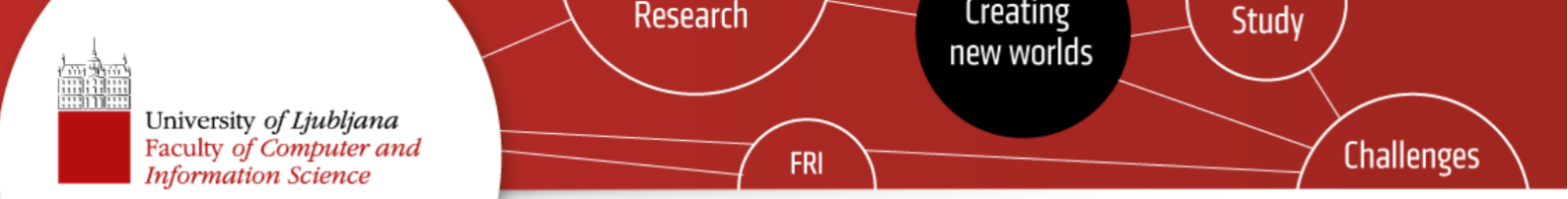


University of Ljubljana
Faculty of Computer and Information Science

Zbornik predstavitev

Digitalna forenzika, 2013/14

Predstavitve seminarskih nalog

Ljubljana, 2014

Zbornik
Digitalna forenzika, Seminarske naloge 2013/2014

Editor: Andrej Brodnik, Rok Povšič

Ljubljana : Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, 2014.

Kazalo vsebine

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Vlada Semenova
Gregor Cimerman

Costa Concordia shipwreck

4. Maj 2014

- **Malo statistike o križarkah (ZDA):**
  - Letni prihodki industrije v ameriškem gospodarstvu: **$37.85 miliard**
  - Število delovnih mest: **314,000**
  - Letno število potnikov: **20,335,000**
  - Povprečna zmogljivost ladje: **104 %**
  - Število križark, ki se so potopile po letu 1979: **55**
  - Skupno število preminulih na križarjenju po letu 1979: **172**
  - Povprečno trajanje potovanja: **7.2 dni**

(statistika je bila zajeta 1.1.2014)

Vir: Wikipedia

Vsebina

- Kako zmanjšati število ponesrečencev
- Kdo je kriv za nesrečo
- Voyage Data Records kako je zgrajen in deluje
- Kako rekonstruirati podatke z brodoloma
- Težave pri rekonstrukciji podatkov (forenzična preiskava)

Voyage Data Recorder (VDR)

- Današnje ladje morajo biti opremljene s sistemom **VDR (Voyage Data Record)**, ki beleži dogajanje na poveljniškem mostu. Težava takšnih sistemov je standardizaciji podatkov, saj vsak proizvajalec implementira lasten način beleženja podatkov in običajno poskrbi za programsko opremo s pomočjo katere je možno podatke obdelati.

- S 1.7.2002 so sprejete zahteve glede sistemov beleženja potovalnih podatkov - IMO A.861 "Performance Standards for Shipborne Voyage Data Records“
- 17.5.2004 so sprejete zahteve poenostavljenega sistema za beleženje potovalnih podatkov - IMO MSC.163(78) "Simplified VDR"

- **Zahteve IMO A861(20):**
  - Naprava bi morala biti v celoti avtomatizirana med normalnim delovanjem
  - Naprava mora zbirati vse podatke z naprav, ki so povezane s statusom, poveljevanjem in kontrolo ladje
  - Naprava mora biti nameščene v svetlo in zaščitno kapsulo ter oddajnikom, ki bo pomagal pri lociranju naprave

- **Podatki, ki jih treba zajet:**
  - Datum in čas, ki se sklicuje na UTC
  - Položaj ladje (zemljepisna širina, zemljepisna dolžina)
  - Hitrost, radarski podatki
  - Visoki frekvenčna (VHF) radijska komunikacija itd.

Voyage Data Recorder (VDR)

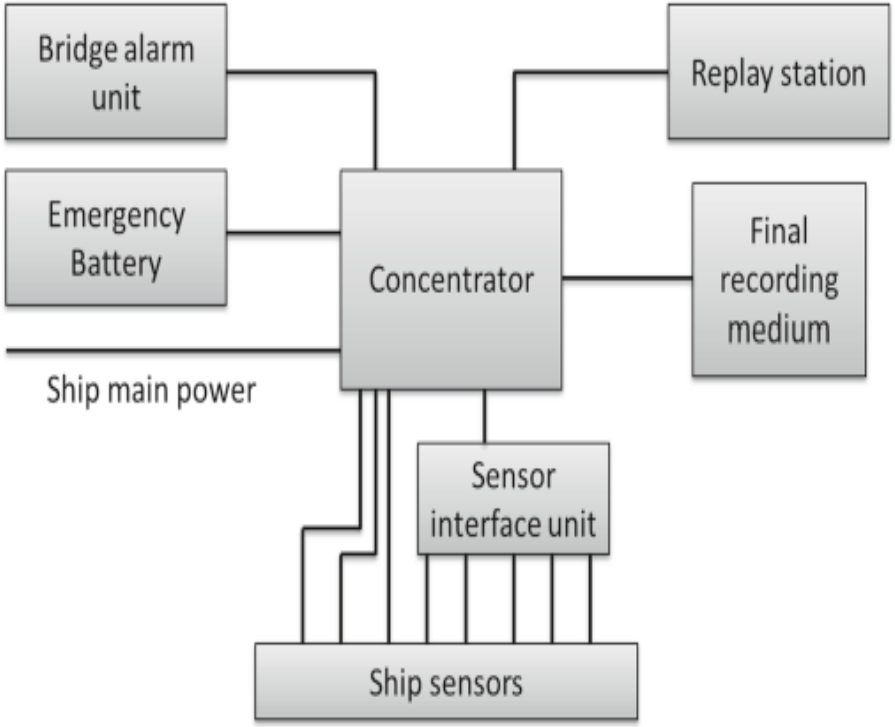


Fig. 1. VDR system schematic.

Podatki zajeti z VDR na modernejši ladiji

- Gyro, compass – smer
- VHF radio in posnetki z mosta
- Radarska slika *
- Echo sounder *
- Glavni alarmi *
- Stanje vrat v trupu ladje *
- Rudder (krmilo) *
- Vodne in požarne zapore *
- Stanje agregata in ladijskega svedra *
- Hitrost in smer vetra *
- Thrusters *

* velja samo za VDR in ni obvezno za S-VDR (Simplified Voyage Data Recorder)

Vir: Wikipedia

Primer Maersk Kendal

Vir: http://maritimeaccident.org/2010/03/maersk-kendal-complacency-btm-culture-and-vdrs/

Problemi pri analizi podatkov z VDR-jev

NEMA nizi

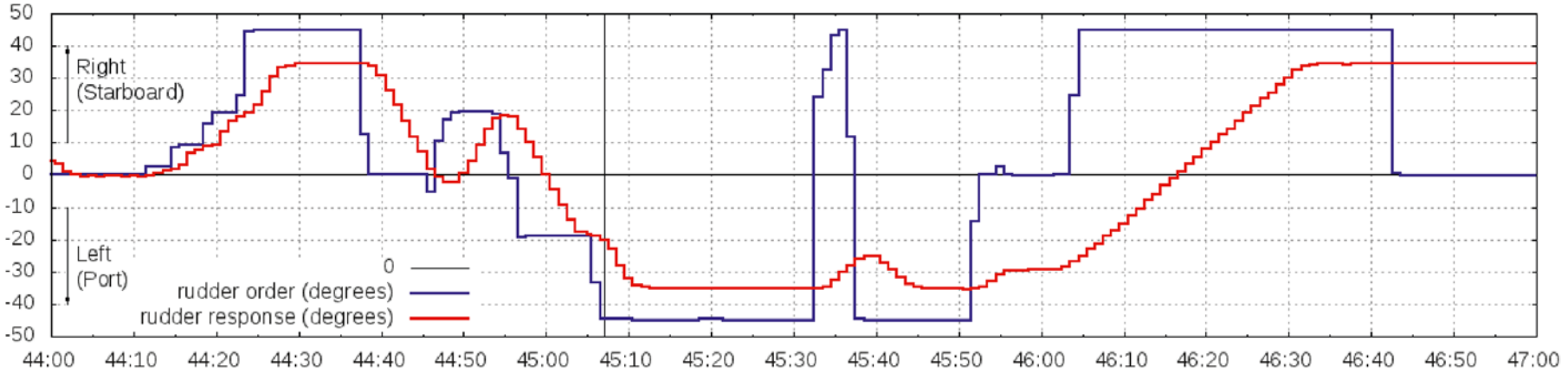
$GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47

$: začetni simbol
GP: prva dva znaka določata izvor podatka (GP - GPS sprejemnik)
GGA: zadnje tri črke so opis zajetih podatkov z izvora (GGA pomeni lokacija glede na GPS)
123519: čas zajetega podatka (12:35:19 UTC)
4807.038,N: latitude
01131.000,E: longitude
1: kvaliteta signala
08: število vidnih satelitov za določitev lokacije
0.9: horizontalna natančnost sistema za pozicioniranje
545.4,M: višina nad srednjo nadmorsko višino (545.4 m)
46.9,M: višina nad WGS84 elipsoidom
prazno polje: time in seconds since last update
prazno polje: ID številka DGPS postaje
*47: kontrolna vsota

Krmilo

$PAVBADC, a, xx.xxx, [a ponovitev xx.xxx], izvor, *hh

a: število podatkov (xx.xxx v tej vrstici) (1–8)
xx.xxx: analog value
izvor: opis izvora
hh: kontrolna vsota



Pot

```
$RAWPL,4418.6000,N,00831.7000,E,0008*45~04
$RAWPL,4419.1000,N,00830.0000,E,0009*44~04
$RAWPL,4418.7000,N,00829.3000,E,0010*40~04
$RARTE,1,1,w,1  Civitavec-Savona,0006,0007,
0008,0009,0010*42~04
$RAWPL,4220.3500,N,01057.1500,E,0007*4D~05
$RAWPL,4223.9200,N,01054.7500,E,0008*49~05
$RAWPL,4252.7000,N,01029.8000,E,0009*42~05
$RAWPL,4418.6000,N,00831.7000,E,0010*4C~05
                                0,E,0011*4D~05
                                -SavonaGI,0007,
```

Vodotesna in požarna vrata

$PSWTD,08,C——,*35
$: začetek
P: nestandarden niz
S: Seanet
WTD: Vodotesna vrata “Water Tight Door”
08: številka vrat (od 1 do 24)
C--: stanje vrat
*35: kontrolna vsota

```
**** Looking for door 08 ****
2012/01/13-21:00:07 - $PSWTD,08,C——,*35~0A
2012/01/13-21:19:15 - $PSWTD,08,O——,*31~0A
2012/01/13-21:19:30 - $PSWTD,08,C——,*35~0A
2012/01/13-21:22:07 - $PSWTD,08,O——,*31~0A
2012/01/13-21:22:54 - $PSWTD,08,C——,*35~0A
2012/01/13-21:26:01 - $PSWTD,08,O——,*31~0A
2012/01/13-21:26:17 - $PSWTD,08,C——,*35~0A
2012/01/13-21:42:45 - $PSWTD,08,O——,*31~0A
2012/01/13-21:43:01 - $PSWTD,08,C——,*35~0A
2012/01/13-21:46:56 - $PSWTD,08,CFV-,*37~0A
2012/01/13-22:32:26 - $PSWTD,08,CFV-P,*3A~0A
2012/01/13-22:32:41 - $PSWTD,08,CFV-,*37~0A
2012/01/13-22:33:13 - $PSWTD,08,OFV-,*33~0A
2012/01/13-22:33:28 - $PSWTD,08,?????,*39~0A
```

Znaki v stanju vrat:
- Položaj: O (open) ali C (closed)
- Napaka: F (fault)
- Opis napake: L (low level of oil), P (low pressure) ali V (voltage loss)

Hvala

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Nejc Bizjak
Dean Črnigoj

-

Rekonstrukcija manipuliranih poizvedb iz InnoDB Redo Log datotek

4. Maj 2014

Namen seminarske naloge

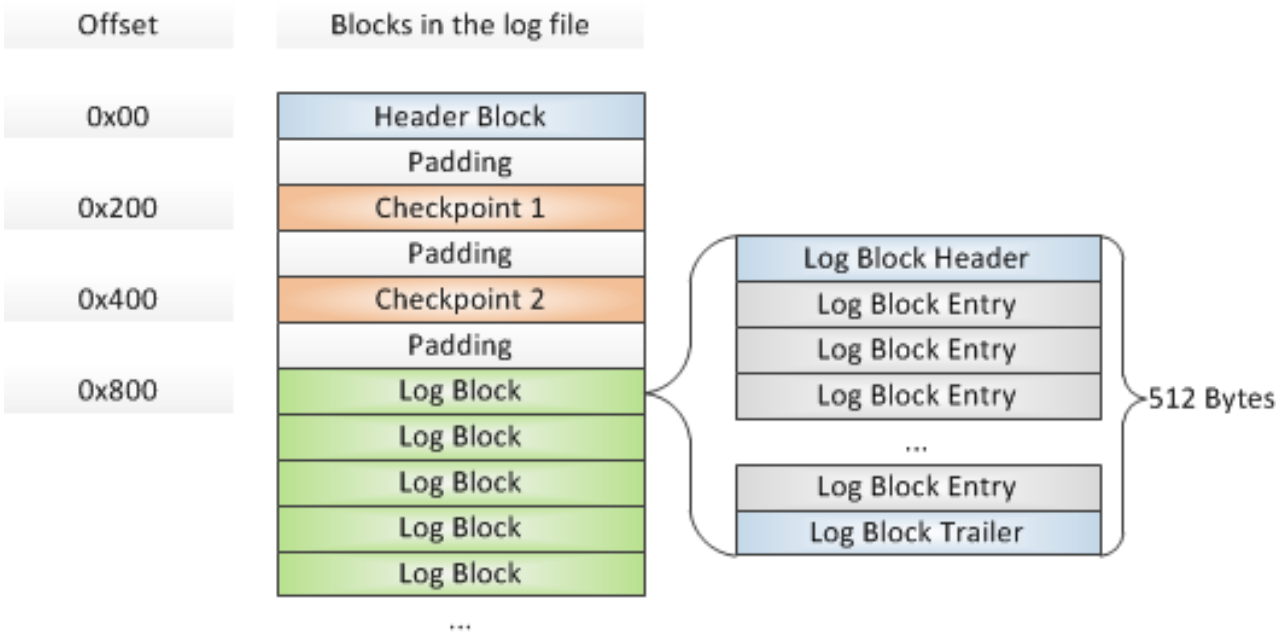
- Podrobno spoznati InnoDB podatkovni sistem
- Pridobiti ustrezna znanja zgradbe Redo Log datotek
- Uspešno izvesti napad ter pridobitev pravih poizvedb iz Redo Log datotek

Predstavitev InnoDB

- Podatkovni sistem za shranjevanje podatkov v MySQL
- Visoka zmogljivost ter zanesljivost
- Privzet podatkovni sistem z MySQL 5.5 ter višjimi
- Zasnova ACID (Atomicity, Consistency, Isolation, Durability) modela
- Podpora zaklepanju vrstic (Row level locking)
- Podpora tablespace

Struktura Redo log datoteke

Tipična MySQL podatkovna baza z InnoDB podatkovnim sistemom vsebuje dve datoteki Redo log kateri se polnita ciklično. Datoteka je razdeljena na več blokov. Primer razdelitve datoteke na bloke je prikazan na spodnji sliki:



Blok glave

Blok glave ponazarja začetek (0x00) v Redo Log datoteki. Njegova dolžina je 48 bajtov in vsebuje polja:

- Group Number (4 bajtov)
- First log sequence number (lsn) (8 bajtov)
- Archived log file number (4 bajtov)
- InnoDB Hot Backup(32 bajtov) samo za rabo z InnoDB Hot Backup

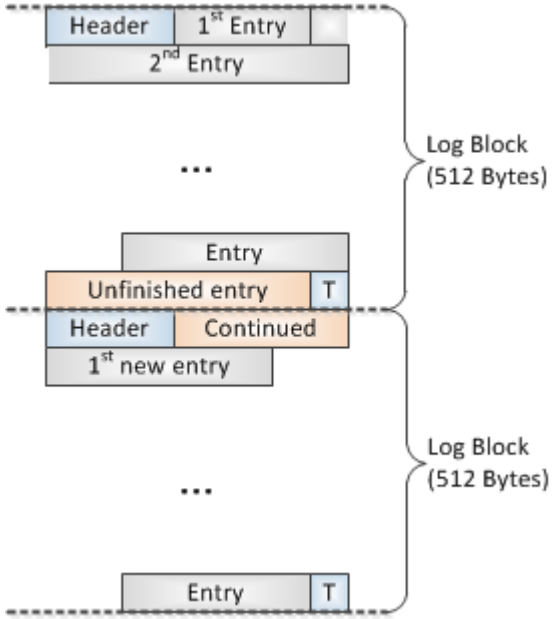
Kontrolni točki

Vsaka Redo log datoteka vsebuje 2 kontrolni točki. Kateri sta fiksno na naslovu (0x200 ter 0x400) ter sta dolžine 304 bajtov. Ob vsakem pisanju v log datoteko se prepiše samo ena kontrolna točka naenkrat tako da je v vsakem času veljavna vsaj ena kontrolna točka. Polja v kontrolnih točkah so naslednja:

- Log checkpoint number (8 bajtov)
- Log sequence number of checkpoint (8 bajtov)
- Offset to the log entry (4 bajte)
- Size of the buffer (4 bajte)
- Archived log sequence number (8 bajtov)
- Prazen prostor (256 bajtov)
- Checksum 1 (4 bajte) (zgoščen izračun vsote polj do praznega prostora)
- Checksum 2 (4 bajte) (zgoščen izračun od tretjega polja do vključno z Checksum 1)
- Current fsp free limit in tablespace 0 (4 bajte) (podan v megabajtih prostora)
- Zaključno polje ki pove ali obstaja prejšno polje (4 bajte)

Struktura Log Bloka

Po bloku glave, ter kontrolnih točkah je datoteka urejena na Log Bloke. Vsak blok je velik 512 Bajtov, začnejo se pa na naslovu 0x800. Log Blok sestavljata Log Blok Glave (14 bajtov), Vsebina, ter rep log bloka (4 bajte). Vsebina poizvedbe se lahko razdeli tudi na več log blokov, slednji scenarij prikazuje spodnja slika:



Rekonstrukcija stavkov

Vsebino iz Log blokov identificiramo ter preverimo kakšne vrste stavkov so bile nazadnje zapisane v podatkovno bazo.

Osredotočimo se na tri vrste stavkov in sicer *Insert*, *Delete* in *Update, saj so te za forenzično analizo največjega pomena.*

Identifikacija stavka

Vsaka identifikacija stavka se določi z prvim bajtom v vsebini log bloka.

Od različnega stavka pa so odvisna tudi različna polja, katera pripadajo stavku.

Kot primer:

Za vsako manipulacijo z podatki, InnoDB ustvari vsaj en zapis *mlog undo insert.*

Rekonstrukcija Insert stavka

- InnoDB ustvari 9 zapisov v dnevnike ob vsaki izvedbi insert stavka.

- Da gre za Insert stavek ugotovimo iz dnevnika mlog_undo_insert ->(0x26)
- V tem vnosu je vsebovanih veliko informacij, ki pripomorejo k rekonstrukciji stavka:
  - Število polj, število polj s primarnim ključem,
  - dolžina raznih polj v zapisu,
  - vsebina insert stavka.
- Za popolno rekonstrukcijo moramo poznati strukturo tabele.

Rekonstrukcija Update stavka

- V zapisu tipa mlog_undo_insert lahko najdemo podatke, ki so bili prepisani.
- Pomembne informacije: število spremenjenih polj, id zadnje transakcije, dolžina in prvotni podatki spremenjenih polj.
- Če sledimo toku zadnjih transakcij, lahko rekonstruiramo celotno zgodovino sprememb v tabeli.

- Novo zapisane podatke lahko pridobimo na isti način kot pri insert stavku.

Rekonstrukcija Delete stavka

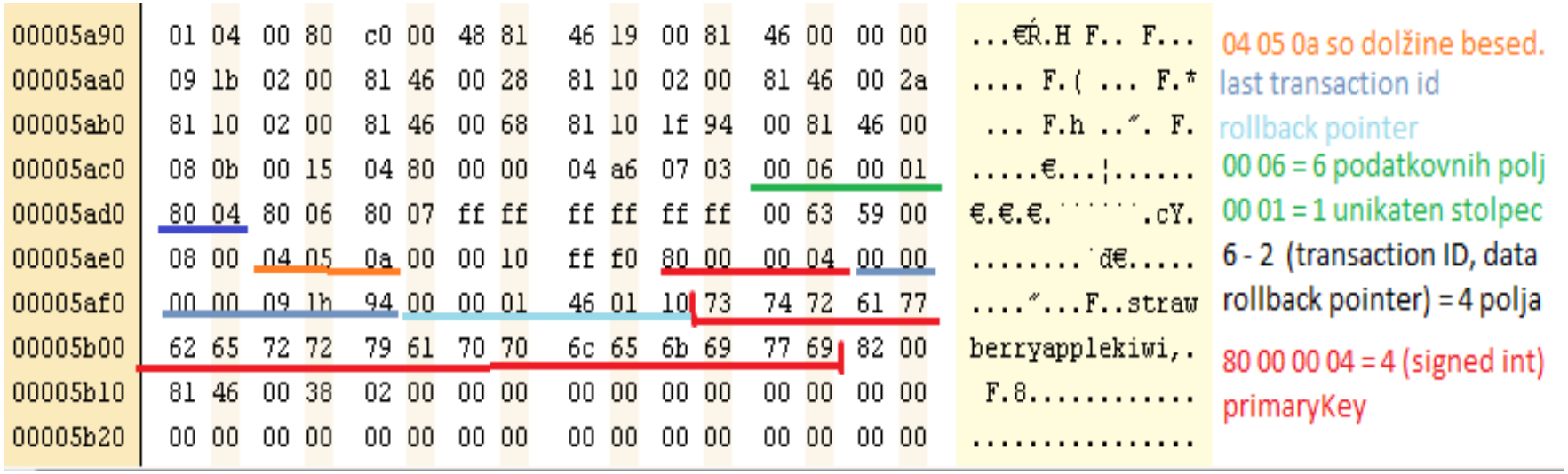
- Delete stavek ne fizično izbriše zapisa v tabeli, ampak ga samo označi kot izbrisanega (hitrejše delovanje).
- Običajno se ob delete stavku ustvarijo štiri zapisi v dnevniku.
- Rekonstrukcija poteka na podoben način kot pri update stavku, ker je tudi struktura zapisa v dnevniku zelo podobna (brez informacije o vsebini polj v tabeli).
- Pogoj za uspešno rekonstrukcijo je poznavanje števila primarnih ključev.

Demonstracija

- CREATE TABLE ‘fruits‘ (
- ‘primaryKey‘ int(10) NOT NULL,
- ‘field1‘ varchar(255) NOT NULL,
- ‘field2‘ varchar (255) NOT NULL,
- ‘field3‘ varchar(255) NOT NULL,
- PRIMARY KEY (‘primaryKey‘)
-) ENGINE=InnoDB DEFAULT CHARSET= utf8;

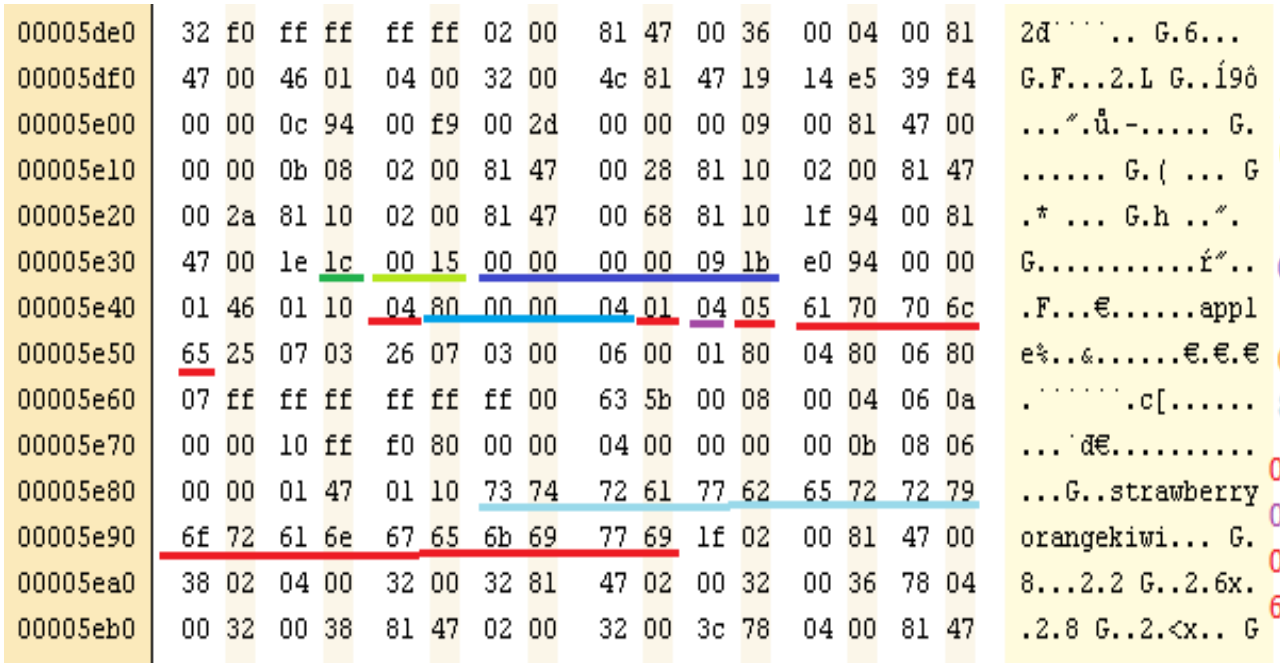
Demonstracija - insert

- INSERT INTO fruits
  (primaryKey, field1, field2, field3)
  VALUES (4, ‘strawberry’, ‘apple’, ‘kiwi’);



Demonstracija - update

- UPDATE fruits SET field2='orange' WHERE primaryKey=4

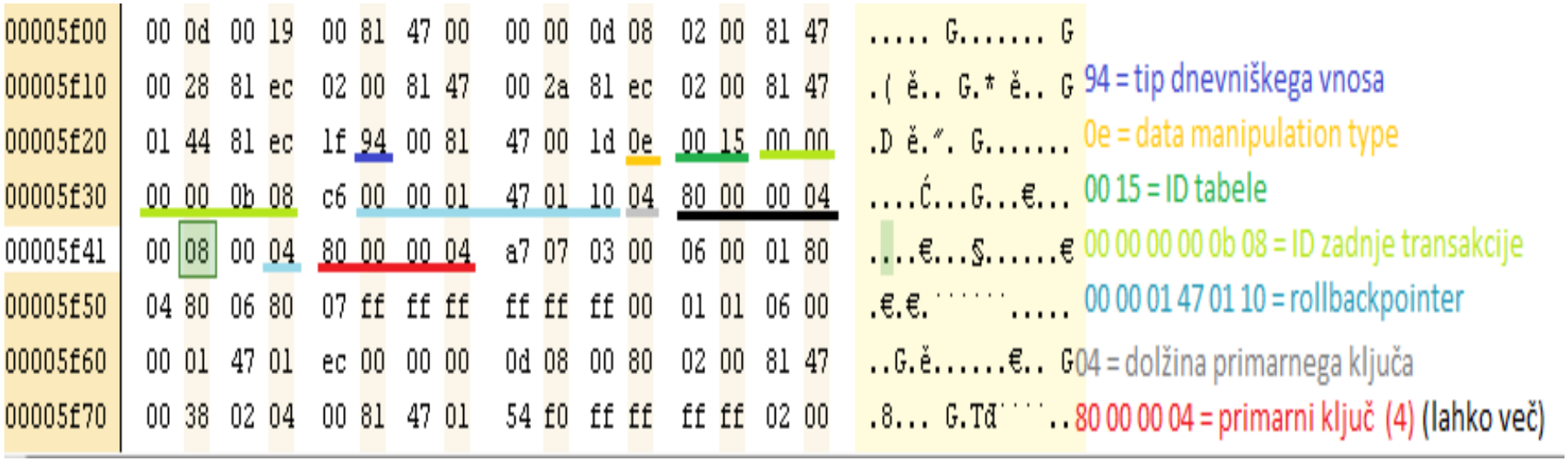


```
00005de0  32 f0 ff ff ff ff 02 00  81 47 00 36 00 04 00 81  2đ˙˙˙˙.. G.6...
00005df0  47 00 46 01 04 00 32 00  4c 81 47 19 14 e5 39 f4  G.F...2.L G..Í9ô
00005e00  00 00 0c 94 00 f9 00 2d  00 00 00 09 00 81 47 00  ...˝.ů.-..... G.
00005e10  00 00 0b 08 02 00 81 47  00 28 81 10 02 00 81 47  ..... G.( ... G
00005e20  00 2a 81 10 02 00 81 47  00 68 81 10 1f 94 00 81  .* ... G.h ..˝.
00005e30  47 00 1e 1c 00 15 00 00  00 00 09 1b e0 94 00 00  G...........ŕ˝..
00005e40  01 46 01 10 04 80 00 00  04 01 04 05 61 70 70 6c  .F...€......appl
00005e50  65 25 07 03 26 07 03 00  06 00 01 80 04 80 06 80  e%..&.....€.€.€
00005e60  07 ff ff ff ff ff ff 00  63 5b 00 08 00 04 06 0a  .˙˙˙˙˙˙.c[.....
00005e70  00 00 10 ff f0 80 00 00  04 00 00 00 00 0b 08 06  ...˙đ€..........
00005e80  00 00 01 47 01 10 73 74  72 61 77 62 65 72 72 79  ...G..strawberry
00005e90  6f 72 61 6e 67 65 6b 69  77 69 1f 02 00 81 47 00  orangekiwi... G.
00005ea0  38 02 04 00 32 00 32 81  47 02 00 32 00 36 78 04  8...2.2 G..2.6x.
00005eb0  00 32 00 38 81 47 02 00  32 00 3c 78 04 00 81 47  .2.8 G..2.<x.. G
```

1c = data manipulation type
00 15 = table ID (fruits po .frm datoteki)
00 00 00 00 09 1b = ID zadnje transakcije
04 = dolžina primarnega ključa
80 00 00 04 = primarni ključ -> 4
01 = eno polje je bilo spremenjeno
04 = četro polje je bilo spremenjeno
05 = dolžina prejšne vrednosti
61-65 = orange

Demonstracija - delete

- DELETE FROM fruits
  WHERE primaryKey=4;



Zaključek

Uspešno smo ugotovili prejšnja stanja podatkovne baze z uporabo metode opisane v seminarski nalogi. Če bi bila omejitev velikosti Redo log datotek neskončna, bi s pomočjo le teh lahko kronološko ugotovili celotno zgodovino spreminjanja podatkovne baze.

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tine Mislej in Blaž Meden

Private browsing

4. Maj
2013

Private browsing?

- Brskalniki hranijo različne podatke o preteklih brskanjih (piškotki, zgodovina, cache, slike, videoposnetki, …)
- Namen: ščitenje uporabnikove zasebnosti (?)
- Incognito (Chrome), Private Browsing (FF, Safari), InPrivate (IE)

2 vidika zaščite zasebnosti

- Lokalno (pred lokalnim napadalcem)

  Uporabnikova aktivnost ne sme ostati zabeležena na napravi (računalniku).

- V spletu (pred spletnim napadalcem)

  Uporabnikova identiteta mora v spletu ostati prikrita.

Zaščita pred lokalnim napadalcem

- Le v primeru, ko napadalec prevzame nadzor nad računalnikom **po** zaključku seje v zasebnem načinu.

- Spletni brskalnik po zaključku seje izbriše vse podatke, ki so se ustvarili v tej seji.

- Problem: Vsi podatki ne smejo biti nujno izbrisani.

Zaščita pred lokalnim napadalcem

4 kategorije podatkov:

- Podatki, ki jih spletno mesto ustvari brez vednosti uporabnika.

- *Podatki, ki jih spletno mesto ustvari s pomočjo uporabnikove interakcije.*

- *Podatki, ki jih ustvari uporabnik.*

- *Podatki, ki niso specifični za uporabnika.*

Zaščita pred spletnim napadalcem

- Napadalec ima nadzor nad spletnimi mesti, ki jih uporabnik obišče.

- 3 cilji:

  Spletno mesto ne sme biti zmožno povezati uporabnika v zasebnem in 'javnem' načinu.

  Spletno mesto ne sme biti zmožno povezati 2 različnih sej uporabnika v zasebnem načinu.

  Spletno mesto ne sme biti zmožno ugotoviti, ali uporabnik brska v zasebnem načinu.

Zaščita pred spletnim napadalcem

- !! Spletno mesto lahko s pomočjo IP naslova in/ali drugih podatkov (resolucija zaslona, nameščeni vtičniki, pisave …) izniči vse 3 cilje.

- “Do not track” (DNT) možnost – zahteva brskalnika po prekinitvi sledenja spletnega mesta uporabniku.

- DNT zahteva ni obvezujoča in jo lahko spletna mesta ingorirajo.

Analiza zasebnega načina brskanja

- Sistematičen postopek z ustreznimi forenzičnimi metodami.
- Analiza najbolj uporabljenih brskalnikov (Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari).
- Primerjava privzetega načina z zasebnim načinom brskanja.

Analiza zasebnega načina brskanja

- Priprava diskov:
  - Prepis diskov z ničlami (3x prepis),
  - namestitev operacijskega sistema (Windows 7),
  - na vsak disk naložen le en brskalnik,
  - vsi brskalniki brez prednaloženih razširitev.

- Konfiguracija diskov izvedena pred priklopom na omrežje.

Analiza zasebnega načina brskanja

- Postavitev forenzičnega okolja:
  - Uporaba okolja za virtualizacijo VmWare ter
  - orodja DaemonFS (za preverjanje integritete in beleženje sprememb na ciljnem sistemu),
  - konfiguracija orodij za analizo sprememb med izvajanjem brskanja.

- DaemonFS nastavljen na beleženje sprememb korenskega imenika (celotne datotečne strukture).

Analiza zasebnega načina brskanja

- Izvedba brskanja v privzetem načinu:
  - Brskanje z uporabo iskalnikov Google in Yahoo,
  - vključuje iskanje (člankov, slik, videov),
  - uporabo uporabniških računov (email, spletno bančništvo)
  - in aktivnosti spletnega nakupovanja.

- Vidne spremembe pri vseh brskalnikih vključujejo datoteke s predpomnilnikom, piškoti, zgodovino ter uporabniške datoteke.

Analiza zasebnega načina brskanja

- Izvedba brskanja v zasebnem načinu:
  - Enake aktivnosti kot pri privzetem načinu,
  - po zaključku brskanja vsi procesi brskalnika preverjeno zaustavljeni,
  - pred in po brskanju izvedeno shranjevanje slike pomnilnika (z orodjem FTK Imager Lite),
  - hkrati prenešen tudi register ter pagefile.sys.

- Po vsakem brskanju računalnik izklopljen in trenutno aktiven disk previdno odstranjen.

Analiza zasebnega načina brskanja

- Forenzična pridobitev evidence:
  - Analiza izvedena s Forensic Toolkitom (FTK) 3.2,
  - priklop posameznega diska preko write-blocker naprave (read-only način dostopa),
  - generiranje slik diskov in izračun izvlečkov,
  - organizacija in analiza podatkov relevantne vrednosti.

Analiza zasebnega načina brskanja

- Rezultati analize:
  - Tudi zasebni način brskanja za seboj pusti sledi,
  - količina sledi odvisna od posameznega brskalnika,
  - pri določenih brskalnikih dovolj podatkov za vzpostavitev povezave z uporabnikom (npr. uporabniška imena in računi - IE),
  - sledi velikokrat najdene na neobičajnih lokacijah,
  - video vsebin ni bilo obnovljenih,
  - glede na količino najdenih informacij si padajoče sledijo: Explorer, Safari ter z približno enako količino Chrome in Firefox.

Analiza zasebnega načina brskanja

- Rezultati analize:
  - Klesanje informacij iz pomnilnika kot najbolj uspešna metoda pridobivanja sledi,
  - za vse analizirane brskalnike najdeni indikatorji uporabe zasebnega brskanja,
  - pridobljene določene informacije o zgodovini brskanja
  - predpomnjene slike (delno ali v celoti),
  - velikokrat opažene spremembe časovnih znamk datotek
  - ter nahajanje informacij v nealociranem prostoru.

Portable browsers

- Spletni brskalniki, nameščeni na prenosnih napravah (USB ključki).
- Prilagojeni uporabniku.
- Vlada prepričanje o večji stopnji zasebnosti.

Raziskava

- Test (portable) spletnega brskalnika Google Chrome.
- Testirani načini:
    - Portable, privzeti način
    - Portable, Incognito način
    - Nameščeni, privzeti način

Raziskava

- Testiranje na podlagi primerjav rezultatov istega spletnega brskanja v vseh načinih.
- (Iskanje videoposnetkov na YouTube, iskanje slik na Google Images, iskanje na eBayu)
- Rezultat raziskave:
  - Največ artefaktov je bilo najdenih na računalniku z

  nameščenim brskalnikom, vendar tudi prenosni brskalnik pusti relativno veliko sledi.

  - Sledi je v obeh primerih dovolj, za rekonstrukcijo

  brskanja.

Raziskava

- Izkazalo se je, da najmanj sledi pusti prenosni brskalnik v zasebnem načinu.

- Google Chrome ni pustil nobenih sledi, razen v datoteki pagefile.sys

- Ta datoteka se velikokrat prepiše, zato je (kvalitetna) forenzična preiskava možna le takoj po zaključku seje.

- SKLEP: Tudi brskanje s prenosnim brskalnikom pušča sledi na gostiteljevem računalniku, zato je stopnja zasebnosti v tem načinu tudi relativno nizka.

