Research Institute
Cyber Defence
Universität der Bundeswehr München

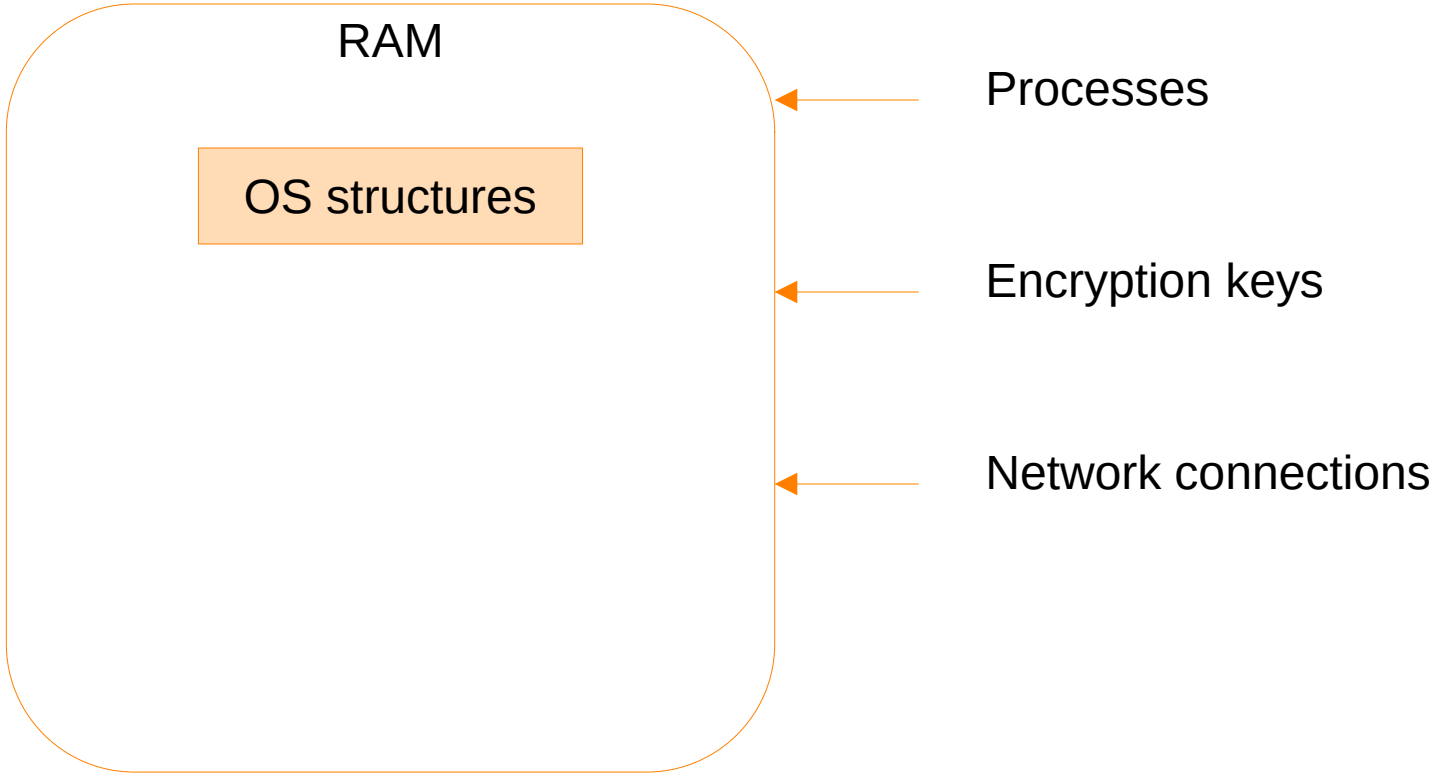
A Scenario-Based Quality Assessment of Memory Acquisition Tools and its Investigative Implications

