostanke v svoje predpomnilniku in jih preverite z zgodovino brskanja

V memory so podatki o brskanju in piškotkih, v disku pa so lahko shranjeni predogledi slik ipd.

Primer pri mozilla:

memory

Number of entries:	81
Maximum storage size:	32768 KiB
Storage in use:	1682 KiB
Storage disk location:	none, only stored in memory

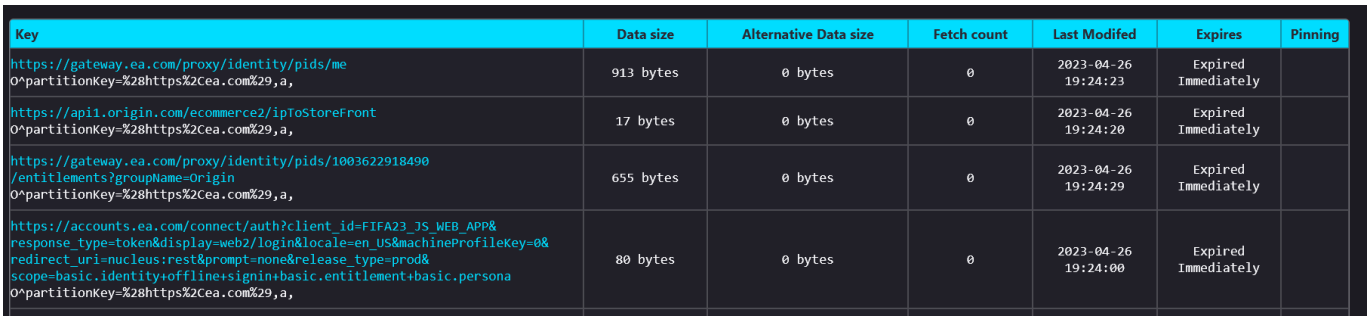
List Cache Entries

disk

Number of entries:	8945
Maximum storage size:	1048576 KiB
Storage in use:	1046738 KiB
Storage disk location:	C:\Users\ivopa\AppData\Local\Mozilla\Firefox\Profiles\kyd1knaw.default-release\cache2

List Cache Entries

Primer memory pri mozilla:



Key	Data size	Alternative Data size	Fetch count	Last Modifed	Expires	Pinning
https://gateway.ea.com/proxy/identity/pids/me O^partitionKey=%28https%2Cea.com%29,a,	913 bytes	0 bytes	0	2023-04-26 19:24:23	Expired Immediately	
https://api1.origin.com/ecommerce2/ipToStoreFront O^partitionKey=%28https%2Cea.com%29,a,	17 bytes	0 bytes	0	2023-04-26 19:24:20	Expired Immediately	
https://gateway.ea.com/proxy/identity/pids/1003622918490 /entitlements?groupName=Origin O^partitionKey=%28https%2Cea.com%29,a,	655 bytes	0 bytes	0	2023-04-26 19:24:29	Expired Immediately	
https://accounts.ea.com/connect/auth?client_id=FIFA23_JS_WEB_APP& response_type=token&display=web2/login&locale=en_US&machineProfileKey=0& redirect_uri=nucleus:rest&prompt=none&release_type=prod& scope=basic.identity+offline+signin+basic.entitlement+basic.persona O^partitionKey=%28https%2Cea.com%29,a,	80 bytes	0 bytes	0	2023-04-26 19:24:00	Expired Immediately	

Podobno je tudi pri disk, razen, da je podatkov več in večji so.

Preverite kakšne vse sledi pušča brskalnik IE, kakšne Mozilla in kakšne Opera

TODO: mislim, da puščajo za sabo podobne podatke.

Unix datotečni sistemi

Čemu je namenjen zapis reclen pri UFS imeniškem vnosu? Se to da izkoristiti za skrivanje podatkov?

Zapis *reclen* nam pove, kakšna je dolžina tega zapisa. Verjetno, lahko reclen zmanjšamo, in tako skrijemo podatke, ki niso pod okriljem te dolžine zapisa. Ti podatki s tem razlogom "plavajo" v disku in o nedostopni, razen, če spremenimo *reclen*, tega inode zapisa.

Kaj je to ACL? Kako je implementiran pri ufs?

ACL (Access control lists), nam omogočajo, da imeniku ali datoteki podamo bolj specifične množice dovoljenj (permissions), brez, da bi (nujno) spreminjali bazno lastništvo ali dovoljenja. Omogočajo, da se na datoteke ali imenike "pripne" dostop az druge uporabnike ali skupine uporabnikov.

Pru *ufs* je implementirana z komando *setfacl*.

Vnosi ACL pri ufs so sledeči:

```
entry-type: [uid|gid]:perms
```

kjer:

- entry-type: tip ACL vnosa, na katerega bi vnesli pravice datoteke (user, mask)
- uid: uporabniško ime ali uporabniški ID (User ID)
- gid: ime skupine ali ID skupine (Group ID)
- perms: Katera dovoljenja ima entry-type. Lahko z *rwx*, ali osmiško številko (isti format kot pri *chmod*).

Poiščite sktukturo nadbloka. Kako vemo, da imamo opravka z UFS datotečnim sistemom? kje to piše? Preberite superblock z vašega unix datotečnega sistema in v njem ugotovite, za kateri datotečni sistem gre.