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

BLAŽ JERŠAN, ZLATKO HRNČIĆ

ANDROID ANTI-FORENSICS

4. April
2014

Definicija

- Anti-forenzika: Vsak poizkus ogrožanja dostopnosti ali uporabnosti dokazov v forenzičnem procesu

- Za mobilne telefone postaja zanimiva, saj imamo na njih vedno več osebnih podatkov, tako da same naprave postajajo pomembne med forenzičnem postopkom

Uvod

- Mobilni telefoni postajajo vse bolj pogosti
- 2.6 miljarde naročnin (2008)
- 6.8 miljarde naročnin (2013) (96% svetovnega prebivalstva)
- Razredi mobilnih telefonov:
  - Osnovni
  - Napredni
  - Pametni

Tipi anti-forenzike

- 1. Uničevanje dokazov

  - zanimive podatke uničimo, tako da postanejo neuporabni za forenzično analizo

- 2. Skrivanje dokazov

  - želimo zmanjšati ali celo izničiti vidnost dokazov med forenzični analizo

- 3. Uničevanje izvorov dokazov

- 4. Ponarejanje dokazov

  - ustvarjanje ponarejenih verzij dokazov

Anti-forenzika mobilnih naprav

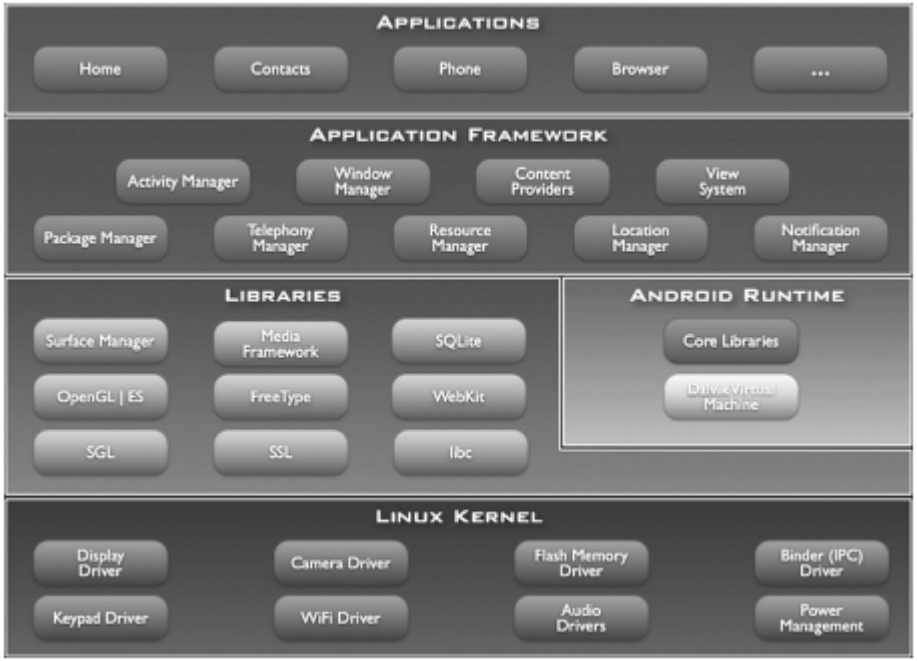
- Tipični forenzični pristopi in orodja pogosto niso primerni
- SIM kartice in spominske (SD) kartice lahko odstranimo in pregledamo z standardnimi procedurami
- Nimamo direktnega dostopa do notranjega pomnilnika, zato je idealni kandidat za uporabo različnih AF tehnik

Android OS

- Odprto kodni operacijski sistem razvit specifično za mobilne naprave
- Poleg OS-a vsebuje še middleware in skupek aplikacij
- Obsega vedno večji tržni delež mobilnih naprav

Android OS - arhitektura

- Sestavljen iz petih glavnih komponent:
  - aplikacije
  - aplikacijski framework
  - knjižnjice
  - android runtime
  - linux kernel



Android OS - varnost

- Izkorišča standardne Linux objekte za upravljanje s procesi in uporabniki, večino varnosti je zaradi tega zagotovljene že na ravni procesov
- Aplikacijam je prepovedano dostopanje oz. manipuliranje z drugimi aplikacijami, OS-om in uporabniškimi datotekami (kontakti, sporočila, ...), razen če jim je to eksplicitno dovoljeno
- Vsaka aplikacija je tretirana kot ločen Linux uporabnik
- Vsa dovoljenja, ki jih damo določeni aplikaciji so določena ob inštalaciji in se kasneje ne morejo spreminjati

Andorid anti-forenzika

- Možna orodja in tehnike
- Zasebna mapa
- Postopek izvoza dokazov
- Postopek uvoza dokazov
- Postopek uničevanja dokazov

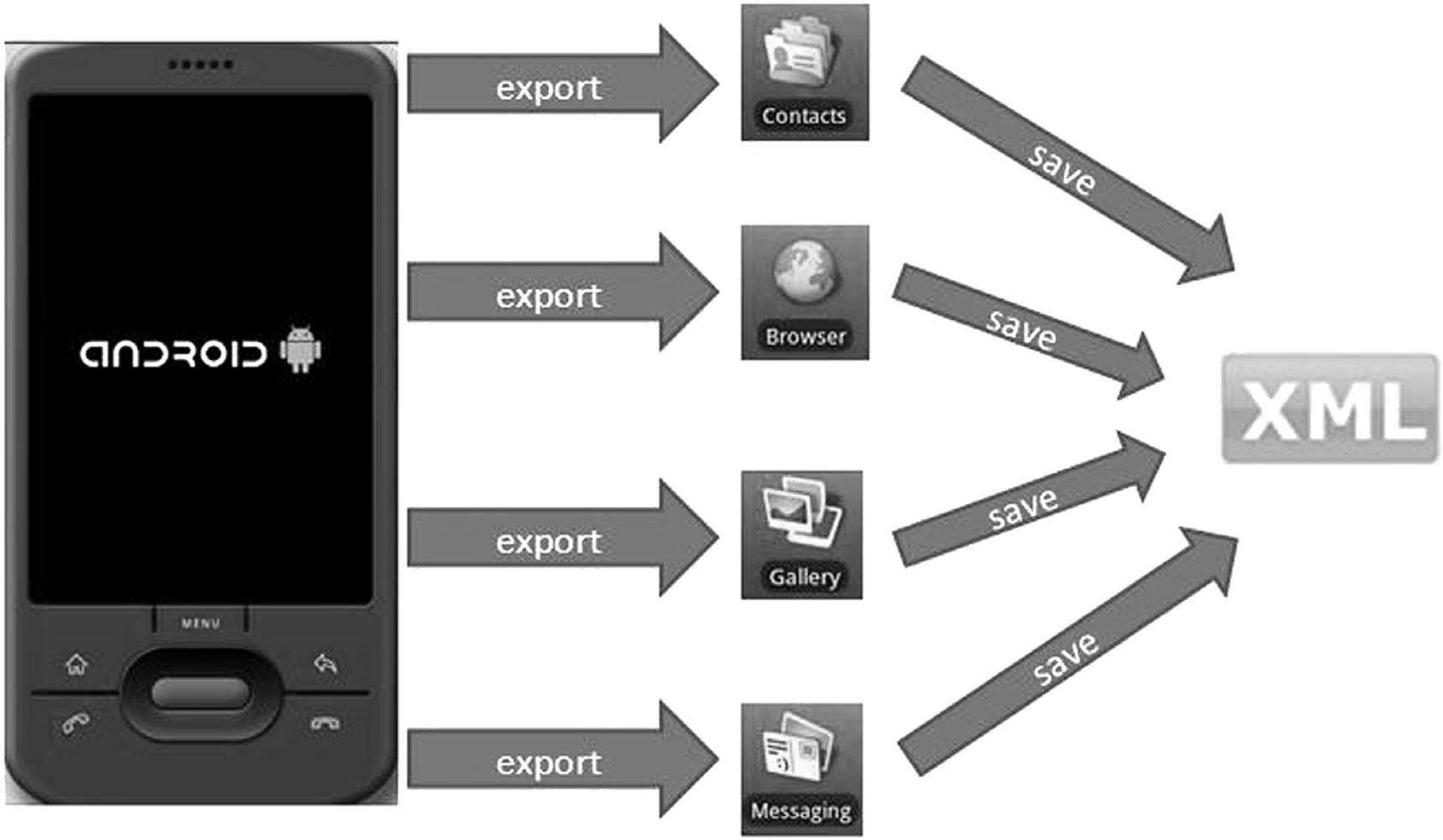
Možna orodja in tehnike

- Android debug bridge(ADB) – interakcija mobilne naprave in oddaljene delovne postaje
- Nandroid backup – kopiranje in obnovitev podatkov
- Fizično preslikovanje z dd – uporaba ukazov Unix komandne linije
- Komercialna orodja - Mobile Internal Acquisition Tool (MIAT)
- Mobilna aplikacija – AFDroid

Zasebna mapa

- Kreiranje v internem pomnilniku pri namestitvi aplikacije
- Nedostopna za vse druge aplikacije
- Shranjevanje vseh vrst informacij
- Brisanje celotne vsebine pri odstranjevanju aplikacije
- Šifriranje vsebine

Izvoz dokazov



Izvoz dokazov

- Brisanje dokazov
  - sporočila, zaznamki brskalnika, dnevnik klicev
  - tajno shranjevanje v zasebni mapi
- Skrivanje dokazov
  - multimedijske datoteke s pomnilniške kartice
- Odstranjevanje virov dokazov
  - multimedijska sporočila
  - spreminjanje identifikatorja pogovora
- Ponarejanje dokazov
  - informacije o stikih
  - priljubljeni stiki in število medsebojnih interakcij

Uvoz dokazov

- Skladiščenje dokazov
  - XML datoteka

```
<database name='BROWSER'>
<table name='bookmarks'>
<row>
    <col name='_id'>1</col>
    <col name='title'>Google</col>
    <col name='url'>http://www.google.com/</col>
    <col name='visits'>7</col>
    <col name='date'>1263761875450</col>
    <col name='created'>0</col>
    <col name='description'>null</col>
    <col name='bookmark'>1</col>
</row>
</table>
</database>
```

- Težave: dostopnost prejšnje slike, obvladovanje orodij, dostopnost opreme

Uničevanje dokazov

- Avtomatski proces
  - brisanje pri odstranjevanju aplikacije
  - izogibanje človeške napake

- Obnova podatkov
  - možnost obnovitve izbrisanih podatkov?
  - Android Data Recovery?

Eksperimenti

- Uporabljeni napravi:
  - Samsung Galaxy i7500, 1.6 SDK
  - HTC Magic 32b, 2.1 SDK
- Uporabljena orodja:
  - MIAT for Android (miaforensics.org)
  - Nandroid
- Eksperimenta:
  - EEP – evidence export process
  - EDP – evidence destruction process

EEP – evidence export process

- Potek poizkusa:
  - Slika naprave z Nandroid orodjem
  - Izvedba AFDroid programa
  - Pridobitev z MIAT orodjem
  - Druga slika naprave z Nandroid orodjem

EEP - rezultati

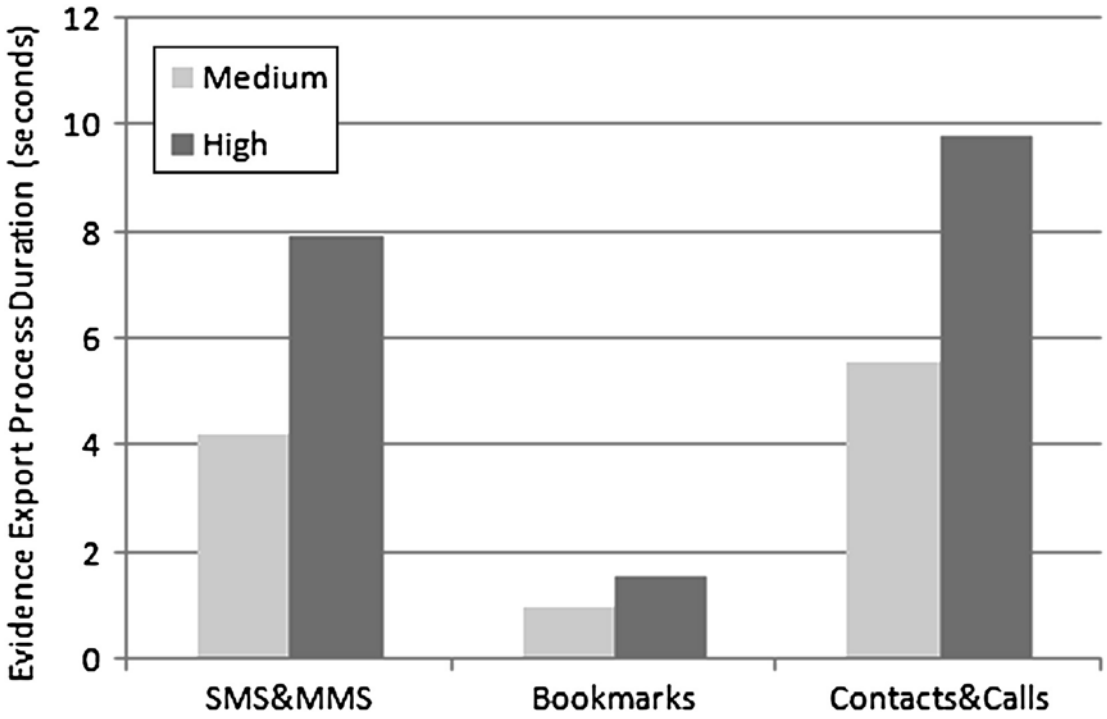


Table 3 – Test Cases for the EEP described in terms of number of elements stored by the target databases.

Load	Contacts & calls	SMS & MMS	Bookmarks
Medium	120	250	45
High	222	591	93

EDP – evidence destruction process

- Potek poizkusa:
  - Slika naprave z Nandroid orodjem
  - Izvedba AFDroid programa
  - Druga slika naprave z Nandroid orodjem
  - Brisanje AFDroid programa
  - Pridobitev z MIAT ordojem
  - Tretja slika naprave z Nandroid orodjem
- Rezultat poizkusa:
  - Orodja niso bila zmožna pridobiti nobene dadoteke po brisanju programa

Zaključek

- Ogromen porast uporabe pametnih telefonov
  - vse več koristnih dokazov v pomnilniku
  - sporočila, stiki, multimedija, brskalniki...
- Slabo razvita mobilna forenzika
  - pomanjkanje orodij in znanj
  - implementacija operacijskih sistemov
- Prihodnost?

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Anton Semprimožnik
mag. Matej Andolšek
Andraž Pajtler

Automated Data Collection and Reporting from a Mobile Device

22. September 2012

Problem

- Novi mobilni operacijski sistemi niso več orientirani na podjetja, temveč na posameznike
- Posledično večanje nevarnosti za varovanje podatkov v podjetjih
- Podjetja uvajajo princip BYOD
- Novi OS nimajo vgrajenega MDM
- Naraščanje third-party MDM sistemov
- Potreba po striktnih varnostnih pravilih za mobilno varnost
- Pomanjkanje funkcionalnosti za avtomatizirano zbiranje uporabniških podatkov
- Te podatki omogočajo visok varnostni nivo

Rešitev

- Android aplikacija
- Monitoriranje android poslovnih naprav
- Cilj so notranje preiskave
- Shranjevanje v lokalno podatkovno bazo na telefonu
- Sinhronizacija z zalednim Ubuntu serverjem (PHP, Apache)
- Lokalna SQLite baza je kriptirana
- Sinhronizacija preko HTTPS protokola

Področje reševanja

Komu so podatki namenjeni?

- Forenzičnim preiskovalcem
- Varnostnim revizorjem

Kaj preiskujemo?

- Kršitve pravil podjetja
- Krajo intelektualne lastnine
- Zloraba podatkov
- Poneverbe
- Sabotaže
- Vohunstvo

Ozadje problema

Model varnosti

- Aplikacije in uporabnik so v peskovniku
- Dovoljenja apikacij morajo biti jasno določena

Rootanje naprave obide varnostni model android – želimo se izogniti rootanju

Vir podatkov (**bold – uporabno za monitoriranje**):

- Aktivnost – uporabniški vmesnik
- Service – dolgo delujoče operacije
- Content provider – uprablanje dostopa do podatkov
- **Broadcast Receiver – upravlja notifikacije**
- **Content Observer – zazna spremembe**
- **Alarm – uprablanje operacij**

Povezano delo

Mobile Device Management (MDM)

- Zenprise
- AirWatch
- MobileIron

Ponujajo SAMO SMS in GPS monitoriranje

- Junuper – zajem večine podatkov

Forensic Snapshots

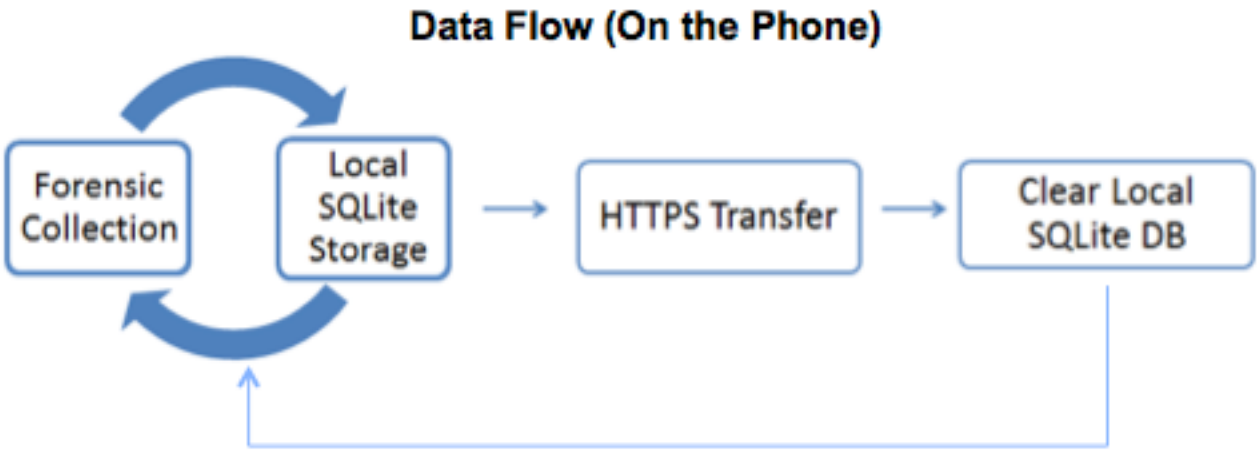
- Encase Enterprise
- AFLogical

Ostali sistemi za monitoriranje

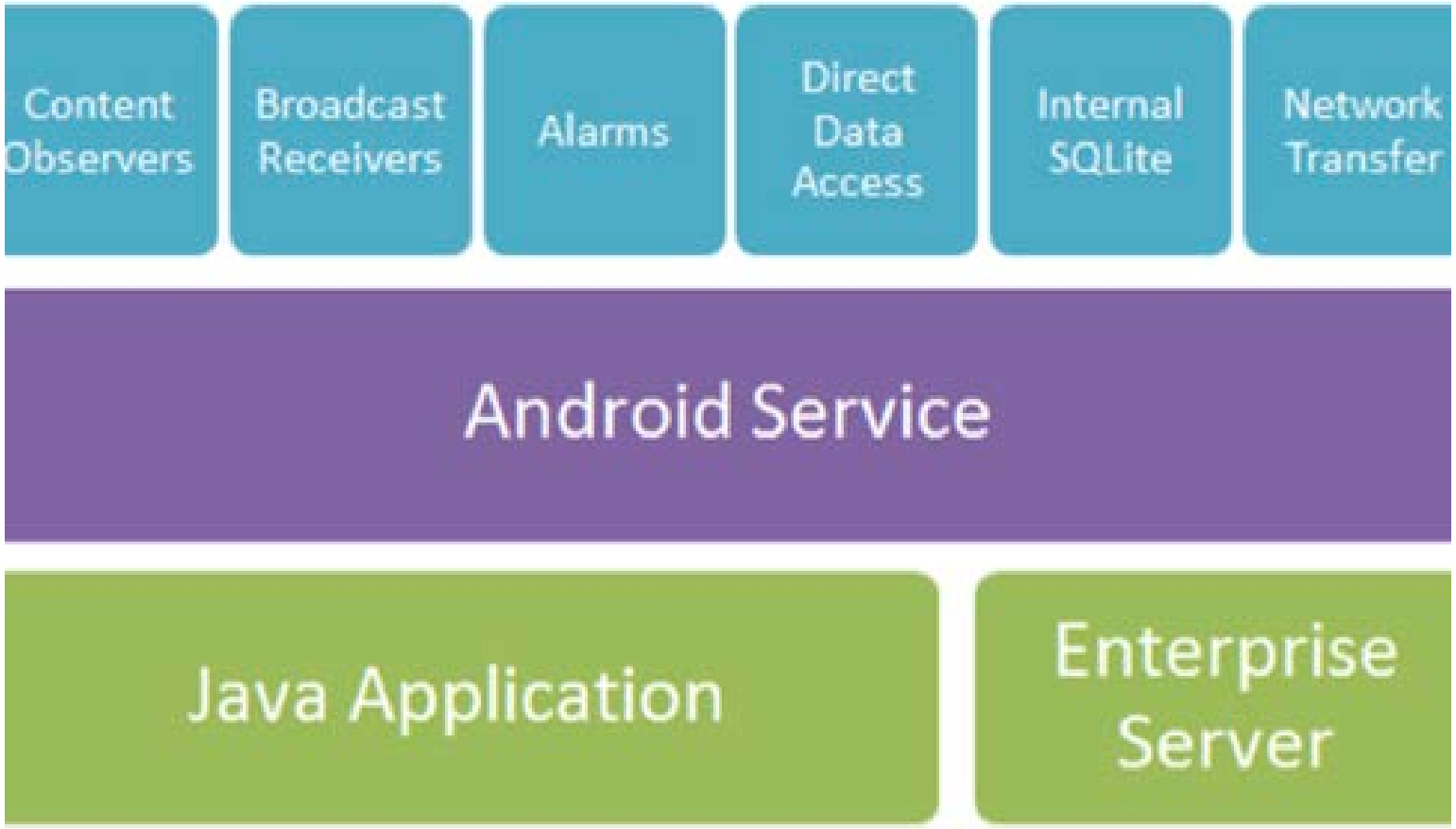
- Osebne vohunske aplikacije

Aplikacija DroidWatch - načrt

- Ponavljajoče zajemanje podatkov
- Prenos podatkov na strežnik podjetja
- Nadzor aplikacijskih komponent za zbiranje podatkov



Aplikacija DroidWatch - načrt



Aplikacija DroidWatch – implementacija

- Na voljo 17 podatkovnih tipov – 15 zbranih

Data set	App component used		
	Broadcast receiver	Content observer	Alarm
App install/removal	✓		
Browser navigation			✓
Browser search			✓
Calendar event			✓
Call log		✓	
Contact list		✓	
Device account[a]			
Device ID			✓
GPS location			✓
GPS location setting	✓		
MMS	✓		✓
Picture gallery		✓	
Screen lock status	✓		
SMS	✓	✓	
Third-party app log			✓

Aplikacija DroidWatch – implementacija

- Zbrani podatki se hranijo v lokalni SQLite bazi
- Dostop samo s strani aplikacije
- Periodni prenos podatkov iz lokalne baze na strežnik
- Periodni prenos v ozadju, ne vpliva na uporabniško izkušnjo

- Ubuntu, Apache, MySQL

Aplikacija DroidWatch – Analiza in evaluacija

- Eksperimen zajemanja podatkov za notranjo preiskavo
- Splošni tredni uporabe naprave (beleženje odklepanja zaslona)
- Sumljivi kontakti in komunikacije
- Lokacijsko monitoriranje
- Spletna zgodovina
- Slabogramje
- Anti forenzika
- Uničevanje dokazov
- Skrivanje dokazov
- Modificiranje zajetih podakov
- Detektiranje forenzičnih aplikacij

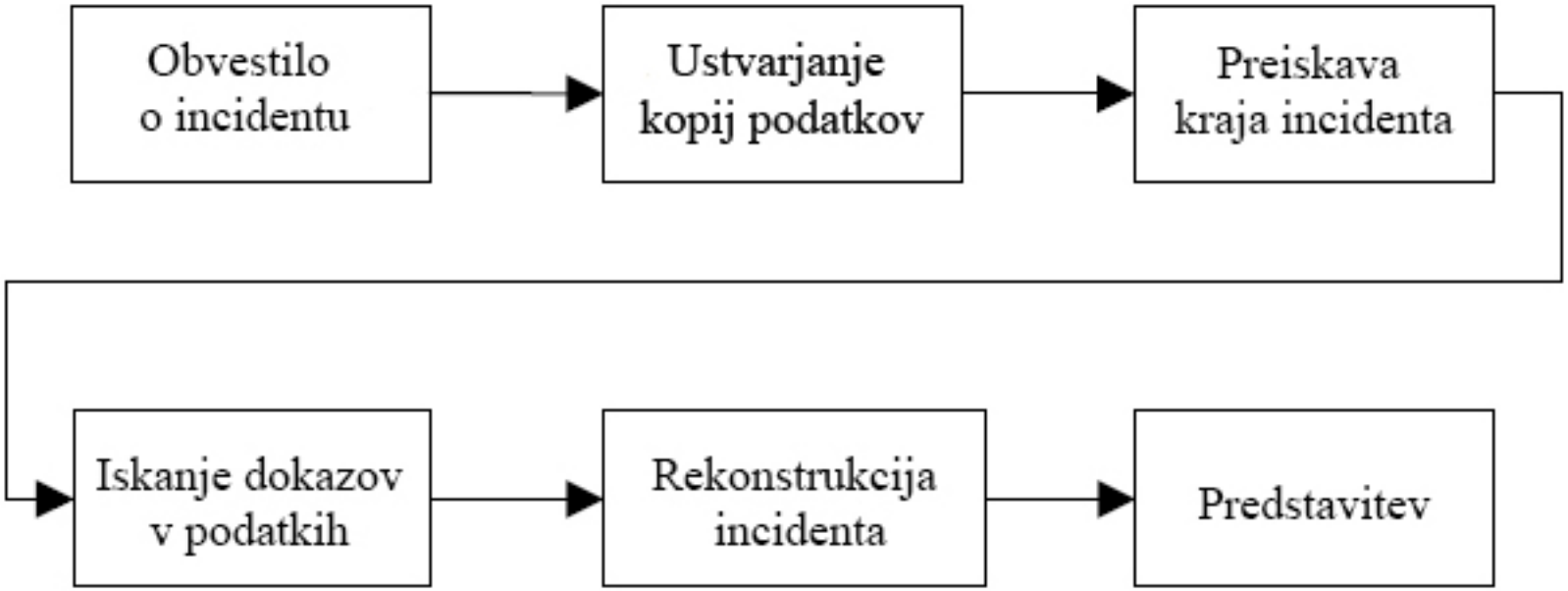
Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Jernej Grosar in Andraž Gregorčič

PLATFORMA ZA OCENJEVANJE FORENZIČNIH ORODJI ZA KREIRANJE SLIKE DELOVNEGA POMNILNIKA

5. Maj 2014

Faze digitalnega preiskovanja



Vir: *A hardware-based memory acquisition procedure for digital investigations – http://grandideastudio.com/wp-content/uploads/tribble_paper.pdf*

Tehnike zajema slik

- Crash Dumps
- LiveKd Dumps
- Hibernation Files
- Firewire
- Cold and Warm reboots
- Virtual Machine Imaging

Članek

- Splošno
- Kriteriji za celovitost slike pomnilnika
- Metode zajema pomnilniške slike na MS Windows
- Arhitektura meritvene platforme
- Preučevanje in rezultati
- Omejitve platforme
- Operativne zmogljivosti orodji za izdelavo slik delovnega pomnilnika

Splošno

- Pridobivanje podatkov iz pomnilnika vedno bolj pomembno
- V zadnjih letih se je to področje zelo razvilo
- V članku je predstavljena arhitektura platforme za določanje pravilnosti, atomarnosti in integritete orodji za zajem pomnilniške slike

Kriteriji za celovitost slike pomnilnika

- Pravilnost:

  zajeta pomnilniška slika je pravilna, če so vrednosti slike za vsa zajeta področja enaka vrednosti pomnilnika ob času zajema.

- Atomarnost:

  slika mora vsebovati podatke celotnega pomnilnika, kateri se nahajajo v njem ob času T (ne prej in ne kasneje).

- Integriteta:

  pomeni, da se vrednosti pomnilniških področji, katera so bila zapisana v sliko niso spremenila po času T.

Metode zajema pomnilniške slike na MS Windows

- Nekoč se je na MS Windowsih uporabljal objekt \\.\Device\PhysicalMemory
- Danes dostop do objekta v uporabniškem prostoru ni več mogoč
- Potrebna uporaba namenskih gonilnikov
- Lahko se pojavijo napake

Arhitektura meritvene platforme

- Odprtokodni Bochs x86 PC emulator
- Uporabljen pristop “bele škatle”
- Večina kode je napisana v C-ju
- Del kode tudi v asemblerju

Preučevanje in rezultati

- Preučevanje:
  - Tri orodja za pregledovanje pomnilnika
  - Računalniški sistem(Intel i5-650, 8GB RAM)
  - 270 eksperimentov

- Rezultati:
  - Pravilnost
  - Atomarnost
  - Integriteta

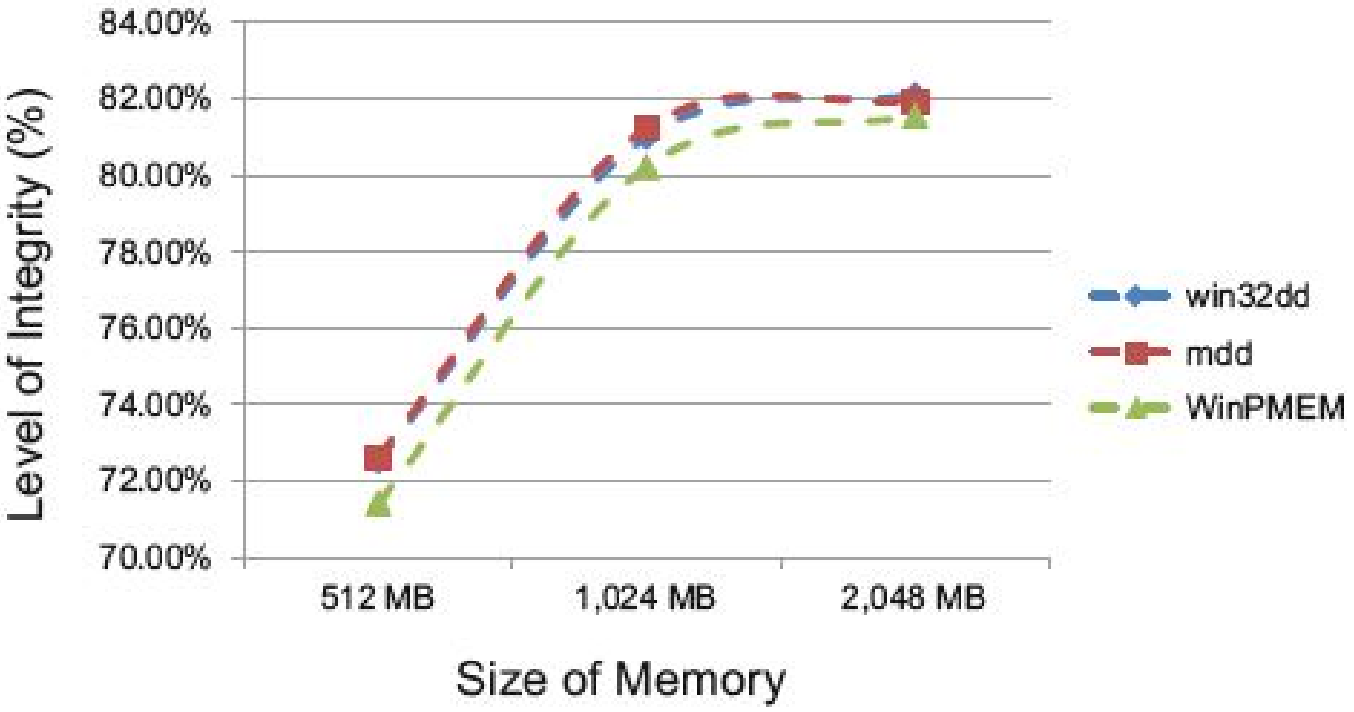
Omejitve platforme

- Poganjanje samo 32-bitnih aplikacij

- Velikost pomnilnika samo 2GB

Operativne zmogljivosti orodji za izdelavo slik delovnega pomnilnika

- Vsa orodja kažejo podobno zmogljivost



Druga orodja

- Programske rešitve
- Strojna orodja

Programske rešitve

- Windows:
  - Belkasoft Live RAM Caputer
  - HBGary
  - FTK Imager
- Linux:
  - /dev/mem
  - /dev/crash
  - Second Look: Linux Memory Forensics
- Mac OS X:
  - Goldfish
  - Mac Memory Reader
- Virtual:
  - Bochs
  - Xen
  - Quemu

Strojna oprema

- Tribble PCI Card (research project)
- Windows Scope CaptureGUARD
- Forensic RAM Extraction Device (FRED) by BBN

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Peter Dolenc in Gašper Žgajnar

-

IMPROVED RECOVERY AND RECONSTRUCTION OF DEFLATED FILES

3. Maj
2014

Metoda za obnovo poškodovanih datotek stisnjenih z algoritmom DEFLATE

Prebran članek:

“Improved Recovery and Reconstruction of DEFLATEd Files”

Ralf Brown

DFRWS 2013

Pregled

1. Algoritem DEFLATE
2. Rekonstrukcija poškodovanega arhiva

1. Rezultati
2. Nadaljnji razvoj, konkurenca…

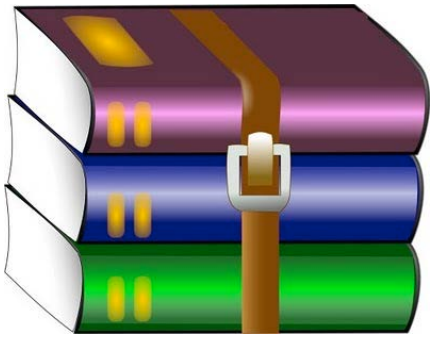
Algoritem DEFLATE

Algoritem DEFLATE

- Brezizgubno stiskanje podatkov

- Kombinacija:
  - **LZ77**: uporaba kodov iz prejšnjega bloka
  - **Huffmanovega kodiranja**

- Uporaba: ZIP, PNG, XML, nekaterih omrežnih protokolih...



Algoritem DEFLATE – blokovna obdelava

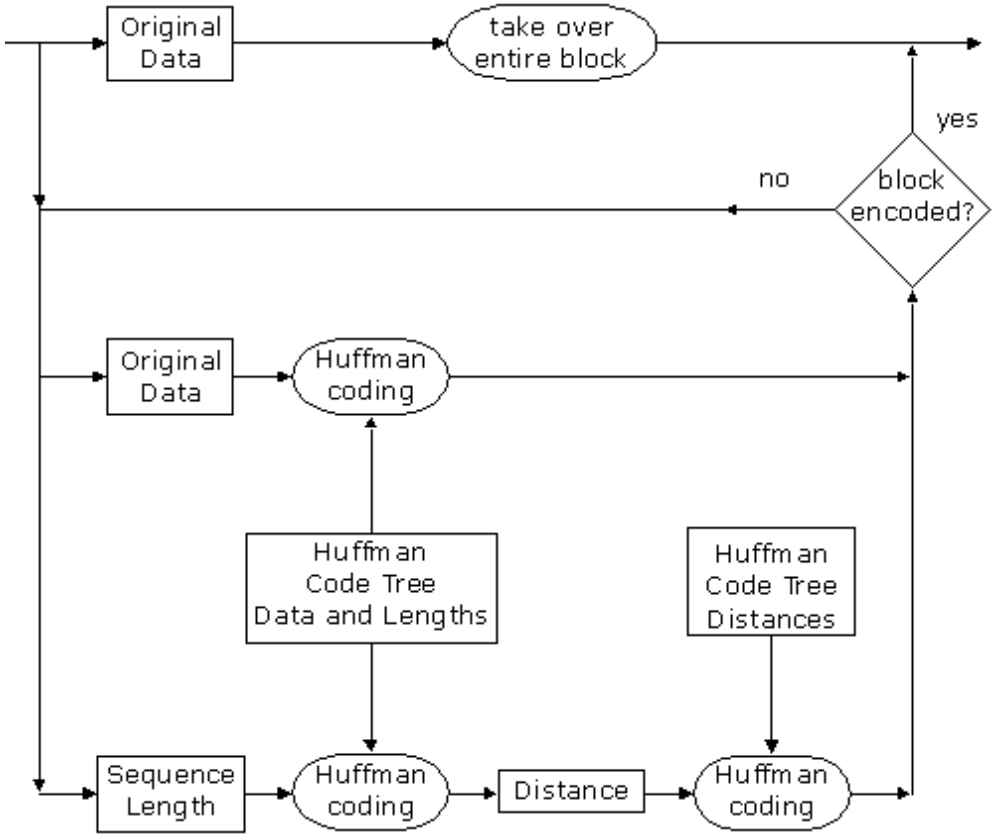
- Deluje nad tokom podatkov
- Obdelava blok po blok
- Vsak blok ima header:
  - Zadnji blok?
  - Način kompresiranja:
    - Nestisnjen blok
    - Stisnjen s standardno tabelo
    - Stisnjen z lastno tabelo

Algoritem DEFLATE - stiskanje

2 koraka stiskanja:

1. Izločanje sekvenc ki so se že pojavile – LZ77

2. Zgoščevanje bitnega zapisa – Huffmanov kod



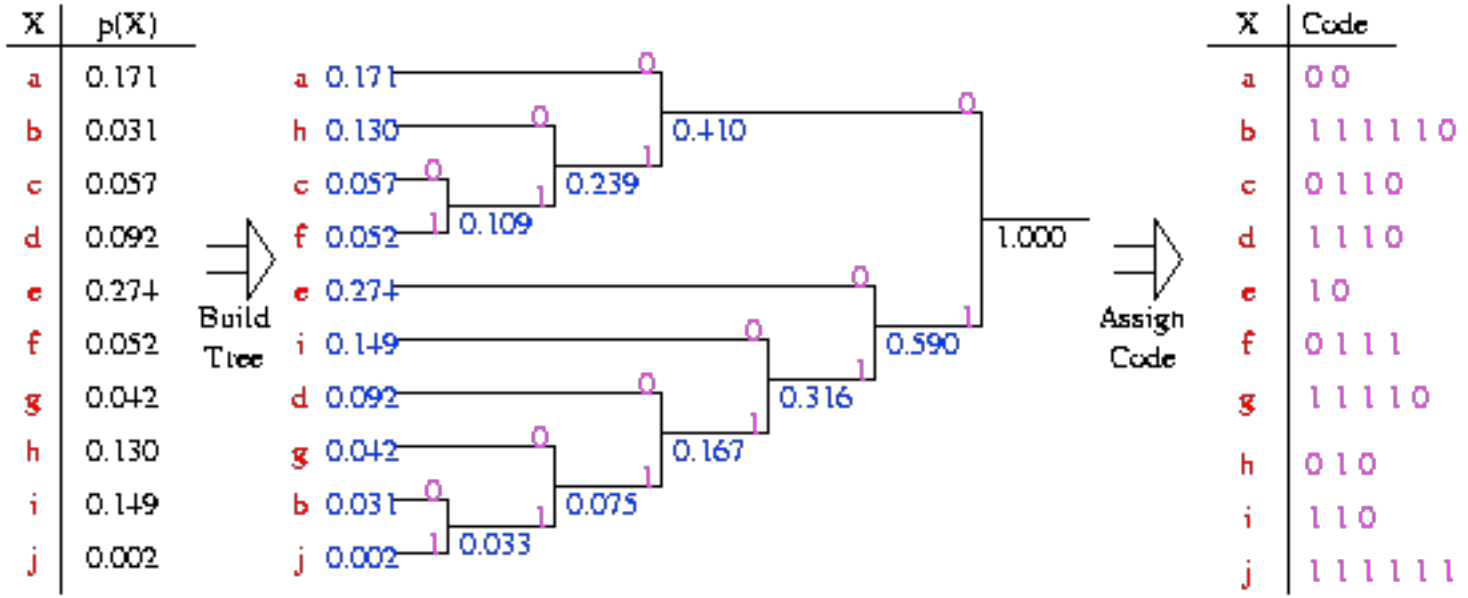
Algoritem DEFLATE – izločanje ponavljanja

- Bistvo LZ77
- Ponavljajoče sekvence glede na zadnjih 32kB podatkov

```
Blah blah blah blah blah!


 vvvvv
Blah blah blah blah blah!
      ^^^^^


Blah blah b


Blah b[D=5,L=5]
```

Algoritem DEFLATE – Huffmanov kod

- Simboli se nadomestijo z uteženimi simboli (glede na pogostost uporabe)
  - Daljši, pogostejši simboli v krajše simbole
  - Krajši, manj pogosti v daljše simbole



Algoritem DEFLATE – Občutljivost dekompresiranja podatkov

- Niz bitov lahko predstavlja:
  - zaporedje Huffmanovih simbolov
  - kazalec na ponavljajočo sekvenco

- Možnosti napak:
  - napačen Huffmanov simbol
  - napačna lokacija ponavljajoče sekvence

- Napaka se prenaša v naslednje bloke.