Lisa Rzepka, Jenny Ottmann, Radina Stoykova, Felix Freiling, Harald Baier

Universität der Bundeswehr München

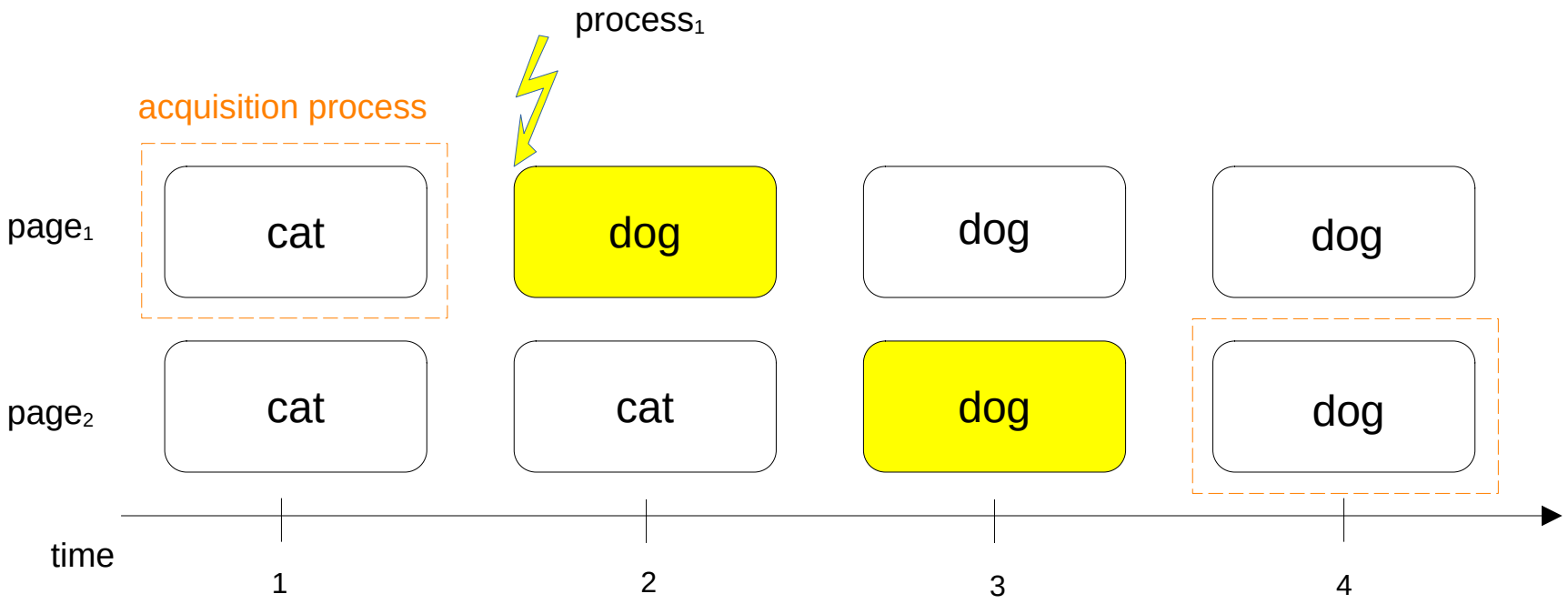
Motivation

Main memory



Motivation

Inconsistencies

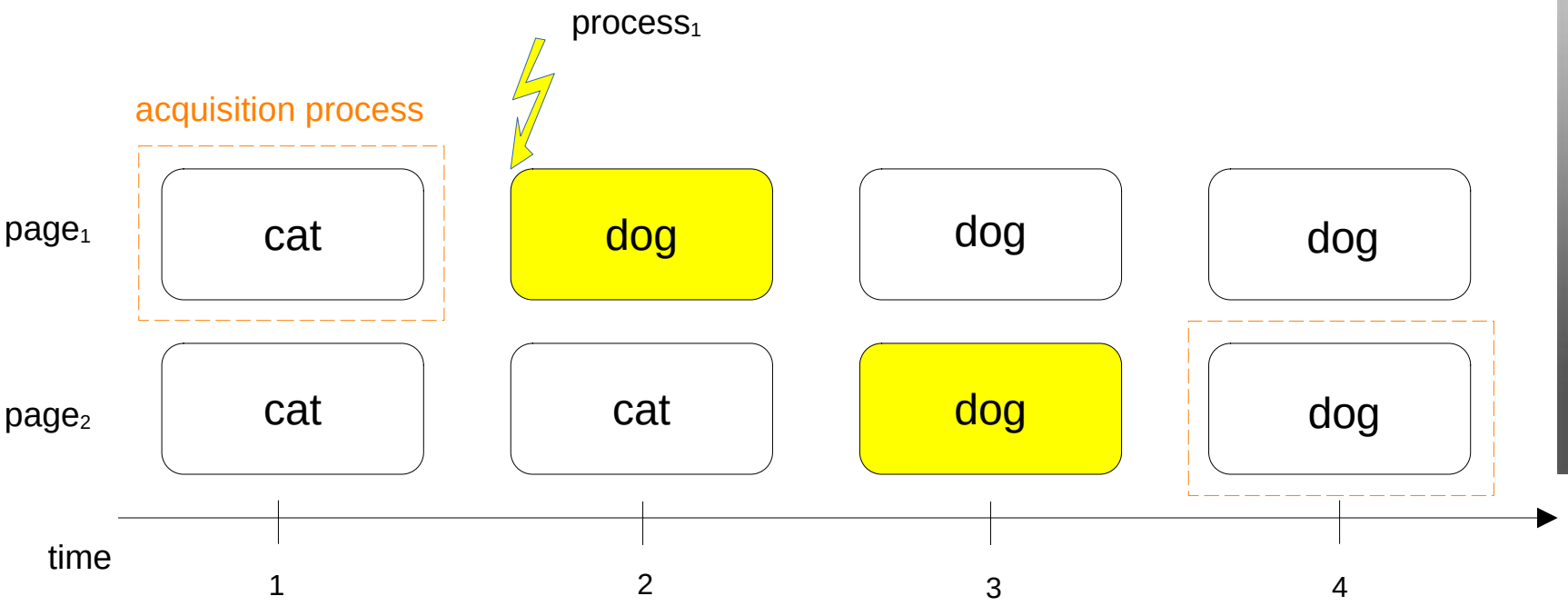


expected result

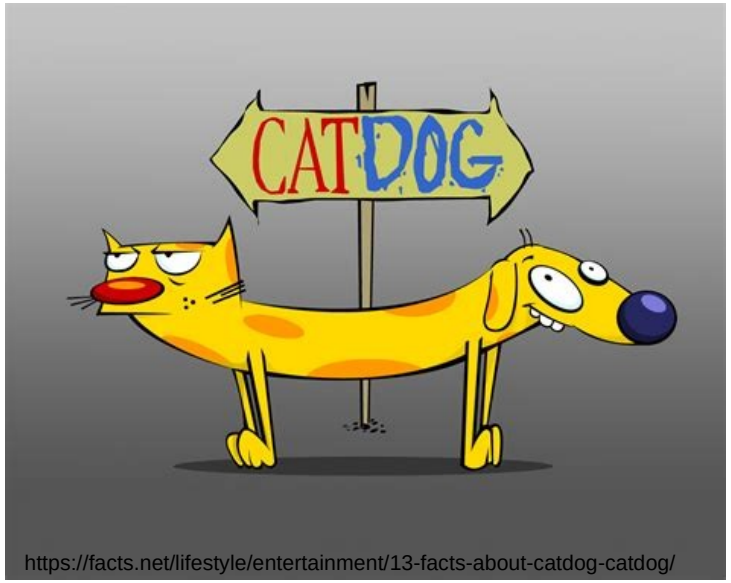
Image generated with ChatGPT