V nadbloku se shranjuje veliko informacij o podatkovnem sistemu, kot so naprimer:

- Velikost in status podatkovnega sistema
- Značka (label) - podatkovnega sistema in imena volumna
- Velikost logičnega bloka podatkovnega sistem
- Datum in čas zadnje posodobitve
- Velikost cilindrične skupine

- Število podatkovnik blokov v cilindrični skupini
- Povzetek podatkovni blok (Summary data block)
- Stanje podatkovnega sistema: *clean, stable, active*
- Pot do prejšnje bhodne točke (mounting point)

Nadblok lahko pogledamo z uporabo komande:

```
root@localhost: dumpe2fs -h /dev/xvda1
dumpe2fs 1.42.9 (4-Feb-2014)
Filesystem volume name:   cloudimg-rootfs
Last mounted on:          /
Filesystem UUID:          f75f9307-27dc-4af8-87b7-f414c0fe280f
Filesystem magic number:  0xEF53
Filesystem revision #:    1 (dynamic)
Filesystem features:      has_journal ext_attr resize_inode dir_index filetype
needs_recovery extent flex_bg sparse_super large_file huge_file uninit_bg dir_nlink
extra_isize
Filesystem flags:         signed_directory_hash
Default mount options:    (none)
Filesystem state:         clean
Errors behavior:          Continue
Filesystem OS type:       Linux
Inode count:              6553600
Block count:              26212055
Reserved block count:     1069295
Free blocks:              20083290
Free inodes:              6470905
First block:              0
Block size:               4096
Fragment size:            4096
Reserved GDT blocks:      505
Blocks per group:         32768
Fragments per group:      32768
Inodes per group:         8192
Inode blocks per group:   512
Flex block group size:    16
Filesystem created:       Sat Sep 27 13:05:57 2014
Last mount time:          Mon Feb  2 14:43:31 2015
Last write time:          Sat Sep 27 13:06:55 2014
Mount count:              4
Maximum mount count:      20
Last checked:             Sat Sep 27 13:05:57 2014
Check interval:           15552000 (6 months)
Next check after:         Thu Mar 26 13:05:57 2015
Lifetime writes:          305 GB
Reserved blocks uid:      0 (user root)
Reserved blocks gid:      0 (group root)
First inode:              11
Inode size:              256
Required extra isize:     28
Desired extra isize:      28
Journal inode:            8
First orphan inode:       396056
Default directory hash:   half_md4
Directory Hash Seed:      2124542b-ea2f-4552-afaa-c5720283d2cd
Journal backup:           inode blocks
Journal features:         journal_incompat_revoke
```

```
Journal size:             128M
Journal length:           32768
Journal sequence:         0x0151d29d
Journal start:            11415<span style="font-size:16px;">
</span>
```

Poiščite strukturo nadbloka ext2. Primerjajte jo s strukturo UFS superbloka

Oba imata podobno strukturo, glavne razlike pa so:

- Velikost: Velikost UFS nadbloka je 32 bytov, velikost ext nadbloka pa je 1024 bytov.
- Lokacija:Pri UFS je nadblok lociran na zažetku podatkovnega sistema (pod boot block), prri ext2 pa je na fiksnem odmiku začetka podatkovnega sistema.
- Vasnostne kopije: UFS ima več varnostnih kopij nadbloka podazdeljenih po sistemu, ext2 pa ima samo eno na fiksni lokaciji.
- Polja: UFS vsebuje polja (npr. povzetek cilindrične skupine, inode in bločna bitna slika), ki jih ext2 nima.
- Kontrolna vsota: UFS nadblok vključuje kontrolno vsoto, medtem, ko jo ext2 ne.

Oba nadbloka igrata podobno vlogo, le da imata drugačni implementaciji.

Kako dobiti nazaj izbrisano datoteko v sistemu ext2 in kako v ext3? Kaj pa v UFS?

Pri ext2 ni možno pridobiti nazaj izbrisano datoteko, brez bralnega dostopa do dejanske naprave, na kateri je bila shranjena datoteka - moraš imeti root dostop.

Nazaj lahko datoteko dobimo z orodjem TestDisk ali pa "na roke". Obastajata dva nalčina:

- Modificiramo obstoječ datotečni sistem, tako, da imajo izbrisanim inodom odstranimo "deleted" zastavico v upanju, da bodo podatki nazaj.
- Bolj varna, a počasnejša metoda je, da pogledamo, kje se podatki nahajajo v datotečnem sistemu in te podatke zapišemo v drug datotečni sistem.

Pri ext3 dobivanje nazaj izbrisanih datotek ni možno, saj je to varnostna funkcija. Naše najboljše upanje je da *grep*-amo dele datoteke in upamo na najboljše.

Pri UFS je podatke možno dobiti nazaj. Obstajajo orodja kot so UFS Explorer in drugi v FTK.

naredite podrobno analizo za omenjene sisteme (reiserFS, XFS, gfs, afs, ext4, HSM) kot smo jo narediti za UFS in ext.

- reiserFS - znan po učinkovitim raznanjem z majhnimi podatki in metapodatki. Uporablja uravnoteženo drevo za strukturo za organiziranje podatkov in uporablja dnevnike za konsistentnost in obnovitev podatkov
- XFS - visoko-zmogljiv sistem namenjen skalabinosti in visoki podpori za sočasnost. Podpira velike podatkovne sisteme in je zmožen delom z velikimi datotekami, ter omogoča visoko učinkovitost V/I operacij
- GFS(Global File System) - je porazdeljen datotečni sistem, namejen gručam računalniških sistemov. Omogoča večim napravam dostop do skupnega spomina skočasno, kar omogoča visoko stopnjo dostopnosti in uravnoteženjem bremena.
- AFS (Andrew File System) - tudi za porazdeljene sisteme. Uporablja client-server model in podpira avtentikacijo in enkripcijo za varen dostop do podatkov
- ext4 - izboljšana različina ext3, ki omogoča večje podatkovne sisteme in datoteke, hitrejše preverjanje podatkovnega sistema in boljšo zanesljivost. Vključuje tudi kontrolne vsote dnevnikov, kasnejšo alokacijo in hiter *fsck*
- HSM (Hierarchical Storage Management) - Podatkovna struktura, ki kombinira več tehnologij, da optimizira shranjevanje in pridobivanje podatkov. Manj uporabljene datoteke premakne v počasnejše naprave, bolj uporabljene pa v hitrejše.

