Forenzika radne memorije

Viktor Kvaternjak

Predrag Pale

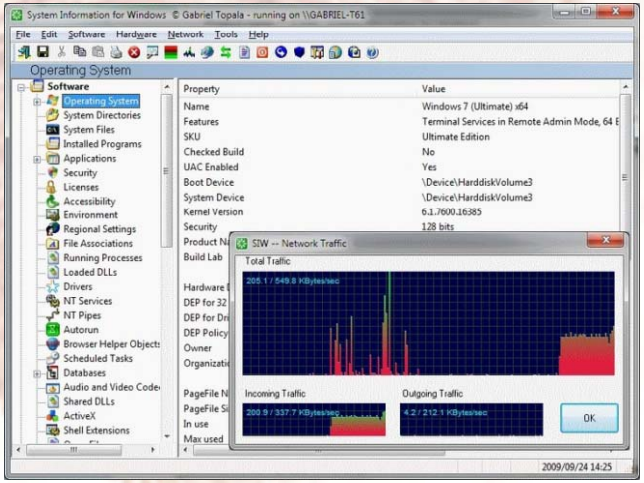
RAM

- Random Access Memory
  - **radna** memorija
    - tamo gdje se programi **izvršavjau**

- tamo gdje se **programi izvršavaju**
  - za razliku od **trajne** memorije (disk, USB memorija, ROM …)
    - gdje su programi (i ostali podaci) **pohranjeni**

Zašto trebamo forenziku radne memorije?

- **Svaka aktivnost** na računalu
  - **modificira** stanje dijela **RAM-a**
- RAM sadržavaj neke informacije koje se **ne nalaze igdje drugdje**
  - kouminkacijske **poruke**
  - **lozinke**, PIN-ovi, …
  - privremeni **tekst**, **brojevi**, …
- informacija **može ostati** u RAM-u **dugo vremena**
- **obilje** informacija o **stanju** računalnog **sustava**
  - **procesi**
  - **podaci**
    - korisnički podaci, lozinke, …
  - **veze**
  - Informacije o **sustavu**
    - opterećenje, prioriteti, …
  - **tehničke** informacije
    - brojači, pokazivači, registri, ….

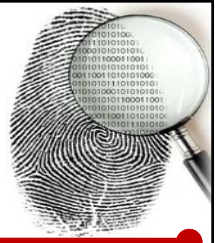


RAM analiza

- **velika količina** binarnih podataka
  - naizgled bez strukture

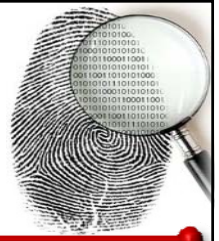
- potrebni su nam **alati za analizu**
  1. **pretraživanje** teksta ili niza bajtova
     - grep, regex, HxD, …
  2. **napredini alati**
     - koji **razumiju strukturu** u memoriji

Informacije u RAM-u



- Procesi
- Jezgra
- Mreža
- Grafičko sučelje
- Windows specifičnosti
  - activity/event log
  - registry
  - datotečni sustav
- Linux specifičnosti
  - bash povijest
  - dmesg
  - kernel spremnici

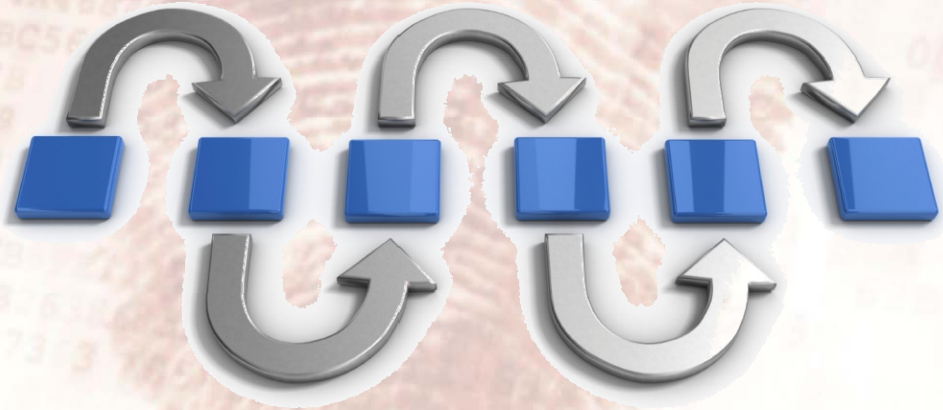
Procesi



- popis svih procesa
- vrijeme početka
  - i kraja, ponekad
- sigurnosni kontekst
  - korisnici, privilegije
- handle-ovi
  - otvorene datoteke
  - veze
- ostali podaci – sadržaj
  - procesirani tekst
  - poruke: mail, chat, …
  - lozinke, PIN-ovi, ..
  - strukture podataka
- upozorenje: neki malware može otežati analizu

Što je proces?

- program u izvršavanju
- njegovi podaci
- kontrolne strukture koje ga podržavaju



Popis procesa u Windowsima

Windows Task Manager

File Options View Help

Applications | Processes | Services | Performance | Networking | Users

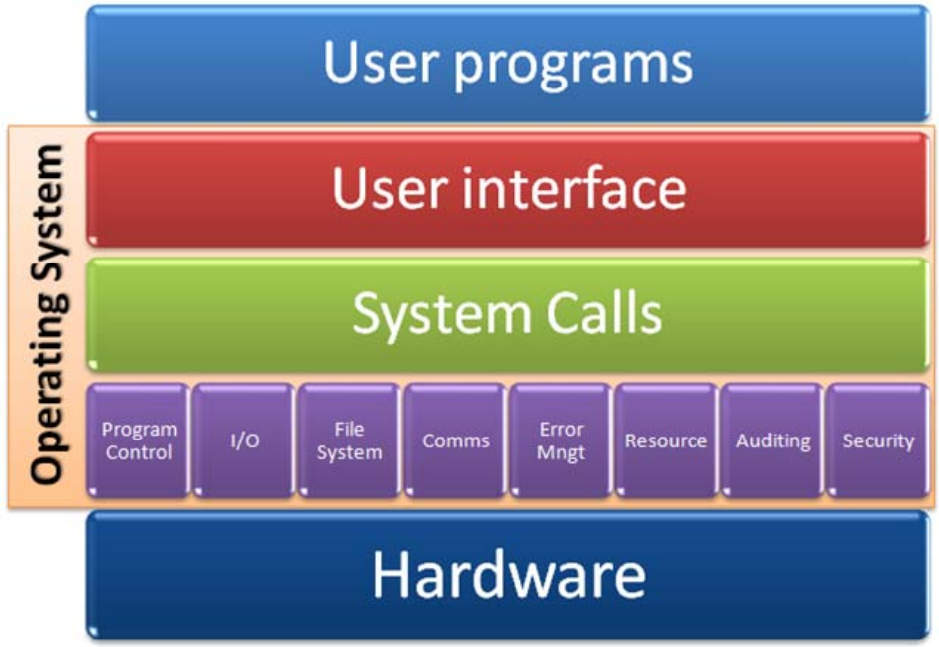
Image Name	User Name	CPU	Memory (Private Wor...	Description
System Idle Process	SYSTEM	96	24 K	Percentage of time the processor is idle
WmiPrvSE.exe	NETWO...	02	7.972 K	WMI Provider Host
taskmgr.exe	ppale	01	4.368 K	Windows Task Manager
OUTLOOK.EXE *32	ppale	01	139.480 K	Microsoft Office Outlook
dopus.exe	ppale	00	36.440 K	Directory Opus 10
Plugin.exe *32	SYSTEM	00	1.960 K	Plugin.exe
Skype.exe *32	ppale	00	139.176 K	Skype
Plugin.exe *32	SYSTEM	00	1.988 K	Plugin.exe
splwow64.exe	ppale	00	4.200 K	Print driver host for 32bit applications
Plugin.exe *32	ppale	00	2.756 K	Plugin.exe
audiodg.exe	LOCAL ...	00	15.636 K	Windows Audio Device Graph Isolation
Plugin.exe *32	ppale	00	1.748 K	Plugin.exe
acCOMpkcs.exe	ppale	00	6.800 K	ActivIdentity PKCS#11 2.11 API - 64 bits CO...
plugincontainer.exe *32	SYSTEM	00	5.076 K	plugincontainer.exe
POWERPNT.EXE *32	ppale	00	50.112 K	Microsoft Office PowerPoint
InputPersonalization.exe	ppale	00	4.624 K	Input Personalization Server
updater.exe *32	SYSTEM	00	1.996 K	updater.exe
GWX.exe	ppale	00	328 K	GWX
svchost.exe	SYSTEM	00	1.040 K	Host Process for Windows Services
unsecapp.exe	ppale	00	2.244 K	Sink to receive asynchronous callbacks for W...
CCC.exe	ppale	00	2.696 K	Catalyst Control Center: Host application
SDTray.exe *32	ppale	00	8.412 K	Spybot - Search & Destroy tray access
avastui.exe *32	ppale	00	14.256 K	avast! Antivirus
Dropbox.exe *32	ppale	00	91.020 K	Dropbox
IAStorIcon.exe *32	ppale	00	9.096 K	IAStorIcon
acsagent.exe	ppale	00	6.636 K	ActivClient Agent