Motivation

Inconsistencies



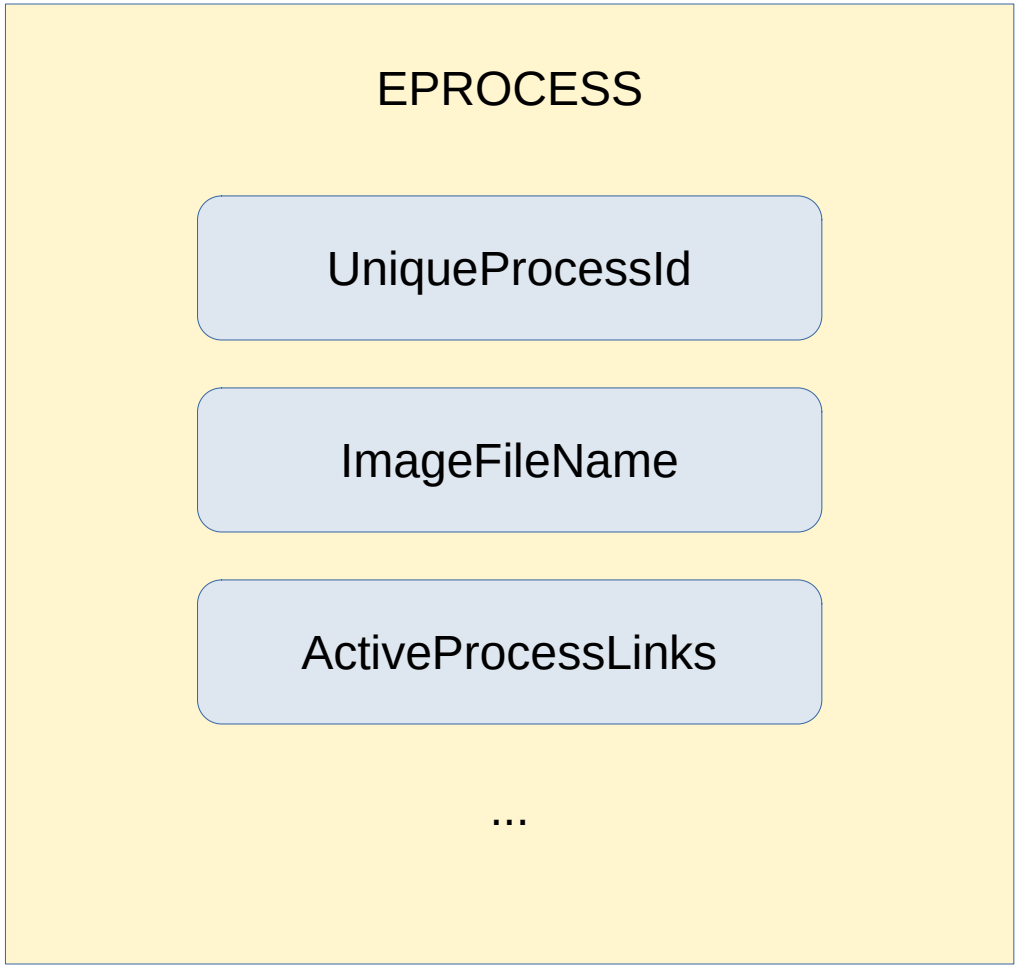
actual result



Motivation

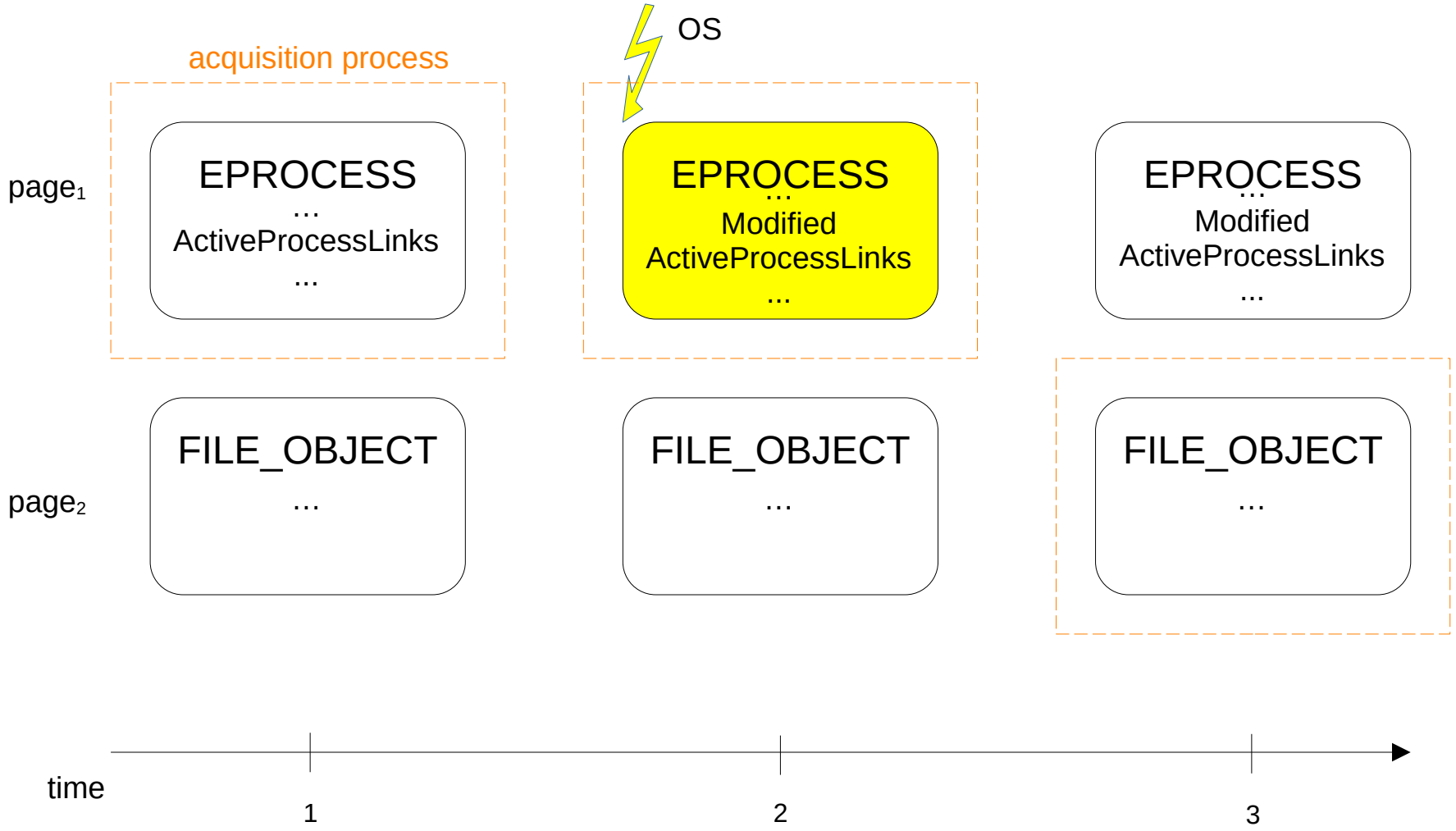
EPROCESS

- OS structure in Windows OS
- Information about (running) process



Motivation

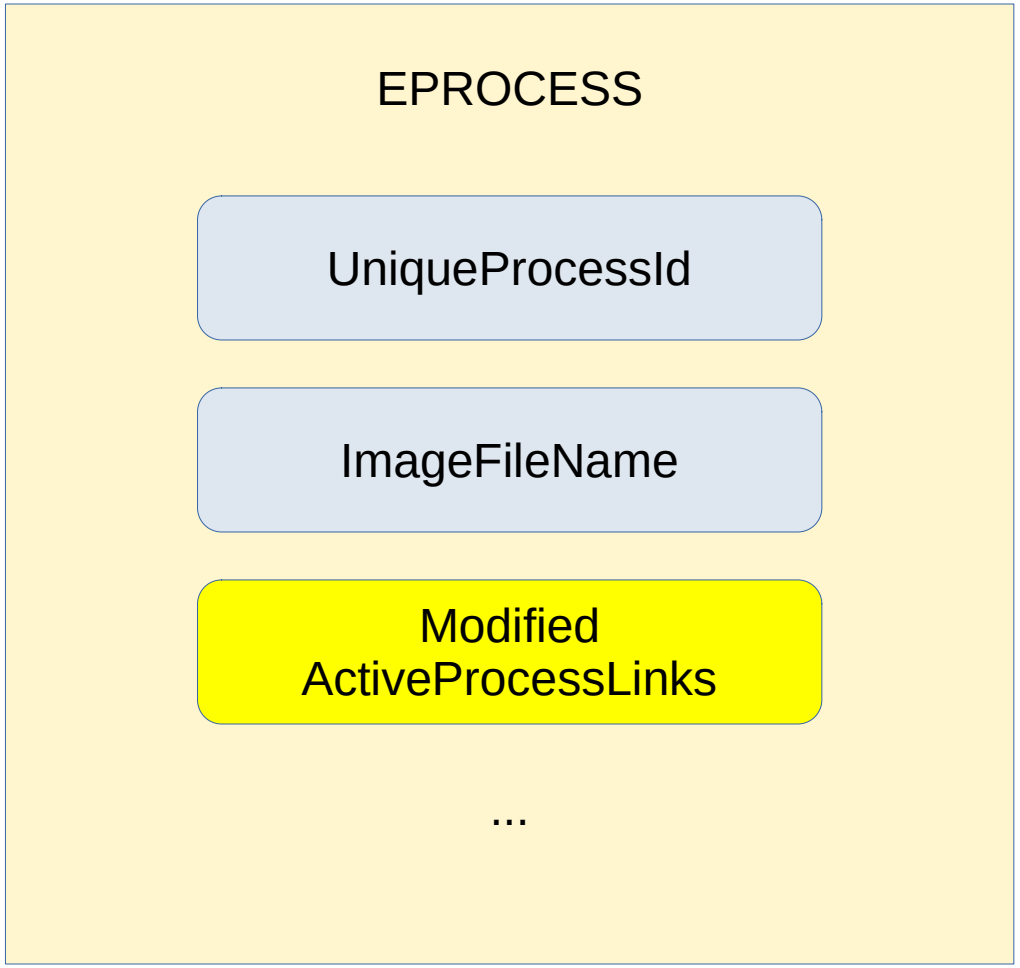
EPROCESS



Motivation

EPROCESS

- Memory dump contains modified EPROCESS structure
- Modification for example removal from list
- Volatility plugin pslist does not find process



Contributions

- Automated, scenario-based methodology to compare memory acquisition tools
- Measurement results for four tools and four scenarios
- Data set consisting of 1600 memory dumps