Rekonstrukcija poškodovanega arhiva

Rekonstrukcija poškodovanega arhiva - testiranje

- Text of the Europarl corpus
- 21 jezikov
- ZIP-an
- Umetna poškodba: 128 – 4096 B

These people were received and cared for by that town, but quite remarkably, they claimed to have been dropped across the border by the French police. The police had picked them up in Calais, taken them from Calais to the Belgian border and had no qualms about subsequently dropping them off in Belgium. A very strange business, all the more so because, according to other witness statements, it appears that this is not the first time this has happened.

Fortunately, this incident has been settled at the highest level between the French and Belgian authorities, and it appears that they found a way of discussing it. However, to my great surprise, I was informed by a Belgian that it is not just the French who get up to these tricks, but also the Dutch and Germans. When I asked him if the Belgians do the same thing, he confirmed this and said, now and again. This leads me to conclude that everyone still has the standard European reflex, namely to pass on their problems to their neighbours.

In my opinion, it is high time that we, as European legislator and as European Parliament, at least pressed for a European reflex. Just as Europe did too little during the oil crisis, it is also making its presence felt insufficiently with regard to this disturbing problem.

Rekonstrukcija poškodovanega arhiva – postopek, metode

1. Odkrivanje napake
2. Obnova napake
3. Rekonstrukcija kazalcev z uporabo konteksta
4. Poravnava okna z zgodovino

Rekonstrukcija poškodovanega arhiva – odkrivanje napake

- Če vemo kje je napaka, jo lahko izpustimo.
  - Težka zaznava
  - Zaznamo jo na koncu, kopreverjamo CRC.
  - Lahko zaznamo, ko je vsaj 128 zaporedno enakih bajtov (00000000….).

- Kje ob odkriti napaki nadaljevati postopek?
  - Resinhronizacijska točka

Rekonstrukcija poškodovanega arhiva – obnova napake

These people were received and cared for by that town, but quite remaonal record for me this autumn!

Yes indeed, Mrs Thors, we shall amend the Minutes accordingly.
(The Minutes were approved)

Presidency communication on the situation in the Middle East
Ladies and gentlemen, in the last few ˆ@-
ˆ@ˆ@ˆ@serious mˆ@ˆ@ˆ@ˆ@ˆ@em. Pleass-
ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@-
ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@e
Comn. Itway of ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ess.
ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@-
ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@ˆ@wtemenhItwanday,Fd
woud a wayˆ@ˆ@ˆ@esspoin-Offhave righset-
ndaould ask ainlgradl youe rtweir sorr!

Yes encyproved)
inhore rigThursdn. Itway of ˆ@ˆ@ˆ@ˆ@-
ˆ@ˆ@euld u Biarritz. Ie the requeomorHg
in theso sychange sur ths all tawith at p is
aayproved)

(a) Standard decompression

These people were received and cared for by
that town, but quite rema??????h????n????F?-
?????????????????????????????????set????????-
????????????l???????twe????????????????????-
???????hor????????????????????????????e????-
u???????????????????????????H????????????y??-
?????sur???s??????a??????????????a???????????-
????????????????????????????????g???u??????-
??s???????s???????????????Dut???????Ger???s?-
??????I????e????m???????????????s???????????-
???h?????????o????m????????????????,????????-
?????????????l????????????o??????????????????-
?????????has???????????rd?????????????lex,???-
??l??????ass???????ir????????????????ir?n????-
b?????
??????????????????? ????????????????????????-
?????????l???????o????????????????????????-
??????????????p?????????????????????????lex.
J????????????????????????t???????????????-
????c??sis?????????????????????s?p???????
?????in??????????l???????????????????????????-
urb??????????????????????????? S???ckx??????-
????no????????????????????????????????????-
?????????????????????????????????????f????????-
?????????????s??????????????????????s?

(b) Recovered

Rekonstrukcija poškodovanega arhiva – rekonstrukcija kazalcev

- Neznani bajti so lahko kazalci na znane
  - Kontekst besedila
- *n*-gram model (n=7,8)
- Desni, levi kontekst
- Ujemanje od daljšega proti krajšemu
- Rezultat zaupanja
- Kaskadno izboljšanje

```
Text: ..  t ? e _ o ? ? ? _ o n e ...
Left:     t ? e _ o ?               - no match
.           ? e _ o ?               - no match
.             e _ o f               p=0.4
.             e _ o n               p=0.6
Right:                ? ? ? _ o n e   - no mtc
.                     n l y _ o n     p=0.9
.                     f o r _ o n     p=0.1
```

Weighted probabilities added to 'f' and 'n'.

```
Text: ..  t ? e _ o ? ? ? _ o n e ...
Len=6:      ? e _ o ? ?           - too ambig
.             e _ o ? ? ?         - no match
.               _ o ? ? ? _       - no match
.                 o ? ? ? _ o     - no match
Len=5:        e _ o ? ?           - no match
.               _ o ? ? ?         - too ambig
.                 o n l y _       p=0.3
```

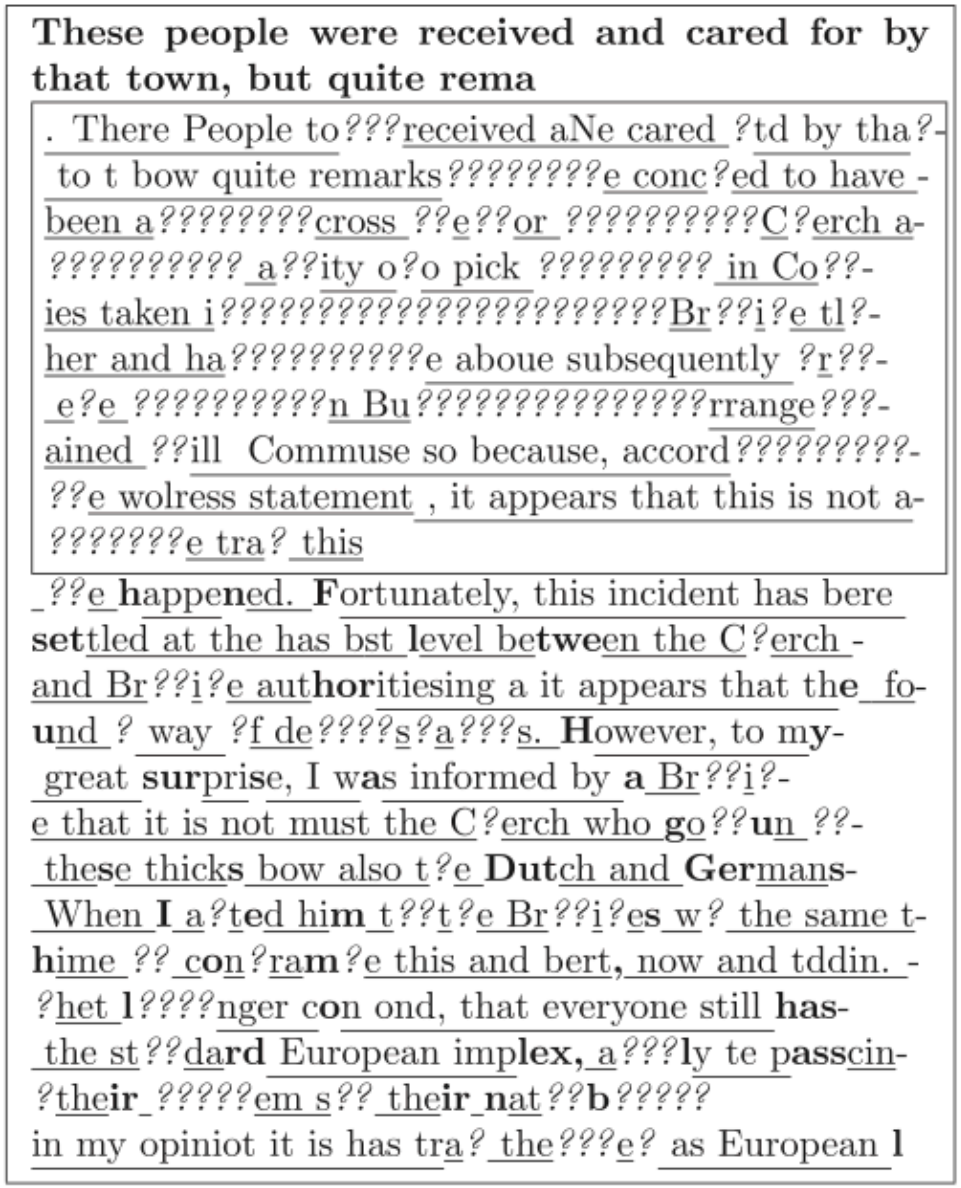
Score for 'n' incremented.

$$ratio = min\left(10000, \frac{highest}{second}\right)$$

$$diff = highest - second$$

$$conf = \sqrt{\frac{context}{occur}} \times (\lambda\ log\ (ratio) \times \mu\ log\ (1 + diff))$$

Rekonstrukcija poškodovanega arhiva



(c) Simple Reconstruction

Rekonstrukcija poškodovanega arhiva – poravnava okna z zgodovino

- Po rekonstrukciji lahko določimo število poškodovanih bajtov
- Vsa naslavljanja na bajte pred poškodbo lahko odpravimo
- Točkovanje vsake poravnave
- Poravnava okna

```
These people were received and cared for by
 The e People wh????ectived ?N? cared ??? b
----------------0000--------0-0-------000--
Net score: -34
```

```
These people were received and cared for by
The e People wh????ectived ?N? cared ??? by
+++-++-+++++++-0000++-+++++0-0+++++++000+++
Net score: +24
```

```
These people were received and cared for by
he e People wh????ectived ?N? cared ??? by
--------------0000--------0-0-------000----
Net score: -34
```

Rezultat rekonstrukcije

These people were received and cared for by that town, but quite remaonal record for me this autumn!

Yes indeed, Mrs Thors, we shall amend the Minutes accordingly.
(The Minutes were approved)

Presidency communication on the situation in the Middle East
Ladies and gentlemen, in the last few ^@-
^@^@^@serious m^@^@^@^@^@em. Pleass-
^@^@^@^@^@^@^@^@^@^@^@^@^@^@-
^@^@^@^@^@^@^@^@^@^@^@^@^@^@e
Comn. Itway of ^@^@^@^@^@^@^@ess.
^@^@^@^@^@^@^@^@^@^@^@^@^@^@-
^@^@^@^@^@^@^@wtemenhItwanday,Fd
woud a way^@^@^@esspoin-Offhave righset-
ndaould ask ainlgradl youe rtweir sorr!

Yes encyproved)
inhore rigThursdn. Itway of ^@^@^@^@-
^@^@euld u Biarritz. Ie the requeomorHg
in theso sychange sur ths all tawith at p is
aayproved)

(a) Standard decompression

These people were received and cared for
by that town, but quite remarks????????-
e coun?ed to have been a????????Kroes ??-
e bor ??????????C?ench a?????????? a??ite t-
?o pick ????????? in Co? it taken i?????????-
??????????????B?utiae te?her and ha??????-
????s abooe subsequently draws??e ???????-
s in Br???????????????rrange???line t??ill ?-
ommuse so because accord???????????e wolress -
statement , it appears that this is not a???????-
e time this has happened. Fortunately, this incident has been settled at the highest level between the C?-
ench and B?utiae authorities, and it appears that th-
ey found a way of discussing it. However, to my great surprise, I was informed by a B?utiae that it is not -
just the C?ench who get up to these tricks, but also the Dutch and Germans. When I asked him if the B?utiaes do the same thing, he confirmed this and said, now and again. This leads me to conclude that everyone still has the standard European reflex, namely to pass on their problems to their neighbours. In my opinion, it is high time that we, as European legislator and as European Parliament, at least pressed for a European reflex. Just as Europe did too little during the oil crisis, it is also making its presence felt insufficiently with regard to this disturbing problem.

(d) Reconstruction with Realignment

Rezultati za različne jezike

Lang	Old algorithm (ZipRec 0.9)		New algorithm (ZipRec 1.0)		Absolute % Change
	Rec%	Corr%	Rec%	Corr%	
bg	82.55	70.44	98.00	97.00	+36.91
cs	83.45	73.30	96.78	95.58	+31.34
da	87.03	86.78	93.09	95.26	+13.15
de	88.35	91.44	96.55	95.84	+11.75
el	91.56	58.26	99.20	99.19	+45.05
en	87.60	89.58	92.72	95.07	+9.67
es	87.35	87.82	92.74	94.92	+11.32
et	84.72	78.60	95.96	95.10	+24.67
fi	85.29	84.23	92.16	93.97	+14.76
fr	87.65	87.91	93.22	95.39	+11.87
hu	86.67	73.82	97.25	96.67	+30.03
it	87.02	89.66	91.08	93.73	+7.34
lt	84.87	76.64	96.43	94.60	+26.18
lv	82.39	73.60	96.42	93.50	+29.52
nl	94.29	90.01	98.48	98.08	+11.72
pl	85.39	78.96	97.10	96.29	+26.07
pt	88.06	85.96	94.00	95.23	+13.82
ro	80.43	78.12	96.43	93.18	+27.02
sk	94.89	86.12	98.69	98.69	+15.68
sl	81.62	78.75	95.81	93.53	+25.34
sv	87.63	84.01	93.53	95.25	+15.46
AVG	86.61	81.14	95.50	95.52	+20.89

Dosedanje metode

- Obstajajo metode, ki razpakirajo nepoškodavne dele datoteke
- Malo (nobena) ne poskuša razpakirati poškodovanih delov
- Gzip Recovery Toolkit
- Bit-by-bit scan

Nadaljni razvoj

- GUI za označevanje poškodovanih območji
- Obratno iskanje (reverse search) za določanje možnih oblih Huffmanovega drevesa
- Zmanjšanje števila odstranjenih bitov pri potnovni sinhronizaciji
- Izboljšave za XML

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Rok Bajec, Jan Robas

KLASIFIKACIJA KODIRANJA FRAGMENT DATOTEK - EMPIRIČNI PRISTOP

4. maj
2014

Vsebina

- Uvod
- Obstoječi pristopi
- Izzivi
- Formulacija problema
- Splošni klasifikatorji
- Stisnjeni podatki z DEFLATE
- Konkretni klasifikatorji
- Stisnjeni podatki in zsniff
- Zaključek

Uvod

- Ideja klasifikacije kodiranja
- Uporabnost pri forenziki
- Hitrost klasifikacije
- Točnost klasifikacije

Obstoječi pristopi

- strojno učenje
- histogram ASCII znakov
- različne statistične metode oziroma kombinacija njih

Izzivi

- kompleksni tipi datotek (kot npr. dokumenti docx) lahko vsebujejo različne tipe vsebin (slike, video..)
- Izbira primerne klasifikacije
- podatki stisnjeni z algoritmom DEFLATE (png, zip, docx, pptx, xlsx, izvršilne datoteke s stisnjeno vsebino...)
- Velikost delčkov datotek

Kaj se moramo vprašati?

- kakšno je osnovno (primitivno) kodiranje fragmenta
- ali kodiranje vsebuje rekurzivna kodiranja (če gre na primer za jpeg sliko, zapisano v base64)
- ali je fragment del sestavljene strukture (slika v docx)

Načini klasifikacije

- **entropija** (visoka, srednja, nizka)
- **Base16/32/64/85** (vsebuje le točno določene znake)
- **iskanje N-gramov** - ključnih nizov, s katerimi prepoznamo kodiranje
- **razčlenjevalniki (angl. parser)**
  - ***mp3* -** okvirji: 12 bitov, nastavljenih na 1 na začetku vsakega okvirja + glava okvirja z osnovnimi informacijami (bitna hitrost, hitrost vzorčenja..)
  - ***jpeg* -** preprosta glava, FF00 na vsakih 191 bajtov
- ***png*, *docx*, *pptx*, *xslx*** – prepoznava možna šele po DEFLATE

Stisnjeni podatki z DEFLATE

- 3 biti v glavi
- v 99,5% gre za dinamično kodiranje Huffman
- sledi Huffmanova tabela za dan blok in nazadnje podatki, sestavljeni iz kod v tabelah
- koda, ki označuje konec bloka, je za vsak blok drugačna (odvisno od podatkov v tabeli)

Stisnjeni podatki z DEFLATE - Glava

- **Prvi bit -** Oznaka za zadnji blok v podatkovnem toku:

  1: to je zadnji blok v podatkovnem toku.

  0: temu bloku sledi vsaj še en blok.
- **Preostala 2 bita -** Metoda kodiranja, uporabljena za prihajajoči blok:

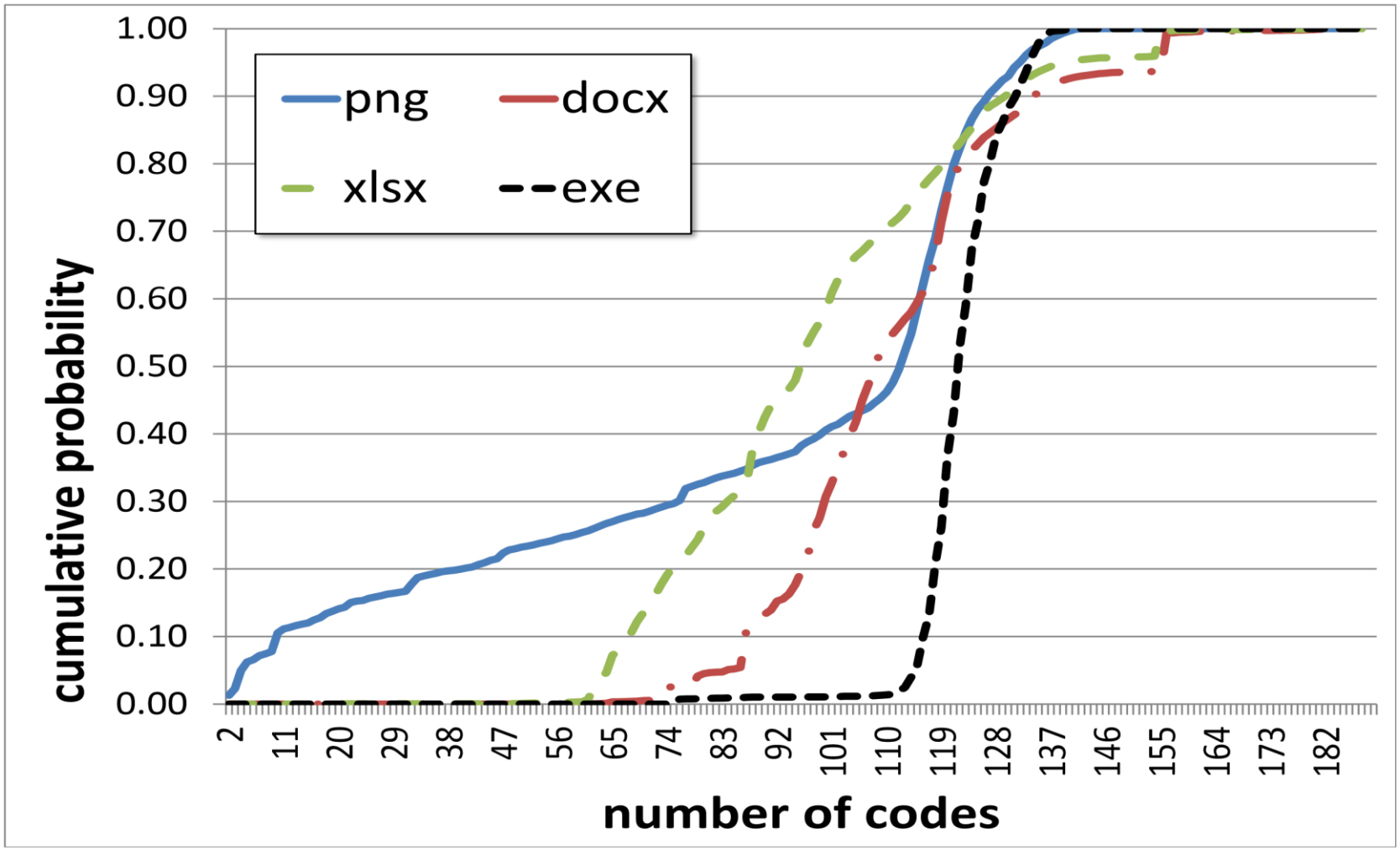
  00: nekompresirana sekcija dolžine med 0 in 65,535 bajti.

  01: blok kompresiran s statičnim Huffmanom - uporaba standardnega, vnaprej definiranega drevesa.

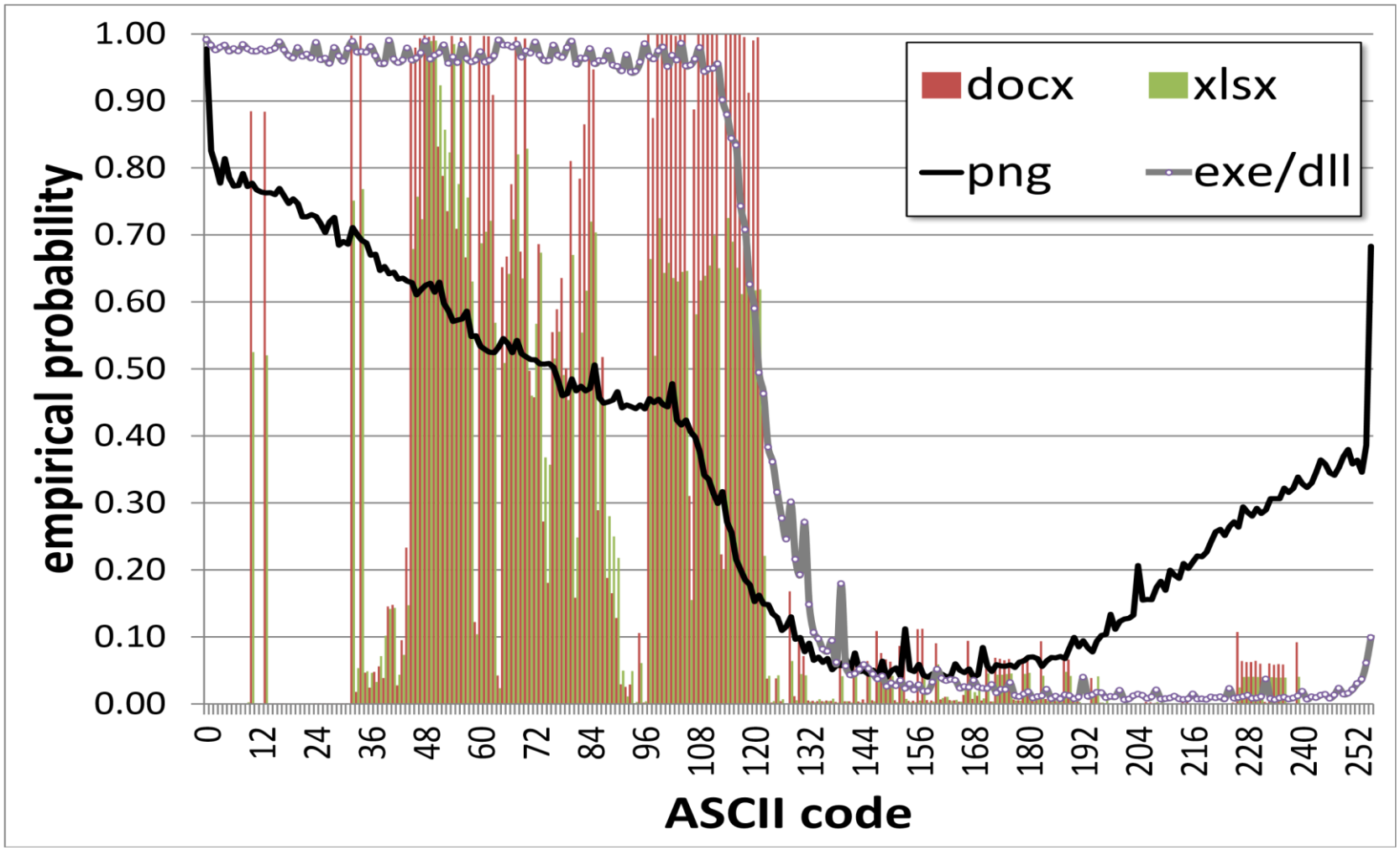
  10: kompresiran blok s priloženo Huffmanovo tabelo. (v praksi uporabljen v 99,5%)

  11: ni v uporabi.

Velikost fragmenta



Pogostost znakov



Stisnjeni podatki in zsniff

- kot del programskega paketa zsniff je implementiran program, ki poskuša podatke v fragmentu odkodirati z DEFLATE z vsemi odmiki in ob uspehu vrne še Huffmane tabele
- da dobimo vsaj en blok, potrebujemo fragment zadostne velikosti
- s statistični analizami Huffmanovih tabel lahko sklepamo na tip vsebine
- število definiranih kod v Huffmanovih tabelah
- za fragmente z različnimi vsebinami (*docx*, *xlsx*, …) preverimo za vsak ASCII znak, ali je definiran v Huffmanovih tabelah
- krajša Huffmanova koda za določen znak posledično pomeni več pojavitev tega znaka v vsebini

Zaključek

- **Statistične metode** nad samimi podatki niso dovolj
- **Velikost fragmenta** vpliva na točnost klasifikacije
- klasificiramo vsebino, je različna glede na tip vsebine
- **Hitrost klasifikacije** je odvisna od tipa datoteke in velikosti fragmenta
- Različne klasifikacije zahtevajo **različne pristope**
- če hočemo ugotoviti del kakšne datoteke je JPEG, moramo v fragmentu imeti dovolj podatkov iz vsebovalnika

Viri

- https://github.com/zsniff/zsniff
- http://dfrws.org/2013/proceedings/DFRWS2013-8.pdf
- http://dfrws.org/2013/proceedings/DFRWS2013-p8.pdf
- http://en.wikipedia.org/wiki/DEFLATE
- http://en.wikipedia.org/wiki/ZIP_(file_format)

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Anže Rezelj
Janez Bindas

-

SSD: ZAČETEK KONCA TRENUTNE PRAKSE V DIGITALNI FORENZIKI?

4. Maj
2014

SSD disk

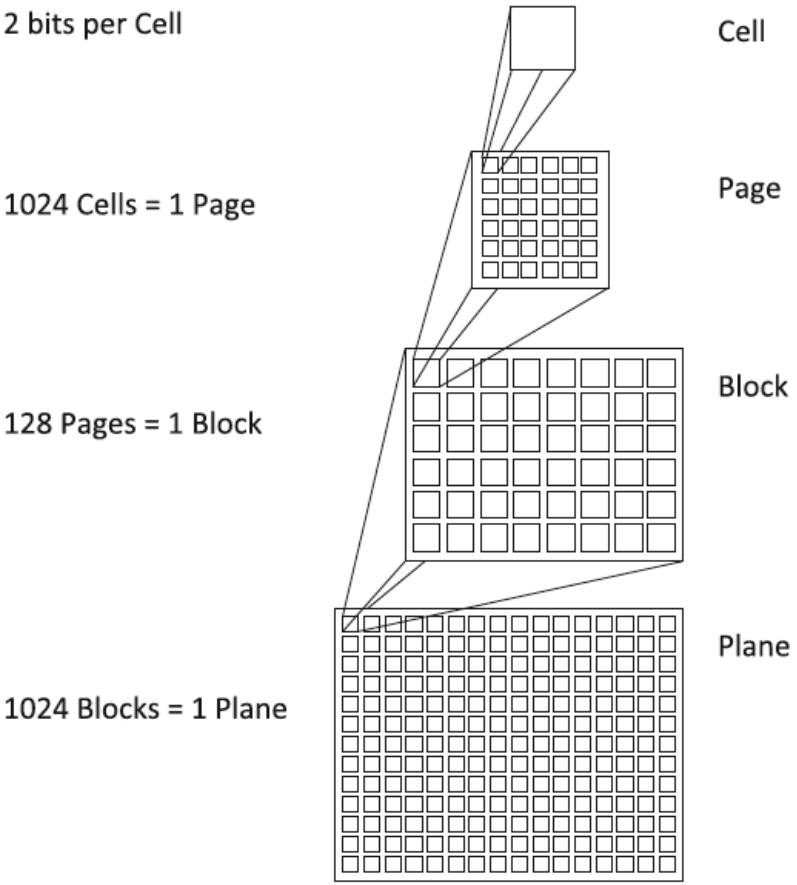
- (kratek uvod, čas zametkov današnjih SSD-jev in podobno)

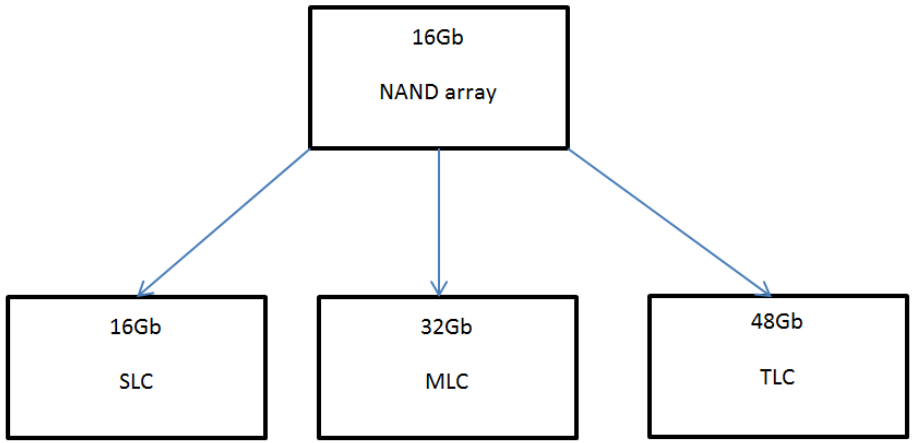
Zgodovina

- (lahko na prešnji prosojnic napišeš kako poved in tu pustiš prazno-odstraniš prosojnico, ali pa tu dodaš kako sliko)

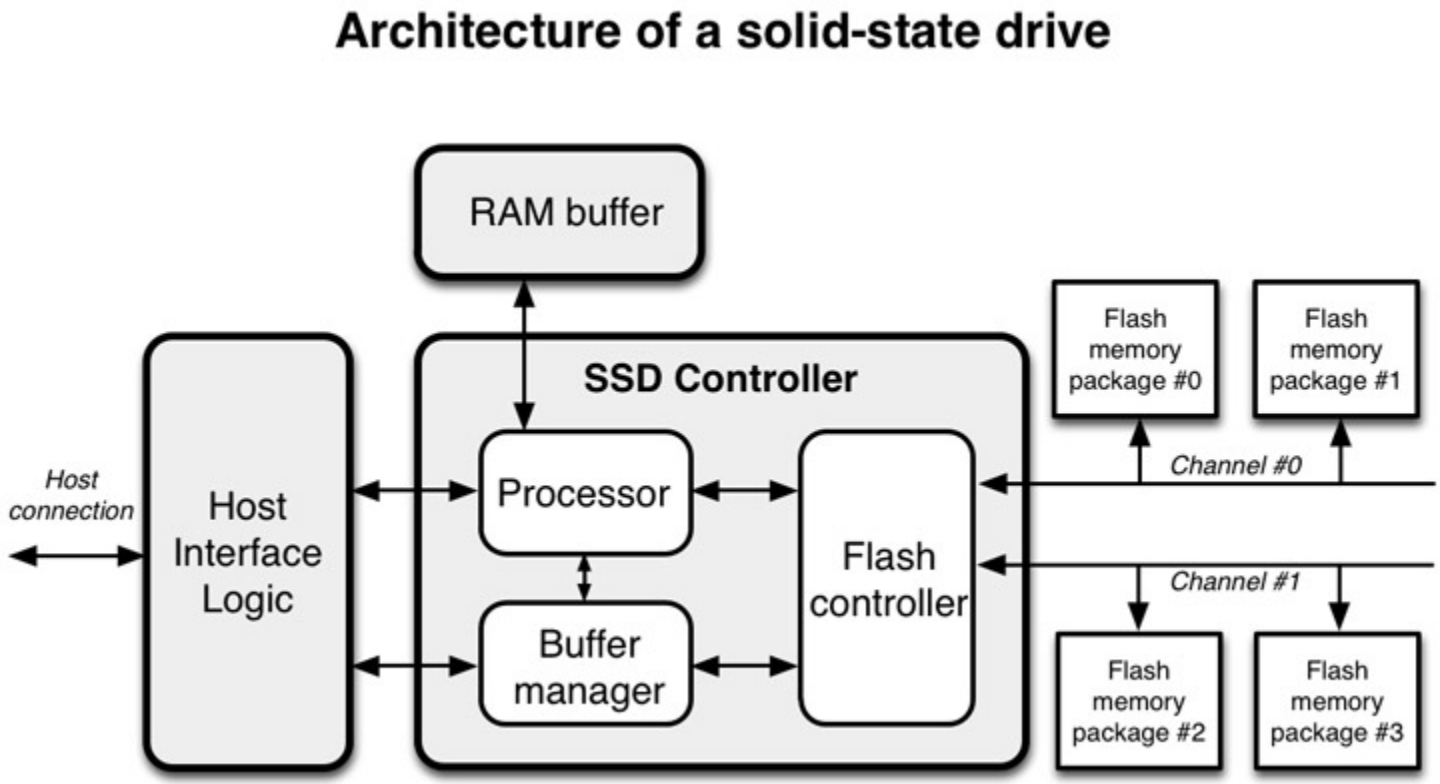
Zgradba

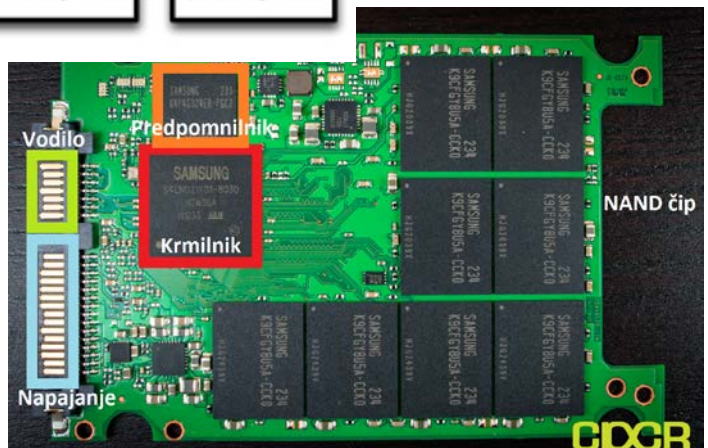
- Osnovna enota je NAND celica
- Poznamo
  - SLC (1 bit/celico),
  - MLC (3 bit/celico),
  - TLC (3 bit/celico),
  - V razvoju 4 bit/celico





