Windows NT pagefile.sys Virtual Memory Analysis

Michael Gruhn

2015-05-18

Friedrich-Alexander-Universität Erlangen-Nürnberg
Department of Computer Science
Chair of Computer Science 1
IT Security Infrastructures
Motivation

System compromised by malware downloaded from example.com
Motivation

System compromised by malware downloaded from example.com

- `strings ram.dump`

Problem:

- What context? Which process? ...

Solved:

Virtual memory analysis ...

... incorporating Windows NT's `pagefile.sys`
Motivation

System compromised by malware downloaded from example.com

- `strings ram.dump | grep "example.com"`
Motivation

System compromised by malware downloaded from example.com

- strings ram.dump | grep "example.com"
  - lists all occurrences of example.com

Problem: What context? Which process? ...

Solved: Virtual memory analysis ...

... incorporating Windows NT's pagefile.sys
Motivation

System compromised by malware downloaded from example.com

- strings ram.dump | grep "example.com"
  - lists all occurrences of example.com
  - **Problem:** What context? Which process? ...
Motivation

System compromised by malware downloaded from example.com

- `strings ram.dump | grep "example.com"
  - lists all occurrences of example.com
  - **Problem**: What context? Which process? ...  
  - **Solved**: Virtual memory analysis

What if the evidence is not in physical RAM but only the pagefile?

- `strings pagefile.sys | grep "example.com"
  - Problem: What context? Which process? ...
  - Solved: Virtual memory analysis
Motivation

System compromised by malware downloaded from example.com

- strings ram.dump | grep "example.com"
  - lists all occurrences of example.com
  - **Problem:** What context? Which process? ...
  - **Solved:** Virtual memory analysis

**What if the evidence is not in physical RAM but only the pagefile?**
Motivation

System compromised by malware downloaded from example.com

- strings ram.dump | grep "example.com"
  - lists all occurrences of example.com
  - **Problem:** What context? Which process? ...
  - **Solved:** Virtual memory analysis

What if the evidence is not in physical RAM but only the pagefile?

- strings pagefile.sys
Motivation

System compromised by malware downloaded from example.com

- `strings ram.dump | grep "example.com"`
  - lists all occurrences of example.com
  - **Problem:** What context? Which process? ...
  - **Solved:** Virtual memory analysis

What if the evidence is not in physical RAM but only the pagefile?

- `strings pagefile.sys | grep "example.com"`
Motivation

System compromised by malware downloaded from example.com

- `strings ram.dump | grep "example.com"
  - lists all occurrences of example.com
  - **Problem:** What context? Which process? ...
  - **Solved:** Virtual memory analysis

What if the evidence is not in physical RAM but only the pagefile?

- `strings pagefile.sys | grep "example.com"
  - **Problem:** What context? Which process? ...
Motivation

System compromised by malware downloaded from example.com

- `strings ram.dump | grep "example.com"
  - lists all occurrences of example.com
  - **Problem:** What context? Which process? ...
  - **Solved:** Virtual memory analysis

What if the evidence is not in physical RAM but only the pagefile?

- `strings pagefile.sys | grep "example.com"
  - **Problem:** What context? Which process? ...
  - **Solved:** Virtual memory analysis ...

... incorporating Windows NT’s pagefile.sys
Motivation

System compromised by malware downloaded from example.com

- `strings ram.dump | grep "example.com"
  - lists all occurrences of example.com
  - **Problem**: What context? Which process? ...
  - **Solved**: Virtual memory analysis

What if the evidence is not in physical RAM but only the pagefile?

- `strings pagefile.sys | grep "example.com"
  - **Problem**: What context? Which process? ...
  - **Solved**: Virtual memory analysis ...