Method

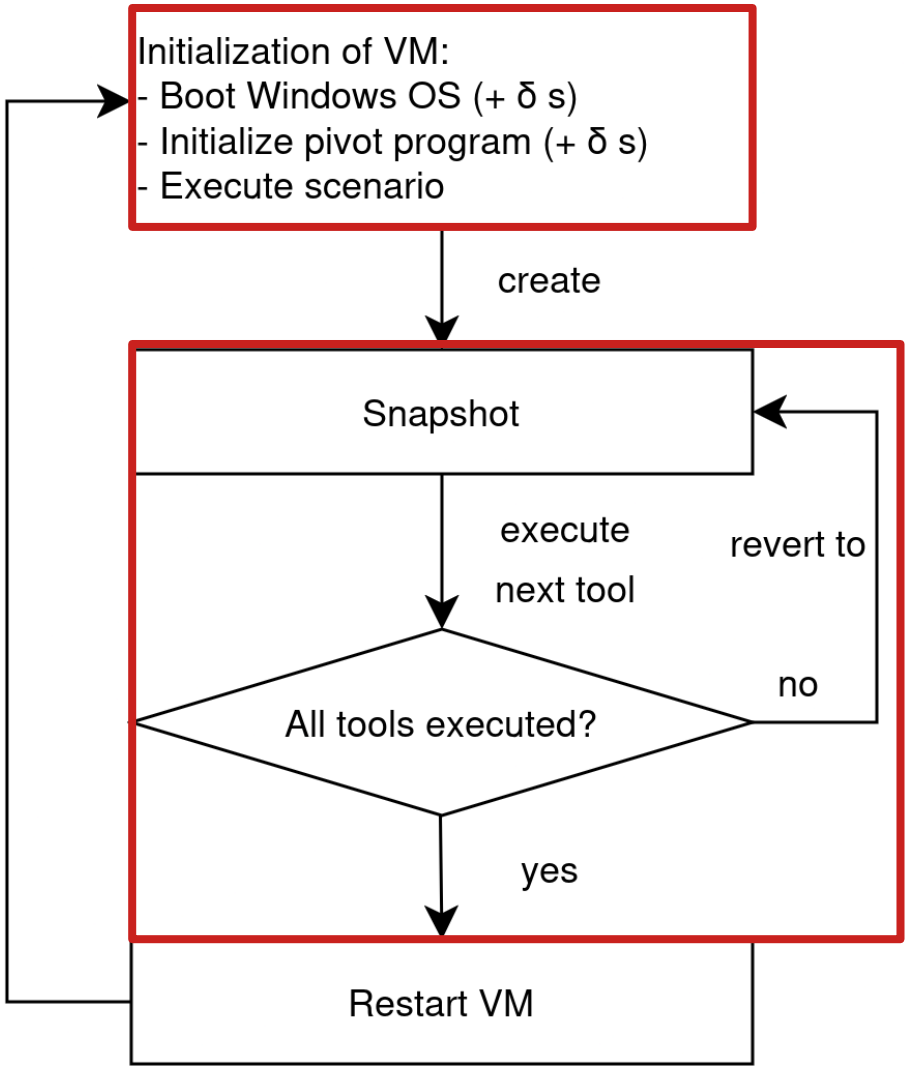
RAM acquisition tools

Tool name	Version	Open/closed source	Commercial/free
Belkasoft RAM Capturer	downloaded 07.02.2024	closed	free
FTK Imager	v4.7.1	closed	free
Magnet RAM Capture	v1.2.0	closed	free
WinPmem	winpmem_mini v4.0 RC2	open	free

Method

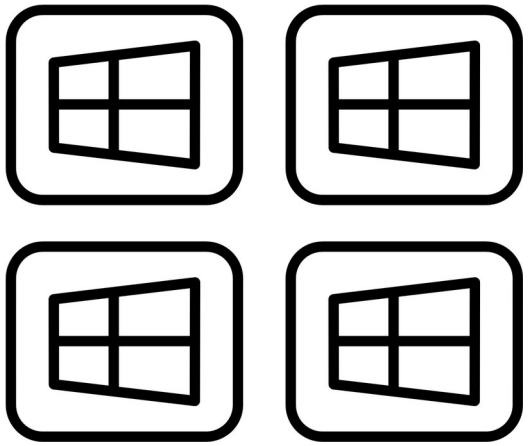
RAM acquisition tools

- Initialization: δ = 60 seconds
- 100 times per tool per scenario = 400 dumps
- In summary 1600 memory dumps
- Subset can be found here: https://zenodo.org/records/14260323

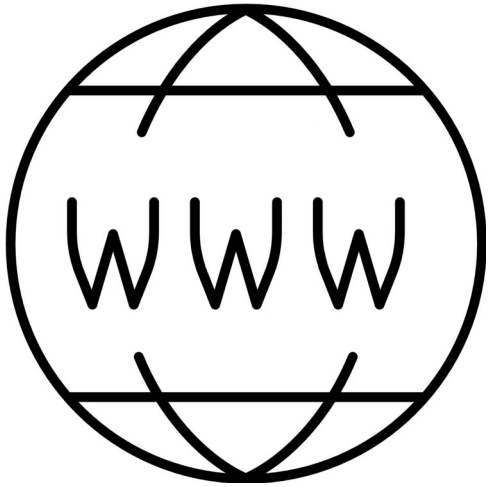


Method

Scenarios



Process



Network connection

VeraCrypt key

jpg

Analysis

Tools

Scenario	Structured analysis tool	Unstructured analysis tool
Executed software	Volatility *pslist*	Volatility *psscan*
Active ssh connection	Volatility *netlist*	Volatility *netscan*
Opened VeraCrypt container	-	*aeskeyfind*
Opened file (jpg)	-	Volatility *filescan*