Popis procesa u Linuxu

```
server:/home/ppale# ps -ale
F S   UID   PID  PPID  C PRI  NI ADDR SZ WCHAN  TTY          TIME CMD
4 S     0     1     0  0  80   0 -   519 -      ?        00:00:10 init
1 S     0     2     0  0  80   0 -     0 -      ?        00:00:00 kthreadd
1 S     0     3     2  0 -40   - -     0 -      ?        00:00:00 migration/0
1 S     0     4     2  0  80   0 -     0 -      ?        00:00:17 ksoftirqd/0
5 S     0     5     2  0 -40   - -     0 -      ?        00:00:00 watchdog/0
1 S     0     6     2  0  80   0 -     0 -      ?        00:00:04 events/0
1 S     0     7     2  0  80   0 -     0 -      ?        00:00:00 cpuset
1 S     0     8     2  0  80   0 -     0 -      ?        00:00:00 khelper
1 S     0     9     2  0  80   0 -     0 -      ?        00:00:00 netns
1 S     0    10     2  0  80   0 -     0 -      ?        00:00:00 async/mgr
1 S     0    11     2  0  80   0 -     0 -      ?        00:00:00 pm
1 S     0    12     2  0  80   0 -     0 -      ?        00:00:00 sync_supers
1 S     0    13     2  0  80   0 -     0 -      ?        00:00:00 bdi-default
1 S     0    14     2  0  80   0 -     0 -      ?        00:00:00 kintegrityd/0
1 S     0    15     2  0  80   0 -     0 -      ?        00:00:05 kblockd/0
1 S     0    16     2  0  80   0 -     0 -      ?        00:00:00 kacpid
1 S     0    17     2  0  80   0 -     0 -      ?        00:00:00 kacpi_notify
1 S     0    18     2  0  80   0 -     0 -      ?        00:00:00 kacpi_hotplug
5 S     0    19     2  0  80   0 -     0 -      ?        00:00:00 kseriod
1 S     0    21     2  0  80   0 -     0 -      ?        00:00:00 kondemand/0
1 S     0    22     2  0  80   0 -     0 -      ?        00:00:00 khungtaskd
1 S     0    23     2  0  80   0 -     0 -      ?        00:02:47 kswapd0
1 S     0    24     2  0  85   5 -     0 -      ?        00:00:00 ksmd
```

Jezgra

- učitani **moduli**
  - upravljački programi za uređaje
  - upravljački programi za datotečne sust
  - mrežni upravljački programi
  - posebni sustavski pozivi
  - *executable interpreter*
- sve **strukture** i njihovi opisivači
  - vezana lista (aktivnih) procesa
  - mrežne veze
  - *cached* ulaz/izlaz
  - brojila
- ponekada i **stari procesi**
  - koji nisu više prisutni u RAM-u
- važno kada tražimo "rootkit-ove"
  - iako, **rootkit ima pristup** svim strukturama jezgre
  - i često **ih mijenja**
  - **da sakrije** sebe i bitne informacije



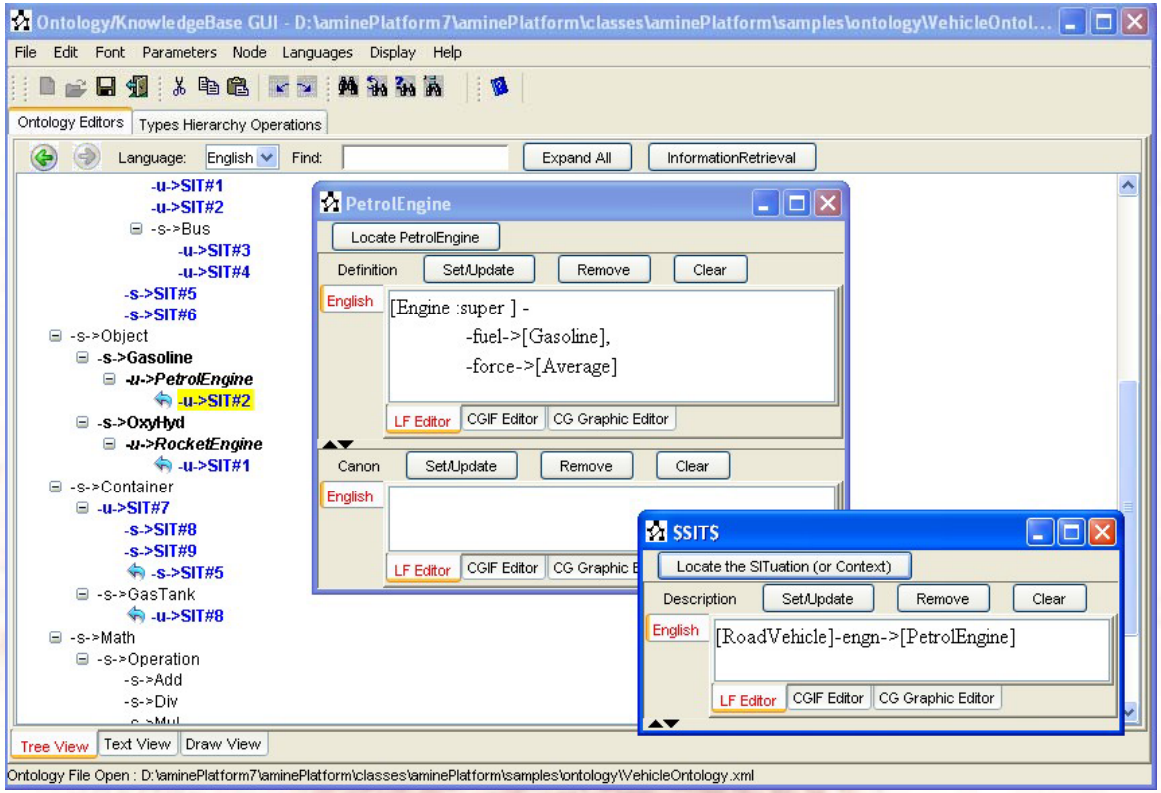
Mreža

- IP adresa i port
  - izvora i odredišta
- vrijeme stvaranja veze
  - i zatvaranja, ponekad
- popis nedavnih DNS zahtjeva
  - otkrivanje prethodnih veza, trenutno neaktivnih
- povijest web preglednika

- tako možemo otkriti prisluškivanje komunikacije

Grafičko sučelje (GUI)

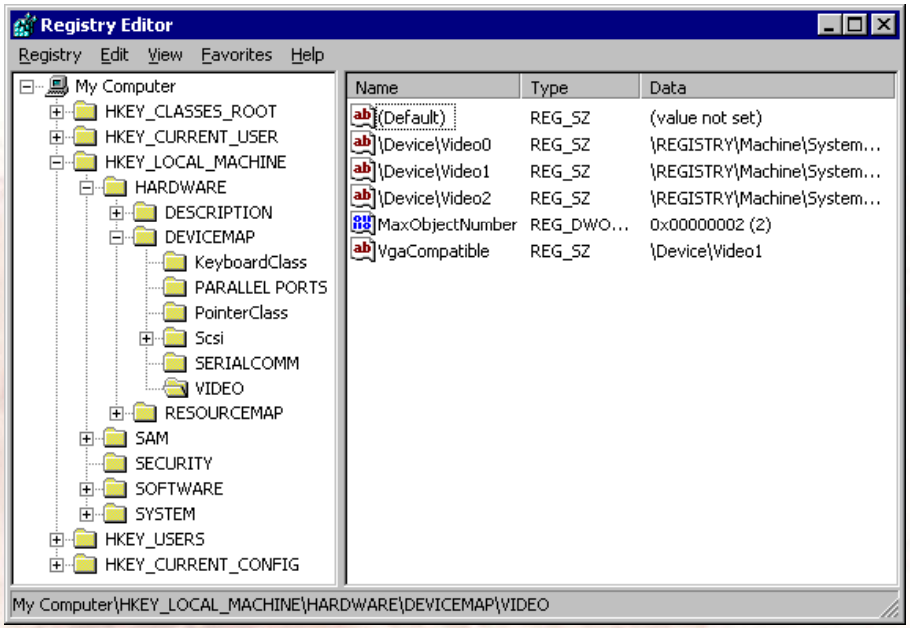
- pregled prozora i statusa komponenata
- *clipboard*



- ***malware*** često **napada** GUI:
  - zapisivanjem pritisnutih tipki *(key logging)*
  - ubacivanjem oglasa