Primerjajte opisanje datotečne sisteme med seboj - v katerem lahko kje skrijemo kakšne podatke?

Pri nobenem ni priporočeno skrivanje podatkov. Podatke lahko skrijemo v AFS, če modificiramo server in client programje.

Katera orodja so na Helix CD? Podobni sistemi njemu.

Najbrš kakšna dobra.

Osnove računalniških omrežij za potrebe forenzike

Preverite kateri računalniki so v vaši mreži. Kako lahko uporabimo protokol v forenzični preiskavi? Kako s protokolom in še kakšnim orodjem sledimo dogodkom v naši mreži?

Postopek je sledeč:

- Odpremo command prompt / terminal / ...
- Vpišemo *ipconfig* / *ifconfig*, da dobimo naslov našega računalnika, ter naslov omrežja v katerega smo povezani
- Vpiemo *arp -a*, kar pokaže ARP tabelo, za vse naprave v omrežju na vseh omrežjih.
- Nato lahko uporabimo *nslookup* z IP-jem omrežja, kjer iščemo, da dobimo vse naprave na omrežju

S protokolom SNMP lahko sledimo napravam v omrežju. Preverimo lahko dostopnost vseh naprav z *SNMP PING*. SNMP je namenjen upravljanju omrežja.

Lahko pa opravljamo tudi zajem omrežja z orodjem **Wireshark**, kjer lahko opazujemo vse pakete na omrežju.

Poiščite orodja za preiskovanje omrežja s protokolom snmp in preiščite svojo okolico.

Lahko uporabimo SNMP PING, lahko pa uporabimo druge metode, kot na primer Nmap-ovo komando snmp-brute:

```
nmap -sU -p161 --script snmp-brute --script-args snmplist=community.lst
192.168.1.0/24*
```

Poiščite z ustreznim okoljem svoj strežnik DNS storitve in preglejte, kaj vse hrani

DNS strežnik pregledamo z orodjem *nslookup*, ki nam pove podatke o infrastrukturi DNS za naše omrežje.

Komande so sledeče:

Parameter	Description
nslookup exit	Exits the nslookup command-line tool.
nslookup finger	Connects with the finger server on the current computer.
nslookup help	Displays a short summary of subcommands.
nslookup ls	Lists information for a DNS domain.
nslookup lserver	Changes the default server to the specified DNS domain.
nslookup root	Changes the default server to the server for the root of the DNS domain name space.
nslookup server	Changes the default server to the specified DNS domain.
nslookup set	Changes configuration settings that affect how lookups function.
nslookup set all	Prints the current values of the configuration settings.
nslookup set class	Changes the query class. The class specifies the protocol group of the information.

To so samo osnovne komande.

Zajeli ste naslednji paket na omrežju:

09:13:01.839003 IP (tos 0x10, ttl 64, id 13571,

offset 0, flags [DF], proto TCP (6), length 180)

www.brodnik.org.ssh>

AndyMac.gotska.brodnik.org.53845: Flags [P.], cksum

0xf181 (correct), seq 1108696419:1108696547, ack

2653946897, win 1040, options [nop, nop, TS val

2247733168 ecr 1042469077], length 128

Komentirajne vsebino in kdo komu pošilja

Kako se v resnici imenuje DNS storitev v sockstat tabeli?

Pomagamo si lahko s tem, da poslušamo promet na vratih, kjer se pogovarja DNS strežnik. ponavadi so ta vrata 53.

```
sockstat -u -l | grep :53
```

zastavice:

- -u pove, da gledamo UDP povezave
- -l pove, da gledamo poslučalske povezave
- grep :53 - vzamemo samo vrstice, ki vsebujejo ':53'

Če dodamo kakšen vnos v /etc/services tabeli, ali se kdaj spremeni pri sockstat, netstat, tcpdump?

`/etc/services` datoteka se uporablja za pretvarjanje številk vrat v človeško-berljiva imena storitev.

S tem ne vpliva na `sockstat` in `netstat`. pri `tcpdump`, pa se ta imena uporabljajo pri zajemanju paketkov, razen če uporabljamo pri tem samo številke z uporabo `-n` zastavice.

Kako operacijski sistem poveže aplikacijo z vrati storitev? Kako se to naredi na Windows, na FreeBSD in Linux?

Pri različnih operacijskih sistemih to naredimo na različne načine:

Windows:

- Dodamo aplikacijo v seznam dovoljenih aplikacij (manj riskantno) - Samo dovoljena aplikacija lahko "odpre luknjo" v požarnem zidu, ko to potrebuje.
- odpremo vrata (bolj riskantno) - Ko odpremo vrata "preluknjamo" požarni zid in s tem lahko kdorkoli dostopa do našega omrežja prek odprtih vrat.

FreeBSD in Lunx:

- Vse poteka prek vtičev (socket API) programično. Najprej vtič kreiramo, nato ga povežemop z vrati, ter poslušamo, ter sprejemamo pakete. Lahko se tudi povežemo z oddaljenimi vrati.
- Lahko odpremo vrata, kar zahteva administratorske pravice.

Kateri protokol ima številko vrat 50 in zakaj se uporablja?

Port 50 je dodeljen re-mail-ck (Remote Mail Checking) protokolu. Uporablja se za preverjaje e-mail sporočil med klientom in serverjem. Po navadi bi maajhnen program na klientovi napravi skozi vrata 50 spraševal server, ali je nova e-popšta prispela.

Kakšni so formati vseh treh etc datotek - hosts, protocols, services?

etc/hosts - Datoteka, v kateri se mapirajo IP naslovi v gostiteljska imena (host name) ali imena domene:

Format je sledeč: *Addesss HostName*.