Zgradba

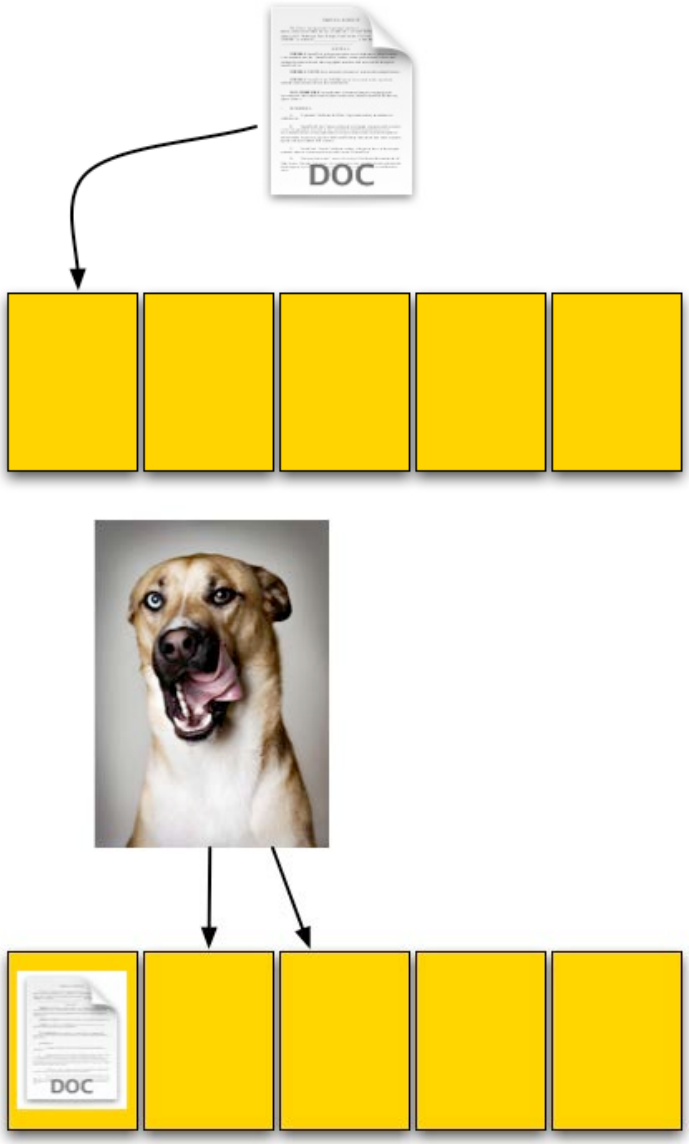

Architecture of a solid-state drive
RAM buffer
SSD Controller
Host connection
Host Interface Logic
Processor
Buffer manager
Flash controller
Flash memory package #0
Flash memory package #1
Flash memory package #2
Flash memory package #3
Channel #0
Channel #1


Vodilo
Predpomnilnik
Krmilnik
NAND čip
Napajanje

Delovanje

Operacije	HDD	SSD
Branje	Prebere sektor	Prebere stran
Pisanje	Zapiše na sektor	Zapiše na stran
Prepis	Prepiše sektor	*Prostor na voljo:* Zapiše na prosto stran *Prostor ni na voljo:* Kopira blok, spremeni, izbriše blok, zapiše blok
Izbris	Označi sektor kot neuporabljen	Označi stran kot neuporabljeno (podprt TRIM: označi kot pripravljen za brisanje)

Delovanje



Forenzika diskov

- (tu napiši današnjo prakso pri forenziki diskov – delanje kopij diskov in opravljanje forenzike na kopijah, uporabe namenskih naprav, ki blokirajo pisanje in podobno)

Forenzika na trdih diskih (HDD)

- (to bova verjetno spustila, ker že prejšna prosojnica to pokriva)

Forenzika na SSD diskih

- Uporabljeni isti postopki kot pri HDD diskih
- Obnovljenih podatkov od 0 do 100%

Test	Control	Imation1	Corsair1 (TRIM)	Crucial1 (TRIM)	PQI1	RiData1	OCZ1 (TRIM)	OCZ2	Patriot1	Patriot2	Kingston1	Intel1 (TRIM)	Intel2 (TRIM)	Intel3 (TRIM)	Intel4	Transcend1
Large File, Low Usage, Win7	100.00%	100.00%	0.00%	0.00%	71.23%	100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	100.00%	70.49%
Large File, Low Usage, WinXP	99.99%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Large File, Low Usage, Linux	99.99%	99.98%	100.00%	99.99%	99.98%	100.00%	100.00%	100.00%	100.00%	99.98%	99.99%	99.98%	99.98%	100.00%	99.98%	100.00%
Large File, High Usage, Win7	100.00%	100.00%	0.00%	0.00%	88.60%	100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	100.00%	100.00%
Large File, High Usage, WinXP	99.99%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Large File, High Usage, Linux	100.00%	99.98%	100.00%	100.00%	99.98%	99.98%	100.00%	100.00%	99.99%	34.78%	100.00%	99.99%	0.00%	99.98%	99.99%	100.00%
Large File, Format, Win7	100.00%	100.00%	0.00%	0.00%	100.00%	100.00%	0.00%	99.87%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	100.00%
Large File, Format, WinXP	99.99%	100.00%	0.00%	0.00%	0.00%	99.67%	100.00%	0.00%	100.00%	100.00%	0.00%	100.00%	0.00%	0.13%	99.40%	99.67%
Large File, Format, Linux	99.86%	100.00%	0.00%	77.88%	0.00%	3.83%	99.87%	100.00%	12.37%	7.36%	3.83%	83.52%	100.00%	100.00%	0.00%	100.00%
Small File, Low Usage, Win7	99.98%	0.00%	25.53%	27.54%	0.00%	99.98%	25.53%	99.98%	99.98%	0.00%	99.98%	0.00%	0.00%	0.00%	99.98%	99.98%
Small File, Low Usage, WinXP	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	0.00%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%
Small File, Low Usage, Linux	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	86.20%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	96.97%	99.98%
Small File, High Usage, Win7	99.98%	99.98%	27.54%	26.28%	99.98%	99.98%	25.53%	99.98%	99.98%	99.98%	99.98%	0.00%	0.00%	0.00%	99.98%	99.98%
Small File, High Usage, WinXP	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%
Small File, High Usage, Linux	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	98.71%	99.56%	99.98%	99.98%	99.98%	98.27%	99.98%
Small File, Format, Win7	0.00%	26.96%	24.46%	0.00%	0.00%	24.63%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	24.61%	0.00%
Small File, Format, WinXP	96.57%	57.21%	24.69%	0.00%	0.00%	54.27%	49.03%	53.05%	46.84%	0.00%	37.73%	59.84%	86.20%	46.76%	58.45%	48.20%
Small File, Format, Linux	99.98%	99.98%	0.00%	99.98%	99.98%	0.00%	99.98%	99.98%	99.98%	0.00%	99.98%	27.41%	99.98%	99.98%	0.00%	99.98%
Average	93.86%	87.62%	49.74%	56.93%	69.60%	81.97%	66.28%	85.12%	86.23%	57.63%	74.12%	59.10%	54.40%	57.77%	81.71%	89.52%

Forenzika na SSD diskih

- Vplivi na procent obnovljenih podatkov:
  - Delovanja smetarja (garbage collector)
  - Mapiranje LBA naslovov
  - OS (če zna uporabljati ukaz TRIM)

Table 2 – Percent blocks recovered on a TRIM-enabled disk with Windows 7

Test	Control	Intel1	Intel2	Intel3	OCZ1	Corsair1	Crucial1
Large File, Low Usage	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Large File, High Usage	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Large File, Format	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Small File, Low Usage	99.98%	0.00%	0.00%	0.00%	25.53%	25.53%	27.54%
Small File, High Usage	99.98%	0.00%	0.00%	0.00%	25.53%	27.54%	26.28%
Small File, Format	0.00%	0.00%	0.00%	0.00%	0.00%	24.46%	0.00%

This chart shows only those disks that support TRIM (and the control), which is 6 of the 16 tested.

Table 3 – Percent blocks recovered on a TRIM-enabled disk with Windows XP.

Test	Control	Intel1	Intel2	Intel3	OCZ1	Corsair1	Crucial1
Large File, Low Usage	99.99%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Large File, High Usage	99.99%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Large File, Format	99.99%	100.00%	0.00%	0.13%	100.00%	0.00%	0.00%
Small File, Low Usage	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%
Small File, High Usage	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%	96.57%
Small File, Format	96.57%	59.84%	86.20%	46.76%	49.03%	24.69%	0.00%

This chart shows only those disks that support TRIM (and the control), which is 6 of the 16 tested.

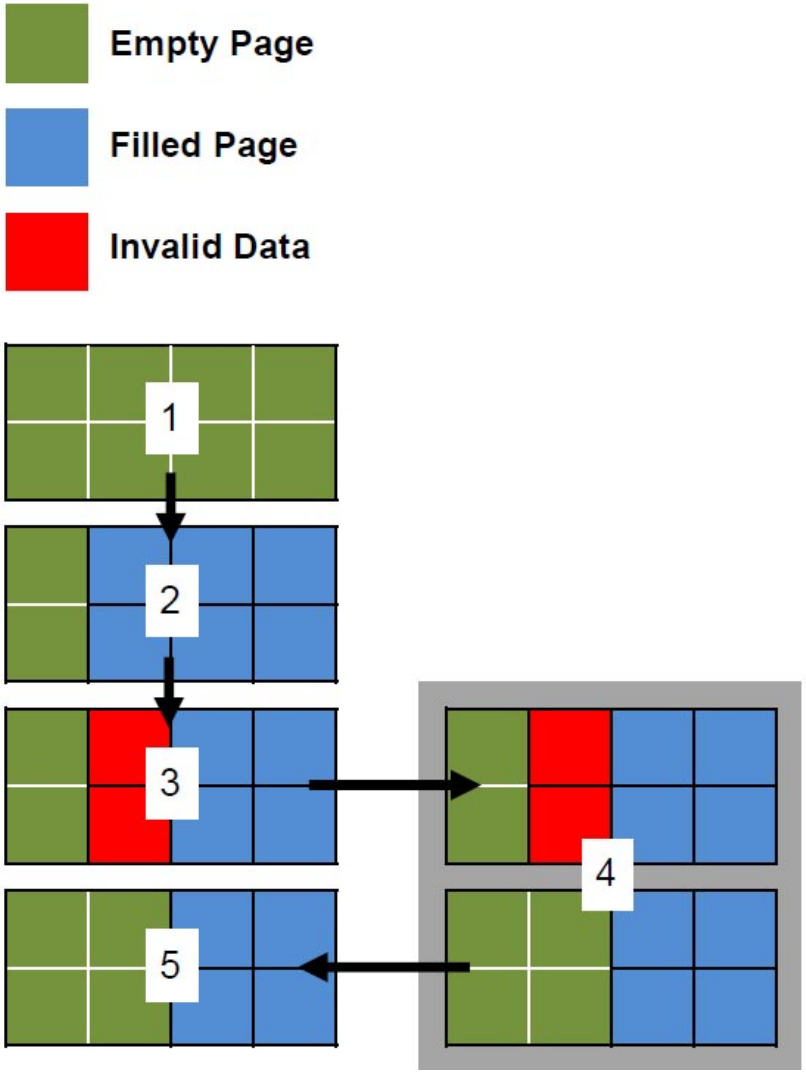
Prihodnost forenzike SSD diskov

- Ukaz TRIM
- Kako pridobiti podatke iz SSD diska ter hkrati zagotoviti, da so ti nespremenjeni
- Namenska strojna oprema
- Zakonodaja?

Ukaz TRIM

- Vzdržuje performance SSD diska
- Olajša delo krmilniku tako, da OS krmilniku sporoči katere lokacije lahko sprosti
- Krmilnik vsebino na lokacijah **pobriše** in jih doda v bazen lokacij pripravljenih za uporabo
- Operacija se izvaja v ozadju

Ukaz TRIM



1.) SSD pages contain no data

2.) User writes data to SSD pages

3.) User deletes some data. Pages are marked as 'not in use' by the host OS, but data remains on SSD.

4.) TRIM command tells SSD controller that pages contain invalid data. Pages with invalid data are cleaned.

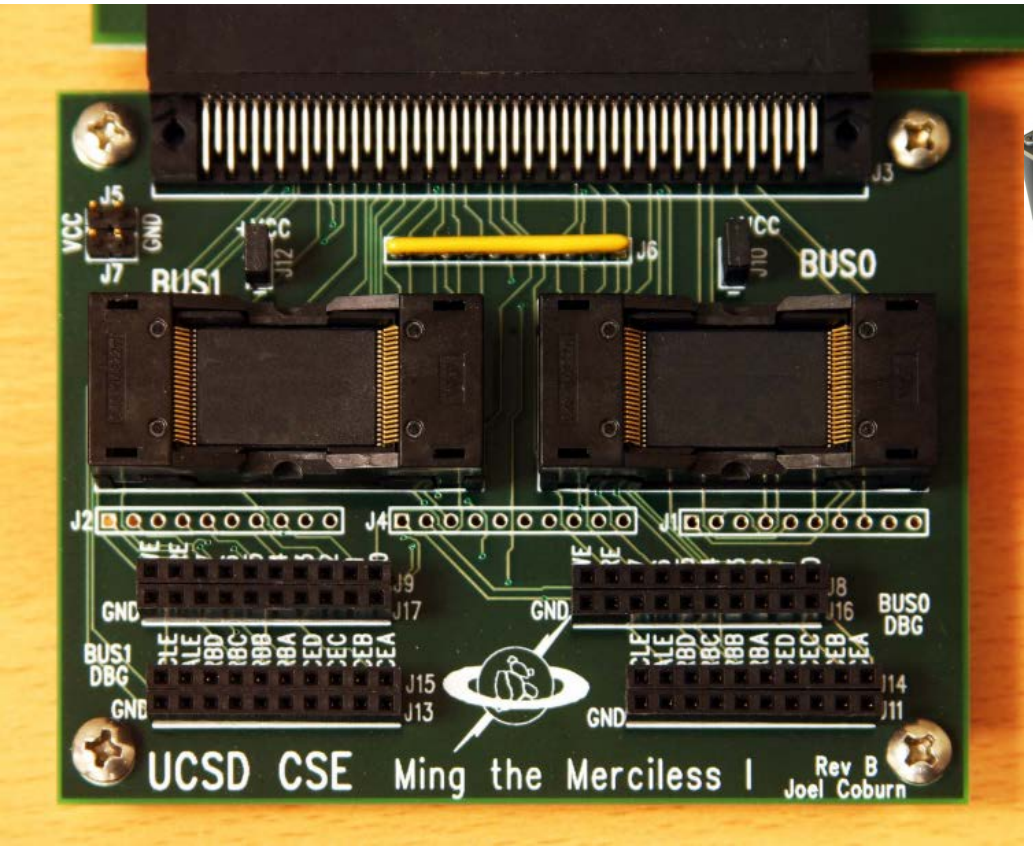
5.) Data is written back to SSD memory cells. The invalid data has been cleaned and data is able to be written to the pages at full speed.

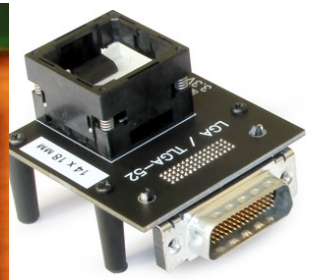
Ukaz TRIM

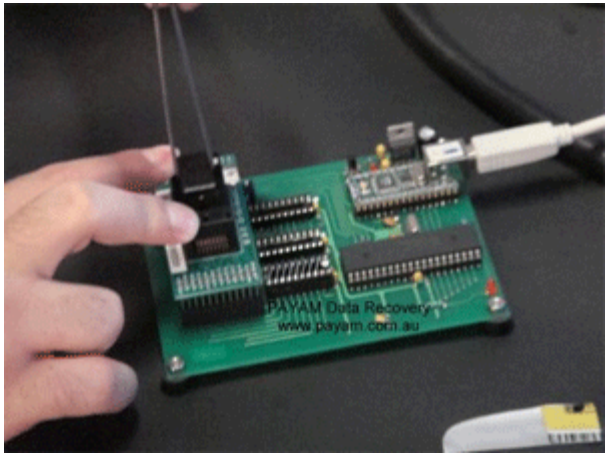
- Omejena podpora
  - Ukaz je opcijski in ga nekateri diski ne podpirajo
  - Podprti vmesniki so SATA, eSATA, SCSI
  - OS ki podpirajo ukaz so Windows 7, Windows Server 2008 R2 in novejši, MacOS X 10.6.8 in novejši (le v naboru z SSD diski, ki jih dobavlja Apple), DragonFLY BSD od Maja 2011, FreeBSD od verzije 8.1, Linux od verzije jedra 2.6.33 (privzeto izklopljeno), Android 4.3, ostali v primeru obstoja ustrezne programske opreme
  - Datotečni sistemi: NTFS, HFS+, Ext4, Btrfs, FAT, GFS2, XFS

Namenska oprema

- Prihodnost v rokah namenske strojne opreme za branje podatkov v NAND čipih?







Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Žiga Zupanec in
Tomaž Tomažič

ANALIZA PODATKOV VOIP KLICEV

3. Maj
2014

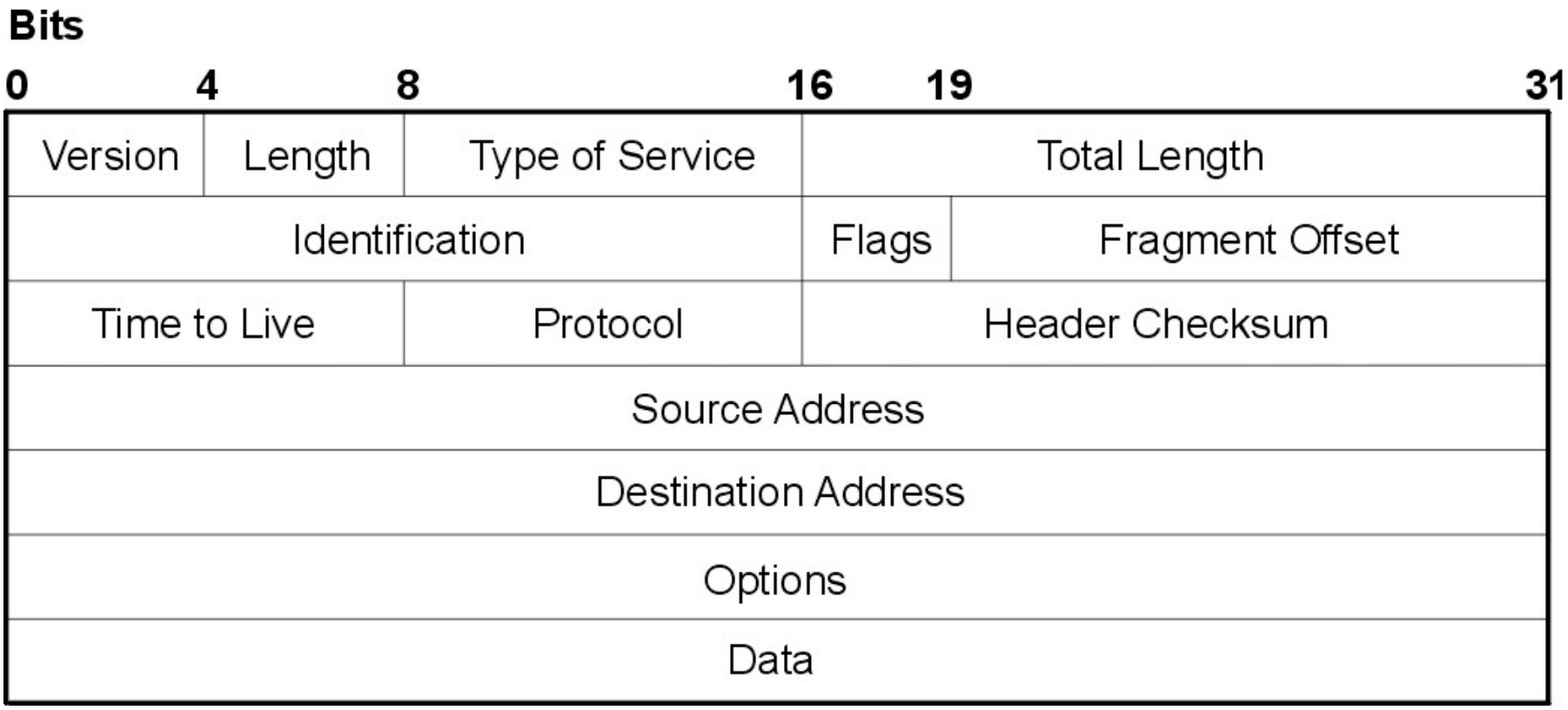
VOIP

- Tehnologija za klicanje
- IP protokol
- Nadomešča PTSN
- Skype, Google Talk, Cisco-phone
- QoS

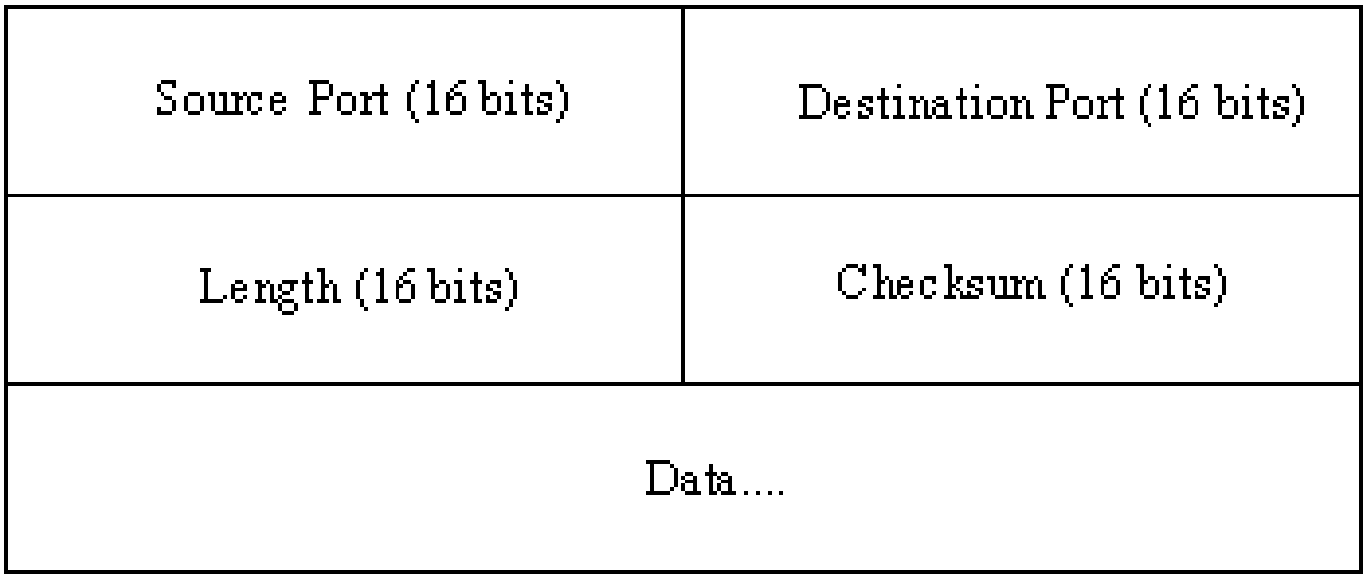
Težave VOIP

- Prisluškovanje ameriškemu predsedniku
- Varnost
- NAT traversal
- Napajanje

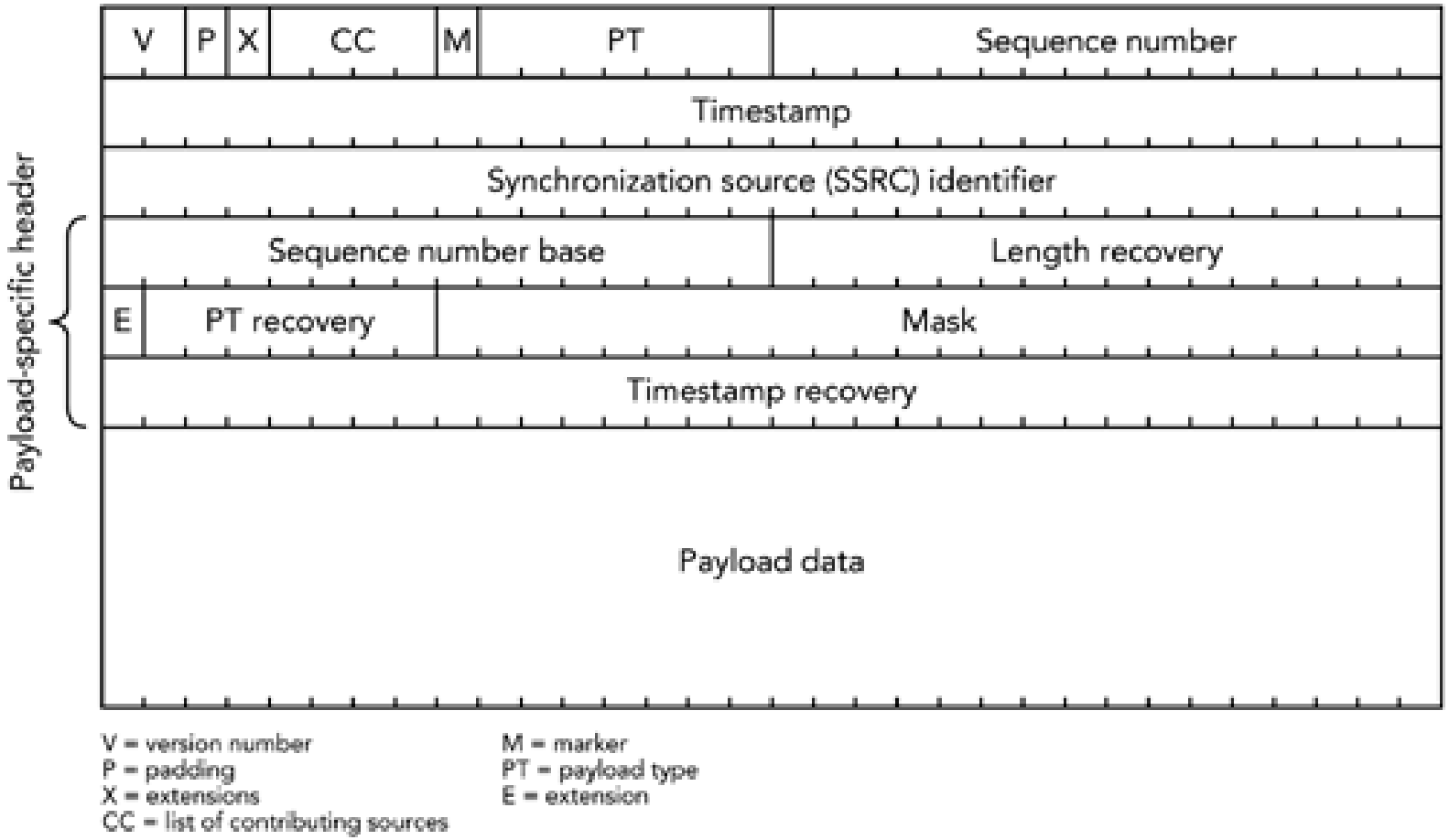
IP glava


Bits
0
4
8
16
19
31
Version
Length
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Data

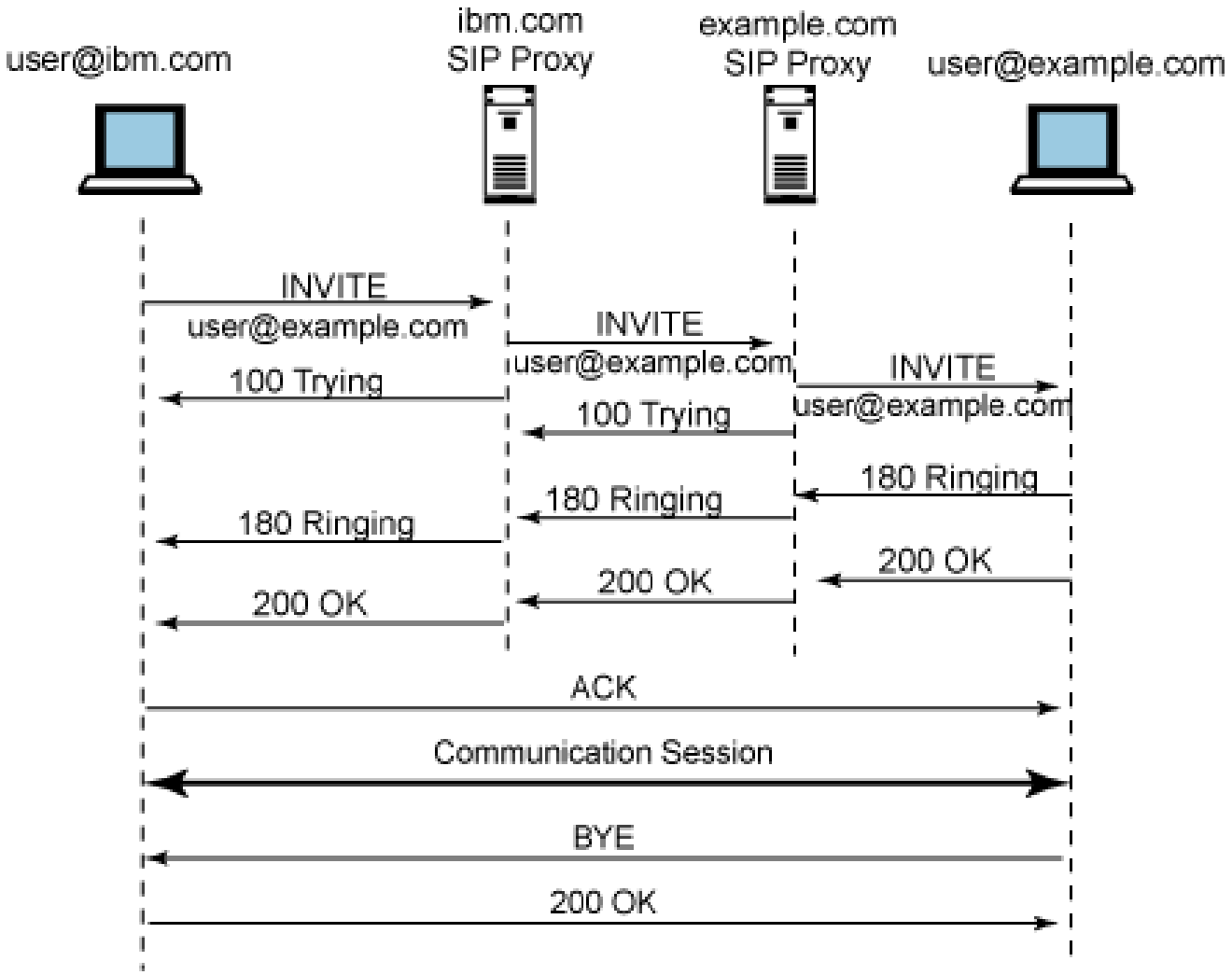
UDP glava


Source Port (16 bits)
Destination Port (16 bits)
Length (16 bits)
Checksum (16 bits)
Data....

RTP glava


V
P
X
CC
M
PT
Sequence number
Timestamp
Synchronization source (SSRC) identifier
Payload-specific header
Sequence number base
Length recovery
E
PT recovery
Mask
Timestamp recovery
Payload data
V = version number
P = padding
X = extensions
CC = list of contributing sources
M = marker
PT = payload type
E = extension

SIP seja


user@ibm.com
ibm.com
SIP Proxy
example.com
SIP Proxy
user@example.com
INVITE
user@example.com
INVITE
user@example.com
INVITE
user@example.com
100 Trying
100 Trying
180 Ringing
180 Ringing
180 Ringing
200 OK
200 OK
200 OK
ACK
Communication Session
BYE
200 OK

Konfiguracija

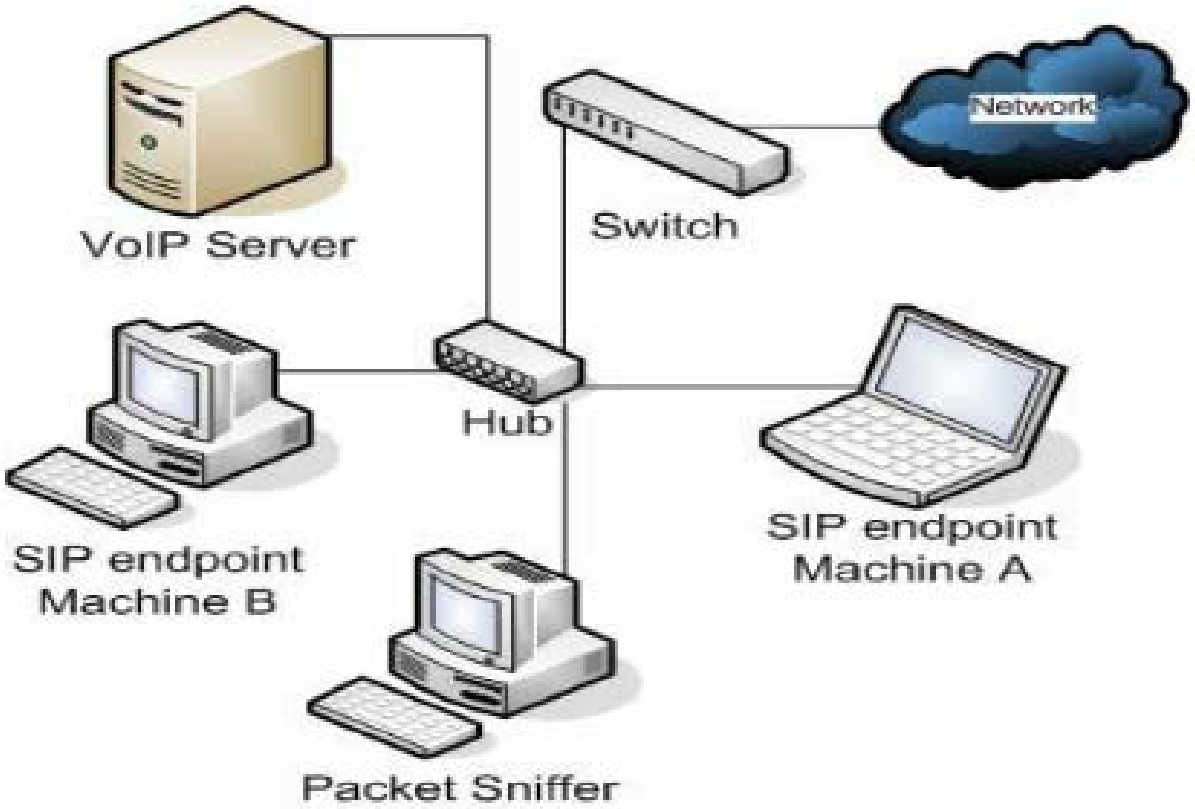


Figure 5 – VoIP call and packet detection setup

Eksperiment HDD

- A pokliče B za n sekund
- Z wiresharkom zajamemo promet
- Promet primerjamo z diskoma virtualk

Eksperiment RAM

- A pokliče B za n sekund
- Z wiresharkom zajamemo promet
- Ram shranimo v sliko
- Promet primerjamo s sliko pomnilnika virtualk

Ugotovitve

- Na disku ni bilo relavantnih podatkov
- V RAMu z našo skripto najdeni paket
- Najden SIP registracijski klicni id

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tjaša Saje,
Katerina Bashova
Žan Anderle

-

Dropbox analysis – Data remnants on user machines

4. Maj
2014

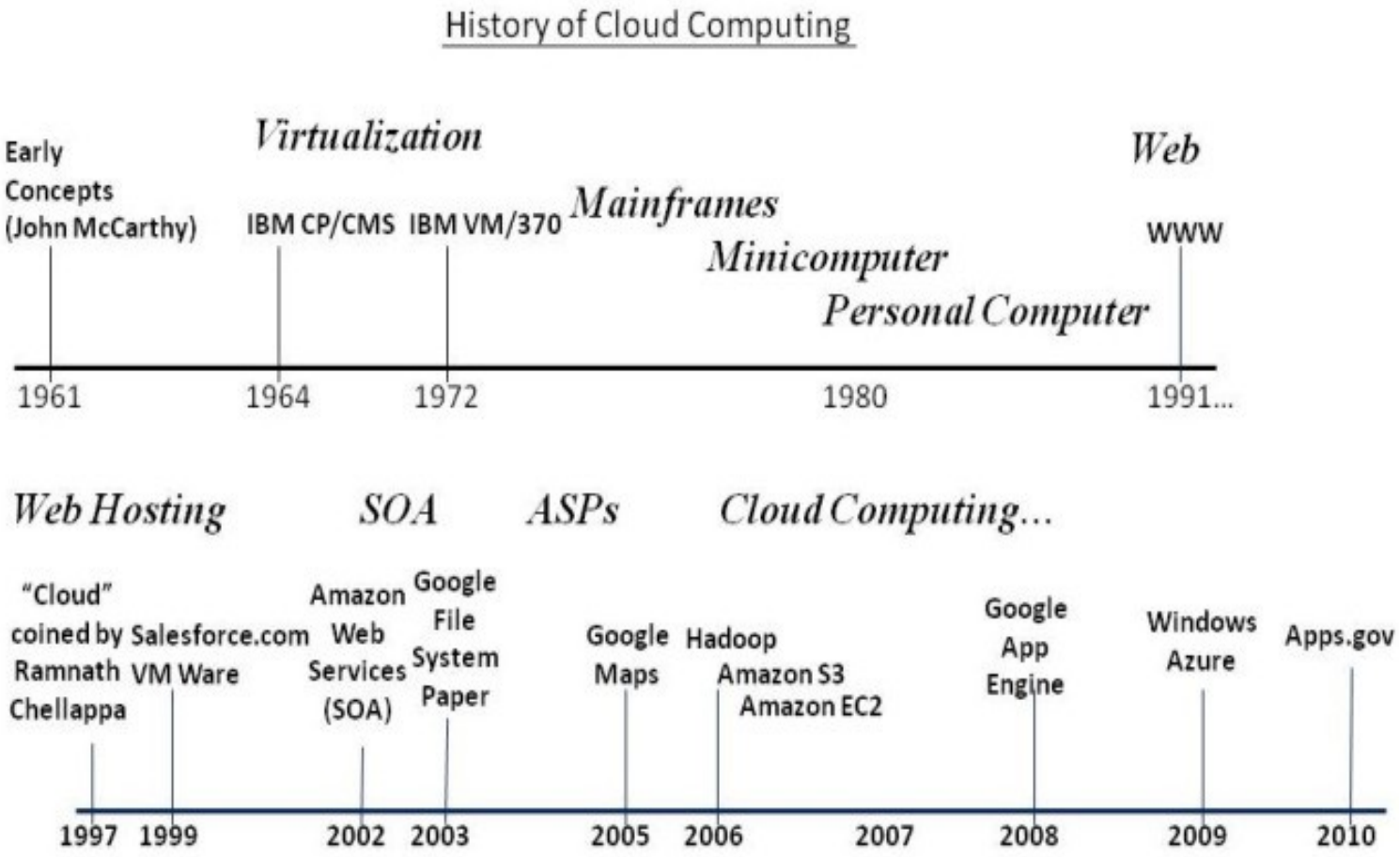
Content

1. Introduction
2. The article
   - Methodology
   - Findings
3. Our research:
   - Methodology
   - Findings
4. Conclusion

Introduction

- Cloud storage as an emerging challenge to digital forensic researchers
- Many providers: Dropbox, Microsoft Skydrive, Google Drive ...
- Possible criminal activity (CP, terrorism-related...)
- An important question in the investigation: has a cloud service been used or not?