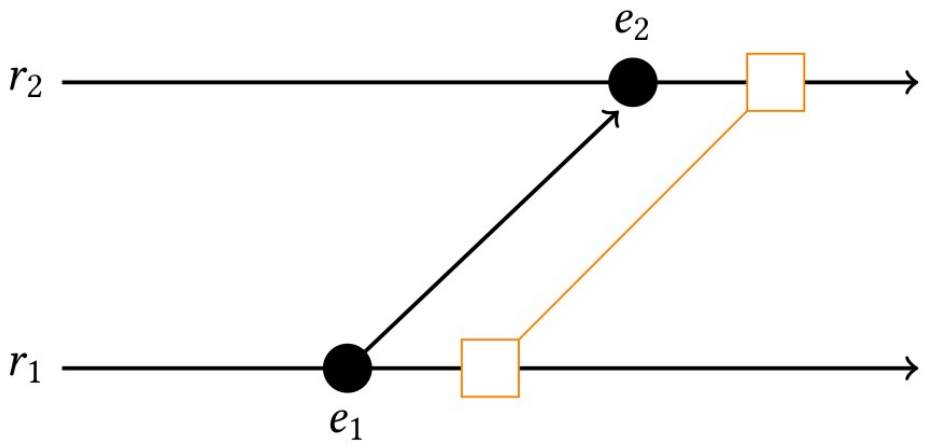
Background

Inconsistency indicators

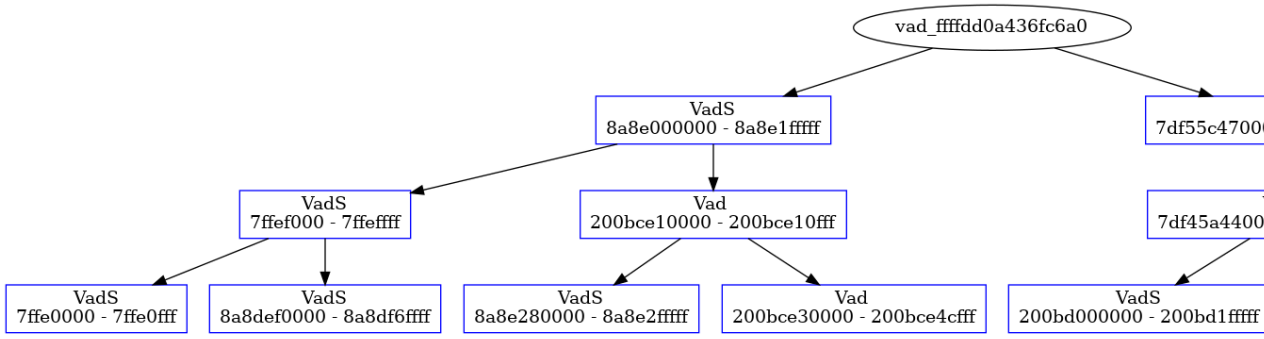
- Two different inconsistency indicators

  1) Causal inconsistency
     - Cause-effect relationships
     - Vector clocks
     - Pivot program

  2) VAD inconsistency
     - VAD tree
     - VadCount
     - Volatility3 plugin



Causally consistent memory snapshot



Part of VAD tree of smss.exe

Analysis

Technical results - Process

	Belkasoft	FTK	Magnet	WinPmem	Ideal
Process (structured)	96/100	96/100	69/100	94/100	10/10
Process (unstructured)	100/100	100/100	100/100	100/100	10/10
Mean VAD inconsistencies	685	785	1909	684	0
Mean causal inconsistencies	18	17	50	20	0

Analysis

Technical results – Network connection

	Belkasoft	FTK	Magnet	WinPmem	Ideal
ssh connection (structured)	98/100	98/100	90/100	94/100	9/10
ssh connection (unstructured)	100/100	98/100	92/100	96/100	10/10
Mean VAD inconsistencies	739	1135	2734	952	0
Mean causal inconsistencies	28	31	56	34	0

Analysis

Technical results – VeraCrypt key

	Belkasoft	FTK	Magnet	WinPmem	Ideal
VeraCrypt key	100/100	100/100	99/100	100/100	10/10
Mean VAD inconsistencies	510	907	2494	513	0
Mean causal inconsistencies	19	23	50	19	0

Analysis

Technical results – Opened file

	Belkasoft	FTK	Magnet	WinPmem	Ideal
Opened jpg file	49/100	49/100	99/100	45/100	10/10
Mean VAD inconsistencies	501	1066	1538	746	0
Mean causal inconsistencies	16	11	41	15	0

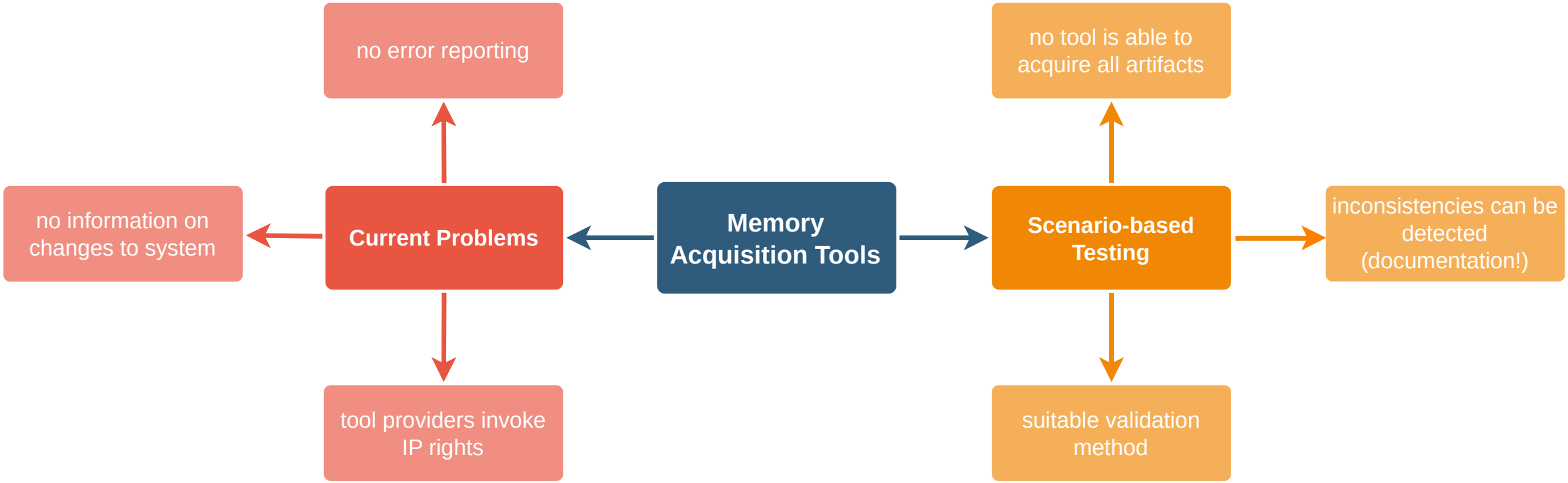
Analysis

Validation requirements for memory acquisition

- ISO17025 standard for testing/calibration of forensic laboratories
- Methods and tools in memory forensics derived primarily from forensic guidelines
- Both define rather broad and imprecise conditions for memory acquisition
- No validation scenarios or measurements given