- polje *Address* vsebuje IP naslov
- polje *HostName* pa hostname v relativni ali polnem domenskem imenskem formatu.

etc/protocols - Datoteka, ki shranjuje informacije o znanih protokolih v uporabi v DARPA Internetu.

Format je sledeč: *official_protocol_name protocol_number aliases*

- *official_protocol_name* - Specificira uradno Internet Protocol ime
- *protocol_number* - Vsebuje številko protokola
- *aliases* - Vsebuje kakršnokoli neuradno ime za protokol

etc/services - Datoteka, ki jo uporeabljajo apikacije, da prevedejo človeško-berljiva imena storitev v številke vrat

Format je sledeč: *service-name port/protocol [aliases] [#comment]*

- *service-name* - Ime omrežne naprave npr. Telnet, FTP
- *port/protocol* - Vrata in protokol, ki se uporabljajo pri storitvi npr. 1/TCP
- *alias* - Alternativno ime storitve
- *comment* - Dodaten komentar pri storitvi

Iskanje podatkov o domeni gov.si ne bo težko. Kaj pa o kakšni drugi, tuji domeni?

Informacije o drugih domenah so lahko težje za pridobivanje podatkov. Za državne domene npr. .si, .ca, .us, .eu, je odvisno kakšne privatnostne regulacije imajo lastnice teh domen (države).

Pri registriranju domenskih imenov, lahko registrant uporablja tudi proxy, da zamaskira svojo lokacijo in podatke o njemu.

Za nekatere domene npr. .onion, pa nemoremo narediti whois iskanje, saj te domene niso registrirane na tradicionalni način, ampak se generirajo avtomatsko z uporabo TOR programskega orodja. Zato se informacije o lastniku domene na .onion ne shranjujejo.

Našli smo naslednje pakete, ki jih komentiranjte, upoštevajte vire informacij, ki smo jih spoznali:

14:59:25.608728 IP xx.domain.netbcp.net.52497 >

valh4.lell.net.ssh: . ack 540 win 16554

14.59.26.610602 IP resolver.lell.net.domain >

valh4.lell.net.24151: 4278 1/0/0 (73)

14:59:26:611262 IP valh4.lell.net.38527 >

resolver.lell.net.domain: 26364+ PTR?

244.207.104.10.in-addr.arpa. (45)

1. paket

- izvorni IP naslov: xx.domain.netbcp.net
- izvorna vrata: 52497
- ciljni IP naslov: valh4.lell.net
- ciljna vrata: ssh (22)
- Zastavice: ACK (Acknowledgement)
- Acknowledgement number: 540
- Velikost okna: 16554

Paket opiše, da je ciljna naprava sprejela podatkoe do zaporedne številke 540 in velikost okna pove, koliko še podatkov lahko pošlje pošiljatelj, preden se čaka na ponovno potrditev. Verjetno gre za SSH povezavo na server xx.domain.netbcp.net s strani naprave na naslovu valh4.lell.net.

2. paket

- izvorni IP naslov: resolver.lell.net
- izvorna vrata: domain (53)
- ciljni IP naslov: valh4.lell.net
- ciljna vrata: 24151 (22)
- Zastavice: Response
- Odgovor: 1/0/0 (73)

Paket predstavlja odziv DNS poizvedovanja s strani naprave na valh4.lell.net. Odgovor je en brez dodatnih informacij. Iz tega paketka lahko izvemo, da je resolver.lell.net DNS strežnik.

3. paket

- izvorni IP naslov: valh4.lell.net
- izvorna vrata: 38527
- ciljni IP naslov: resolver.lell.net
- ciljna vrata: domain (53)
- Zastavice: Query
- Odgovor: PTR? 244.207.104.10.in-addr.arpa. (45)

Ta paket potrdi, da je resolver.lell.net DNS strežnik. Naprava je poslala reverse DNS lookup zahtevek na DNS strežnik, ki je v paketu predstavljena v napačnem vrstnem redu (10.104.207.244).

Reverse dns lookup se naredi z komando:

```
dig -t ptr 244.207.104.10.in-addr.arpa
```

Mobilne naprave

Katere podatke še vse vsebuje SIM kartica (razen MCC, MNC, serijska)?

MCC- Mobile country code (386 slovenija)

MNC - Mobile Network code (41 mobitel)

Lahko vsebuje še:

- Identiteto uporabnika
- Lokacijo in tel. številko
- Podatke za mrežno avtorizacijo
- Osebne privatne ključe
- SMS sporočila
- Imenik

Kaj je to LAI in kaj je IMSI?

LAI (Location Area Identity) - Vsaka lokacija mobilnega omrežja ima svojo identifikacijsko številko, ki jo imenujemo LAI. Vsaka oddajna postaja ima svoj LAI, ki ga redno prenaša skozi broadcast control channel.

IMSI (International Mobile Subscriber Identity) - Je unikatna številka, ki identificira vsakega uporabnika celičnega omrežja, vsak SIM ima unikaten IMSI. Vsebuje MCC, MNS in MSIN-serijska številka, ki jo ima mobilni operater za identifikacijo posamezne sim.

Kaj vsebuje vaša SIM kartica? Kakšne so vrednosti teh podatkov? Kakšna je identifikacijska številka mobilne naprave?

Poiščite geografske podatke v vašem telefonu

To lahko dobimo s pomočjo zapiskov, informacij shranjenih v apliakcijah tretjega vira ali pa to vidimo v nastavitvah.

V svojem telefonu imam vklopljen Google Timeline, ki ima shranjene geografske podatke tudi skoi čas.

Poiščite koledarske podatke v vašem telefonu

V nekaterih napravah so podatki shranjeni v aplikaciji ali pa v oblaku. Android in iPhone oba omogočata shranjevanje koledarskih poratkov v obblaku. Drugače pa do njih dostopamo preko aplikacij.