Some history



The article

Quick & Choo (2013)

Dropbox analysis: Data remnants on user machines

- Windows 7 computer & Apple iPhone 3G
- user interaction with the cloud (storing, uploading, accessing data etc.)
- different browsers may have differing effects on the nature of remnants (Internet Explorer, Mozilla Firefox, Apple Safari and Google Chrome)
- browser vs. software access
- anti-forensic methods to conceal evidence (Eraser and CCleaner)

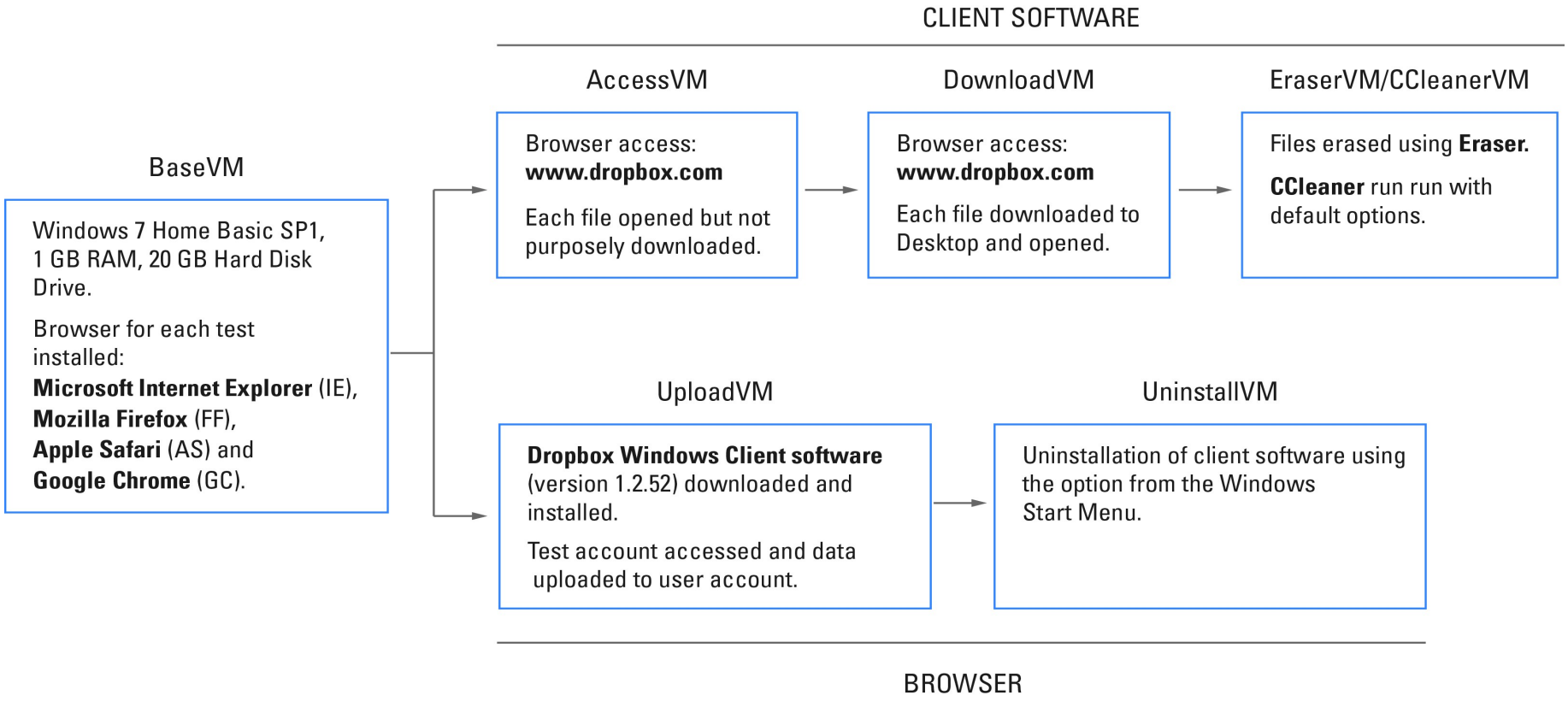
The article

Quick & Choo (2013)

- seven distinct typical use situations: **BaseVM**, **UploadVM**, **UninstallVM**, **AccessVM**, **DownloadVM**, **EraserVM**, **CCleanerVM**
- Research design: 7 x 4 (28 Virtual Machines)
- Enron Sample files
- analysis undertaken with Guidance Software EnCase (version 6.19.4) and AccessData FTK (versions 1.81.6 and 4.01)

The article

Quick & Choo (2013)



The article

Quick & Choo (2013)

	Control BaseVM	**Client software** UploadVM	**Browser access** AccessVM	**Browser download** DownloadVM	**Eraser** EraserVM	**CCleaner** CCleanerVM
Username	○	●	●	●	●	○
Password	○	●	○	○	○	○
Software	○	●	○	○	○	○
URL	○	●	●	●	●	●
Test filenames	○	●	●	●	●	●
Test files	○	●	●	●	●	○
KWS matches	●	●	●	●	●	●

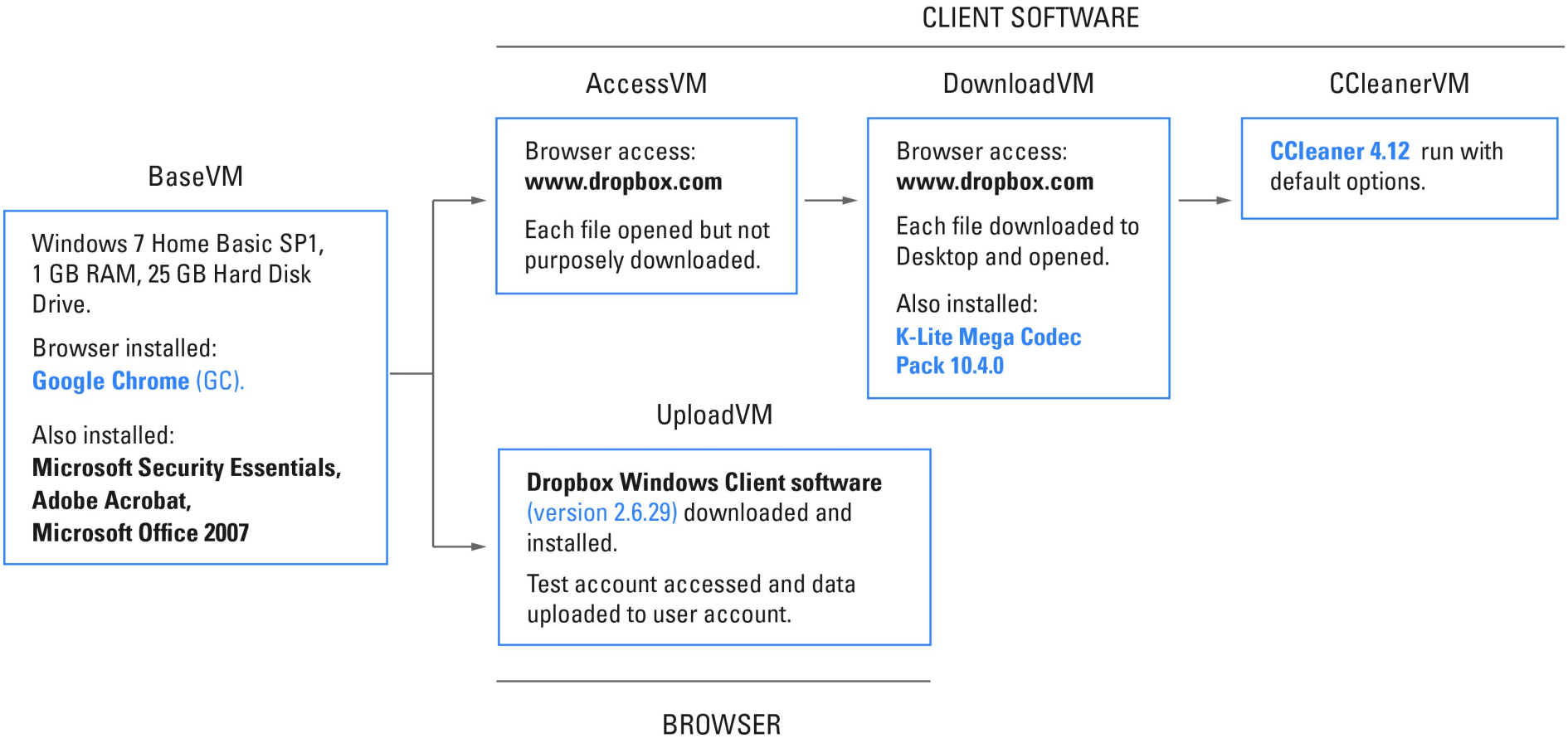
Our research - methodology

- Research aim: replication of research inquiry, extension of researched area, increase of generalizability
- Research scope: Google Chrome on Microsoft Windows 7 64bit OS
- Research focus: web browser and software access, anti-forensic methods
- Research design: 5 x 1
- Five typical user activities: BaseVM, UploadVM, AccessVM, DownloadVM, CCleanerVM

Our research - methodology

- Oracle VirtualBox 4.3.10 and CloneVDI
- 17 distinct test files - including extensions: .txt, .docx, .pdf, .png., .jpg, .avi, .mp3, and .zip.
- persona: Raymond Beck
- Data analysis: Autopsy, SQLite Expert Personal, sqliteman, Registry Decoder

Our research - methodology



Our research - findings

	Control BaseVM	**Client software** UploadVM	**Browser access** AccessVM	**Browser download** DownloadVM	**CCleaner** CCleanerVM
Username	○	●	●	●	○
Password	○	●	○	○	○
Software	○	●	○	○	○
URL	○	●	●	●	●
Cookies	○	●	●	●	○
favicon	○	●	●	●	○
Test filenames	○	●	●	●	○
Test files	○	●	●	●	○
KWS matches	●	●	●	●	●

Our research - UploadVM

- Installed dropbox and all uploaded files
- Two cookies in Windows/Cookies folder
- Chrome browsing history:
  - Downloads (installer),
  - download url chains,
  - urls and various
  - other locations.
- In the “Cookies” database many entries were found
- In “Favicon” database Dropbox icon was found

Our research - findings

	Control BaseVM	**Client software** UploadVM	**Browser access** AccessVM	**Browser download** DownloadVM	**CCleaner** CCleanerVM
Username	○	●	●	●	○
Password	○	●	○	○	○
Software	○	●	○	○	○
URL	○	●	●	●	●
Cookies	○	●	●	●	○
favicon	○	●	●	●	○
Test filenames	○	●	●	●	○
Test files	○	●	●	●	○
KWS matches	●	●	●	●	●

Our research - DownloadVM

- Linkfiles
- Chrome browsing history:
  - In the “Cookies” database many entries were found
  - “Favicon” database Dropbox icon was found
  - Dropbox found in:
    - downloads (dropbox.zip) ,
    - download url chains, and
    - many other
  - In “Web Data” database user’s login email was found in clear text (under autofill)
  - in “Login data” database dropbox url was found, indicating a login

Our research - CCleanerVM

	Control BaseVM	**Client software** UploadVM	**Browser access** AccessVM	**Browser download** DownloadVM	**CCleaner** CCleanerVM
Username	○	●	●	●	○
Password	○	●	○	○	○
Software	○	●	○	○	○
URL	○	●	●	●	●
Cookies	○	●	●	●	○
favicon	○	●	●	●	○
Test filenames	○	●	●	●	○
Test files	○	●	●	●	○
KWS matches	●	●	●	●	●

Our research - CCleanerVM

- Found traces in Google Chome’s SQLite databases
  - In “History” database https://dl-web.dropbox.com/zip_batch?_subject_uid=283704793 was found
  - In “Favicons” database Dropbox icon was found in and some links
    - http://dropbox.com/
    - https://dropbox.com/
    - https://www.dropbox.com/
    - https://www.dropbox.com/login
    - https://www.dropbox.com/home
    - https://www.dropbox.com/photos
    - https://www.dropbox.com/links
    - https://www.dropbox.com/share
    - https://www.dropbox.com/events

Conclusion

- research objectives met
- limitations: research scope, volume of data, additional scenarios

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tomaž Bartol, Jernej Jerin, Tadej Vodopivec

-

Kdo sem jaz ? Analiza Digitalnih oseb v Preiskavah „spletnega” kriminala

1. Maj 2014

Cybercrime – spletni kriminal

- Kriminalci – splet
- Digitalna identiteta – oseba
- Velika količina pridobljenih podatkov
- Breme preiskovalcev spletnega kriminala je ogromno
- ISIS orodje

Internet

- Novi načini za dostop do potencialnih žrtev
  - Socialna omrežja
- Skrivanje digitalnih osebnosti
  - Relacija 1:n
  - Relacija n:1
- Pridobitev zaupanja potencialnih žrtev
- Primeri, ki vsebujejo izkoriščanje digitalnih osebnosti v nelegalne namene :
  - Pedofili,
  - Prevaranti na podlagi romance,
  - Skrajne ideološke skupine,...
- Analiza komunikacij
  - Orodja za pridobivanje podatkov (Encase)
  - Orodja za analizo pridobljenih podatkov

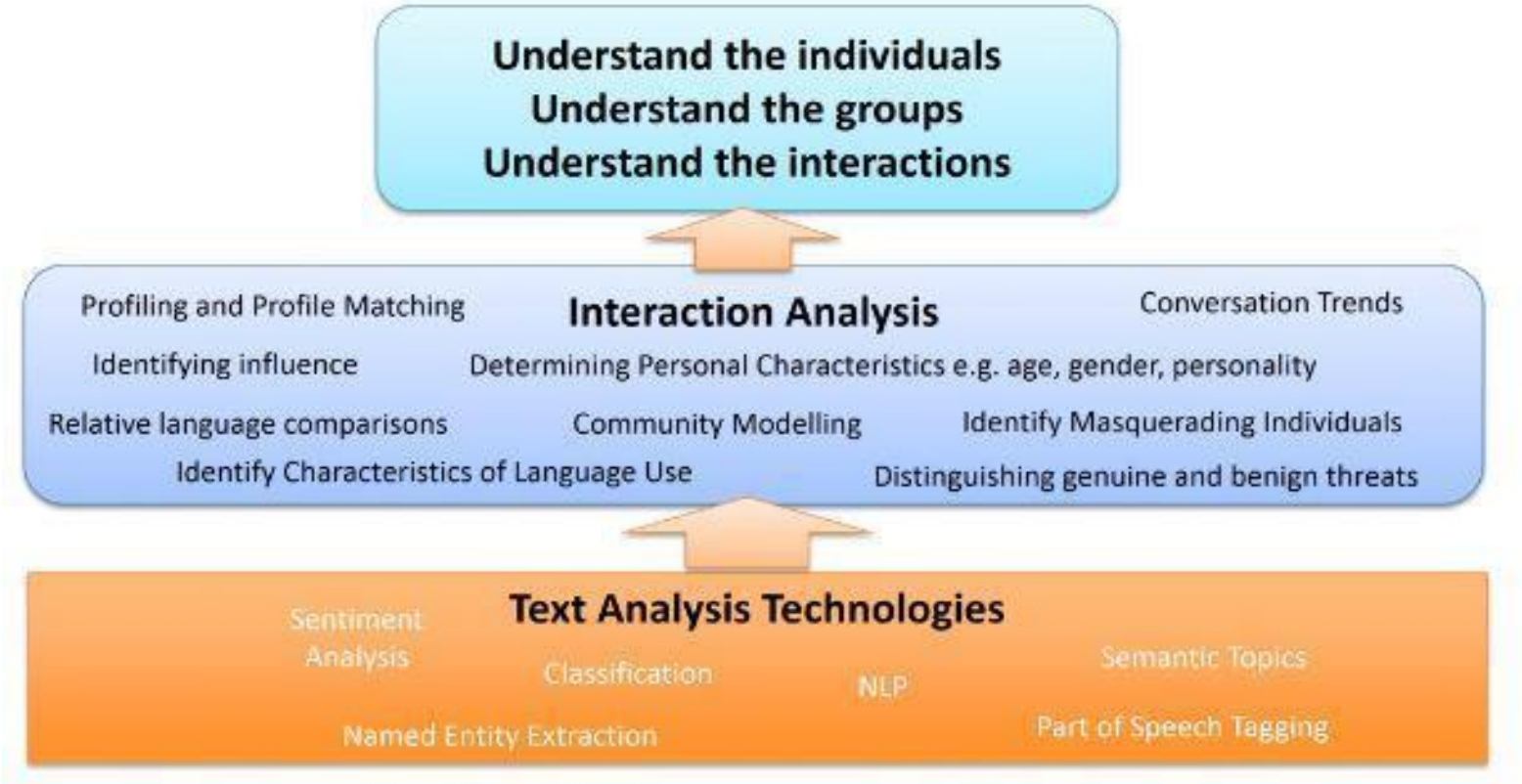
ISIS orodje

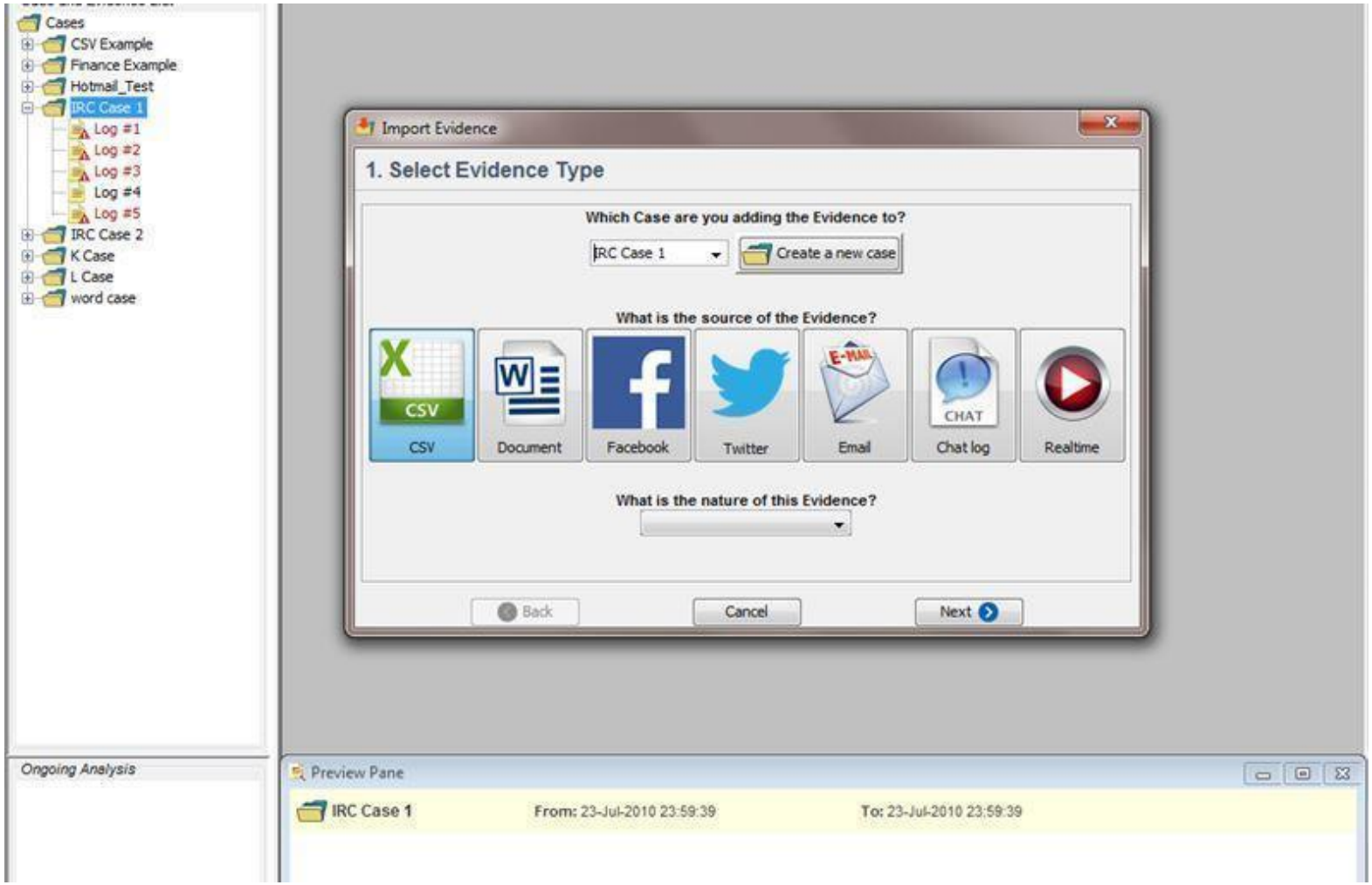
- **Isis orodje** deluje na principu statističnih metod za procesiranje naravnega jezika.
  Takšne metode omogočajo naslednje funkcionalnosti:
  - Profiliranje ključnih besed,
  - Primerjanje frekvenc določenih besed,
  - ….

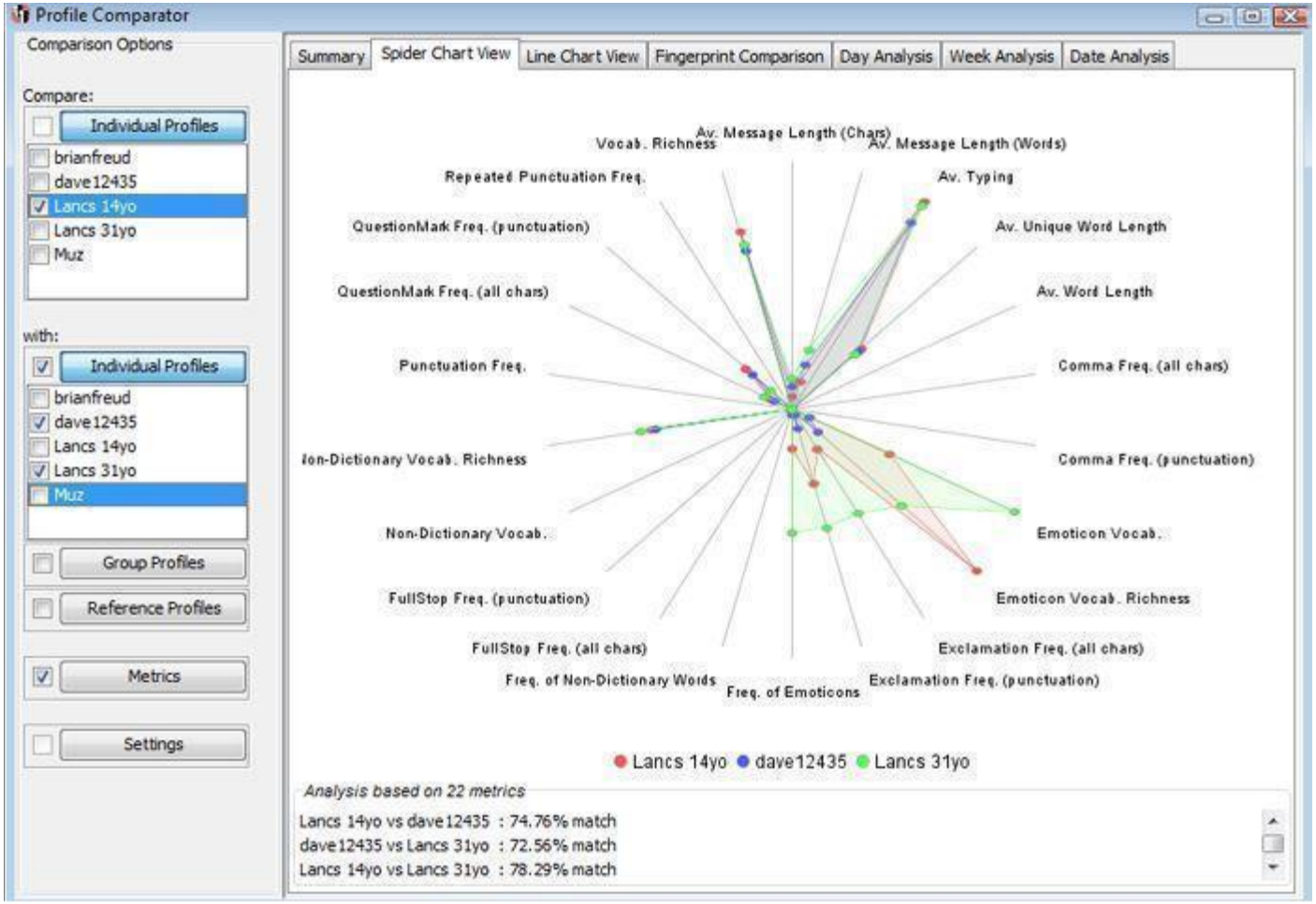
- Baza učnih podatkov
- Tuji jeziki
- Pridobitev jezikovnega stilskega profila oseb v različnih starostnih skupinah in spolu

- ISIS orodje omogoča naslednje zmožnosti preiskovanja:
  - Vzpostavljanje jezikovnega stilskega profila, ki ga uporablja oseba,
  - Vzpostavljanje starosti in spola osebe,
  - Vzpostavljanje vzorca prisotnosti na medmrežju in ostalih vzorcev komunikacije.

Ključna tehnologija za vse ISIS forenzične rešitve je njegov „Interaction Analysis Engine“




Cases
CSV Example
Finance Example
Hotmail_Test
IRC Case 1
Log #1
Log #2
Log #3
Log #4
Log #5
IRC Case 2
K Case
L Case
word case
Import Evidence
1. Select Evidence Type
Which Case are you adding the Evidence to?
IRC Case 1
Create a new case
What is the source of the Evidence?
CSV
Document
Facebook
Twitter
Email
Chat log
Realtime
What is the nature of this Evidence?
Back
Cancel
Next
Ongoing Analysis
Preview Pane
IRC Case 1
From: 23-Jul-2010 23:59:39
To: 23-Jul-2010 23:59:39


Profile Comparator
Comparison Options
Compare:
Individual Profiles
brianfreud
dave12435
Lancs 14yo
Lancs 31yo
Muz
with:
Individual Profiles
brianfreud
dave12435
Lancs 14yo
Lancs 31yo
Muz
Group Profiles
Reference Profiles
Metrics
Settings
Summary
Spider Chart View
Line Chart View
Fingerprint Comparison
Day Analysis
Week Analysis
Date Analysis
Av. Message Length (Chars)
Vocab. Richness
Av. Message Length (Words)
Repeated Punctuation Freq.
Av. Typing
QuestionMark Freq. (punctuation)
Av. Unique Word Length
QuestionMark Freq. (all chars)
Av. Word Length
Punctuation Freq.
Comma Freq. (all chars)
Non-Dictionary Vocab. Richness
Comma Freq. (punctuation)
Non-Dictionary Vocab.
Emoticon Vocab.
FullStop Freq. (punctuation)
Emoticon Vocab. Richness
FullStop Freq. (all chars)
Exclamation Freq. (all chars)
Freq. of Non-Dictionary Words
Freq. of Emoticons
Exclamation Freq. (punctuation)
Lancs 14yo
dave12435
Lancs 31yo
Analysis based on 22 metrics
Lancs 14yo vs dave12435 : 74.76% match
dave12435 vs Lancs 31yo : 72.56% match
Lancs 14yo vs Lancs 31yo : 78.29% match

Jezikovni stilski profil

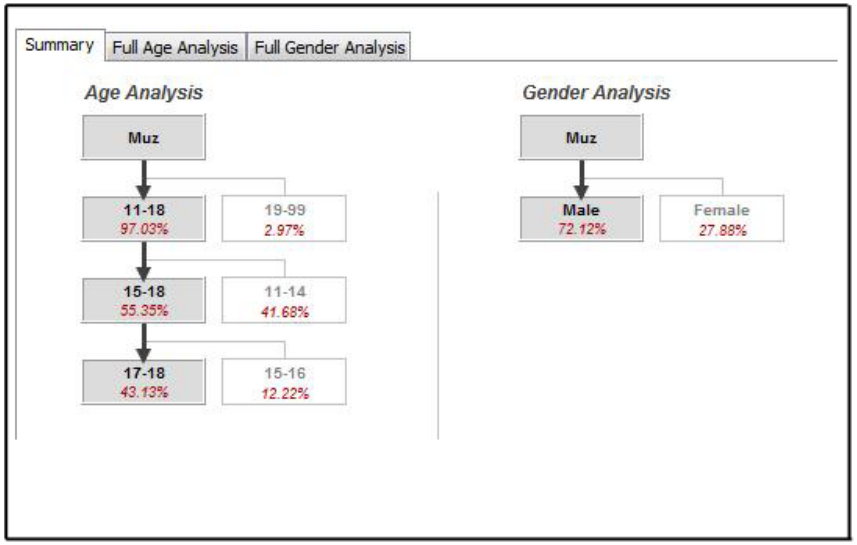
- Iz vsake povedi oziroma besede lahko izluščimo določene vzorce, ki so značilni samo za določeno osebo
  - Uporaba ločil,
  - Uporaba emotikonov,
  - Frekvenca besed glede na slovar.

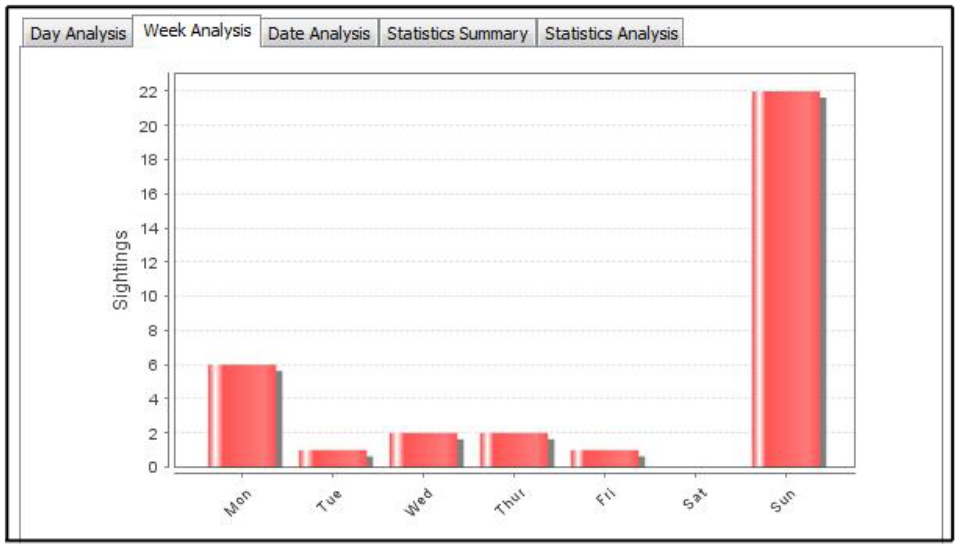
- Metrike
  - Število klicajev, vprašajev, vejic,
  - Indikator širine nabora besed,
  - Dolžina sporočil,
  - Tip sporočila glede na lokacijo objave.

- Učni vzorec
  - Kakšna oseba ga je napisala (spol, starost, izobrazba, spolna usmerjenost,…),
  - Kje je bilo sporočilo objavljeno,
  - V kakšnem kontekstu je bilo objavljeno.
- Na podlagi množice takšnih sporočil lahko primerjamo dobljene vrednosti metrike za sporočilo neznane osebe z izračunanimi metrikami znane osebe. Če so rezultati podobni, lahko z veliko verjetnostjo trdimo, kakšna oseba je napisala to sporočilo.

Analiza na podlagi jezika in starosti

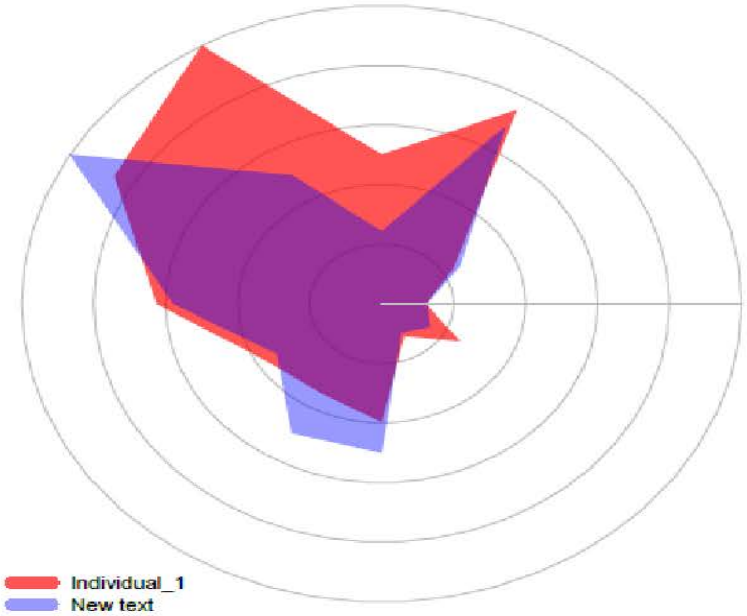
- Odvija se v 4 korakih
  1. Vhodno sporočilo je razbito na posamezne besede in ločila.
  2. Vsako besedo označimo glede na pomen.
  3. Štetje značilnosti posameznih besed po določeni značilnosti.
  4. Pripravimo referenčne podatkovne baze, na podlagi katerih bomo primerjali vrednosti metrik

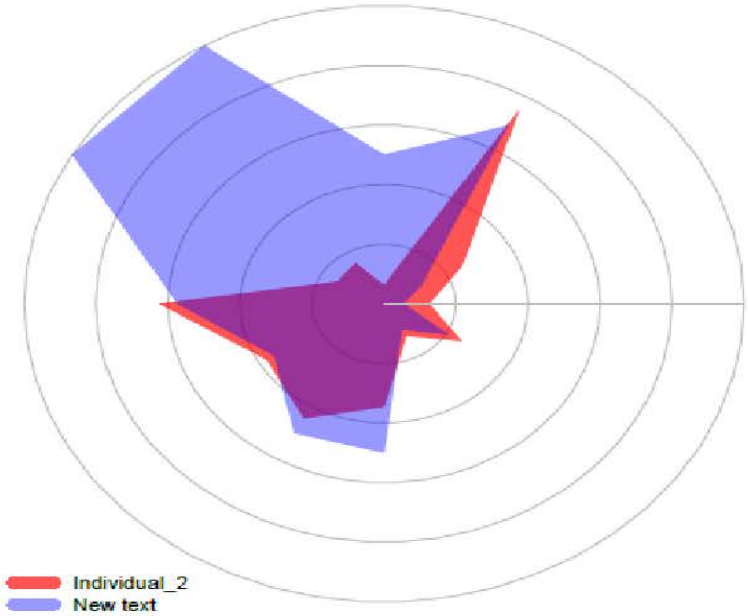




Primerjava stilnih odtisov

- Radar graf
- Ujemanje z obstoječim jezikovnim stilnim odtisom
- Ugotovitve: starost, spol ter možna primerjava besedila -> ugotovitev ali gre pri dveh različnih besedilih za delo iste osebe





Medmrežni vzorci sodelovanja

- Iz zajetih log datotek lahko pridobimo strukturirane podatke, ki nam razkrijejo določene vzorce vpletenih oseb. Pomembnejši so naslednji vzorci:
  - Datum in čas povezave na komunikacijsko storitev.
  - Število objavljenih sporočil.
  - Število deljenih povezav.
  - itd.

- Spremljanje dinamike pomembnih vzorcev
- Sledenje preklapljanju med različnimi digitalnimi osebami - časovnica

Profiliranje kibernetskih kriminalcev in žrtev

- Isis orodje omogoča avtomatsko profiliranje kriminalcev in žrtev na podlagi zajete komunikacije. Celoten profil je zgrajen na podlagi naslednjih elementov:
  - Uporaba jezika,
  - Starost / spol analiza,
  - Aktivnost na medmrežju.

Razlikovanje pristnih digitalnih oseb od varljivega obnašanja
Isis orodje v praksi

- Primer uporabe Isis orodja v praksi in rezultati. Rezultati so na podlagi dveh testov:

1) Test v katerem ni zavajajočega obnašanja, torej digitalne osebe se ne izdajajo za 3. osebo
   - baza British National Corpus (BNC),
   - 1684 oseb,
   - orodje nam pripravi razpon verjetnosti za posamezna starostna obdobja kot so 11-18 let, 19-30 let,...

2) Test v katerem se oseba izdaja za 3. osebo

- nadzorovani test, ki je po naravi podoben Turingovem testu
- skupina otrok, v starosti 11-18 let
- skupina 10 oseb (5 oseb otroci iste starosti in 5 oseb, ki se je izdajalo za otroke)
- Izkazalo se je, da je Isis orodje precej bolj natančno klasificiralo dejansko starost in spol osebe na drugi strani komunikacije kot pa otroci.

Povzetek - zaključek

- Z prihodom socialnih omrežij je postala zloraba digitalne identitete pomemben del taktike kriminalnih organizacij.
- Tako je postala potreba po orodjih, ki so zmožna analizirati in klasificirati pomembne atribute digitalne osebe, kot je spol in starost.
- Pokazili smo, da je s pomočjo takšnih orodij možno doseči zelo dobre rezultate.
- Izkazalo se je, da orodje deluje bolje, kadar se oseba izdaja za drugo osebo, torej uporablja taktiko zavajanja.

Povzetek - zaključek

- Toda zaradi narave človeškega jezika ta orodja ne dosegajo 100% natančnosti pri klasifikaciji.
- Tako pridemo do zadnje ključne točke, da je ekspertno znanje še vedno nepogrešljivi del raziskovanja.
- Ugotovimo lahko, da so ta orodja najmočnejša ravno v kombinaciji z bogatimi izkušnjami kriminalistov.