... incorporating Windows NT’s pagefile.sys = This Talk
Outline

Introduction
Virtual Address Translation (Refresher)
Inferring Address Translation via Graybox Testing (Our Research)

Windows NT Page Table Entries (PTEs)
Hardware IA32e (x64) PTEs
Software IA32e (x64) PTEs
Software Generic Overview

Evaluation
Problem Cases
Windows NT Versions

Conclusion and Future Work
Virtual Address

0xdeadbeef

Virtual Address Space

Data of Interest

0xdeadbeef

Data of this process

0xffffffff

0x00000000
Virtual Address
0xdeadbeef

Data of Interest
What you want for Analysis
Data of this process
0xdeadbeef

Virtual Address Space
0xffffffff
0x00000000
0x00000000
0xffffffff
Virtual Address

0xdeadbeef

Physical Address Space

Virtual Address Space

Data of Interest

Data of different process

What you get

What you want for Analysis

Data of this process

0xffffffff

0x00000000

0xdeadbeef

0xdeadbeef

0x00000000

0xffffffff

0xdeadbeef
Virtual Address
0xdeadbeef

Physical Address Space

Virtual Address Space

What you get

Data of Interest

Data of different process

CR3 Register
0xdeadbeef

What you want for Analysis

Data of Interest

Data of this process

Page Directory

Page Directory Entry

Page Directory Entry

...
Virtual Address

0xdeadbeef

Physical Address Space

Virtual Address Space

Data of Interest

Data of different process

Page Directory

Page Directory Entry

Page Directory Entry

...

_EPROCESS

Directory Table Base

0xffffffff

0x00000000

0xdeadbeef

Data of Interest

Data of this process

CR3 Register

0xdeadbeef

What you get

What you want for Analysis

What you get
Physical Address Space

Virtual Address

0xdeadbeef

Physical Page

Data of Interest

Data of different process

Page Table

Page Table Entry

Page Table Entry

Page Directory

Page Directory Entry

Page Directory Entry

CR3 Register

0xdeadbeef

Data of Interest

Data of this process

_EPROCESS

Directory Table Base

0xffffffff

0x00000000

What you get

What you want for Analysis

0xffffffff

0x00000000
What you get
Data of different process
Data of this process

What you want for Analysis

Data of Interest

Virtual Address

0xdeadbeef

Physical Address Space

Virtual Address Space

Physical Page

Data of Interest

Data of different process

Page Table

Page Table Entry

Page Directory

Page Directory Entry

CR3 Register

0xdeadbeef

0xffffffff

0x00000000

_DATA OF _EPROCESS

DIRECTORY TABLE BASE

_0x00000000
Virtual Address

0xdeadbeef

Physical Address Space

Virtual Address Space

CR3 Register

0xdeadbeef

Data of Interest

Data of different process

Page Table

Page Directory

Page Directory Entry

Page Table Entry

... Data of this process

Data of this process

What you get

What you want for Analysis

Directory Table Base

_EPROCESS

0xffffffff

0x00000000
Physical Address Space

Virtual Address

Data of Interest

Data of this process

Page Table

Page Directory

CR3 Register

What you get

Physical Page

Data of different process

Page Table Entry

Page Directory Entry

What you want for Analysis

Virtual Address Space

Data of Interest

Data of this process

.Directory Table Base

EPRECESS

SOLVED!
Inferring Address Translation via Graybox Testing
Inferring Address Translation via Graybox Testing

Virtual Memory

Physical Memory

Memory Page

Pagefile

Memory Frame

Pagefile Frame

Virtual Address Translation
Inferring Address Translation via Graybox Testing
Inferring Address Translation via Graybox Testing

Virtual Memory

Physical Memory

Virtual Address Translation

Memory Page

Crib Page

Pagefile

Frame

Memory Frame

Pagefile Frame

Crib Frame

0x00000000
0x00000001
...
0x00000fff
0x00000ffe
...
Inferring Address Translation via Graybox Testing
Outline

Introduction
- Virtual Address Translation (**(Refresher)**)
- Inferring Address Translation via Graybox Testing (**Our Research**)

**Windows NT Page Table Entries (PTEs)**
- Hardware IA32e (x64) PTEs
- Software IA32e (x64) PTEs
- Software Generic Overview