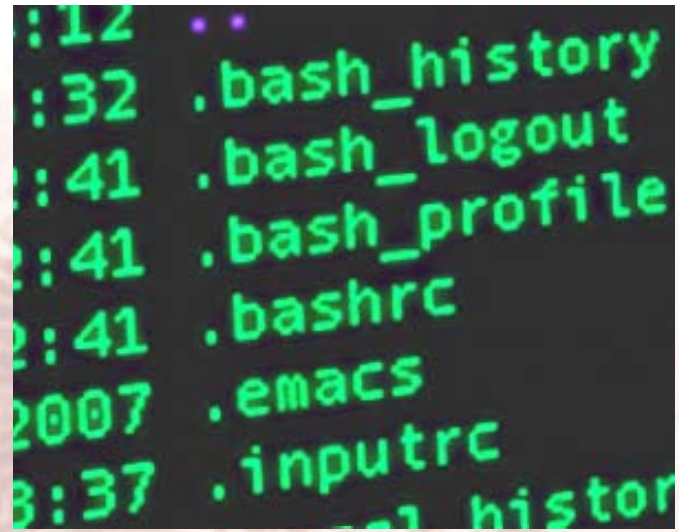
Windows specifičnosti

- dnevnik događaja (*event log*)
  - **problemi** aplikacija
  - **instalacija** programa
- *registry*
  - nedavno korišteni
    - programi i datoteke
  - informacije koje nisu na disku
    - HKLM\Hardware
      - stvoren pri dizanju sustava
      - identificira sav *hardware*
      - prije učitavanja upravljačkih programa
      - ove informacije su presudne za ispravan rad sustava
- datotečni sustav
  - npr. MFT od NTFS-a
    - metapodaci datoteka i čak cijele male datoteke su u RAM-u
    - pomaže pri analizi šifriranih diskova



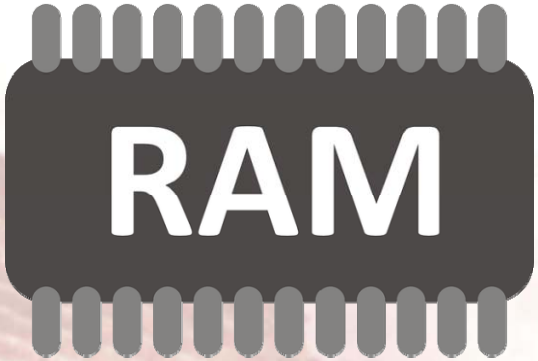
Linux specifičnosti

- Bash povijest
  - spremljena na disku
    - može se isključiti
  - ali ostaje u RAM-u
- dmesg
  - upravljački programi šalju poruke
    - koje se pohranjuju u **spremniku u jezgri**
  - kasnije su spremljeni u dnevniku na disku
- mrežni spremnik
  - pristup aktivnim porukama



Kako se RAM analizira

- **slika** RAM-a se prvo **izolira**
  - u datoteku



1. **jednostavna pretraga** za poznatim sadržajem
   - grep, regex
2. **napredni alati** koji razumiju strukture jezgre
   - **Volatility** framework
     - http://www.volatilityfoundation.org
   - **WinDbg**
     - službeni, besplatni, Microsoftov alat za debugiranje
     - https://msdn.microsoft.com/en-us/windows/hardware/hh852365.aspx
   - **Mandian Redline**
     - https://www.fireeye.com/services/freeware/redline.html

Volatility framework

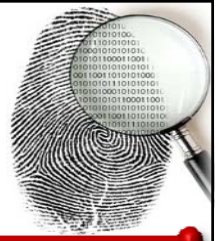
http://www.volatilityfoundation.org

- besplatan, open source
- podržava: Windows, Mac OS X, LInux
- isključivo sučelje komandne linije (CLI)
  - no drugi autori su razvili GUI-je
- podržava razne formate slika RAM-a
  - od čistih do hibernacijske datoteke
- mnoštvo modula:

clipboard	mftparser
cmdline	netscan
devicetree	pslist
consoles	screenshot
dlllist	svcscan
evtlogs	truecryptmaster
hashdump	vadtree
iehistory	yarascan

- Rekall
  - projekt nastao od Volatility-ja
  - cilja poboljšati performanse i modularnost

Volatility moduli



- **clipboard** – prikazuje sadržaj **clipboard-a**
- **cmdline** – prikazuje **argumente** poslane **procesu** pri pokretanju
- **devicetree** – lista **spojenih uređaja**
- **consoles** – **povijest naredba** konzole
- **dlllist** – lista **učitanih DLL-ova**
- **evtlogs** – prikazuje **event log** (XP/2003)
- **hashdump** – lista **hasheva lozinki**
- **iehistory** – **povijest** IE web **preglednika** (Internet Explorer)
- **mftparser** - pristup **MFT-u** od NTFS-a
- **netscan** – prikazuje **veze** i priključke
- **pslist** – lista **procesa** (koristeći listu EPROCESS objekata)
- **screenshot** – rekonstruira izgled **desktop-a**
- **svcscan** – lista **servisa**
- **truecryptmaster** – pokuša dohvatiti **ključ** spremnika šifriranih TrueCrypt-om
- **vadtree** – prikazuje **memorijske alokacije**
- **yarascan** – **pretražuje** memoriju za **nizove** opsiane Yara pravilima

WinDbg

- https://msdn.microsoft.com/en-us/windows/hardware/hh852365.aspx

- službeni, besplatni, Microsoftov alat za debugiranje

- korišten za
  - debugiranje programa, upravljačkih programa i operacijskog sustava
  - analiza *crash dump* slika