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Matevž Černe in Klemen Marolt

-

ESTIMATION OF HUMAN HEIGHT FROM SURVEILLANCE CAMERA FOOTAGE: A RELIABILITY STUDY

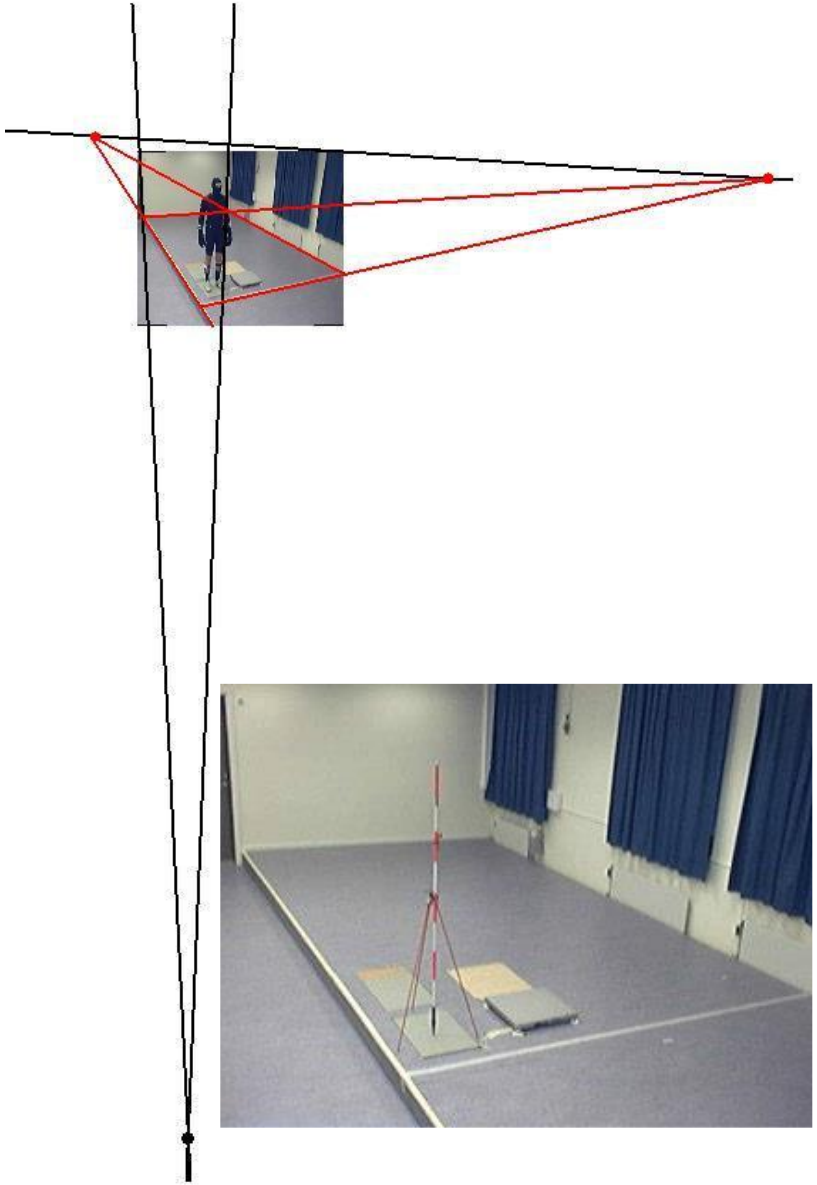
5. maj
2014

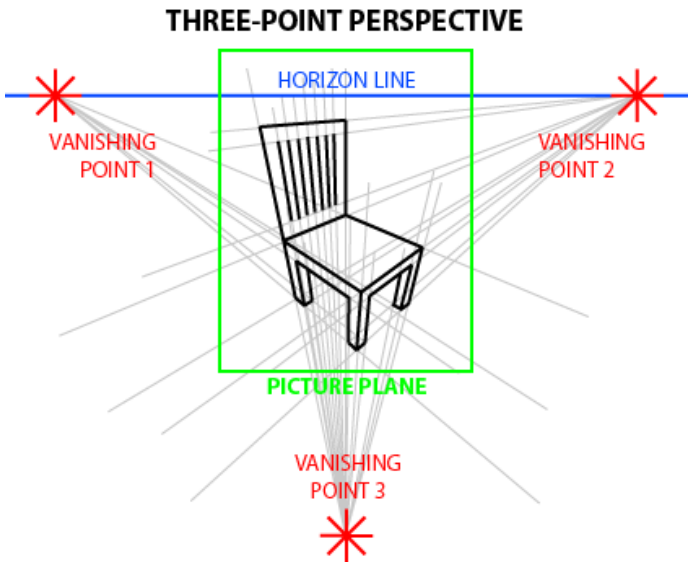
Predstavitev teme

- Definicija telesne višine
- Otežena ocena telesne višine
- Pomemben dejavnik pri identifikaciji
- Veliko kamer, slaba kvaliteta
- Uporaba posnetkov

Ozadje področja

- SVM
  - Kalibracija
  - Popačenje
  - Bežišče (vanishing point), horizont (horizon line)
  - Kalibracijska palica





Cilji

- Oceniti meritve in raziskati vpliv drže
- Kako natančna je metoda SVM pri ocenjevanju telesne višine oseb na slikah?
- Kako drža vpliva na višino osebe v primerjavi z dejansko telesno višino te osebe ko le-ta stoji, hodi in teče?
- Kateri položaj med hojo in tekom se najbolje ujema z dejansko višino?

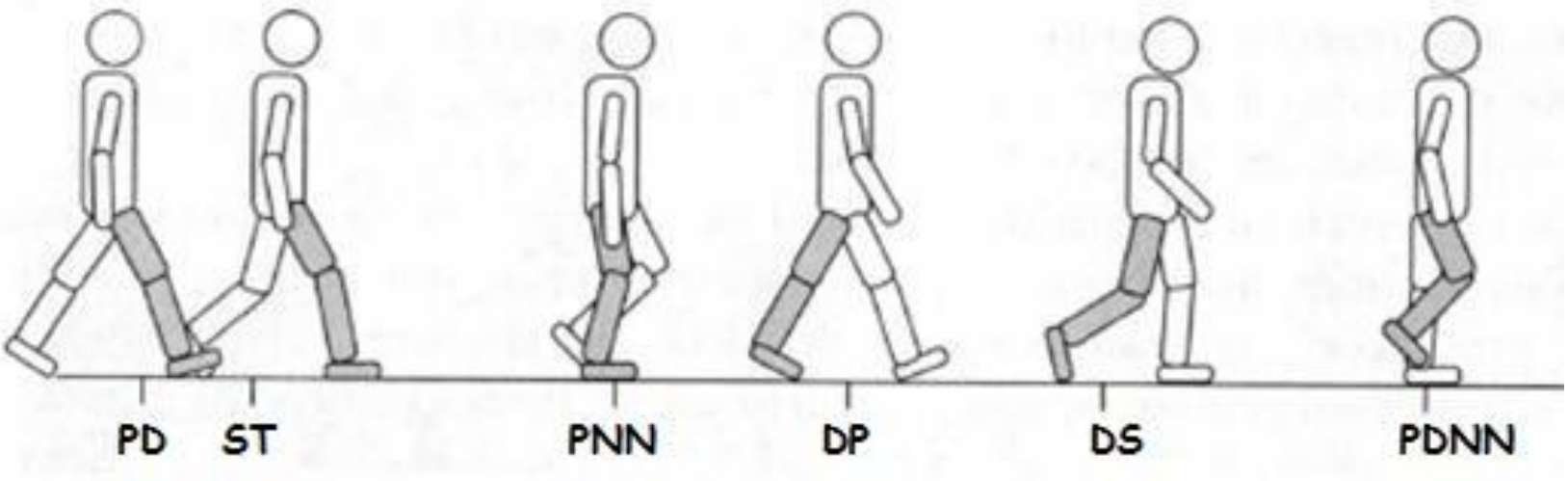
Metode

Subject	Height (cm)	Weight (kg)	BMI	Age
1	176.2	68.0	21.90	21
2	164.5	66.5	24.57	28
3	186.6	85.5	24.55	21
4	185.9	82.0	23.72	27
5	185.0	84.9	24.82	25
6	175.4	67.3	21.87	21
7	189.7	70.9	19.71	33
8	168.0	62.7	22.22	28
9	182.7	83.5	25.01	24
10	172.0	75.7	25.60	28

- Osebe
  - 10 moških
  - 15 – 30 let
  - Povp. 25.6 let, 180.7 cm, 23.43 ITM
- Zajem podatkov
  - Enaka oblačila
  - Čevlji
  - Položaji osebe:
    - Stanje pokonci
    - Stanje sproščeno
    - Stanje na eni nogi
    - Počasna hoja
    - Hitra hoja
    - Tek

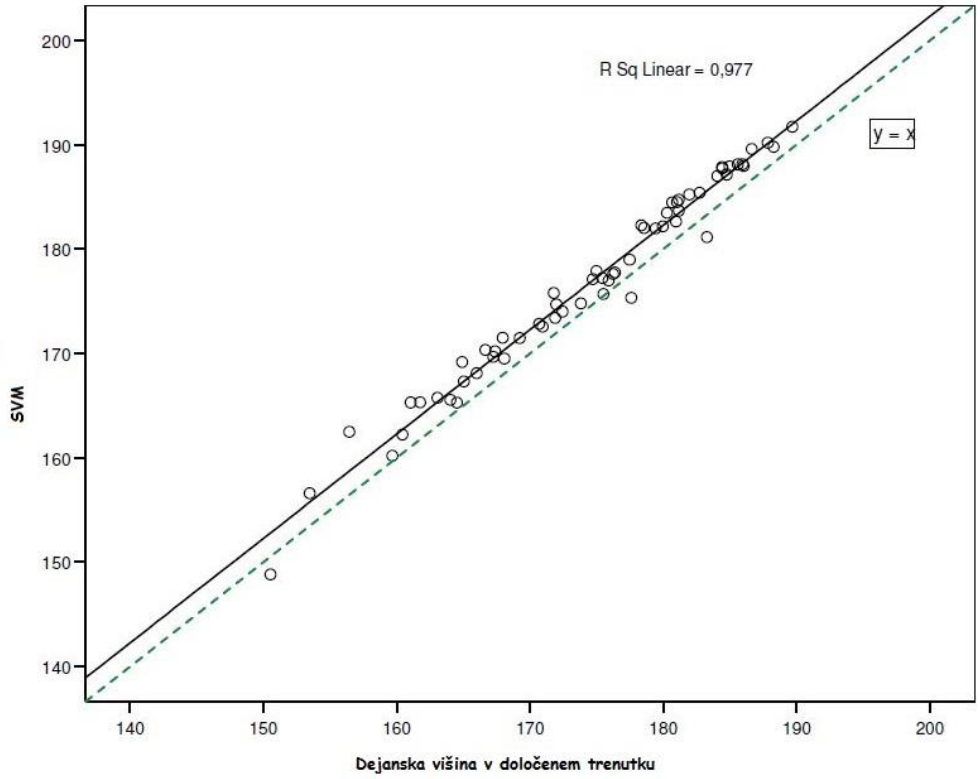
Metode

- Obdelava podatkov
  - Položaji pri hoji
  - Najboljši položaj



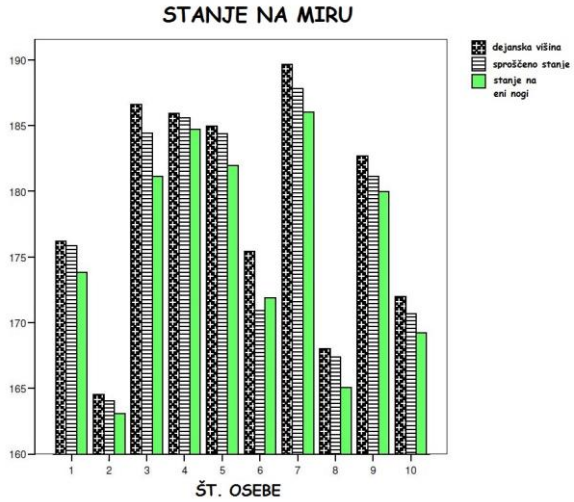
Rezultati

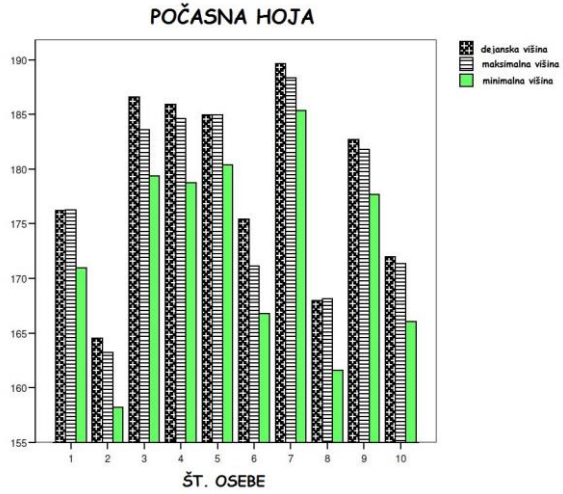
- Ovrednotenje metode SVM
  - SVM: 176.7 cm, dejanska višina: 174.4 cm
  - Povprečna razlika: 2.30 cm

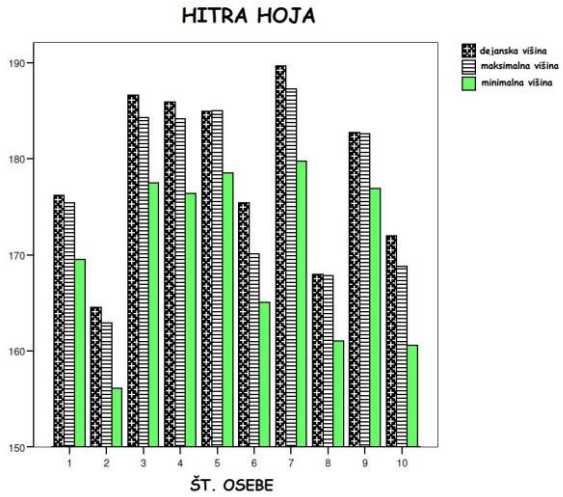


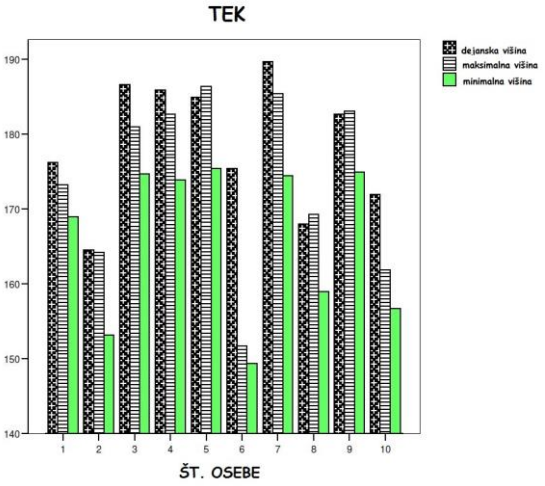
Rezultati

- Vpliv drže na višino



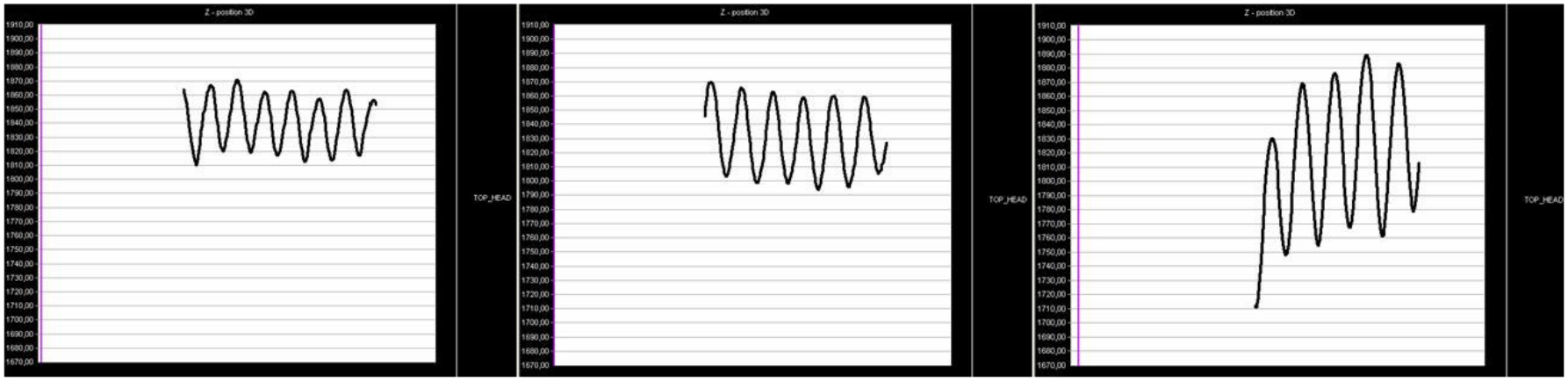






Rezultati

- Spreminjanje višine pri hoji in teku



Počasna hoja Hitra hoja Tek

Zaključek

- Kako natančna je metoda SVM pri ocenjevanju telesne višine oseb na slikah?
  - Povprečna napaka +2.30 cm
- Kako drža vpliva na višino osebe v primerjavi z dejansko telesno višino te osebe ko le-ta stoji, hodi in teče?
  - Stoja sproščeno: 99.2 %, Stoja na eni nogi: 98.4 %, Počasna hoja: 99.3 %, Hitra hoja: 99.0 %, Tek: 97.4 %
- Kateri položaj med hojo in tekom se najbolje ujema z dejansko višino?
  - Hoja: položaj premika noge naprej, Tek: obe nogi v zraku

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Svetlana Nikić
Anže Škerjanc
Nejc Škerjanc

TRIAŽNI MODEL ZA ISKANJE DOKAZOV

4. maj
2014

Problemi preiskovanja

- Le majhen del podatkov je relevanten za problem
- Zasebnost preiskovancev
- Onemogočanje delovanja podjetja
- Vse več podatkov
- Časovna omejitev
- Pomanjkanje denarnih sredstev

Možna rešitev?

triaža

Triaža

- **SSKJ: triaža** triáža -e ž (á) med. *razvrščanje bolnikov, poškodovancev v skupine glede na vrsto in težo poškodbe, obolenja, nujnost obravnave:* opraviti triažo; triaža in prevoz ranjencev ◊ ped. triaža mladoletnih prestopnikov

- Slabosti
- Alternativa triaži

- Administrativna in tehnična triaža

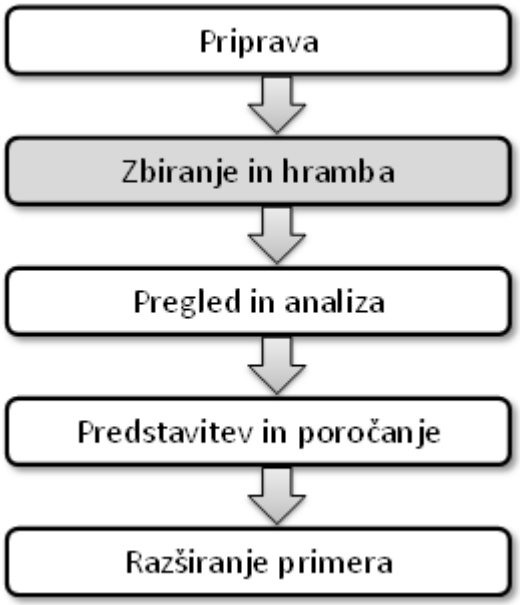
Nov model in pravno ozadje

- Opis je določen z odredbo
- Trenutno: pri vsakem primeru več subjektivnih mnenj
- Cilj: uveljaviti objektiven standard

- Po celem svetu se spreminjajo zakonodaje
- Razlike v zakonih med državami
- Težave v praksi
- Smernice za ravnanje z digitalnimi dokazi

Predlagan pristop

- Digitalni preiskovalni model
- Selektivno preiskovanje na kraju zločina samem
- Upoštevanje do sedaj znanim proceduram v sodstvu



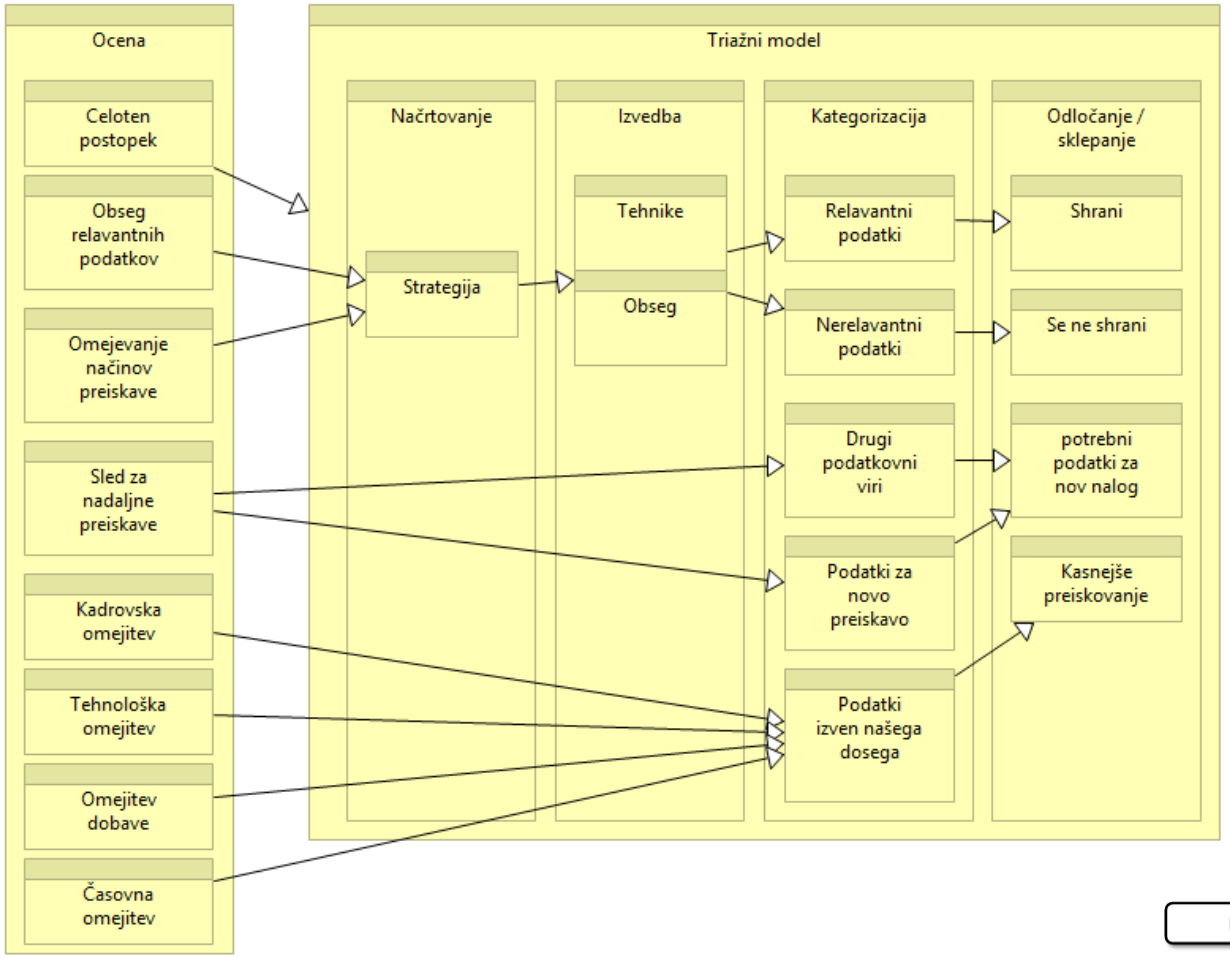
Osnova algoritma

- Faze:
  - Presoja
  - Vzpostavitev triažnega modela
  - Periodično vzpostavljanje nove presoje

Faza presoje

- Postavitev ciljev preiskave
- Oblikovati pristop preiskovanja
- Upoštevati omejitve pri preiskavi
- Oceniti obseg relevantnih podatkov

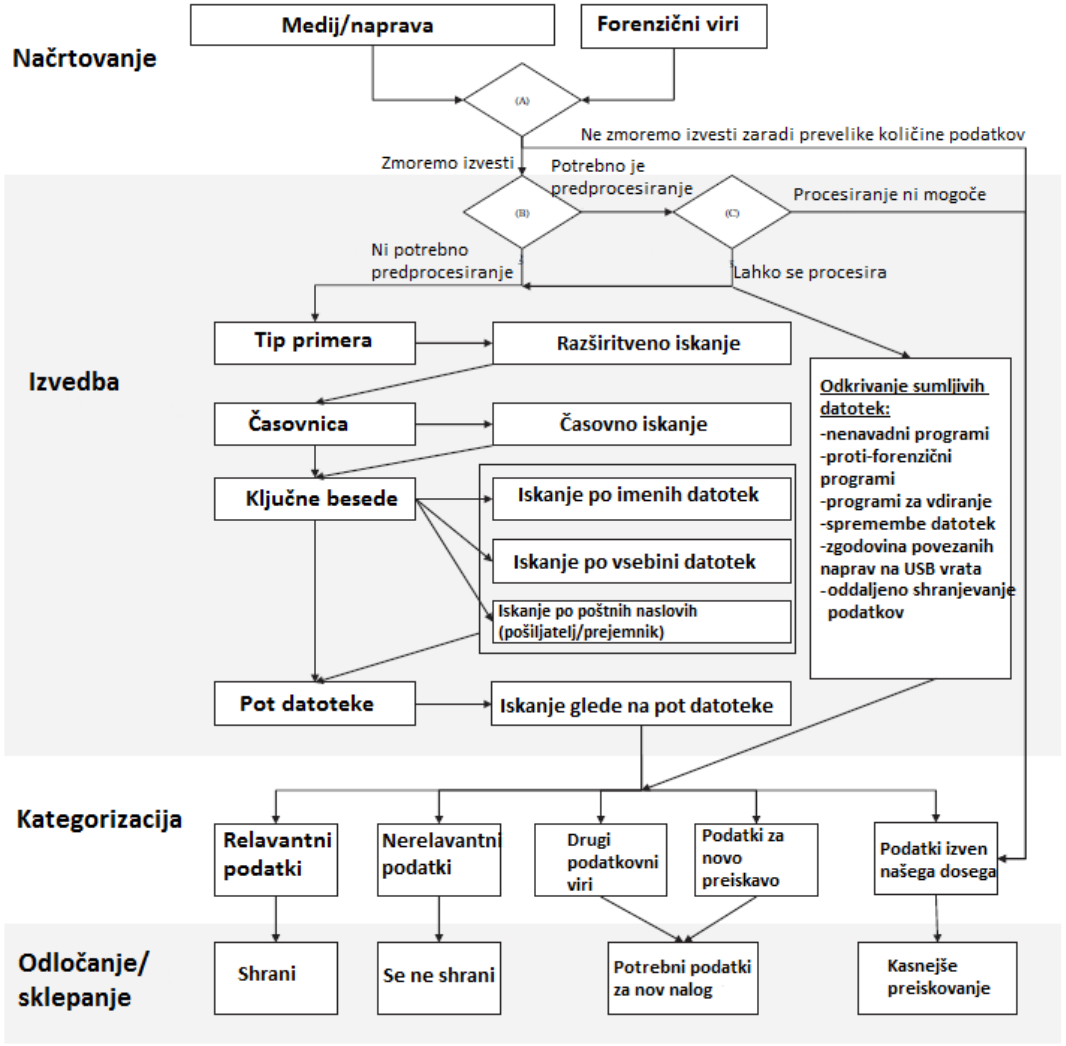
Vzpostavitev triažnega modela



Periodično vzpostavljanje nove presoje

- Pri spremembah v preiskavi
- Namen: Triaža ustreza sedanjemu stanju na terenu

Triažni model



Načrtovanje

- tip datoteke,
- velikost,
- stanje naprave,

- Omejitve?

Izvedba

- odločitev glede na tip kriminalnega dejanja,
- odločitev glede na čas uporabe/kreiranje,
- odločitev glede na meta podatke,
- odločitev s pomočjo meta podatkov,
- odločitev glede na standarne poti.

Kategorizacija in odločanje/sklepanje

- podatki, ki so (ne)pomembni za preiskovan zločin
- zunanji podatki,
- podatki za novo preiskavo,
- podatki, ki so izven našega dosega.

Vprašanja?

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Miha Mohorčič
Rok Povšič
Marko Škrjanec

Preprečevanje nepooblaščene rabe mobilnega telefona s pomočjo biometričnih naprav

Predstavitev

- Biometrični sistemi
  - Razlogi za uporabo
  - Načini realizacije
- Biometrični sistemi v mobilnih napravah
  - Načini prepoznave uporabnika
  - Varnost sistemov
  - Forenzična vrednost
- Načrti za prihodnost

Biometrični sistemi

- Kaj je biometrični sistem

- Načini realizacije
  - Računalniški vid
  - Prepoznava glasu
  - Prstni odtisi
  - Kombinirani

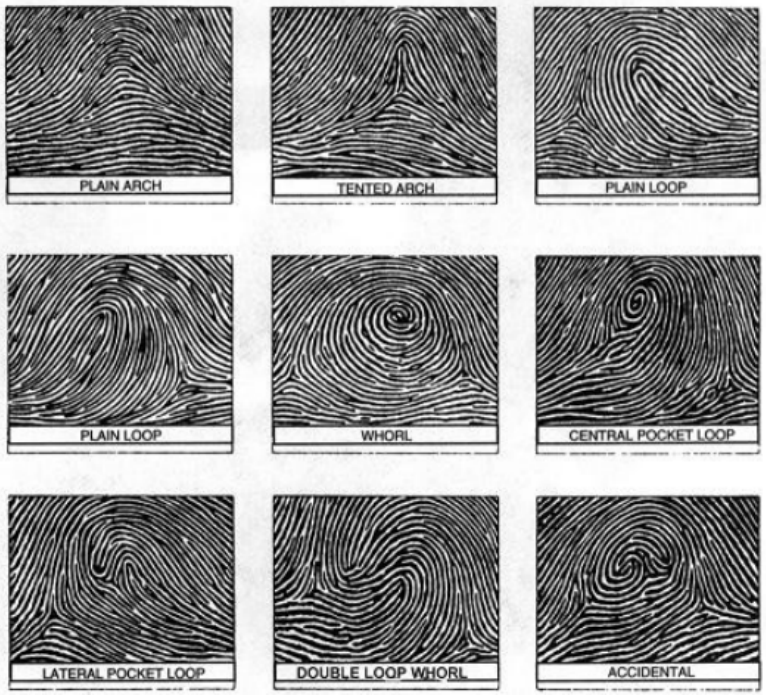
- Potrebna strojna in programska oprema

Eksperiment: Android prepoznava obrazov

- Vtisi o delovanju
  - Preprostost uporabe
  - Napake prvega in drugega tipa
- Načini neavtoriziranih dostopov
  - Enostavni (proces)
  - Preprosto izvedljivi (brez posebnih orodij)
- Naši predlogi
  - Identifikacija in ne avtentikacija
  - Hranjenje podatkov

Prstni odtisi

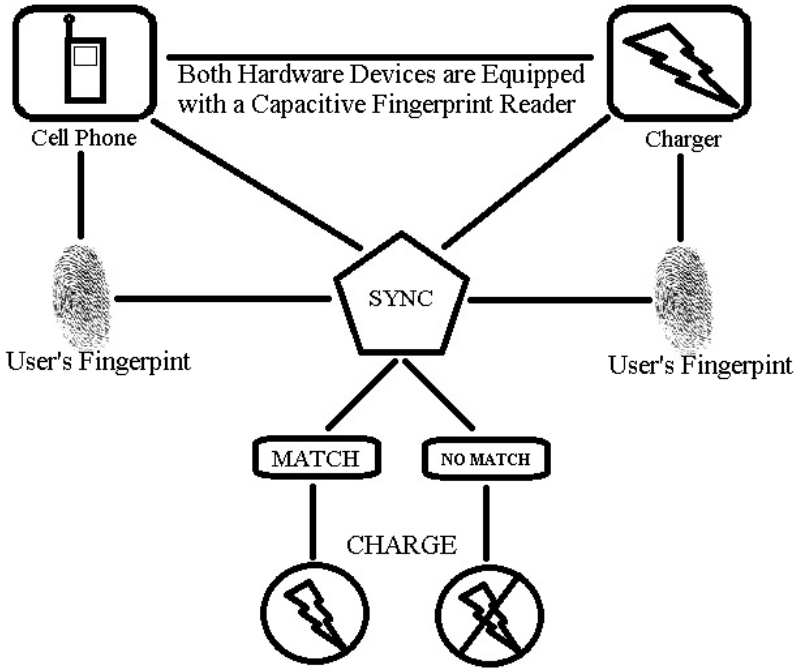
- Vtisi o delovanju
  - Preprostost uporabe
  - Napake prvega in drugega tipa
- Strojna in programska oprema
- Načini neavtoriziranih dostopov
- Naši predlogi
  - Identifikacija in ne avtentikacija
  - Hranjenje podatkov



*Vir slike: Preventing Cell Phone Intrusion and Theft using Biometrics

Prstni odtisi v mobilnih napravah

- Predlagana rešitev
  - Bralniki na napravi in polnilcu
  - Zapisano ob nakupu
- Spreminjanje funkcije gumba za odklepanje
- Velik poseg v strojno in programsko opremo
- Oteži uporabo lastniku



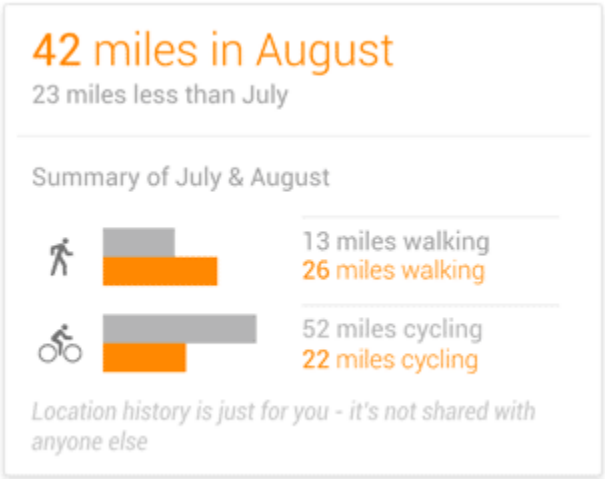
*Članek in vir slike: Preventing Cell Phone Intrusion and Theft using Biometrics

Kombinirani

- Združujejo več biometričnih sistemov
  - Uporaba že znanih metod
- Povečana varnost
- Moteča uporaba
  - implementacija
- Odvračanje od kraj lastnine in osebnih podatkov
- Umetna inteligenca
  - Inteligentna integracija večih sistemov

Umetna inteligenca

- Neopazna uporaba
  - Zbiranje podatkov o zgodovini
  - Inteligentno sklepanje
- Povečana varnost
  - Količina podatkov
  - Težko ponovljivi vzorci
- Implementacija
  - Znani sistemi + programska podpora
- Komu zaupati podatke in interpretacijo



*Vir slike: https://www.google.com/landing/now/#cards

Zaključki

- Zrelost sistemov
- Identifikacija, ne avtentikacija
- Možne forenzične izboljšave
  - Oddaljeno hranjenje zgodovine
    - Zaupanje v shrambo!
  - Interpretacija podatkov

HVALA ZA POZORNOST

Vprašanja in razprava

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Saša Makorič
Sandi Šemrov

-

Ponarejanje SMS sporočil

22. September 2012

Ali je možno ponarediti SMS?