Analysis

Procedural results



Summary

- Inconsistencies have greater impact on structured analysis methods
- Unstructured methods are more robust, but no context
- Artifacts of opened (jpg-)files difficult
- Scenario-based testing can help in assessing limitations of tools

Future Work

Questions?

- Experiments with unstructured analysis methods
- Quality of memory analysis tools
- Additional inconsistency indicators and their relationship
- Artifacts of opened files

Subset of dataset can be found here:
https://zenodo.org/records/14260323

Lisa Rzepka
Research Institute CODE
Universität der Bundeswehr München

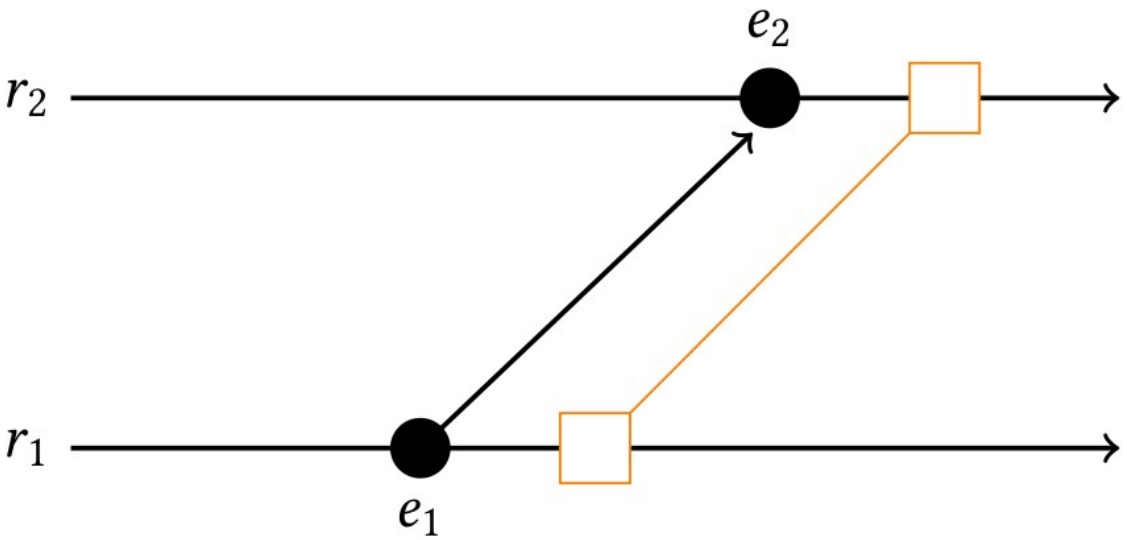
lisa.rzepka@unibw.de

Research Institute
Cyber Defence
Universität der Bundeswehr München

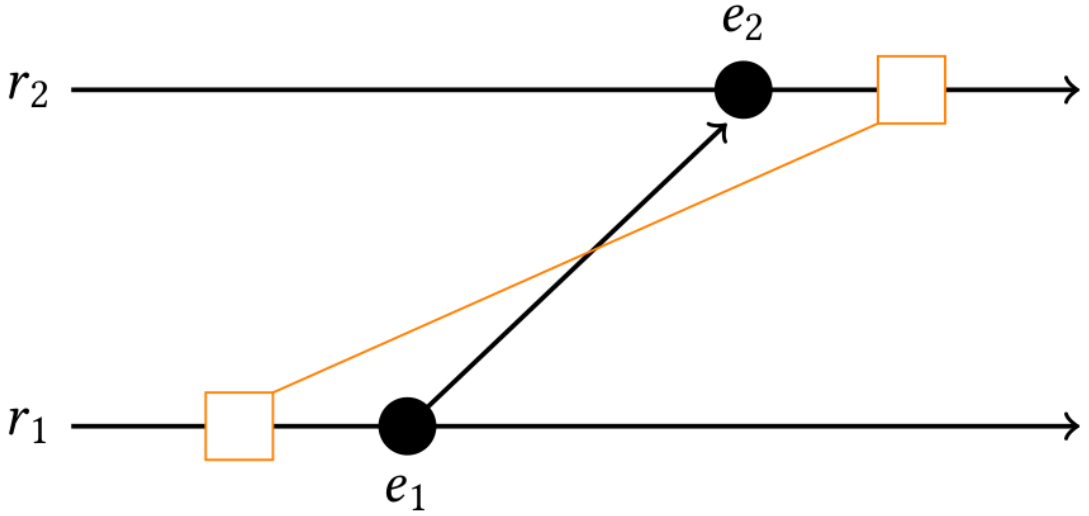
Background

Causal consistency

- 2 memory regions r1, r2
- 2 events e1, e2
- Orange rectangle = memory acquisition process
- X axis = time