- najprikladniji za analizu Windows struktura
  - jer ga podržava Microsoft

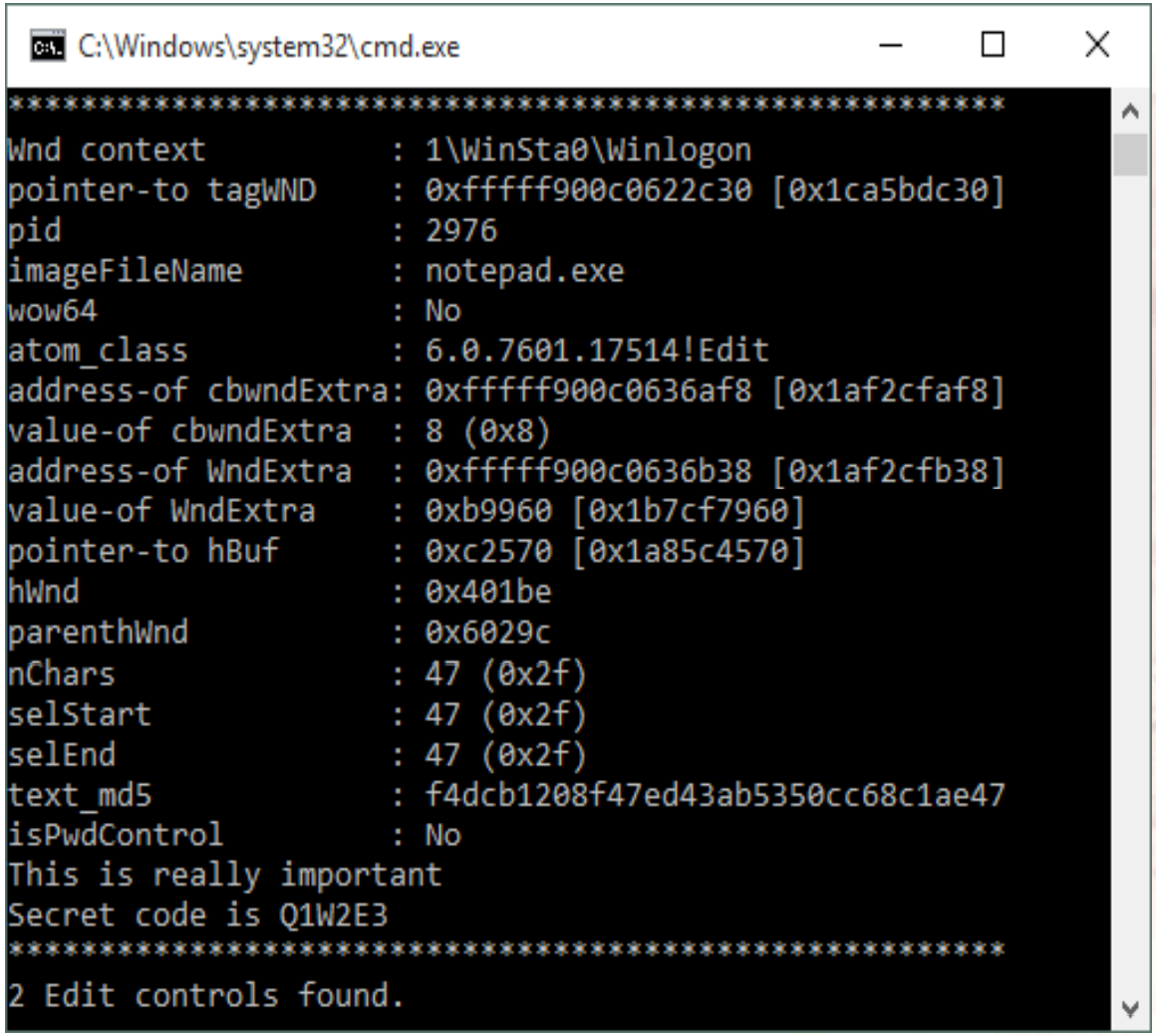
Mandian Redline

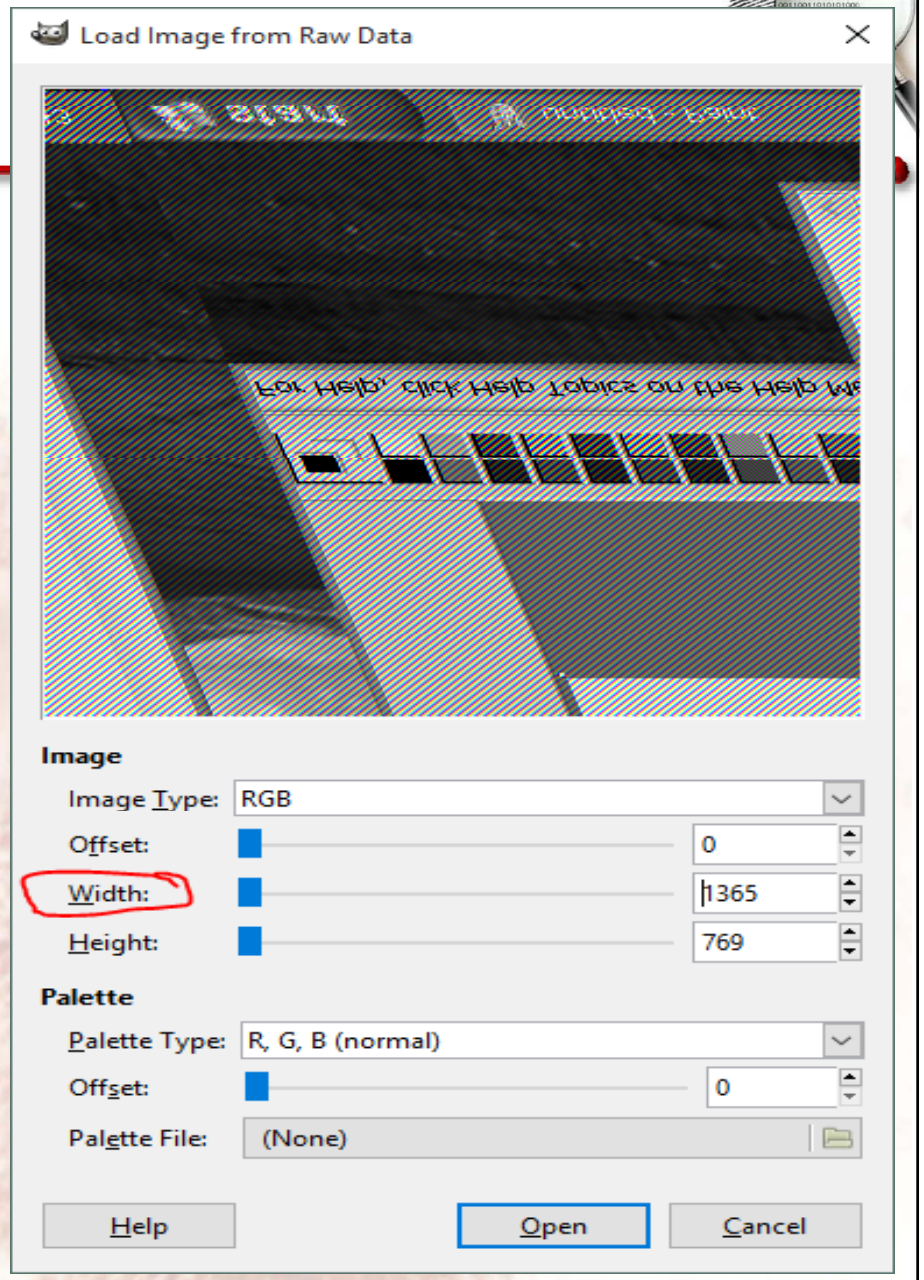
- https://www.fireeye.com/services/freeware/redline.html

- besplatni, profesionalni alat
- podržava: Windows XP do 8
- GUI dizajniran za stvaranje forenzičkih izvještaja
- analiza:
  - svih pokrenutnih procesa
  - upravljačkih programa
  - datotečnog sustava
  - dnevnika događaja
  - veza
  - registry-a
  - web povijesti
- posebna se pažnja posvećuje
  - kornološkom toku
  - i filtriranju
- da pomogne u pronalaženju
  - trenutka infekcije
  - inficiranih datoteka

Alati

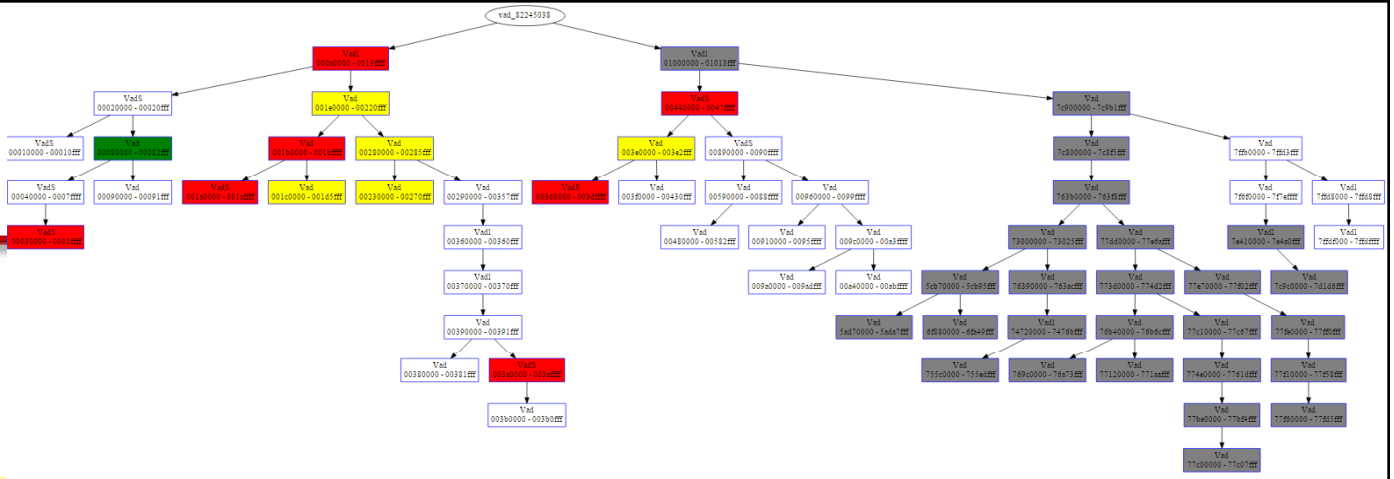
Volatility s “editbox” plug-inom detektira/izvlači tekst iz procesa “notepad.exe”



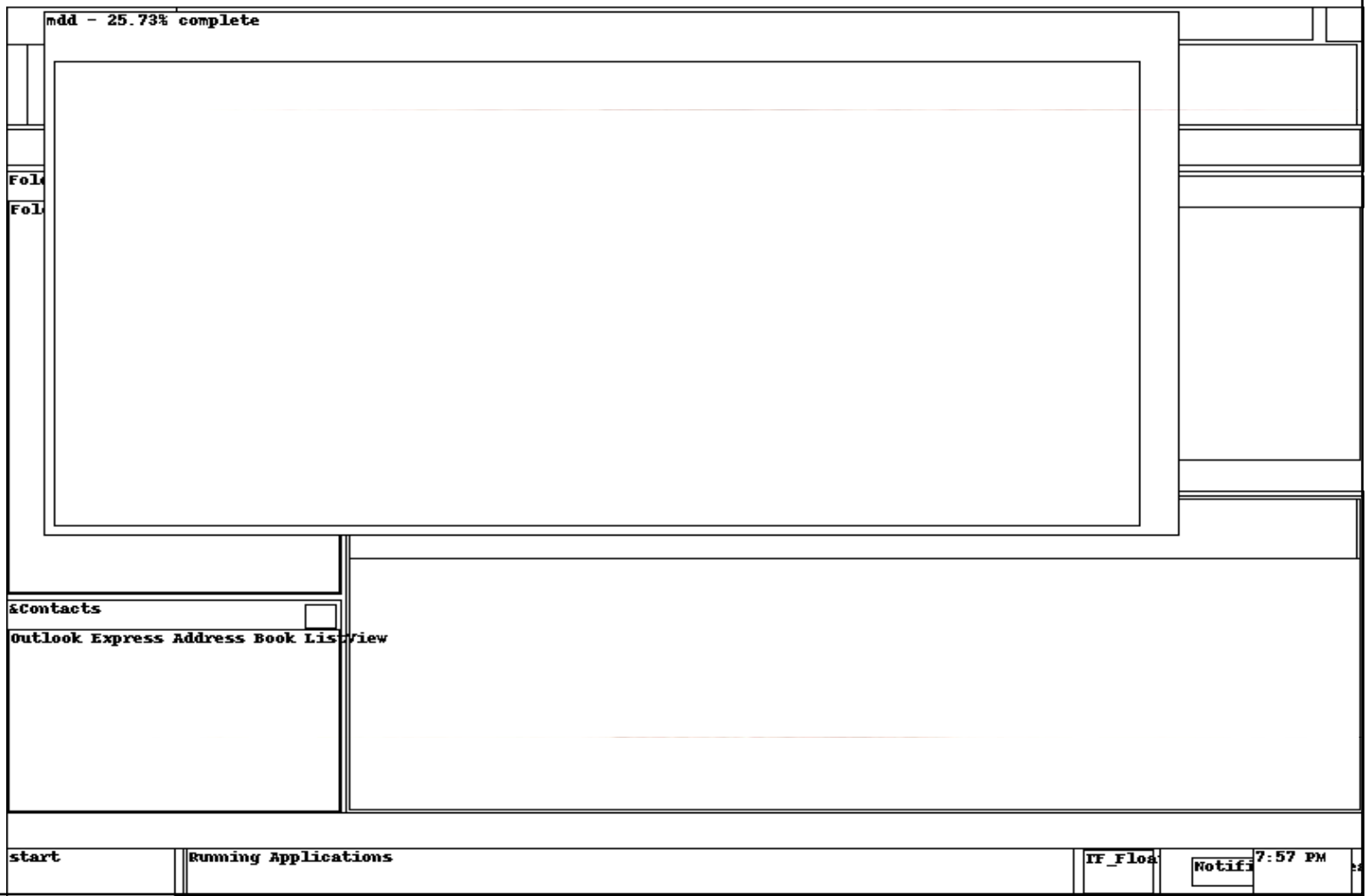


Volatility s “vaddump” plug-inom izvlači slike iz procesa “paint.exe”