Kako deluje MobileSpy?

- Najprej moramo program namestiti na telefon, katerega hočemo slediti
- Nato MobileSpy pobira podatke iz telefona, kot so dnevniki klicev, SMS sporočila, GPS lokacija in internetna aktivnost. Lahko se tudi uporablja za zajeme zaslonov, zajem tipkanja, ter dostopa do kamere in mikrofona
- Nato se ti podatki v realnem času pošljejo strežnik v oblaku
- Uporabniki Lahko nato pogledajo informacije, ki so shranjene v oblaku, če imajo dostop do njih.

Programje, ki nam lahko škoduje na Android sistemu in iPhone?

Na sistemu Android je veliko bolj enostavno naložiti programje, ki nam ahko škoduje, saj sistem Android omogoča da namestimo aplikacije tretjega vira in ne nujno iz Google Play store. pri iPhone pa lahko nalagamo samo aplikacije iz trgovine App Store. iPhonei so tudi znani po tem, da imajo bolj restriktivna varnostna dovoljenja.

Preučite orodje DFF in kako se ga uporablja?

DFF (Digital Forensics Framework) je multi-platformna in odprtokodna aplikacija, ki ponuja vrsto storitev in je visoko modularna. Cilj je forenzični skupnosti dati pravo ogrodje za uporabo orodij tekom poteka analize.

Poiščite SMIL datoteko in jo preučite

SMIL (Synchronised Multimedia Integration Language) je XML markup jezik namenjen predstavi multimetijskkih vsebin. Definira merkup za čas, pstaitev, animacije, prehode in vdelavo multimedijskih vsebin. Najbolj znana aplikacija je SVG slike.

Kako bi dostopili do podatkov na vaši SIM kartici?

na iPhone:

- kliknemo na Settings meni
- izberemo "Mobile data"

- izberemo "SIM applications"

na Android:

- kliknemo na Settings
- kliknemo na "About phone"
- kliknemo "Status"
- kliknemo "SIM staus"

Na obeh mestih se skrivajo podatki o napši SIM karici.

Ali se hrani celotna zgodovina GPRS usmerjanja?

Telefon sam po sebi ne potrebuje vse zgodovine GPRS usmerjanja, zato je tudi ne shrani. Informacije o usmerjevanju hrani GPRS omrežje. Telefon uporablja signalne protokole za upravljanje seje (sesion) in poskrbi, da se paketi pošiljajo pravilno. Signalne informacije se lahko shranjujejo v telefonu začasno, a se ponavadi ne držijo za dolgo časa.

Lahko pa telefon hrani dnevniške informacije o povezavah GPRS, katerih pa je lahko cela zgodovina.

Naštejte EF, v katere lahko piše uporabnik

- EF Phonebook - imenik: Uporabnik lahko v ta EF piše svoje kontakte
- EF SMS: Tu se shranjujejo SMS podatki. Tipično lahko uporabnik v to datoteko piše.
- EF IMSI: Shranjuje IMSI podatke. V nekaterih primerih lahko uporabnik modificira te informacije.
- EF GID: Shranjujeo podatke o uporabnikovem ponudniku storitve in obračunskem načrtu. V nekaterih primerih lahko uporabnik modificira te informacije,.

Recimo, da se je zgodil zločin v predavalnici, v avli, v računalnici, ... Naredite načrt zavarovanja mesta digitalnega zločina

Za zavarovanje mesta zločina uporabimo ACPO priporočila za prripravo za delo na mestu digitalnega zločina:

1. Najprej moramo opraviti nadzor dostopov na mesto zločina:

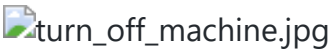
    - Že obstoječe nadzorne sisteme ugasnemo, da se podatki ohranijo. V našem primeru je to kamere, ki so po fakulteti.
    - Žična in brezžična omrežja ugasnemo, da ne pride do nehotenega ali drugega dostopa, ki bi lahko "kvaril" dokaze. V našem primeru je to brezžično omrežje eduroam in druga brezžična in žična omrežja na fakulteti.

2- Nato zamrznemo mesto zločina:

- Dokaze premišemo z ustreznimi napravami, te jih podpišemo in pravilno shranimo. npr. najdemo USB ključ na mestu zločina, ga zapakiramo v ustrezno embalažo, podpišemo, ...
- Zavarujemo oddaljene podatke, v našem primeru podatki, ki so v oblaku ali na stžnkih, ki niso na fakulteti, npr. spletna učilnica.
- Zavarujemo nedigitalne dokaze v našem pimeru npr. prstni odtis.

Prejšnji testi

Pri hišni preiskavi smo našli prižgan, a zaklenjen računalnik. Predpostavljamo, da je tudi disk zašifriran. Kako lahko postopamo? Utemeljite odgovor.



Najprej pregledamo okolico, če je slučajno na mestu dokaza kakšno geslo za bodisi odklep računalnika, ali pa enkripcijski ključ računalnika, saj nam to delo mnogo olajša.

Odvisno od enkripcije diska lahko ključ dobimo tudi z "brute force" metodo. Če je kriptiran z DES, to ni velik problem, saj imamo metode za hito razbitje te enkripcije, če pa je zakodiran z AES, pa to težko naredimo. Izvedemo lahko npr. napad z hladnim zagonom (cold-boot attack), ki poskuša izkoristiti lastnosti DRAM-a, da lahko dobimo posnetem RAM-a in s tem tudi ključ za dekripcijo.

Podatke laahko dobimo tudi, če se bomo prijavili v sistem kot administrator in s tem lahko odklenili zakodirane podatke. To lahko naredimo bodisi z ugibanjem ali pa kakšno drugo "hekersko" metodo, kot so razni znani "expoiti", ki nam dobijo administratorske pravice.