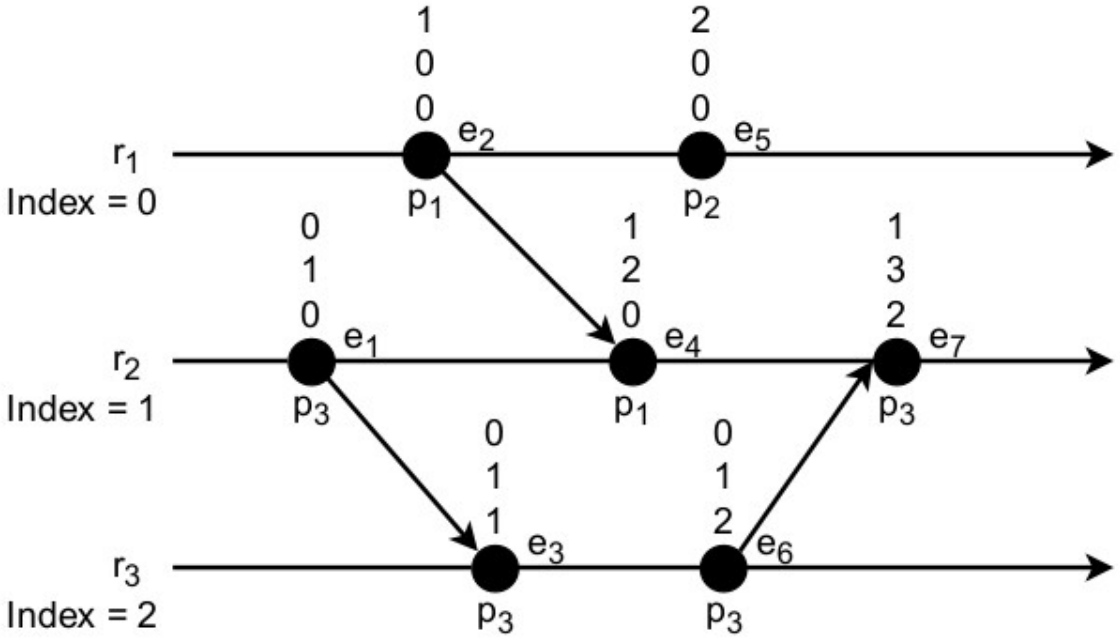
Causally consistent memory snapshot



Causally inconsistent memory snapshot

Vector clocks

- Each memory region is assigned a row in a vector
- Index is updated each time event happened in memory region (local counter)
- Processes save vector clocks and update them



Background

Virtual Address Descriptor (VAD) Tree

- Adelson-Velsky/Landis (AVL) tree
- Allocated memory for each process
- 3 node types
- VadCount

Type	Abbreviation
MMVAD_SHORT	VadS
MMVAD	Vad
MMVAD_LONG	VadL

```
typedef struct _RTL_AVL_TABLE {
  RTL_BALANCED_LINKS            BalancedRoot;
  PVOID                         OrderedPointer;
  ULONG                         WhichOrderedElement;
  ULONG                         NumberGenericTableElements;
  ULONG                         DepthOfTree;
  PRTL_BALANCED_LINKS           RestartKey;
  ULONG                         DeleteCount;
  PRTL_AVL_COMPARE_ROUTINE      CompareRoutine;
  PRTL_AVL_ALLOCATE_ROUTINE     AllocateRoutine;
  PRTL_AVL_FREE_ROUTINE         FreeRoutine;
  PVOID                         TableContext;
} RTL_AVL_TABLE;
```

Method

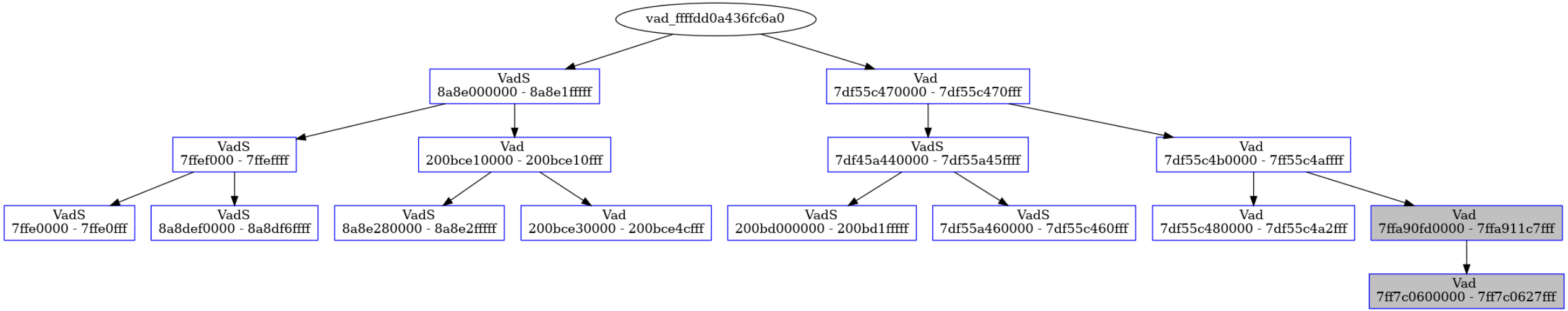
Volatility 3 VadDiff plugin

PID	Process	VadCount	Count	Difference
92	Registry	82	73	9
452	csrss.exe	182	176	6
540	csrss.exe	113	114	1
588	winlogon.exe	95	94	1
668	services.exe	62	61	1
684	lsass.exe	153	152	1
780	svchost.exe	156	152	4
888	svchost.exe	92	78	14
400	svchost.exe	74	72	2
812	svchost.exe	57	53	4
1096	dwm.exe	254	279	25
1368	svchost.exe	111	105	6
1384	svchost.exe	102	103	1
1416	svchost.exe	67	68	1
1448	svchost.exe	117	116	1
1676	svchost.exe	78	76	2

...

Background

Virtual Address Descriptor (VAD) Tree



Background

Virtual Address Descriptor (VAD) Tree