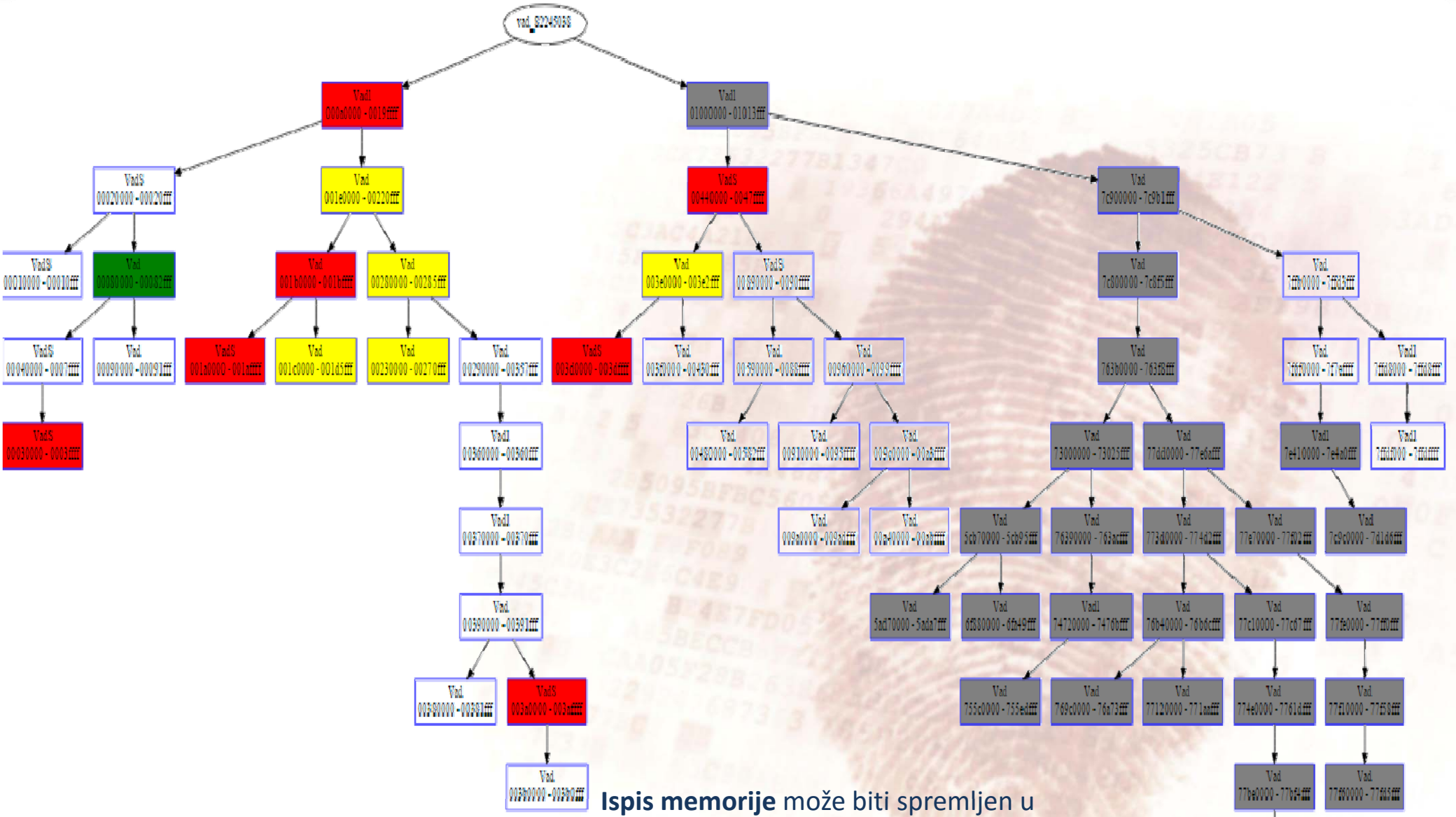
Rezultati



verysecurepassword



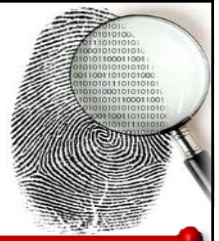
Primjer organizacije memorije jednog procesa



Ispis memorije može biti spremljen u

- **jednoj** kontinuiranoj **datoteci**
- ili **razdvojen u datoteke** (prikazano)

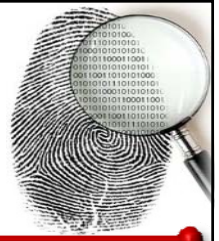
Kako snimiti sliku (stanje) memorije



1. Virtualni stroj
   - ugrađeni alati
     - za pauziranje i debugiranje
2. Kopiranje uz pomoć software-a
   - alati slučni upravljačkim programima kopiraju sadržaj
     - zahtjeva eskalaciju privilegija – superuser/admin
3. Pomoću hardware-a
   - sabirnica sa DMA pristupom
     - FireWire – samo prvih 4 GB
     - PCI express – hot plug potreban
     - Cold Boot – DDR2 OK, no DDR3 & DDR4 ?

- Upozorenje: snimanje slike memorije može srušiti sustav
  - nestabilan upravljački program i sl. …

Komplementarni izvori na disku



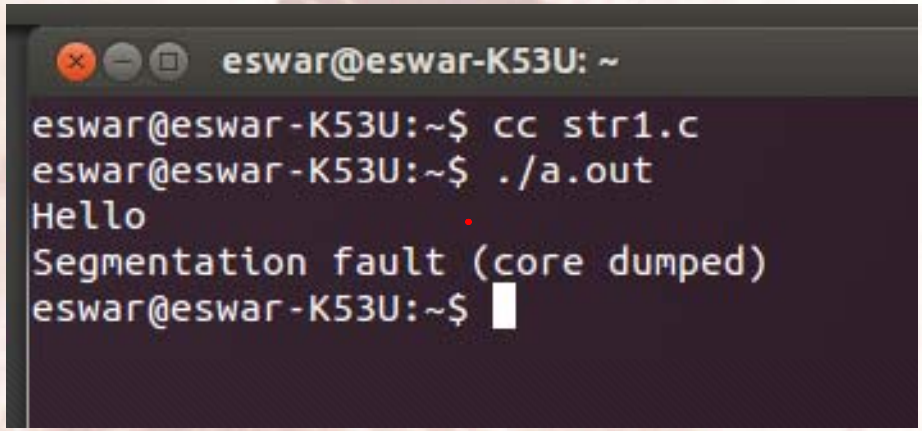
1. *Crash dump* datoteka
   - sadržava (obično) samo dio RAM-a
   - nakon kritične greške sustava

2. Hibernacijska datoteka
   - sadržava kompletni sadržaj RAM-a prije gašenja

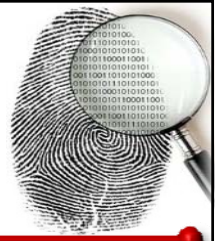
3. Datoteka straničenja
   - sadržava trenutno neaktivne stranice memorije

1. Crash dump

- kada operacijski sustav detektira fatalnu grešku
- gasi se
- prije toga
  - sprema sliku RAM-a u datoteku na disku
- može spremiti:
  - cijelu sliku RAM-a ili
  - minimalnu jezgru ili
  - samo početni dio memorije
- nedostaci su:
  - slika obično ne sadržava prve sektore
    - sa MBR-om, početnim lozinkama
  - možda nema dovoljno mjesta na disku
    - ili je disk šifriran
  - slika je možda oštećena
    - zbog utjecaja malware-a
- crash dump može biti namjerno potaknut
  - od strane upravljačkog programa
    - manipuliran ili oštećen