Za to, da je dokazno gradivo sprejemljivo na sodišču, mora zadoščati patim osnovnim pravilom. 1. katera so ta? Utemeljite za vsako od pravil, zakaj mu mora dokazno gradivo zadočati. 2. za tri pravila navedite primer, ko gradivo ne zadoča glede na to pravilo.

1.

- Relevantnost gradiva za primer. Če je gradivo relevantno, lahko prepriča žirijo o napačnem zaključku
- avtentičnost gradiva (zajem, sledljivost). Če gradivo ni avtentično, je lahko neznanega izvora in je lahko nerelevantno za primer.
- niso govorice (dokaz sam niso govorice, če ni govorec prisoten). Govorice niso podkrepljene s konkretnimi dokazi, lahko spravijo do napačnih zaključkov.
- najboljši možen dokaz (original in kopija). Če je dokaz slab, spet lahko privede do napačnih zaključkov.
- dokazno gradivo brez potrebe ne napeljuje na zaključke. Če je možnost, da gradivo ne napeljuje na zaključek, se mora tudi to upoštevati.

2.

avtentičnost: Zajeli smo trdi disk, a ga nismo pravilno hranili, zato se je v raziskavi zamenjal z drugim trdim diskom, ki ni relevanten.

Relevantnost gradiva za primer. Naprimer najdemo dokaze, da je osumljenec prakticiral satanizem in ta dokaz uporabi tožilec na sodišču. To naredi samo zato da prepriča žirijo, da je slab človek. prikažemo napačne zapisnike youtuba...

Najboljši možen dokaz: V kopiranju dokaza so se zgodile napake in dokaz ni več dovolj dober za zaključke.

Peter Zmeda sumi, da mu je nekdo vrinil virus v zagonski ram-disk (initial ram dist, initrd). 1. Je sploh to mogoče? Če ne zakaj? Če da, kako? 2. Peter bi se rad znebil initrd-ja. Je to sploh mogoče? Če ne zakaj? Če ja, kako?

1.

initrd je datoteka v imeniku /mnt/, zato lahko notri zapišemo karkoli, če imamo administratorski dostop. Moral bi narediti svojo initr datoteko. Z uporabo orodij kot so unmakeinitramfs & mkinitramfs, ki zapakirajo našo kodo v initramfs image.

2.

Peter lahko zamenja star okužen initrd z novim initrd iz spletne strani proizvajalca njegove distribucije Linux sistema. Lahko pa tudi nastavi nov initrd. To naredi tako, da konfigurira in compila krenel sam.

Peter Zmeda je dobil v preiskavo disk z datotečnim sistemom XFS. Da ne bi uničil podatkov, ga je priklopil samo za branje (-o ro). Nato je skopiral vse datoteke. 1. Katere podatke je uničil? 2. Na katere podatke je pozabil? 3. Kako bi moral disk v resnici pregledati? Zapišite zaporedje ukazov in vsakega utemeljite.

1.

Lahko ej uničil podatke o zadnjem dostopu do datotek an disku, število priklopov diska, zadlje priklapljanje diska, ...

2.

Lahko je pozabil skopirati skrite datoteke in metapodatke

3.

Disk bi moral samo priklopiti in ne mountati (vklopiti). potem bi moral izračunati varnostno vsoto za priklopljeno napravo, skopirati napravo v surovo datoteko z uporabo dd ali cat oz. kakršnega koli drugega namenskega orodja, ki ne spremeni vsebine datotek in nato še izračunati varnostno vsoto kopije, ki bi morala biti enaka varnostni vsoti originalnega diska. Nato bi moral originalno disk odklopiti in raziskovaje nadaljevati na kopiji diska.

```
sha512sum /dev/disk
cat /dev/disk > kopija.img
modprobe nbd max_part=32
qemu-nbd /dev/nbd0p1 kopija.img
mount /dev/nbd0p1 /mnt/disk
```

modprobe nbd max_part=32 naredi novo bločno napravo (Network block device), ki jo lahko uporabljamo za vklop diska na njo. To naredimo, ko imamo omejeno prostora na disku.

qemu-nbd /dev/nbd0p1 kopija.img datoteko kopija.img prilepi kot bločno napravo na nbd0p1 NBD napravo na sistemu QEMU NBD server.

Čemu je enako število možnih vnosov tabele FAT? Utemeljite odgovor.

Število možnih vnosov je enako maksimalnemu številu gruč na nosilcu. To izračunamo tako, da velikost diska delimo z velikostjo gruče. Pove nam koliko različnih gruč lahko ima disk. Se pravi če imamo 1GB disk in 4kB (FAT 12) velikost gruče to pomeni 262144 vnosov v FAT tabelo.

Velikost gruče: 512B do 8kB za FAT12, 512B do 64kB za FAT16 in 512B do 32kB za FAT32,

Velikost diska: največ $cluster\_size * 2^{xx}$

Dnevniški zapisi so se pojavlili kot del datotečnega sistema iz več razlogov. 1. Opišite vsaj eno težavo, ki jo dnevniški zapisi odpravljajo na sistemu. Kako? 2. Pri dnevniških zapisih ext datotečnega sistema obstajajo 4 vrste blokov. Katere? 3. Dva od štirih blokov nikoli ne nastopita hkrati v isti transakciji. Katera in zakaj? 4. skicirajte particijo in označite, kje se v njej nahajajo dnevniški zapisi.

1.

Omogočajo popravljanje nekonsistentnosti v datotekah, ki nastanejo ob izpadu elektrike ali kakšni drugi operaciji nad datotekami. Dnevniki sledijo spremembam v sistemu, ki se še niso dokončno zapisale na disk.

2.

1. Opisni blok - kaže začetek transakcije
2. Metapodatkovni blok - Hrani podatke o opisu transakcije
3. zaključni blok (commit block) - kaže zaključek transakcije
4. preklicni blok (revoke block) - če pride do napake vsebuje seznam blokov v datotečnem sistemu, ki jih je potrebno ponovno namestiti (restavrirati).