- Da
- Ne prek omrežja, kot pri elektronski pošti
- Z ustrezno programsko/strojno opremo

Programska/strojna oprema

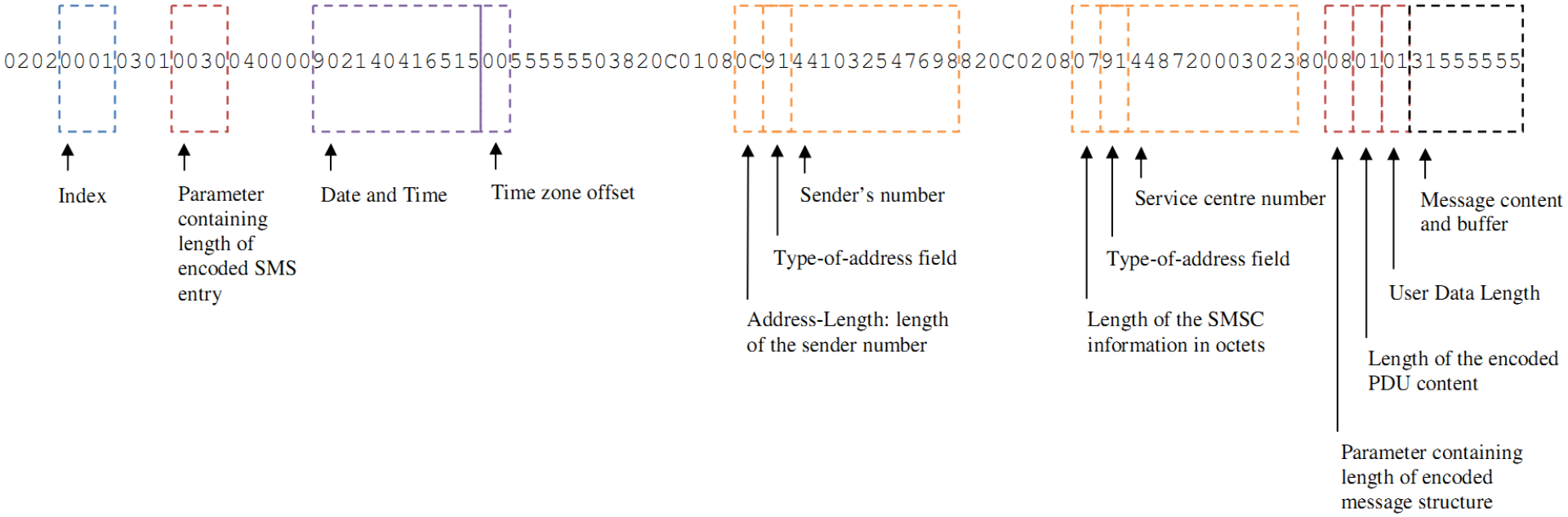
- COTS (Commercial Off-The-Shelf) SW/HW
  - Sarasoft UFS/HWK – „Tornado“
  - Cyclone Box
  - Advance Turbo Flasher by AdvanceTeam
- Nokia 6021
- Standardiziran način shranjevanja podatkov
- Velik tržni delež (2009)

Način shranjevanja podatkov

- PM tabele
  - Ključi, podključi
- Nokia 6021 sporočila SMS
  - Ključ: 140, podključi so sporočila

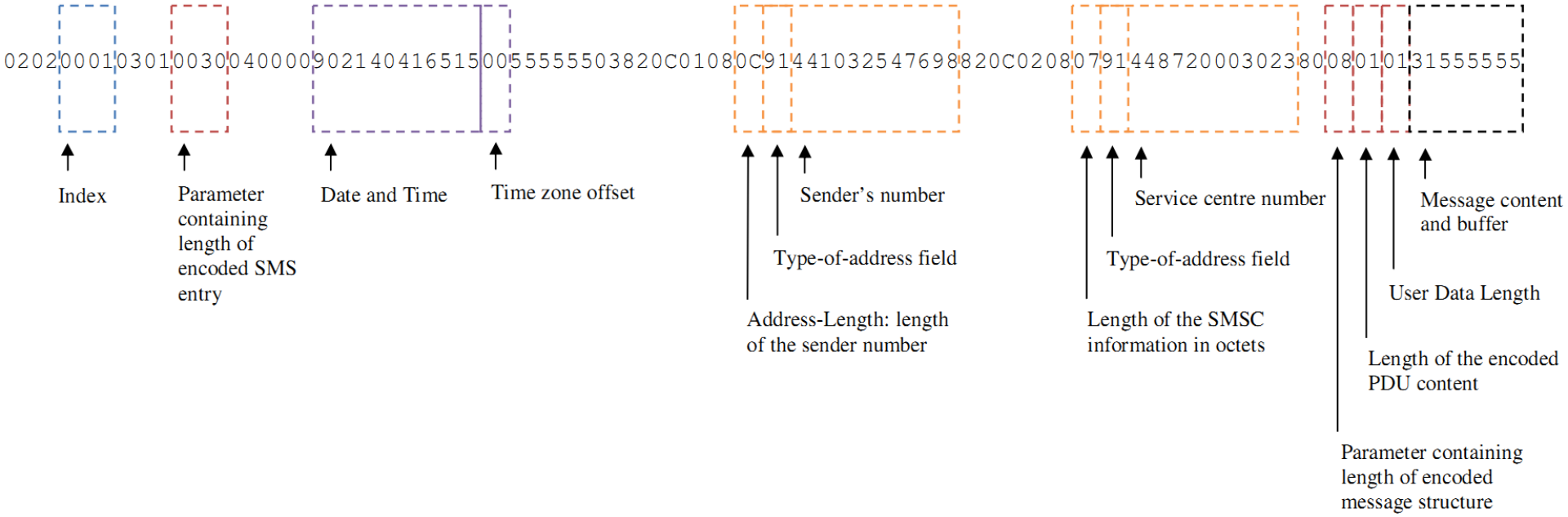
Sestava sporočila SMS

- Ni v standardnem formatu GSM 3.40
- Index = offset 6 (+ 2 prej (offset 4) za več kot 255 sporočil)
- 2 parametra dolžine (off. 14 + off. 12 in off. -14)



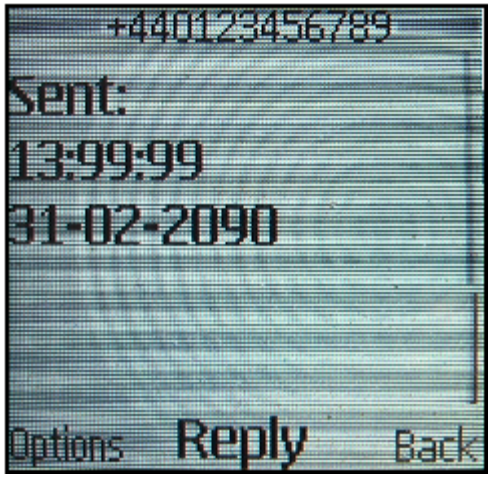
Sestava sporočila SMS (2)

- Datum (format po GSM spec. YYMMDDhhmmssTZ)
  - 1. v mesecu je obratnem vrstem redu „10“
- Vsebina SMS v formatu PDU (dolžina sporočila v User Data Length)



Testiranje

- Ustvarjanje novih sporočil uspe do neke mere
- Testiranje znotraj meja
  - Potrebno je posodobiti polje dolžin
  - Datum je možno spremeniti
- Testiranje zunaj meja
  - Vpis datuma, ki ni možen (npr. 31. 2.)
    - Leto [00 = 2000..99 = 1999]
    - Mesec [01..12]
    - Dan [01..31]
    - Ura [00..23]
    - Za minute in sekunde [00..99]
    - Dovoljen zapis ure (npr. 23:99:99)



Ponarejanje SMS sporočil na Android napravah

- Testiranje na android verzije 2.3.6 (Gingerbread)
- Pregled strukture shranjevanja SMS sporočil
- Ročno ponarejevanje
- Ponarejevanje s uporabo obstoječih aplikacij
- Pregled ponarejenih spročil

VsebStruktura shranjevanja SMS sporočil na Android napravahina

- Potreben superuser dostop
- Shranjevanje v SQLite podatkovni bazi
- Shranjevanje v predpomnilnik

Struktura shranjevanja SMS sporočil na Android napravah

- addr
- android_metadata
- attachments
- canonical_addresses
- drm
- mychannels
- part
- pdu
- pending_msgs
- rate
- raw
- sms
- sqlite_sequence
- sr_pending
- threads
- words
- words_content
- words_segdir
- words_segments

_id	thread_id	address	person	date	protocol	read	status	type	reply_path	subject
9283	306	123456789		0		1	-1	1		
9285	306	123456789		0		1	-1	2		
9291	306	123456789		0		1	-1	1		
9292	306	123456789		0		1	-1	2		

body	service_center	locked	error_code	seen	deletable	delivery_date
fake msg		0	0	1	1	
fake msg reply		0	0	1	1	
Ponarejanje sms sporocil		0	0	0	1	
Ponarejanje sms sporocil, reply sms		0	0	0	1	

Ponarejanje SMS sporočil

- Ročno – preko SQL ukazov
- Uporaba aplikacij
  - Fake SMS Sender
  - SMS Editor

Pregled ponarejenih sporočil

- Nekoherentnost podatkov
  - Polja brez podatkov
  - Novejša sporočila s starejšimi časi nastanka

Tehnike za preverjanje pristnosti

- Ujemajoči podatki s tistimi, ki jih ima ponudnik storitev
- Ponudnik beleži le določene stvari
- Beležke, kopije tabel ipd. na računalniku ponarejevalca sporočil

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Grega Gašperšič, Karmen Bezlaj

ANALIZA SISTEMOV ZA IZSLEDITEV IP NASLOVA

05. Maj 2014

Motivacija

- pojavitev napadov kot sta:
  - DoS (Denial of Service)
  - DDoS (Distributed Denial of Service)
- kompleksnost internet
- zaupanje v IP protokol
- ...

Cilj

- analiza pristopov za preprečevanje napadov
- pristopi za prepoznavanje vira napada
- primerjava pristopov

Pristopi za preprečevanja napadov

- Skupine:
  - Preprečevanje vdora
  - Zaznavanje vdora
  - Blaženje vdora
  - Odziv na vdor
- Osredotočimo se na izsledite IP-ja
  - spada v skupino za odziv na vdor
  - dva obetava sistema:
    - DPM (Deterministic Packet Marking)
    - DFM (Deterministic Flow Marking)

Izsleditev IP naslova

- Trije vidiki razvrščanja trenutnih implementacij:
  - Osnovni principi
  - Metode procesiranja
  - Lokacija (pošiljanja podatkov o izsleditvi IP-ja)

Izsleditev IP naslova – Osnovni principi

- Logging (metode logiranja)
  - usmerjevalnik ohrani informacije o potovanju paketov
  - slabost: velika poraba CPU-ja in RAM-a na usmerjevalnikih
- Marking (metode označevanja)
  - nekateri ali vsi usmerjevalnik v poti napada pošiljajo dodatne informacije
  - informacije dodane v glavo IP paketa ali poslane z novimi paketi

Izsleditev IP naslova – Metode pocesiranja

- Deterministic (deterministične metode) *
  - vsak paket je obdelan na izvoru in cilj
  - slabost: dolg čas obdelave paketov, veliko pasovna širina
- Probabilistic (verjetnostne metode)
  - več procesiranja, večja natančnost
  - manjši čas obdelave in pasovne širine kot pri *
  - bolj zapletena obdelava paketo na cilji strani
  - primer: PPM, iTrace, ...

Izsleditev IP naslova - Lokacija

- Source group method (robni usmerjevalnik)
  - namen je identifikacija izvora napada, ne poti
- Network group method (vsi (ali nekateri) usmerjevalniki na poti napada)
  - večina implementacij spade v to skupino
  - namen je identifikacija cele ali del poti napada
  - slabost: sinhronizacija med večimi usmerjevalniki, velika poraba virov (CPU, RAM)

DPM (Deterministic Packet Marking)

- Vidiki razvrščanja:
  - Osnovni principi: Marking
  - Metode procesiranja: Deterministic
  - Lokacija (pošiljanja podatkov o izsledítvi IP-ja): Near the source

DPM (Deterministic Packet Marking)

- Marking:
  - uporablja 17 bitov v glavi IP-ja (16 bitov identifikacija, 1 bit – označevalna informacija)
  - vsak paket je označen
- Deterministic:
  - IP naslov razdeljen na 2 segmenta (0..15, 16..31)
  - ob prejemu paketa na robnem usmerjevalniku se z verjetnostjo P izbere 1 segment in ga vstavi v polje za identifikacijo (žrtev vzdržuje polje)
  - 1 bit rezerviran za izbiro segmenta
  - dohodni paketi so označeni, odhodni niso

DPM (Deterministic Packet Marking)

- Izboljšave:
  - uvedba hash funkcija v označevalni informaciji
  - označevalna informacija se razdeli na 3 dele:
    - segment vstopnega naslova – a
    - indeks segmenta - d
    - razgrajen vstopni naslov – k
  - najboljša konfiguracija: a = 4, d = 3, k = 10
    a + d + k = 17

Analiza DPM metode

- CPU obremenjenost:
  - nizka, označuje samo robni usmerjevalnik, ki je najbližji napadalcu
  - lažje procesiranje, ne išče poti do napadalca
- Poraba RAM-a:
  - nizka, majhno polje potrebno za rekonstrukcijo IP naslova (cca 64 Kb)
- False Positive
  - FP < 1 %
- Število potrebnih paketov za izsleditov IP-ja:
  - # paketov = 32 / a
  - primer: a = 4, # paketov = 8

Slabosti DPM metode

- FP < 1 % če število napadalcev v DDoS napadu manjše kot omejeno število o
- najde IP naslov blizu napadalca in ne natančnega IP-naslova
- Večja natančnost kot verjetnostne metode, ampak označuje vse pakete v omrežju
- DPM domneva da informacija označevanja ostaja nespremenjena dokler paket prehaja skozi omrežje (ni realno)

DMF (Deterministic Flow Marking)

- Vidiki razvrščanja:
  - Osnovni principi: Marking (vsakega toka)
  - Metode procesiranja: Deterministic
  - Lokacija (pošiljanja podatkov o izsledítvi IP-ja): Source (IP napadalca)

Načini označevanja toka pri DFM

- IP naslov izstopnega vmesnika na robnem usmerjevalniku
- NI-ID - identifikator dodeljen vsakem vmesniku, vezan na MAC ali na VLAN ID
- Node-ID - identifikator dodeljen vsakemu MAC naslovu vhodnih podatkov

Identifikacijski podatki

- DFM označi vsak tok z 60 biti identifikacijskih podatkov, ki vsebujejo:
  - 32 bitov za IP naslov izstopnega vmesnika
  - 12 bitov za NI-ID
  - 16 bitov za Node-ID
- 60 bitov je razbito na K fragmentov, kjer je:
  - M=60 / K bitov: identifikacija podatkov
  - $S=\log_2(K)$ bitov: identifikacija fragmenta

- Uporablja zastavice za identifikacijo označenih in neoznačeni pakete v toku.

Identifikacijski podatki

- Prvih K odsekov vsebuje:
  - M bitov namenjenih identifikaciji podatkovnih odsekov
  - s bitov - predstavljajo enega od 2^s možnih fragmentov
  - 1 bit - namenjen zastavici F (“1” označeni, “0” neoznačeni paket)

ID toka (ID flow)

- ID toka je peterica:
  - Izvorni IP naslov
  - L4 vrsta protokola (ICMP)
  - Vrsta ICMP
  - Koda ICMP
  - ICMP ID za ICMP tok.

Analiza DFM metode

- CPU obremenjenost:
  - nizka
    - manj kot pol milisekunde za podpis zastavice
    - manj kot eno milisekundo za preverjanje digitalnega podpisa
- Uporaba RAM-a (manjša od DPM):
  - zanemarljiva na usmerjevalnikih (cca 25 Kb)
  - majhno polje potrebno za rekonstrukcijsko IP naslova (23 Kb)

Analiza DFM metode

- False Positive
  - 0 % - preprečujejo jih ID-ji tokov.
- Število potrebnih paketov za izsleditov IP-ja:
  - # bitov = 32
  - # paketov za DFM = 2 * 16
  - # paketov za izsleditev = 5
  - # paketov = 7

Prednosti DFM metode

- izsledimo lahko IP napadalca, ne le njegovo delovno skupino oz. okolje
- onemogoča pokvarjanje podatkov (tudi napadalčevih).
- zagotavlja da informacije označevanja poti niso bile spremenjene.
- Vpletenost ISP je minimalna.

Unikatna prednost pred vsemi TB algoritmi:

- omogoča izsleditev napadalca vse do izvornega vmesnika omrežja še več, do LAN naslova za izvornim usmerjevalnikom.

Primerjava DPM in DFM

TABLE I. EVALUATING BOTH DPM AND DFM ON THE CAIDA DATASET, USING THE SAME METRICS

Comparison Metrics	**DPM**	**DFM with *K*=2**	**DFM with *K*=5**
Number of Marked Packets	241,589,706	24,059,752	32,470,758
MR	100%	9.96%	13.44%
Traced traffic in term of Number of Packets	23,948,7875	22,445,5742	219,912,254
TR in term of Number of Packets	99.13%	92.91%	91.03%
Traced traffic in term of Size (byte)	72,019,480,296	70,178,321,305	69,615,277,632
TR in term of traffic Size	99.26%	96.72%	95.95%

Primerjava DPM in DFM

TABLE III. COMPARISON OF DPM AND DFM

Comparison Metrics	DPM	DFM
Percentage of marked packets	100%	If $K = 2$: 9.96% If $K = 5$: 13.44%
Mark Spoofing by subverted routers	Yes	No
Maximum traceback ability	Up to the ingress interface of the edge router	Up to the attacker node
Mark Spoofing by Attacker	No	No
Computational Overhead on routers	Low	Fair
Computational Overhead on victim	Low	Fair
Memory Overhead on routers	Low	Low
Memory Overhead on victim	Low	Low
Bandwidth Overhead	None	Low
Tracdeback Rate	Good	Fair
False Positive Rate	Low, but the number of concurrent attackers is limited	Low
Number of required packets for traceback	8	2 or 5
ISP Involvement	Low	Low
Ability to handle Fragmentation	No	No
Ability to handle major DDoS attacks	Fair, The Maximum Number of Concurrent Attackers is limited	Good
Number of Marking bits	17	If $K = 2$: 16 If $K = 5$: 32

Vprašanja?

Hvala za pozornost.

Lep dan.

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tadej Jagodnik, Jan Češnjevar

VPLIV VZORČENJA NA ALGORITME ZA DETEKCIJO ANOMALIJ V OMREŽNEM PROMETU

maj, 2014

Uvod

- pojav vzorčenja v omrežnem prometu
- različne tehnike vzorčenja
- algoritmi za detekcijo anomalij
- ocenitev uspešnosti algoritmov pod različnimi tehnikami vzorčenja
- nova tehnika vzorčenja (Online Selective Sampling)

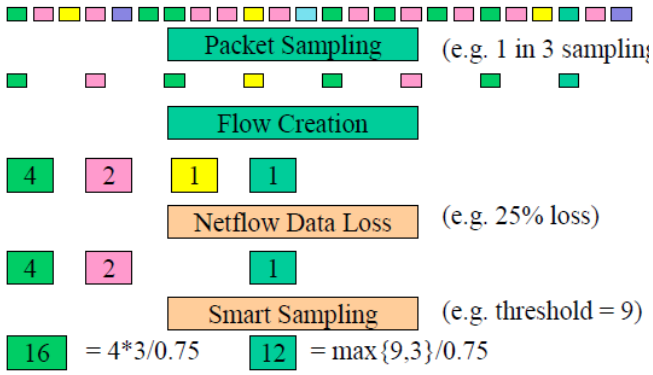
Pojav vzorčenja v omrežnem prometu

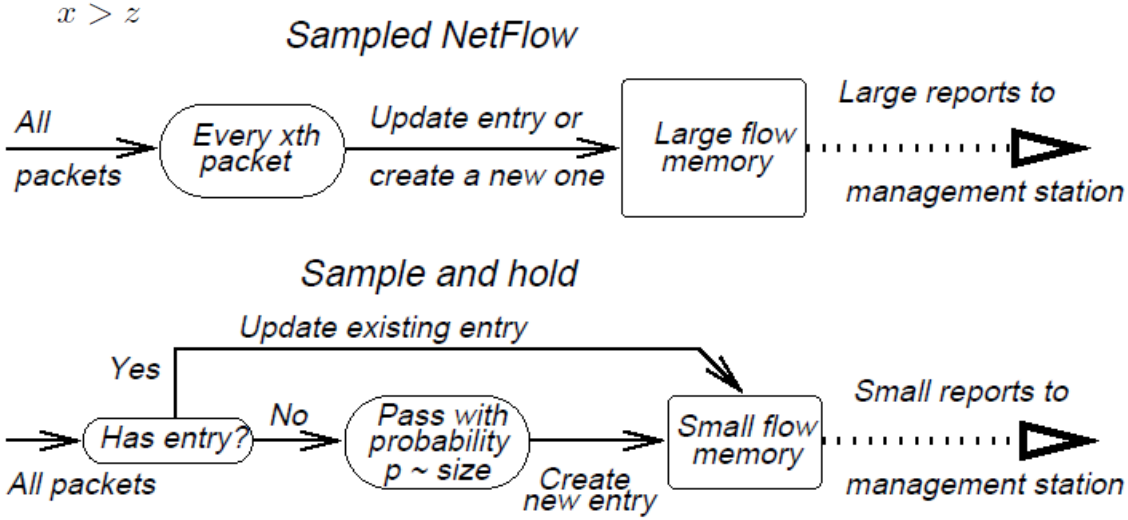
- Zakaj vzorčenje?
- dve vrsti anomalij:
  - nenadne spremembe v količini paketov (volume)
  - skeniranje (non-volume)

Tehnike vzorčenja

- vzorčenje paketov (packet sampling)
- vzorčenje tokov (flow sampling)
- pametno vzorčenje (smart sampling)
- vzorči in zadrži (sample-and-hold)
- vzorčenje z izbiranjem (selective sampling)

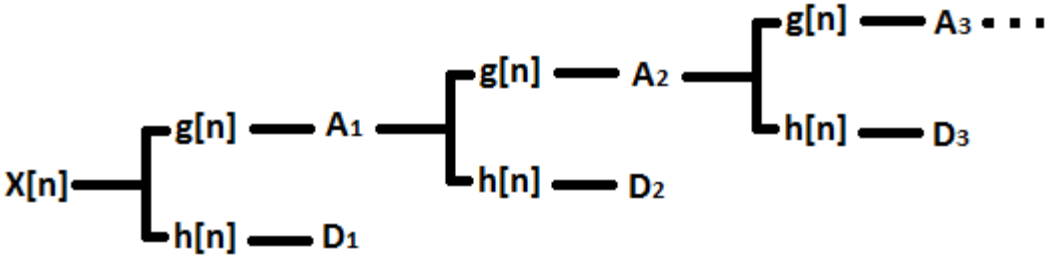
$$p(x) = \begin{cases} c & x \leq z \\ z/n \cdot x & x > z \end{cases}$$





Algoritmi za detekcijo anomalij (volume)

- Discrete Wavelet Transform (DWT)
  - Postopek transformacije signala
  - Prehod v domeno frekvence in časa
  - Postopek dekompozicije
    - Nizkopasovni (lowpass) filter
    - Visokopasovni (high pass) filter
- Algoritem
  - Trije deli:
    - Dekompozicija časovnih vrst
    - Ponovna sinteza
    - Detekcija



Algoritmi za detekcijo anomalij (non-volume)

- Threshold Random Walk (TRW)
  - H_0,verjetnost da je nenevaren gostitelj
  - H_1,verjetnost da je scanner

$$\Lambda(Y) = \prod_{i=1}^{n} \frac{P_r[Y_i|H_1]}{P_r[Y_i|H_0]}$$

- Time Access Pattern Scheme (TAPS)
  - vzorec dostopa

- Entropy-based Scan Detection

$$H(X) = -\sum_{i=1}^{M} p(x_i) \log_2 p(x_i)$$

Splošna resnica

- Izbira testne množice
- Izvedba algoritmov nad testno množico z optimalnimi parametri
- Uporaba FIM
- Končna množica (ground truth)

$$SR = \frac{resnicni\ scannerji\ pod\ vzorcenjem}{vsi\ scannerji\ iz\ splosne\ resnice}$$

$$FP = \frac{detektirani\ scannerji,\ ki\ to\ niso}{vsi\ scannerji\ iz\ splosne\ resnice}$$

Ocena uspešnosti (volume)

- Primerjava števila detekcij na:
  - Originalnih časovnih vrstah in
  - Vzorčenih časovnih vrstah
- Tehnika vzorčenja z najboljšimi rezultati:
  - Vzorčenje tokov (flow sampling)
- Z večanjem intervala se manjša število detektiranih anomalij

Sampling interval	10	100	1000
Percentage of flows (%)	36.7	8.03	1.47
Random packet sampling	19	6	1
Random flow sampling	21	18	13
Smart sampling	18	1	1
Sample-and-hold	18	2	1

Ocena uspešnosti (non-volume)

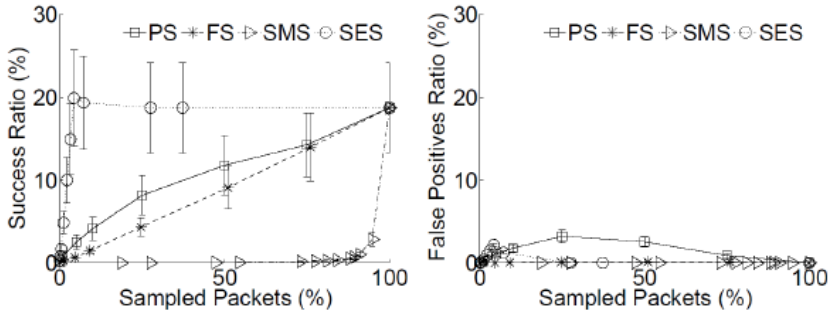


Figure 2: Vpliv vzorčenja na algoritem TRW [6].

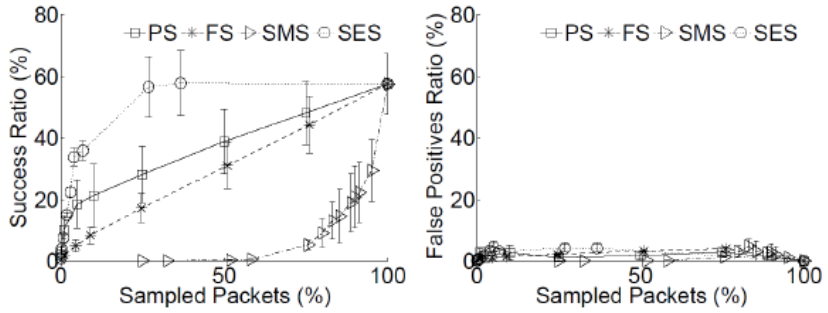


Figure 3: Vpliv vzorčenja na algoritem TAPS [6].

Online Selective Sampling

- Problem vzorčenja z izbiranjem (SES):
  - Pred vzorčenjem toka potrebno zajeti vse pakete
  - Velika poraba virov (ni v skladu s ciljem vzorčenja)
- Lastnosti OSES:
  - Sprejema odločitve na posameznem paketu
  - Manjša poraba virov
  - Zmožnost delovanja na spletu
  - Vzorčenje toka dokler je še majhen (vzdrževanje)
- Rešitve:
  - Uporaba zgoščevlane (hash) tabele
  - Uporaba Bloomovih filtrov
- Cilj OSES

Zaključek

- Aktualno raziskovalno področje
- Algoritmi za detekcijo:
  - Brez vzorčenja:
    - Slabo odkrivajo anomalije
  - Pod vzorčenjem:
    - V veliki meri se odkrivanje anomalij poslabša
- Veliko prostora za izboljšave:
  - Razvoj novih algoritmov
  - Razvoj novih tehnik vzorčenja
  - Primer: uspešnost nove tehnike OSES

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Leon Noe Jovan,
David Novak,
Dejan Petrovič

ZAŠČITA PRED BOTNETI

4. Maj
2014

Uvod

- Spletni kriminal – več 100 milijard letno
- Več kot prodaja marihuane, heroina in kokaina skupaj
- Ustanovljen European Cybercrime Centre
- Eno glavnih orodij spletnega kriminala - botneti

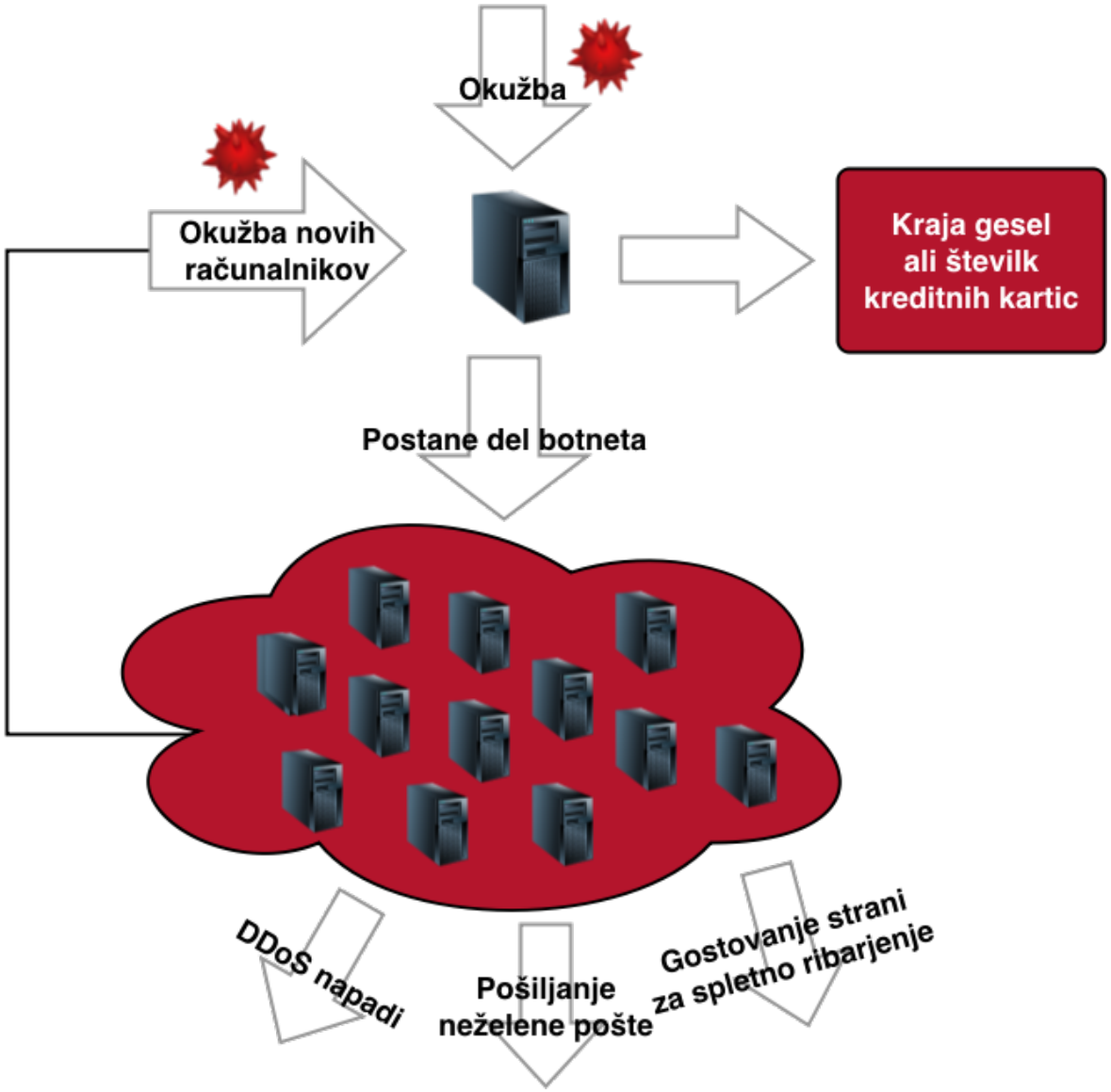
Kaj so botneti?

- Gruča računalnikov, okuženih z isto zlonamerno programsko opremo
- Stroj večinoma postane ogrožen, ko uporabnik odpre ali prenese zlonamerno programsko opremo
- Najprej uporabljani legalno (IRC)

Delovanje botnetov (1)

1. Distribucija programske opreme (npr. v obliki elektronske pošte)
2. Uporabnik prenese in zažene priponko
3. Njegov računalnik postane del botneta – zombi
4. Rekrutiranje novih računalnikov

Delovanje botnetov (2)



Uporaba botnetov (1)

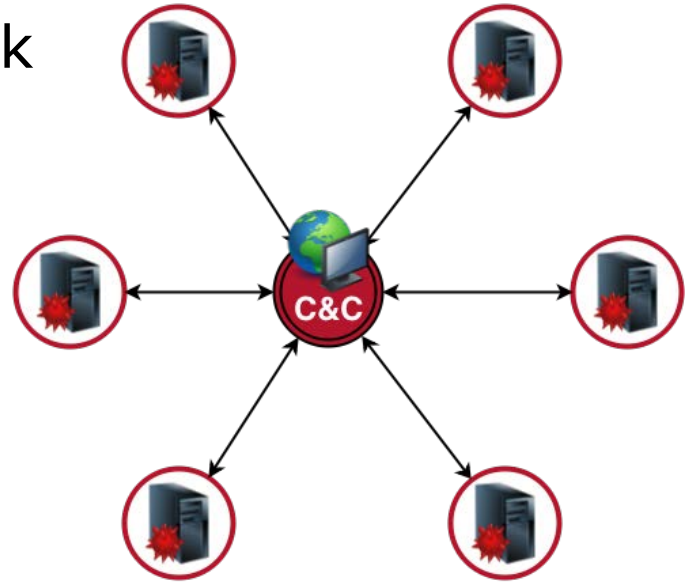
- Porazdeljen napad za zavrnitev storitve (DDoS)
- Vohunjenje (Spyware)
- Pošiljanje neželene pošte (E-mail spam)
- Goljufije s klikanjem (Click fraud)
- Gostovanje strani (Phishing)
- Okužba drugih računalnikov
- Hranjenje nelegalnih vsebin

Znani botneti

Ime	Število botov	Širina prenosa (mrd/dan)	Namen
BredoLab	30.000.000	3.6	Spam
Mariposa	12.000.000	?	DDOS, Spyware, Adware
Conficker	10.500.000	10	Kraja gesel
Marina BotNet	6.200.000	92	Spam
TDL-4	4.500.000	?	Spam, Adware
Zeus	3.600.000	?	Kraja bančnih podatkov: Phishing, Keylogging

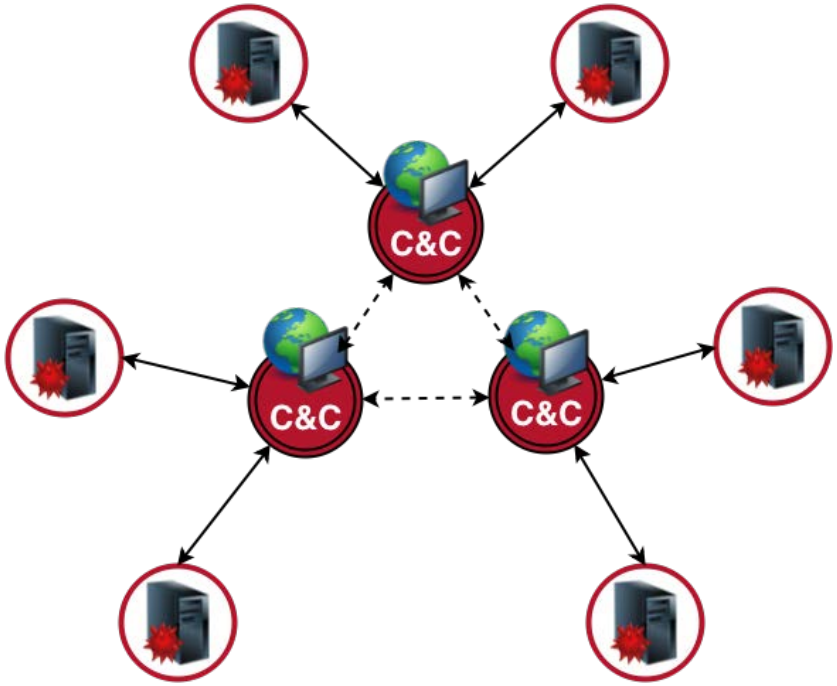
Oblike botnet omrežij - zvezda

- Boti direktno komunicirajo s skupnim centralnim nadzornim računalnikom
- Najbolj ranljiva oblika topologije
- Z izpadom centralnega računalnika se onesposobi celoten botnet
- Lahko izslediti centralni računalnik



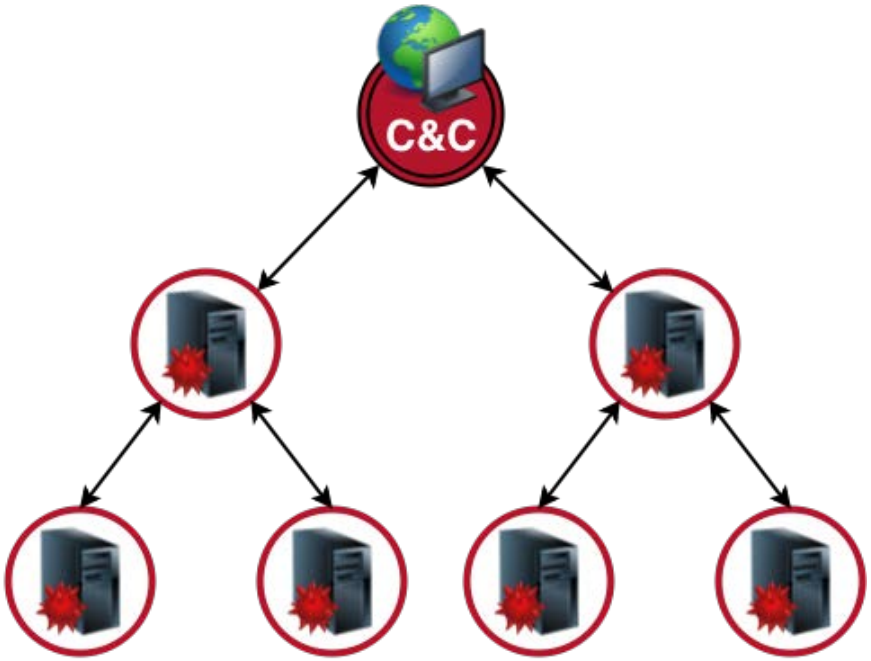
Oblike botnet omrežij - obroč

- Razširitev zvezde – več nadzornih računalnikov
- Višja odpornost
- Pri izpadu enega nadzornega računalnika botnet še vedno deluje



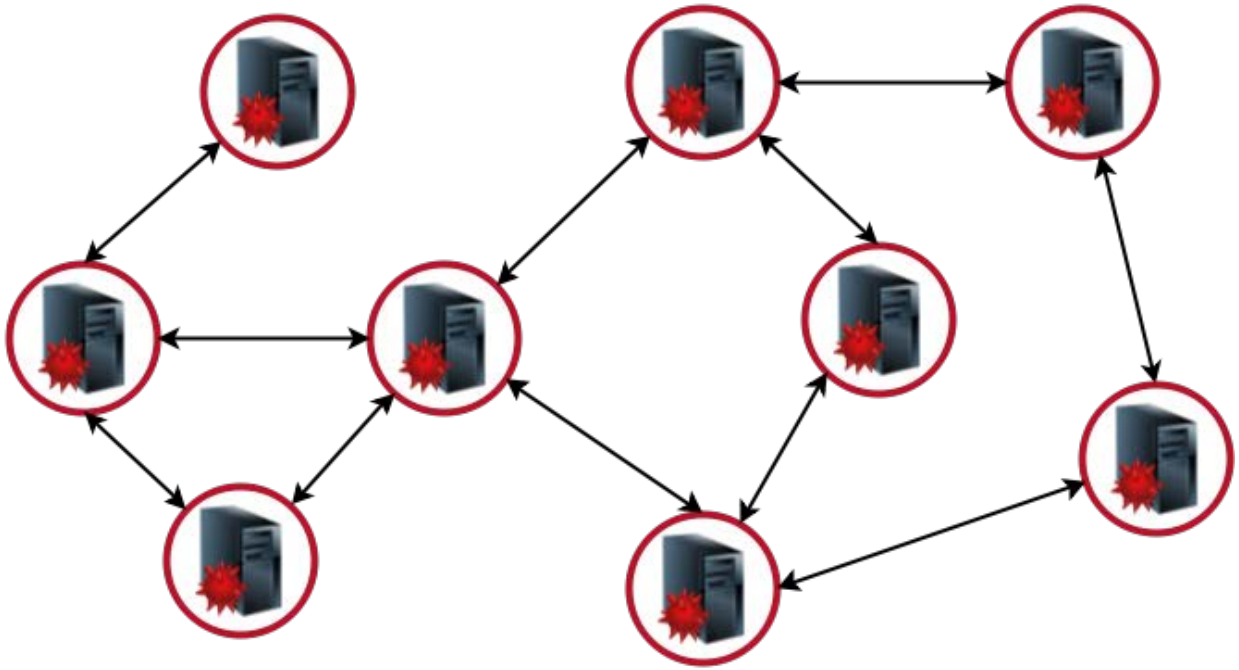
Oblike Botnet omrežij - hierarhija

- Nadzorni računalnik veliko težje izslediti
- Vmesni računalniki služijo kot proxy strežniki
- Napadalci bolj varni, a je pošiljanje ukazov počasnejše
- Ni primerna za upravljanje v realnem času



Oblike botnet omrežij - naključna

- Boti so med seboj povezani naključno
- Nima centralizirane nadzorne infrastrukture
- Vsak zombi je lahko nadzorni računalnik
- Najbolj odporna oblika botnetov