2. Hibernacijska datoteka



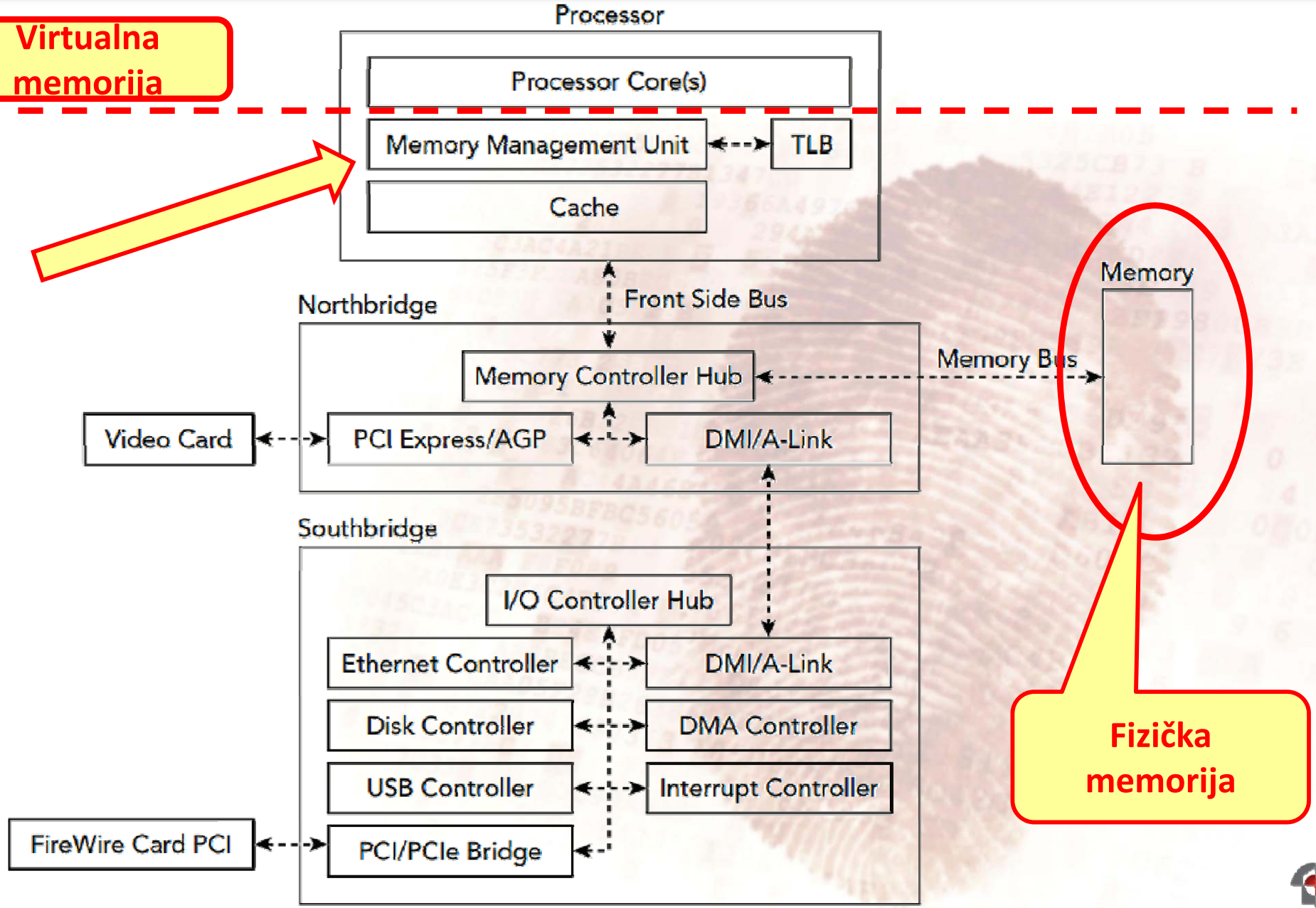
- većina operacijskih sustava podržava “hibernaciju”
  - **trenutna** obustava operacija
  - i isključenje cijelog računala
  - uz zadržavanje **mogućnosti nastavka** svih operacija
    - nakon ponovnog uključenja

- cijela slika RAM-a je spremljna na disk
- **potpuna** RAM **forenzička** analiza može biti izvršena
  - na hibernacijskoj datoteci
- hibernacijska datoteka je sigurnosni rizik
  - jer može sadržavati lozinku šifriranog diska

3. Datoteka straničenja

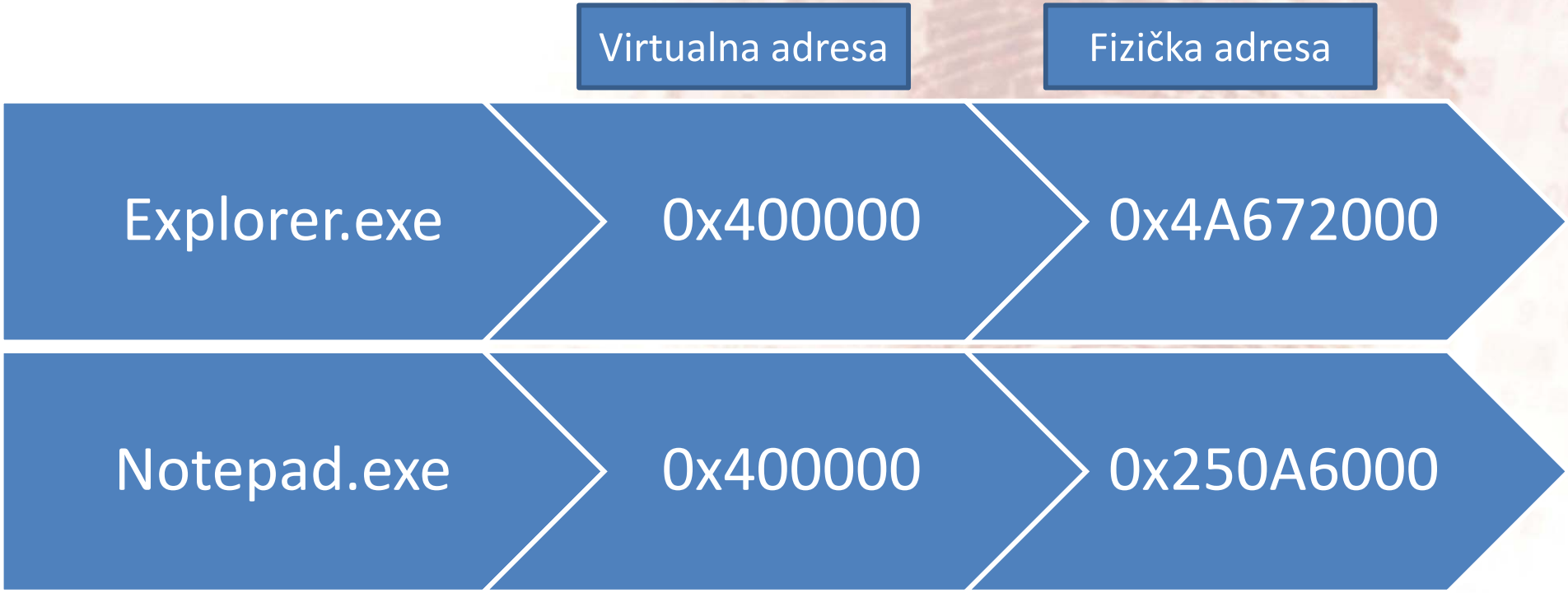
- stranice?
- virtualna memorija?

Arhitektura računala



Virtualna naspram fizičke memorije

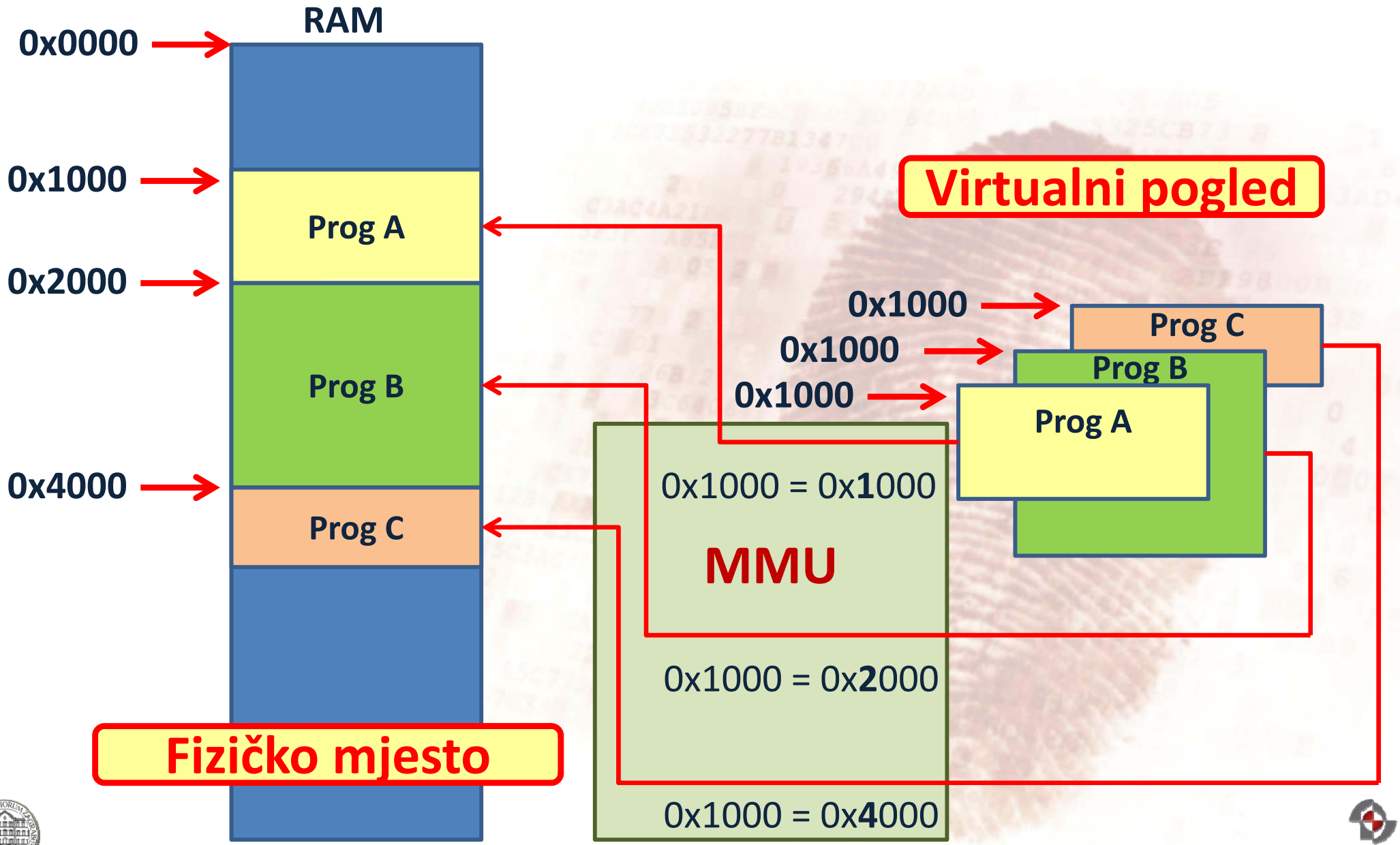
- **Procesor** koristi **fizičke** adrese
- ali **proces** koristi **virtualne** adrese