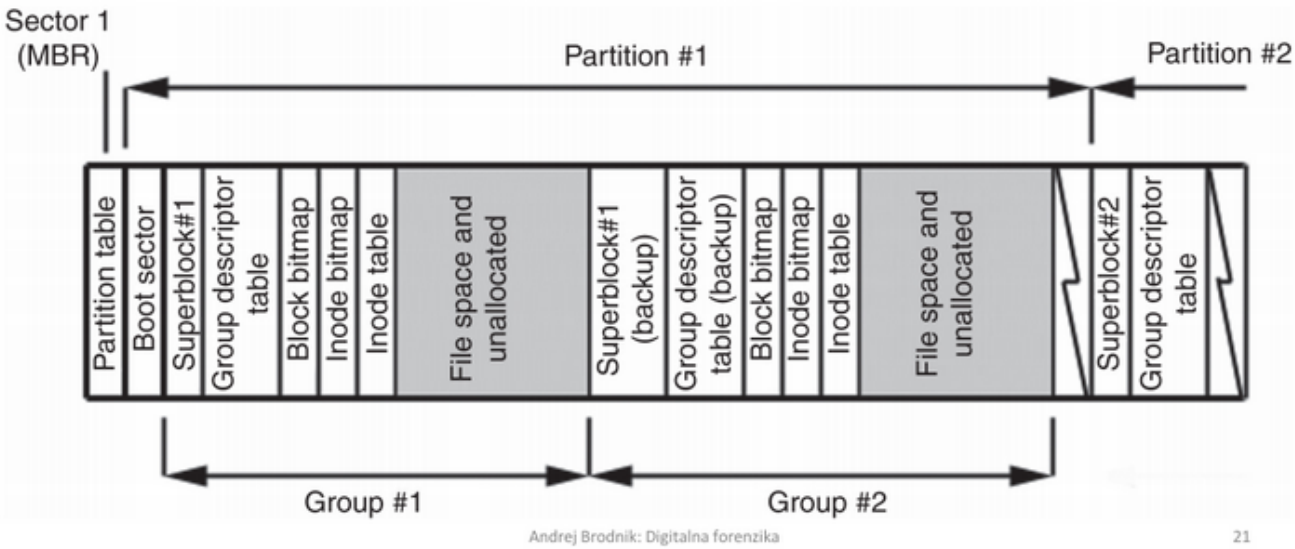
3.

Nikoli ne nastopita skupaj preklicni in zaključni blok, saj če se transakcija , potem ne pride do napake in ne nastopi preklicni blok.

4.

Odvisno od datotečnega sistema. V primeru NTFS, se dnevniški podatki shranjujejo na korenu NTFS particije v $LogFile.

V primeru ext2/3, pa se shranjujejo na začetku particije v t.i. "dnevniškem bloku", pred prvo skupino blokov,pri Boot sectorju, med superblock in group descriptor table.



Peter je v pregled dobil računalnik z OS Windows XP. Zanima ga samo, kdo in kolikokrat se je prijavljal na računalnik. Ima orodje, ki sprejme pot do datotečnega sistema in izpiše vse prijave. Na žalost si ne more privoščiti, da bi skopiral celoten disk, saj je le-ta velik 4TB in skoraj povsem zaseden, Peter pa ima le 500GB prostora. Katere datoteke mora dejansko skopirati?

Potrebuje kopirati samo zabeležke sistema, ki jih najdemo na za XP: %systemroot%\system32\config in za win7: Windows\System32\winevt\logs*.evtx . Te datoteke ne bodo zasedle veliko prostora, sakoraj zagotovo manj kot 500GB.

Najznačilnejša lastnost mobilnih naprav je, da so mobilne. 1. Opišite tri načine kako lahko Peter ugotovi, kje se nahaja mobilna naprava osumljenca. 2. Za vsakega od načinov opišite, kje naj Peter išče podatke o nahajanju naprave. 3. Peter sumi, da je Luka po mobilnem telefonu pogovarjal s strašnim razbojnikom. Zapišite pet hipotez, kje in kako lahko Peter preveri če je to res. Seveda hipoteze morajo biti smiselne.

1., 2.

- Lahko pogleda zgodovino prehodov med baznimi postajami, na katero bano postajo je trenutno povezan. Te informacije lahko pridobi pri mobilnem operaterju.
- Lahko pogleda GPS podatke v napravi, če so dostopni na daljavo npr. prek SpyMobile
- Lahko se osumljencu pošlje phishing SMS z linkom, ki ga klikne in nato zabeležimo njegov IP in lokacijo.

3.

- Peter se je pogovarjal z razbojnikom, zato se podatki o tem skrivajo v zgodovini klicev naprave. To lahko preveri s tem, da ima dostop do naprave.
- Peter se je pogovarjal z razbojnikom, in podatke o tem ima mobilni operater. To lako preveri s tem, da mobilnega operaterja prosi za podatke o klicih.
- Peter se je pogovarjal z neznano številko, ki je lahko razbojnik. Peter se mora prepričati, da je neznana številka res razbojnikova. To lahko naredi na mobilnem operaterju, kjer pogelda zgodovino klicev in SMS-ov
- Peter se je pogovarjal z razbojnikom saj sta bila telefona v neposredni bližini. Potrebuje GPS podatke obeh telefonov.
- Peter se je pogovarjal z razbojnikom, saj sta se pogovarjala preko skupne tretje osebe. To lahko preveri s pogledom v telefon tretje osebe, ali pa izpraša tretjo osebo.

Kateremu napadu so podvržene naprave, ki zaupajo ostalim napravam zgolj na podlagi njihovega IP naslova? Utemeljite odgovor, kako se tak napad izvede?