Zaščita pred botneti - preventiva

- Posodabljanje operacijskega sistema, protivirusnih programov, brskalnikov in ostale programske opreme
- Nastavitev večje stopnje varnosti v brskalniku
- Izogibanje sumljivim spletnim stranem
- Ignoriranje priponk elektronskih sporočil neznanega izvora

Zaščita pred botneti - okužba

- Upočasnjeno delovanje računalnika ali povečan promet po omrežju

1. Odklop računalnika iz omrežja
2. Odstranitev škodljive programske kode
3. Zamenjava gesel
4. Ponoven priklop, opazovanje delovanja računalnika

Zaščita omrežja pred botneti

- Črne liste IP-jev in domen znanih botnetov
- Ustrezna tehnologija za zaščito omrežja:
  - anti-virus, anti-spam, požarni zid, UTM, IDS/IPS
- Spremljanje dnevnikov požarnega zidu/UTM-a
- Spremljanje nenavadnega porasta omrežnega prometa
- Uporaba DDoS omrežne zaščite
- Hitro ukrepanje pri okužbah
- Uporaba vabe za detekcijo botnetov (Honeypot)

Samoozdravljivi sistemi

- Težava: evolucija botnetov
- Ideja iz narave - prilagajanje organizmov proti bakterijam in virusom
- Prilagodljiv obrambni sistem
- Minimalen poseg človeka
- Omogoča avtomatično detektiranje in zdravljenje okuženega sistema
- Cilj sistema je vzdrževanje čim višje dostopnosti, odpornosti in zdravja sistema

Uporaba samoozdravljivih sistemov

- Operacijski sistemi
  - Ponovno nalaganje programske kode
  - Izolacija posameznih komponent
  - Avtomatski ponovni zagon
- Vgrajeni sistemi
  - Mirujoče instance sistema

Arhitektura sistema

- 5 modulov:
  - Komunikacijski modul
  - Dnevniški modul
  - Zaznavni modul
  - Obnovitveni modul
  - Nadzorni modul

Komunikacijski modul

- Upravlja z vsemi komunikacijami sistema (tako vhodnimi kot izhodnimi)

Dnevniški modul

- Dokumentira vso dejavnost sistema
- Obvešča administratorja o nepravilnostih
- Generira (in arhivira) dnevna, tedenska in mesečna poročila

Zaznavni modul

- Nadzoruje dejavnost na omrežju
- Pregleduje DNS datoteke in dodaja izjeme
- Spremljanje prometa na posameznih vratih
  - Lahko jih določi administrator
  - Avtomatsko na osnovi učenja iz omrežja
- Izvajanje MD5 kontrolne vsote pomembnih datotek (TCPIP.sys)

Obnovitveni modul

- Poizkuša odstraniti bota iz okuženega računalnika
- Vsak računalnik v omrežju ima svojega agenta
- Obnovitveni modul ukazuje agentom:
  - ukinjanje posameznih storitev
  - zapiranje vrat
- Lahko deluje kot DNS sinkhole
- Zaščita tudi v primeru druge domene C&C

Nadzorni modul

- Zadnji modul v procesu razreševanja okužb
- Vklopi se v primeru neuspešne obnovitve sistema
- Računalnik odklopi iz omrežja
- Pošlje poročilo administratorju
- Zahteva človekov poseg

Povzetek

- Botneti se neprestano razvijajo, njihovo število pa strmo narašča
- Postajajo vedno večja grožnja za tako za osebne računalnike, kot tudi velike institucije
- Odgovor so samoozdravitveni sistemi
- Omogočajo prilagodljivo obrambo pred botneti
- Minimizirajo človekov poseg
- Modularna zasnova sistema omogoča lažje spreminjanje in nadgrajevanje sistema

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Rok Gomišček, Igor Lalić,
Jon Premik

-

DETECTING INFLUENTIAL SPREADERS IN COMPLEX, DYNAMIC NETWORKS

22. September 2012

Omrežja ljudi

- Družbena in poslovna
- Veliko število
- Hitra rast
- Kompleksna
- Dinamična
- Računalniške družbene vede

Računalniške družbene vede

- Zbiranje podatkov
- Analiza
- Odkrivanje skritih vzorcev
- Iskanje vplivnih vozlišč

Namen

- Teroristična omrežja
- Širjenje virusov
- Preprečevanje širjenja škodljivih informacij
- Vplivi na širjenje okužb

Odkrivanje širjenja

- Teorija grafov
- Povezave med vozlišči
- Najkrajša pot
- Centralna vozlišča
- Človeški vplivi
- K-shell

Centralnost

- Iskanje centralnih vozlišč
- Stopnja vozlišča
- Razdalja do drugih
- Nevarnost: vozlišča stopnje 1

Človeški vplivi

- Starost
- Spol
- Stan
- Zaupanje

K-shell dekompozicija

- Iterativno odstranjevanje vozlišč
- Temelji na „jedrosti“ vozlišč
- Položaj vozlišča v *k*-shell dekompoziciji
- Enostaven algoritem
- Ni primeren za dinamična omrežja
- Visok *k* ne pomeni velikega vpliva

μ-PCI

- μ-power community index
- Mešanica jedrosti in centralnosti
- Išče vozlišča v gostih predelih
- Tudi za dinamična omrežja
- Za različne velikosti

μ-PCI

- μ-PCI(v) = k;
  do μ * k vozlišč v μ-soseski v s stopnjo ≤ k

Zaključek

- Pri $\mu \leq$ bolje odkrije vplivna vozlišča
- Bolj monotona distribucija
- Enostavno računanje

Hvala za pozornost

Network Intrusion Investigation

Digital Forensic

Branislav Todorov
Jovan Buragev

Network Intrusion Investigation

- Introduction
- Network Intrusion
- Intrusion Prevention and Detection
- Summary

Network Intrusion

- Common types of network attacks

Investigation prevention and detection

- Intrusion prevention
- Technologies used in preservation of attacks
  - Snort – prevention and detection system

Intrusion investigation

- Identifying the intrusion
- Analysis
- Collecting the evidence
- Preparing the evidence for the court

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tomaž Borštnik, 63090025,
Darko Božidar, 63090023,
Gregor Čepin, 63090008

POSTOPEK FORENZIČNE ANALIZE OMREŽJA

4. Maj
2014

Uvod

- Več vidikov preiskave varnostnih incidentov
- Podatki za preiskavo iz štirih različnih virov
- Opis postopka preiskave
- Vrednotenje virov podatkov
- Signature programa Snort

Zlonamerna programska oprema

- Programska oprema namenjena oviranju delovanja sistemov
- Računalniški virusi (computer viruses)
- Računalniški črvi (computer worms)
- Trojanski konji (Trojan Horses)
- Vohunska programska oprema (spyware)
- Omrežje računalniških robotov (botnet)

Pridobivanje podatkov 1/3

- ETH Zurich
  - Zelo raznolik sistem (prenosniki, strežniki, …)
  - Sistem brez omejitev

- Snort
  - Analiza omrežnega prometa v realnem času
  - Sistem za zaznavanje in preprečevanje vdorov
  - Trije načini delovanja(sniffer, packet logger, NIDS)

Opozorila IDS

- Množici pravil (VRT, ET)
- 37 388 različnih signatur
- Nad dobljenimi opozorili uporabljen korelator
  - Grupiranje
  - Izločanje lažnih opozoril (false positive)
- Veliko podatkov - 37 milijonov opozoril
- 200 združenih dogodkov

Pridobivanje podatkov

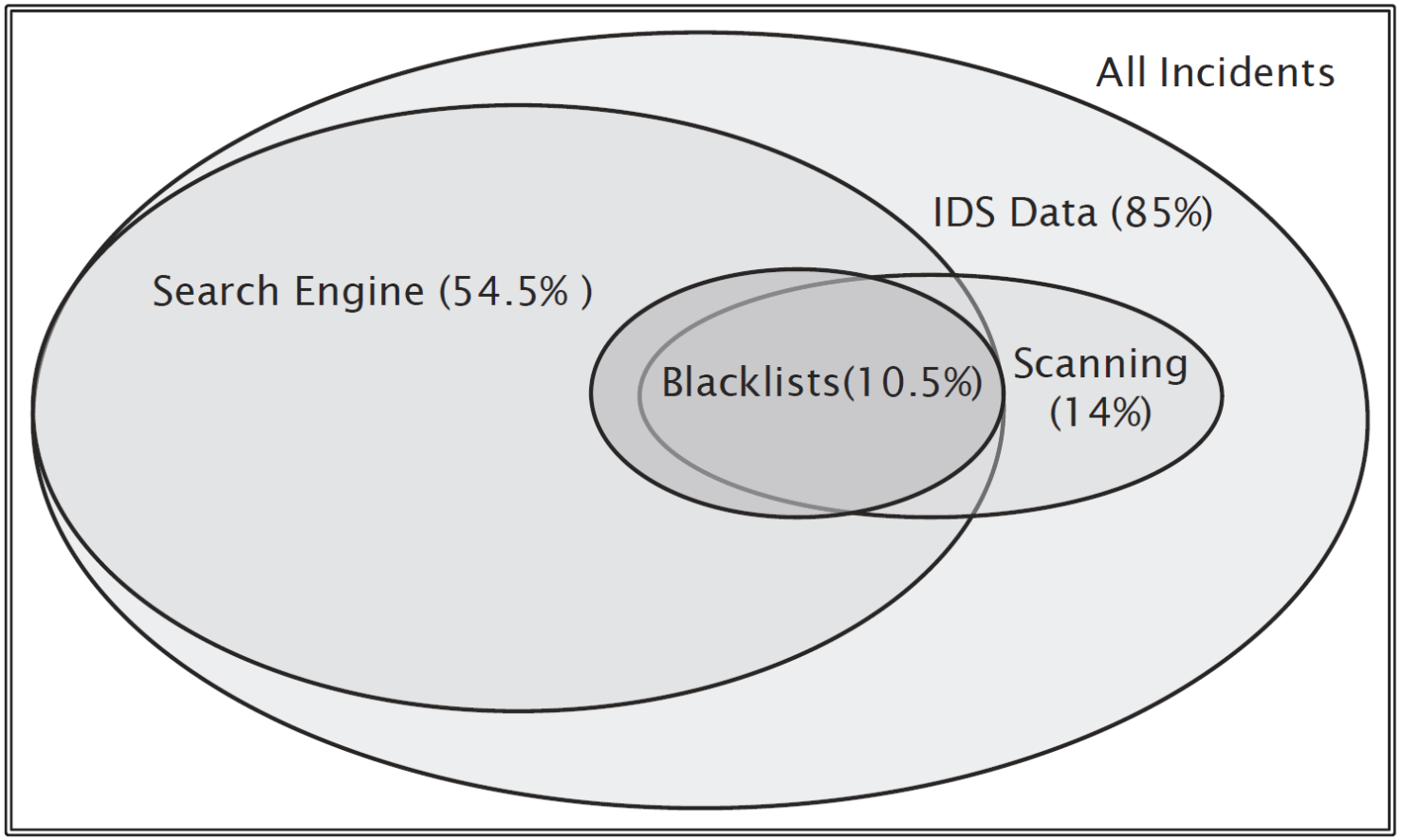
- Poročila ranljivosti in pregledovanja:
  - Zbiranje podatkov o gostiteljih v omrežju
  - Preiskovanje ranljivosti (Nessus, OpenVas)
  - Pregled omrežja (whois, nmap)
- Črne liste:
  - Iskanje povezav z zlonamernimi domenami
  - 5 črnih list
- Iskalnik Google:
  - Vhod: naslov IP in ime domene
  - Uporaba oznak na rezultatih iskanja
    - Malware, trojan, spam, bot, …

Okužba Torpig

- Prenosi Drive-by
- Namesti se s pomočjo JavaScripta
- Pridobivanje zaupnih informacij
- Odprte storitve HTTP, Skype in FTP
  - Skladno z delovanjem Torpiga
- Ključne besede: trojan, bot

Komplementarnost virov 1/2

- Opozorila Snort – najboljši vir informacij
- Iskalnik zagotavlja ključne vire za analizo



Komplementarnost virov 2/2

- 4 skupine zlonamerne programske opreme
- V 41% primerih potrebna dva vira
- V 14% primerih potrebni vsaj trije viri

Malware Type (#incidents)	Variant (#incidents)	IDS Logs	Search Engine	Blacklist Data	Active Scans
Trojans(85)	FakeAV(27)	✓	✓		
	Simbar(26)	✓	✓		
	Monkif(18)	✓	✓		
	Torpig(10)	✓	✓	✓	✓
	Nervos(4)	✓	✓		
Spyware(59)	AskSearch(50)	✓			
	MySearch(9)	✓			
Backdoors(18)	SdBot(5)	✓	✓	✓	✓
	ZBot(5)	✓	✓		✓
	Blackenergy(4)	✓	✓	✓	✓
	Parabola(2)	✓	✓		✓
	Ramsky(2)	✓			✓
Worms(8)	Koobface(6)	✓	✓		
	Conficker(2)	✓	✓		✓

Dejavnosti zlonamerne programske opreme

- Posodabljanje svoje strojne kode
- Pošiljanje zaupnih podatkov žrtve
- Prenos dodatnih zlonamernih programov
- Preusmerjanje uporabnika na zlonamerne spletne strani
- Nadaljnje širjenje

Primerjava različnih signatur Snort

- 170 incidentov
- Korelacija incidentov s signaturami Snort
- 138 dobrih signatur Snort
- 3.198 običajnih signatur Snort

Primerjava dobrih in običajnih signatur

- Preverjajo večje število bajtov podatkov (23.5 vs 11)
- Preverjajo večje število polj (2.8 vs 1.2)
- Pogosteje preverjajo zamik bajtov (28% vs 8%)
- Pogosteje uporabljajo regularne izraze (50% vs 15%)
- Pogosteje preverjajo vrata prejemnika (22% vs 17%)
- Pogosteje preverjajo velikost paketa (15% vs 7%)

- Podrobnejše preverjanje
  - boljši rezultati
  - počasnejše delovanje

Literatura

- E. Raftopoulos and X. Dimitropoulos, Understanding network forensics analysis in an operational environment, *Security and Privacy Workshops (SPW)*, pages 111 - 118, Maj 2013

- E. Raftopoulos and X. Dimitropoulos, Detecting, validating and characterizing computer infections in the wild, In *ACM SIGCOMM IMC*, Berlin, Germany, November 2011

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Nejc Sever, Anže Sodja, Nejc Saje

FROST: Forenzična orodja za oblačno platformo OpenStack

22. Maj 2014

Oblačno računalništvo

- računalniški viri dostopni na zahtevo
- viri so elastični
- uporabnik si “postreže” sam
- abstrakcija virov
- fokus na “Infrastructure as a Service”, infrastruktura kot storitev

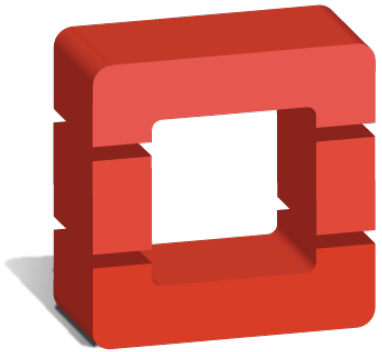
Oblak - forenzični izzivi

Lastnost oblaka	**Forenzični izziv**
neodvisnost od lokacije	lociranje dejanske strojne opreme, jurisdikcija
upravljanost s strani uporabnika in elastičnost	ohranitev dokazov, integriteta podatkov
replikacija podatkov	dokazna veriga, integriteta dokazov
veliko uporabnikov	zajem podatkov, dokazna veriga

Plasti zaupanja v IaaS

Plast	Plast oblaka	Metoda zajema	Potrebno zaupanje
6	Gostujoča aplikacija/podatki	odvisno od podatkov	omrežje, strojna oprema, gostiteljski OS, hipervizor, gostujoči OS
5	Gostujoči OS	forenzična orodja za oddaljeni zajem	omrežje, strojna oprema, gostiteljski OS, hipervizor, gostujoči OS
4	Virtualizacija	introspekcija	omrežje, strojna oprema, gostiteljski OS, hipervizor
3	Gostiteljski OS	dostop do navideznega diska	omrežje, strojna oprema, gostiteljski OS
2	Strojna oprema	dostop do fizičnega diska	omrežje, strojna oprema
1	Omrežje	prestrezanje paketov	omrežje

OpenStack



openstack™
CLOUD SOFTWARE

- odprtokoden projekt
- platforma za oblačno računalništvo
  - Nova: upravitelj navideznih strojev
  - Swift: hramba objektov
  - Glance: hramba diskovnih slik
  - Keystone: identiteta in avtorizacija
  - Horizon: spletni vmesnik
  - Neutron: omrežne storitve za navidezne stroje

FROST funkcionalnosti

1. **pridobitev slik navideznih diskov**

   (in preverjanje integritete)

2. **pridobitev dnevniških zapisov API zahtevkov**

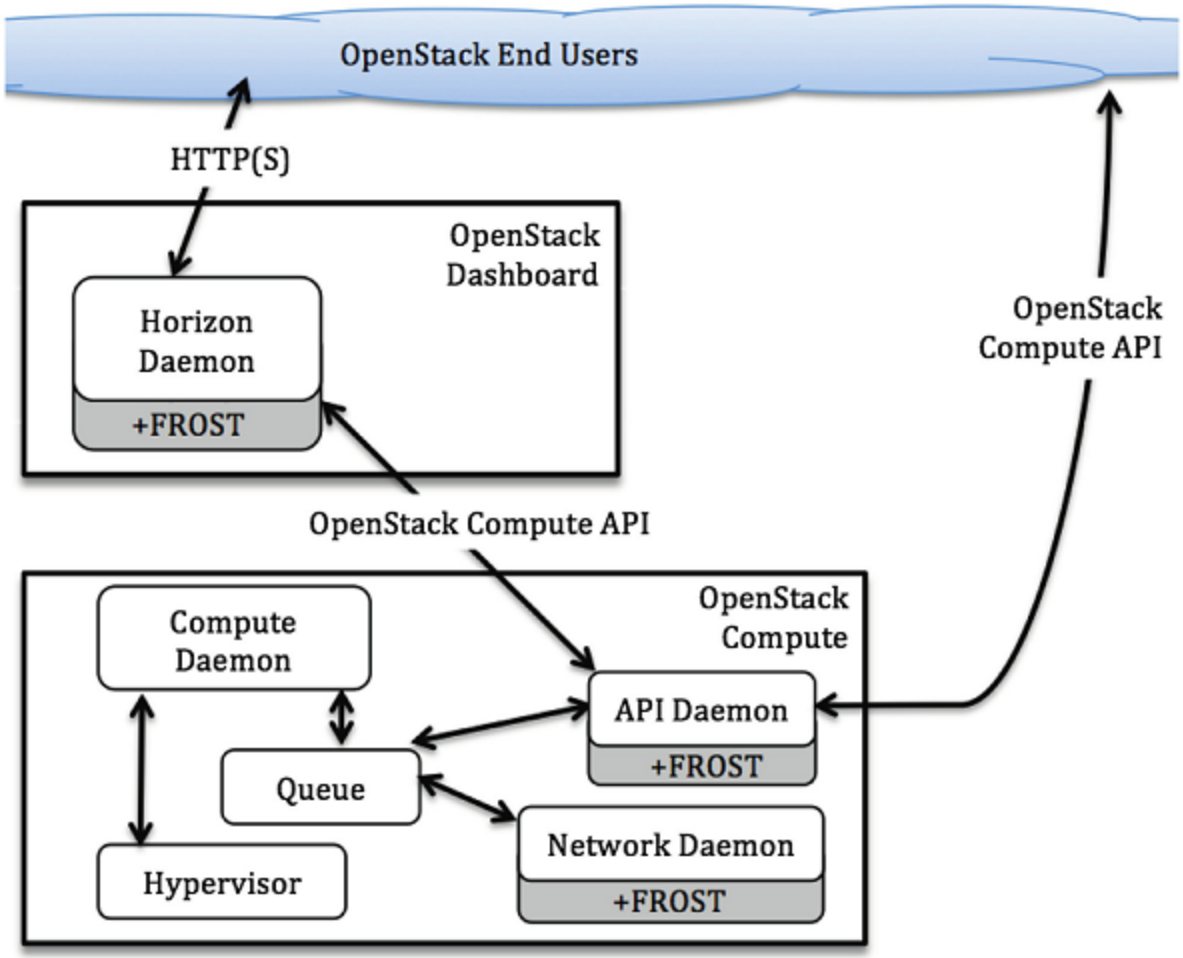
   (in preverjanje integritete)

3. **pridobitev dnevniških zapisov požarnega zidu**

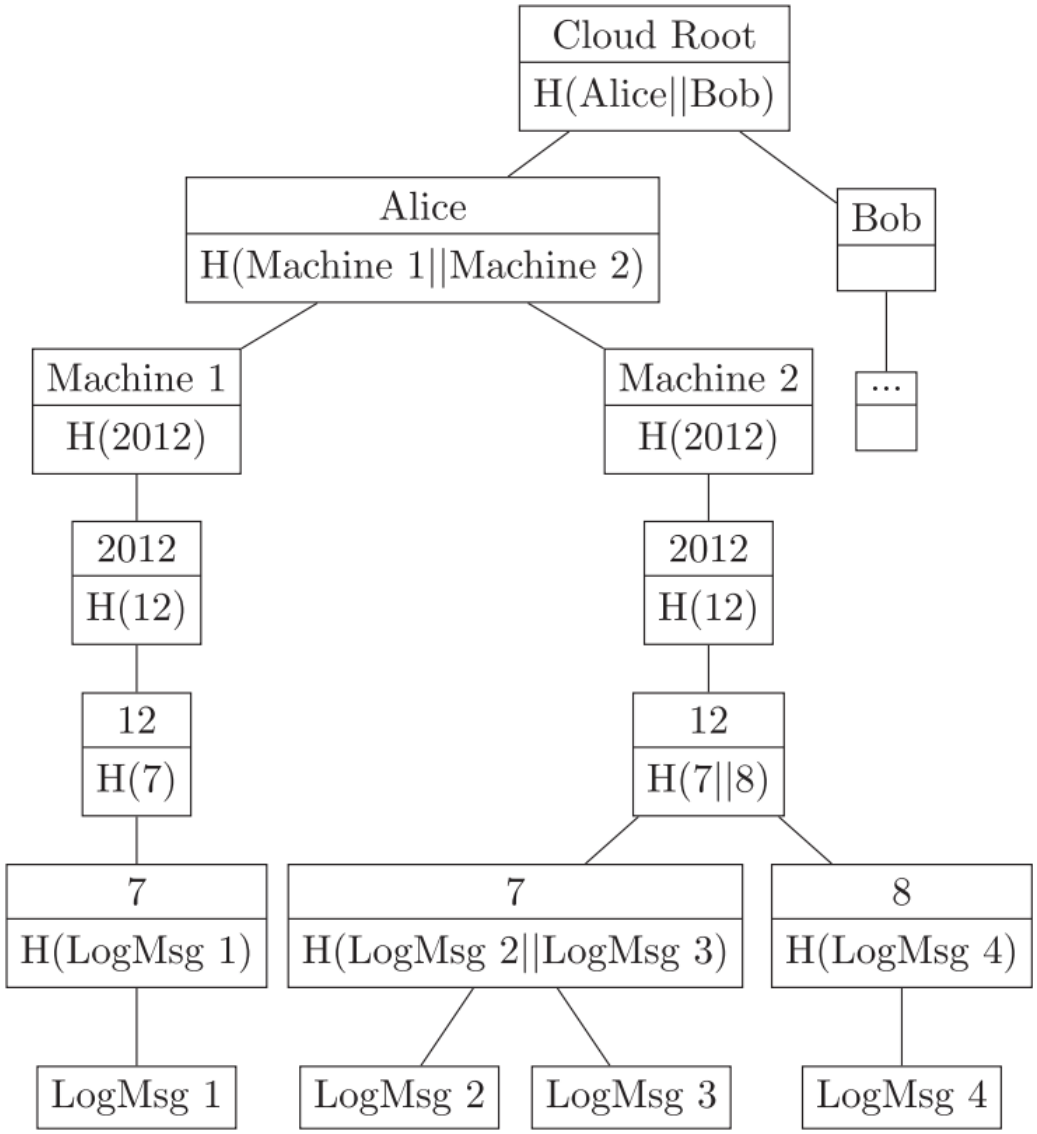
   (in preverjanje integritete)

Na voljo preko spletnega vmesnika in API-ja.

FROST implementacija



Zgoščevalna drevesa



Uporaba

- Dnevniški zapisi API zahtevkov

```
$ nova get-nova-logs 0afcfbcd-b836-4593-a02c-25d8d3a94b00 verify.xml
[truncated]
2012-12-01 13:30:49 INFO nova.api.openstack.wsgi [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo]
    POST http://10.34.50.142:8774/v2/5ee3040fa890428387f56111576cf819/servers
2012-12-01 13:30:49 DEBUG nova.quota [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] Created
    reservations ['915e9c89-b3bc-4091-8b75-3b555961ec3e', '72c39d24-0a96-42ca-96f1-593da3aa9f81',
    '57843316-872b-4b40-a853-2aa7c730262e'] from (pid=16036) reserve /opt/stack/nova/nova/quota.py:697
2012-12-01 13:30:50 DEBUG nova.compute.api [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] Going to
     run 1 instances... from (pid=16036) _create_instance /opt/stack/nova/nova/compute/api.py:492
[truncated]
```

- Dnevniški zapisi požarnega zidu

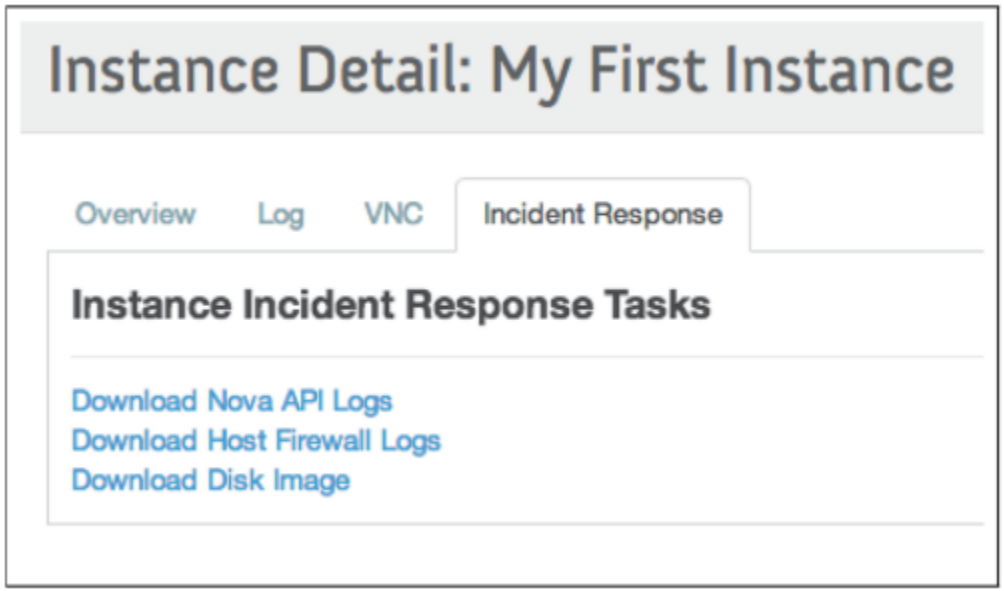
```
$ nova get-firewall-logs 0a18799f-c198-4dbb-b369-b49184e3dfbc verify.xml
0a18799f-c198-4dbb-b369-b49184e3dfbc: Nov 28 11:13:38 domU-12-31-39-17-29-5D kernel: [  310.765760]
    IPTables-Dropped: IN=eth0 OUT= MAC=12:31:39:17:29:5d:fe:ff:ff:ff:ff:ff:08:00 SRC=130.85.36.72 DST
    =10.97.42.171 LEN=52 TOS=0x00 PREC=0x00 TTL=48 ID=29222 DF PROTO=TCP SPT=55739 DPT=443 WINDOW=1002
    RES=0x00 ACK URGP=0
0a18799f-c198-4dbb-b369-b49184e3dfbc: Nov 28 11:13:36 domU-12-31-39-17-29-5D kernel: [  309.623023]
    IPTables-Dropped: IN=eth0 OUT= MAC=12:31:39:17:29:5d:fe:ff:ff:ff:ff:ff:08:00 SRC=172.16.0.23 DST
    =10.97.42.171 LEN=103 TOS=0x00 PREC=0x00 TTL=64 ID=42188 PROTO=UDP SPT=33905 DPT=53 LEN=83
[truncated]
```

Uporaba

- Pridobitev slike diska

```
$ nova get-disk myvol-e9a5612d report.xml
MD5:  b17ee04095b2a3d81eed98628072eab6
SHA1: 399f5ffaccd09fe43d642d5f0d996875ca650c9f

$ sha1sum myvol-e9a5612d
399f5ffaccd09fe43d642d5f0d996875ca650c9f myvol-e9a5612d
```

- Spletni vmesnik



Povzetek

- oblačno računalništvo - izziv za digitalno forenziko
- FROST
  - zaupanja vredni dokazi
  - neodvisno od ponudnika oblačnih storitev
  - v rokah uporabnikov, organov pregona ter forenzikov - ne ponudnika
  - še vedno moramo zaupati ponudniku oblačnih storitev

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Peter Miklavčič

Forenzika v brezžičnih lokalnih omrežjih

Maj 2014

Varnostni mehanizmi

Šibki

- Skrivanje SSID
- Filtriranje MAC naslovov
- WEP
- Captive portali
- WPS
- WPA

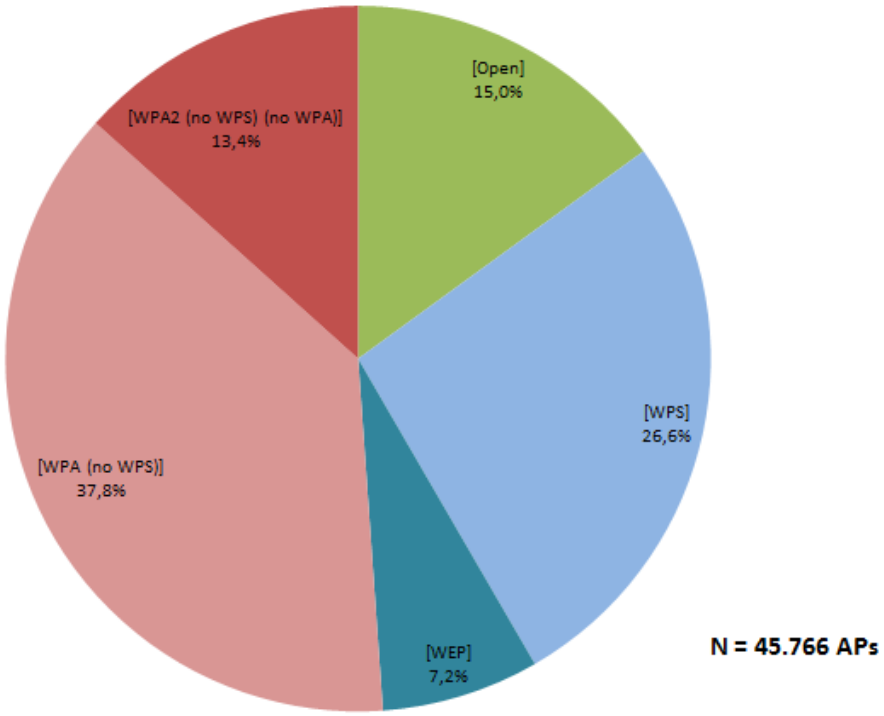
Močnejši, a ne nujno

- WPA2; a z dobrim geslom
- EAP; certifikat je sicer odlično geslo, a ne koristi če je slaba implementacija (eduroam)

Primer slabega gesla:
`1nc0n5p1cu0u5Pass`

Primer dobrega gesla:
`7vwmzdsxgnqfjnsn3`

Zakaj forenzika brezžičnih omrežij?



Vir: Laboratorij za telekomunikacije Fakultete za elektrotehniko

Z drugimi besedami: ~¾ omrežij je *crackable*!

Tipičen ''router''

- Med drugim res da vsebuje router, tipično pa ima integriran še switch, access point, firewall, server (DNS, DHCP, HTTP, SMB...), lahko tudi modem...
- Linux
- Do 1 GHz CPU
- Do 128 MB RAM
- Do 64 MB flash za firmware (*mount -o ro /*)
- Do nekaj kB NVRAM za nastavitve (*ne nujno*)

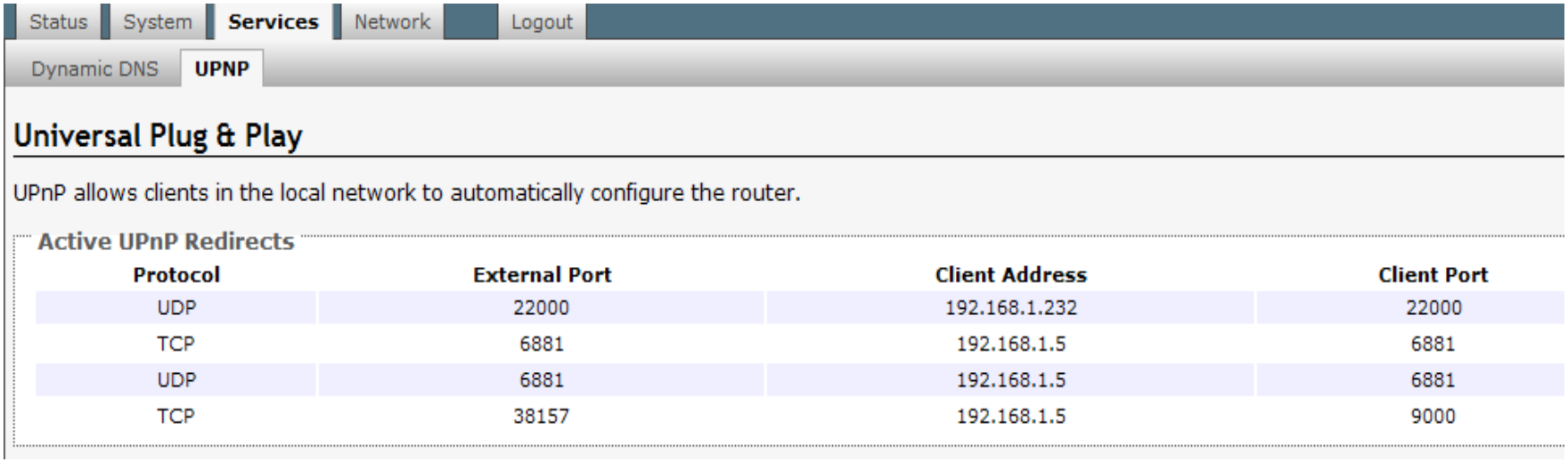
...v bistvu je računalnik!

Forenzična vrednost routerja

- Uptime
- Syslog
- Firewall
- DHCP

```
May  4 06:01:21 OpenWrt daemon.info hostapd: wlan0: STA cc:          :4a WPA: group key handshake completed (RSN)
May  4 06:06:52 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: authenticated
May  4 06:06:52 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: associated (aid 2)
May  4 06:06:53 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: pairwise key handshake completed (RSN)
May  4 06:11:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 06:11:29 OpenWrt daemon.info hostapd: wlan0: STA cc:          :4a IEEE 802.11: deauthenticated due to local deauth request
May  4 06:21:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 06:31:29 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: deauthenticated due to local deauth request
May  4 06:31:52 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: authenticated
May  4 06:31:52 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: associated (aid 1)
May  4 06:31:53 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: pairwise key handshake completed (RSN)
May  4 06:41:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 06:51:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 07:01:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 07:11:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 07:21:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 07:31:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 07:41:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 07:51:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 08:01:29 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: deauthenticated due to local deauth request
May  4 08:03:52 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: authenticated
May  4 08:03:52 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: associated (aid 1)
May  4 08:03:53 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: pairwise key handshake completed (RSN)
May  4 08:11:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 08:17:52 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: authenticated
May  4 08:17:52 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 IEEE 802.11: associated (aid 1)
May  4 08:17:52 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: pairwise key handshake completed (RSN)
May  4 08:21:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 08:31:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 08:41:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 08:51:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 09:01:21 OpenWrt daemon.info hostapd: wlan0: STA 00:          :b5 WPA: group key handshake completed (RSN)
May  4 09:03:02 OpenWrt daemon.info hostapd: wlan0: STA cc:          :4a IEEE 802.11: authenticated
May  4 09:03:02 OpenWrt daemon.info hostapd: wlan0: STA cc:          :4a IEEE 802.11: associated (aid 2)
```

Forenzična vrednost routerja



- UPnP tabela
- DNS cache
- PPPoE gesla

Skeniranje omrežij na napravah

- Pri **pasivnem** skeniranju omrežij AP oddaja becon frame ~10x na sekundo z SSID ali brez, naprave jih pa zaznajo.

- Pri **aktivnem** skeniranju omrežij naprave oddajajo probe request z SSID, pravi AP pa se oglasi z probe response. Če se SSID ne oddaja, je to edini način da se najdeta.

Problem sondiranja

Which frames are Not protected [edit]

Infeasible/Not possible to protect the frame which are sent before 4-ways handshake because it is sent prior to key establishment **Infeasible to protect**

- Beacon and Probe Request/Response
- Announcement traffic indication message (ATIM)
- Authentication request/response
- Association request/response
- Spectrum Management Action

– Any Management frame that is sent before key establishment is infeasible to be protected

– The Management Frames, which are sent after key establishment, can be protected

Vir: http://en.wikipedia.org/wiki/IEEE_802.11w-2009

Problem te veje forenzike

Wireless Local Area Networks

WLANs are standardized under the IEEE 802.11 series.

Common encryption technologies used by these networks are: WEP, WPA/WPA2-PSK, some networks have no encryption at all.

In order to decrypt intercepted secured WLAN traffic you should crack the encryption key. Note, that the only option for cracking WPA/WPA2-PSK keys is to do a brute-force password guessing attack. There are several WPA-PSK rainbow tables available.

Many commercial network forensics systems can intercept and decrypt WLAN traffic, for example:

- Mera Systems NetBeholder Mobile
- E-Detective Wireless Detective System

As well as some open-source tools:

- aircrack-ng

WPA/WPA2-PSK cracking-only solutions with GPU acceleration (15-100 times faster than in CPU-only mode):

- ElcomSoft Distributed Password Recovery
- Pyrit

Vir: http://www.forensicswiki.org/wiki/Wireless_forensics