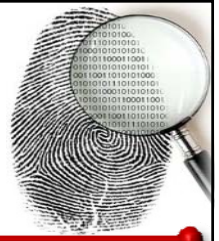
Zašto trebamo virutalnu memoriju?

1. Poznata početna adresa
   - za izvršavanje svakog programa
2. Razdvajanje procesa
   - na robustan i siguran način
3. Neograničena memorija za proces
   - i sve procese

1. Poznata početna adresa



2. Razdvajanje procesa



- za svaki **proces**
- operacijski sustav programira **MMU**
- da **dopusti pristup** procesu
  - samo **specifičnom dijelu** fizičke memorije

- svaki **pokušaj** procesa
- **da pristupi** nekoj memoriji **izvan** alociranog prostora
- **stvara prekid** procesoru

3. Neograničena memorija za proces

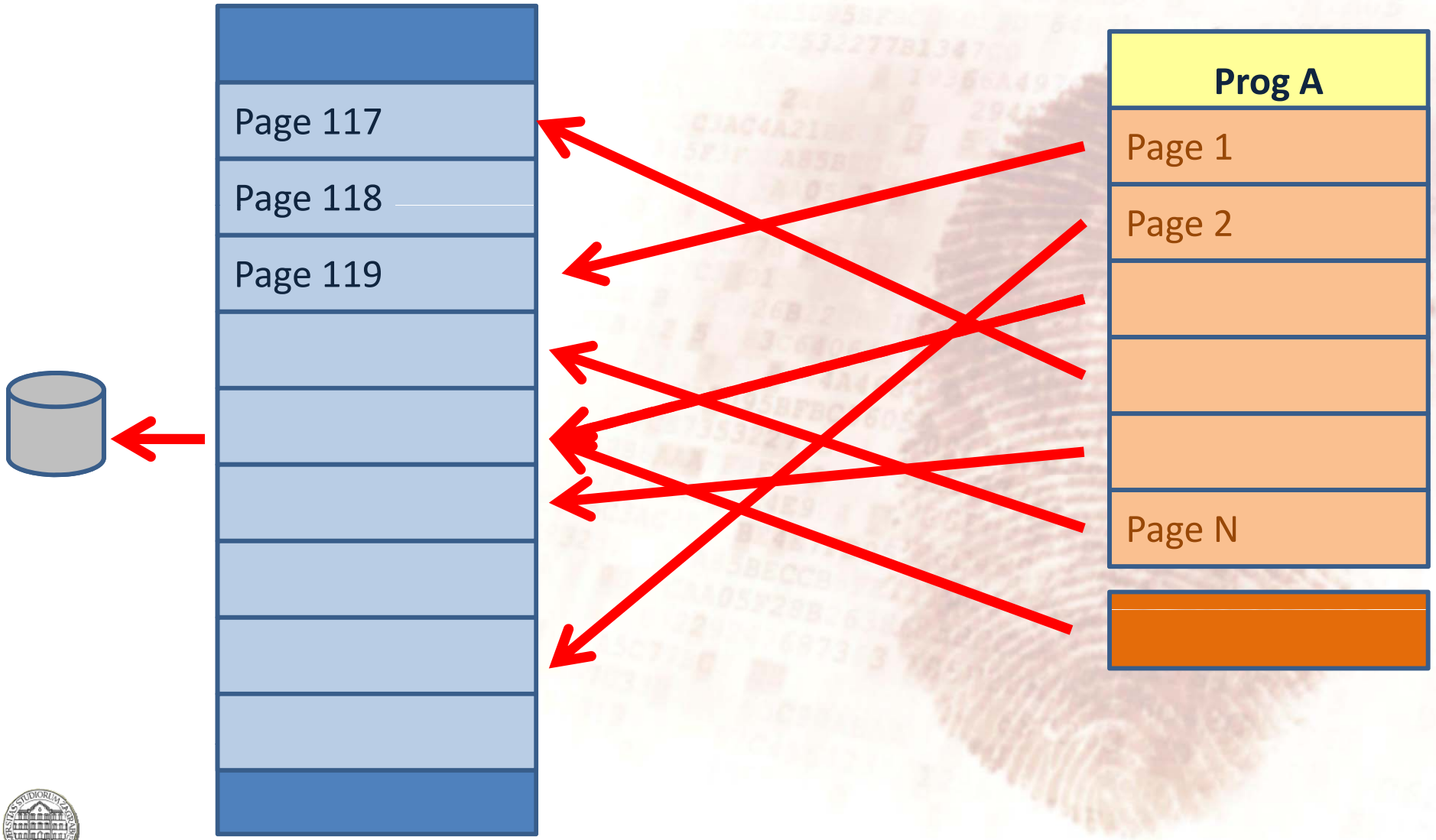
- **Memorija** procesa
- je **podijeljena** u blokove fiksne veličine = "**Stranice**"

- kada **proces zahtijeva više** memorije
  - **nego** što je fizički **dostupno**
- operacijski sustav
  - bira **stranicu** memorije procesa koja se **ne koristi**
  - **zapiše** ju **na disk**
  - i **alocira** tu fizičku memoriju procesu
  - **kao novi** (prošireni) dio virtualne memorije

Alociranje nepostojeće memorije

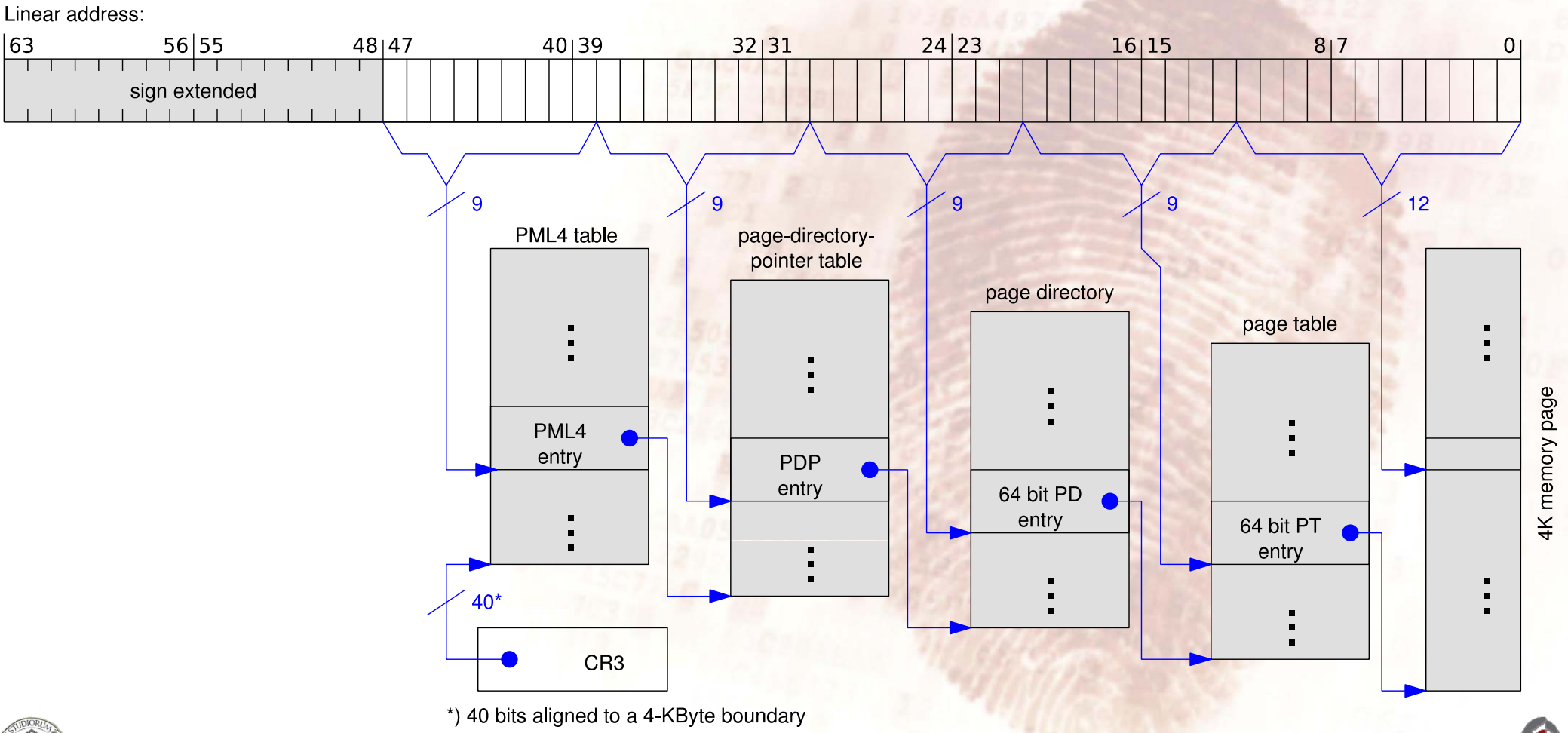
Fizička memorija

Virtualna memorija



Straničenje

- memorijski prostor je grupiran u “stranice” od 4KB
- stranice mogu biti u RAM-u ili na disku