Te naprave so podvržene napadom lažnih IP naslovov (IP spoofing) in lažni ARP odziv (ARP table spoofing), pri obeh se napadalec pretvarja, da je druga naprava v omrežju kot dejansko je. Pretvarja se, da je zaupanja vredna naprava. Napadalec dobi IP in MAC zaupanja vredne naprave in nato pošlje lažen ARP odziv s svojim MAC naslovom. MAC naslov lahko zamenja samov primeru, da onesposobi zaupanja vredno napravo, saj ni nujno da bo napadalec dobil vse pakete.

Peter je v preiskavo dobil računalnik z dvema diskoma. Korenski imenik oz. C: je na njegovi delovni posatji, na kateri poganja Linux, dostopen kot /dev/md0. Naredil je kopijo korenskega imenika, ne da bi datotečni sistem prej priklopil. Nato je raziskavo izvajal na tej kopiji. Na sodišču so ga obtožili, da je uničil dokaze. Jih je res? Če da, kako? Kaj bi moral storiti, da jih ne bi? Če ne, kaj je moral storiti, da lahko dokaže, da jih ni.

Peter je lako uničil dokaze, saj je samo kopiral korenski imenik. Korenski imenik vsebuje le trenutno stanje datotek, ter njihove atrubite, ne vsebuje pa zgodovine sprememb in metapodatke. Te bi lahko pridobil z uporabo forenzičnih orodij kot so `dd` ali `dc3dd`, ki naredijo dejansko bitno kopio diska, vključno z vsemi sektorji in metapodatki.

Kateri od principov ni osnovni princip, katerega se morajo držati digitalni preiskovalci na mestu zločina?

a) najprej poiščemo osumljence, da ne pokvarijo dokazov.

b) podatkov na preiskovalni napravi ne spreminjamo

c) voditi moramo zapis o vseh dejavnostih na mestu zločina

d) vse našteto

A) ni osnovni princip, saj ne potrebujemo poiskati osumljence, moramo samo zavarovati mesto zločina, da bodo dokazi pridobljeni s kraja zločina verodostojni.

Obstaja več načinov oz modelov vodenja preiskave. 1. Če modele posplošimo dobimo 5 osnovnih korakov. Katere? 2. Zamslite si neko kaznivo dejanje in ga opišite. Nato za vsakega od petih korakov zapišite tipično opravilo, ki se izvaja v njem, pri obravnavi zamiljenega kaznivega dejanja

1.

1. Priprava: priprava načrta preiskave
2. pregled/identifikacija: kaj je potrebno zajeti in kako
3. shranjevanje: forenzična korektnost zajetega gradiva
4. raziskava (examination) in analiza: zajeto gradivo se ustrezno pripravi an analizo, ki temelji na znanstvenih metodah.
5. predstavitev gradiva: izsledke preiskave se ustrtezno namenu predstavi.

2.

Zgodil se je rop trafike na slovenski cesti. Rop se je zgodil ob 9 uri zjutraj pozimi s pištolo. strelov ni bilo ustreljenih.

1. priprava: pogledati moramo fizične dokaze (odtise čevljev, lasje, prstni odtisi, ...) in izprašati očevidce.
2. Potrebno je zajeti odtise čevljen, dnk vzorce, na način, ki ga predlaga forenzična skupina
3. Forenzilčne dokaze je potrebno shranjevati v posebnih posodah/vrečkah, ki so vse podpisane s strani nadrejenega in prej poslikane.
4. Gradivo ustrezno izoliramo in analiziramo, na podkagi teh lahko naredimo zaključke.
5. Predstavimo izsledke dela nadrejenemu preiskovalcu primera.

V katere kategorije po parkerju spada računalnik, vpleten v zločin?

Računalnik kot:

1. predmet (objekt) zločina -> kraja računalnika ali uničenje
2. osebek (subjekt) zločina -> Zločin je bil narejen nad računalnikom
3. orodje za pripravo in/ali izvedbo zločina (instrument) -> kopiranje dokumentov, hekanje
4. Uporaba po svojih lastnostih v zločinu (symbol) -> ponujanje storite ali zmožnosti storitev: dobitki na bozri, VPN gateway, ...
5. Vir podatkov -> ostanki datotek, e-pošte

Dokazno gradivo je osrednji element v forenziki in za dokaz o pravilnem rokovanju z njim uporabljamo pojem dokazne verige. 1. Kje se dokazna veriga prične in kje konča? 2. Zapišite primer vsebine posameznega člena dokazne verige in razložite, kaj dokazuje vap primer. 3. Zakaj mora biti dokazna veriga nepretrgana? Kje in kako bi lahko kdo izkoristil pretrganost verige?

1.

Dokazna veriga se prične pri delavcu, ki je prvič dokumentiral dokaz. Konča pa se, ko se dokaz poda na sodišču ali pa se ga izroči nazaj lastniku.

2.

Vsak člen dokazne veriga ima:

- Identifikacijsko številko objekta
- Datum
- Kdo je dal dokaz in podpis
- Komu je dal dokaz in podpis
- Komentarji

3.

Če bi bila dokazna veriga pretrgana, bi lahko bli dokazi spremenjeni in ne bi več bili uporabni za forenzično preiskavo ali v sodnem postopku.

Peter je v roke dobil star disk. ob priklopu je disk javil, da ima 256 glav. Ko ga je odprl je videl le eno ploščico in ročico, ki se ob njej premika. 1. Koliko bralno/pisalnih glav dejansko ima njegov disk? 2. Zakaj bi disk lagal glede števila glav?

1.

Njegov disk ima eno bralno/pisalno glavo.

2.

Lahko je disk starejši in ima drugačno konfiguracijo, kot sodobnejši sistemi. Dejansko ni pomembno koliko glav ima disk dejansko in koliko logično, če vse deluje. Vse načeloma obdela disk.