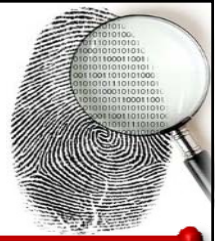


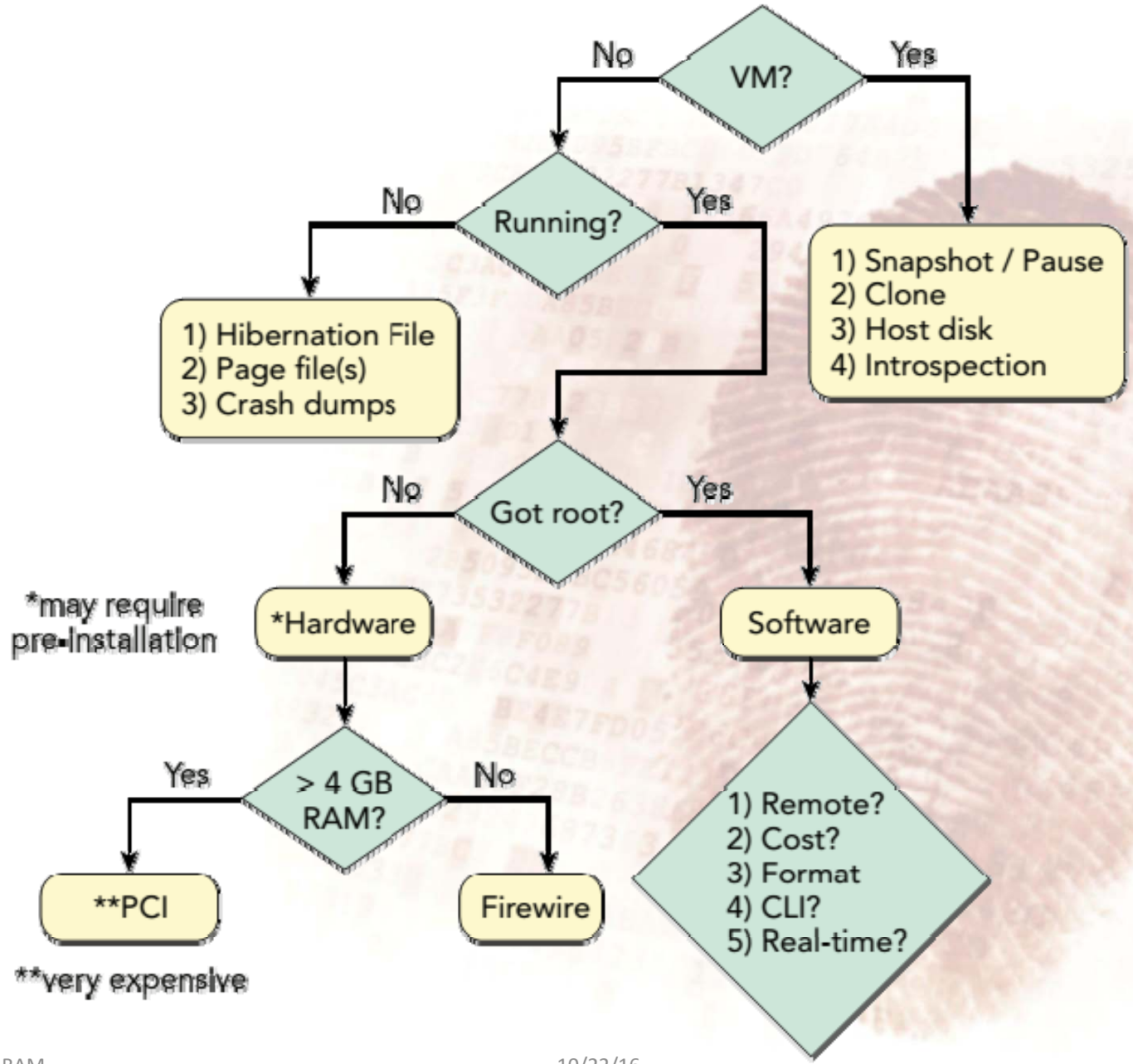
Slika RAM-a u stranicama

- datoteka straničenja sadržava trenutno nekorištene dijelove RAM-a
- stranice su u nasumičnom poretku
- tako da nam treba tablica stranice
  - da bismo mogli interpretirati njen sadržaj
- Linux koristi odvojenu particiju za straničenje

- no, napredni alati za analizu stranica
  - su tek još u razvoju

Akvizicija memorije – dijagram toka



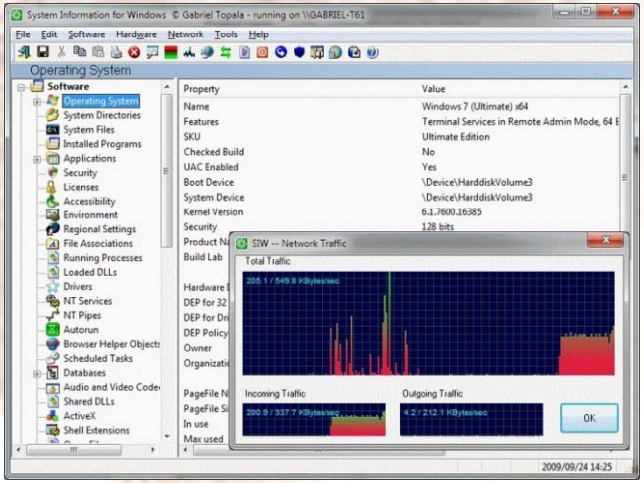


Ponovimo

- **zašto** nam je potrebna RAM forenzika
- **koje** informacije su u RAM-u
- koristimo **Volatility** framework
- **kako** steći sliku RAM-a

Zašto trebamo forenziku radne memorije?

- **Svaka aktivnost** na računalu
  - **modificira** stanje dijela **RAM-a**
- RAM sadržavaj neke informacije koje se **ne nalaze igdje drugdje**
  - kouminkacijske **poruke**
  - **lozinke**, PIN-ovi, …
  - privremeni **tekst**, **brojevi**, …
- informacija **može ostati** u RAM-u **dugo vremena**
- **obilje** informacija o **stanju** računalnog **sustava**
  - **procesi**
  - **podaci**
    - korisnički podaci, lozinke, …
  - **veze**
  - Informacije o **sustavu**
    - opterećenje, prioriteti, …
  - **tehničke** informacije
    - brojači, pokazivači, registri, ….

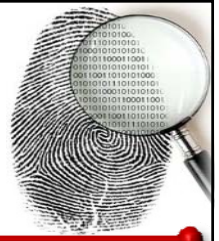


Informacije u RAM-u

- Procesi
- Jezgra
- Mreža
- Grafičko sučelje

- Windows specifičnosti
  - activity/event log
  - registry
  - datotečni sustav
- Linux specifičnosti
  - bash povijest
  - dmesg
  - kernel spremnici

Volatility framework



http://www.volatilityfoundation.org

- besplatan, open source
- podržava: Windows, Mac OS X, LInux
- isključivo sučelje komandne linije (CLI)
  - no drugi autori su razvili GUI-je
- podržava razne formate slika RAM-a
  - od čistih do hibernacijske datoteke
- mnoštvo modula:

clipboard
cmdline
devicetree
consoles
dlllist
evtlogs
hashdump
iehistory
mftparser
netscan
pslist
screenshot
svcscan
truecryptmaster
vadtree
yarascan

- Rekall
  - projekt nastao od Volatility-ja
  - cilja poboljšati performanse i modularnost

Kako napraviti sliku memorije

- Virtualni stroj
- Kopiranje pomoću software-a
- Pomoću hardware-a

- Komplementarni izvori na disku
  - Datoteka straničenja
  - Hibernacijska datoteka
  - Crash dump datoteka

Zaključak

- prije otprilike 10 godina
- istražitelji bi ugasili računalo
  - bez oklijevanja
- i koristili samo disk
  - za analizu

- RAM analiza je danas
  - aktivno područje istraživanja
  - veliki broj entuzijasta i korisnika

- Ako napadači mogu instalirati—vi možete detektirati!


ComFor.zesoi.fer.hr
RacFor@zesoi.fer.hr