Evaluation
- Problem Cases
- Windows NT Versions

Conclusion and Future Work
IA32e (Hardware) Paging

<table>
<thead>
<tr>
<th>Reserved</th>
<th>Address of PML4</th>
<th>Ignored</th>
<th>PCD</th>
<th>PWT</th>
<th>Ignored</th>
<th>CR3</th>
</tr>
</thead>
<tbody>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address of PDPT</th>
<th>Ignored</th>
<th>Reserved</th>
<th>PCD</th>
<th>PWT</th>
<th>Ignored</th>
<th>PML4E</th>
</tr>
</thead>
<tbody>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address of PD</th>
<th>Ignored</th>
<th>Reserved</th>
<th>PCD</th>
<th>PWT</th>
<th>Ignored</th>
<th>PDPE (PD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address of PT</th>
<th>Ignored</th>
<th>Reserved</th>
<th>PCD</th>
<th>PWT</th>
<th>Ignored</th>
<th>PDE (PT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address of 4 KiB frame</th>
<th>Ignored</th>
<th>Reserved</th>
<th>PCD</th>
<th>PWT</th>
<th>Ignored</th>
<th>PTE (4 KiB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
<tr>
<td>XD</td>
<td>Ignored</td>
<td>Reserved</td>
<td>A</td>
<td></td>
<td>Reserved</td>
<td>1</td>
</tr>
</tbody>
</table>

Straight from the Intel Specification!
### IA32e Windows NT IA32e (x86) Software Paging

<table>
<thead>
<tr>
<th>Bit</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>63 62</td>
<td>NoExecute</td>
<td>M M-1</td>
</tr>
<tr>
<td>52 51</td>
<td>SoftwareWsIndex</td>
<td></td>
</tr>
<tr>
<td>32 31</td>
<td>reserved1</td>
<td></td>
</tr>
<tr>
<td>28 23</td>
<td>PageFrameNumber</td>
<td></td>
</tr>
<tr>
<td>22 19</td>
<td>reserved0</td>
<td></td>
</tr>
<tr>
<td>18 15</td>
<td>CopyOnWrite</td>
<td></td>
</tr>
<tr>
<td>14 11</td>
<td>Global</td>
<td></td>
</tr>
<tr>
<td>10 7</td>
<td>Dirty</td>
<td></td>
</tr>
<tr>
<td>6 4</td>
<td>Accessed</td>
<td></td>
</tr>
<tr>
<td>3 1</td>
<td>WriteThrough</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Valid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MMPTE_HARDWARE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MMPTE_SOFTWARE</td>
<td></td>
</tr>
</tbody>
</table>

**Straight from the Windows NT Research Kernel Source Code!**
# IA32e Windows NT IA32e (x86) Software Paging

## Table of Contents
- PageFrameNumber
- PageFileHigh
- PageFileLow

---

### PageFrameNumber

<table>
<thead>
<tr>
<th>Bit</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>63</td>
<td>NoExecute</td>
<td>Specifies no execution of the page frame.</td>
</tr>
<tr>
<td>62</td>
<td>SoftwareWsIndex</td>
<td>Software Working Set Index.</td>
</tr>
<tr>
<td>52-51</td>
<td>reserved1</td>
<td>Reserved.</td>
</tr>
<tr>
<td>32-31</td>
<td>PageFrameNumber</td>
<td>Page Frame Number.</td>
</tr>
<tr>
<td>23-22</td>
<td>reserved2</td>
<td>Reserved.</td>
</tr>
<tr>
<td>14-13</td>
<td>reserved3</td>
<td>Reserved.</td>
</tr>
<tr>
<td>4-3</td>
<td>reserved4</td>
<td>Reserved.</td>
</tr>
<tr>
<td>0</td>
<td>MMPTE_HARDWARE</td>
<td>Matrix Page Table Entry Hardware.</td>
</tr>
</tbody>
</table>

### PageFileHigh

<table>
<thead>
<tr>
<th>Bit</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>52-51</td>
<td>Reserved</td>
<td>Reserved.</td>
</tr>
<tr>
<td>32-31</td>
<td>UsedPageTableEntries</td>
<td>Used Page Table Entries.</td>
</tr>
<tr>
<td>23-22</td>
<td>Transition</td>
<td>Transition.</td>
</tr>
<tr>
<td>14-13</td>
<td>Prototype</td>
<td>Prototype.</td>
</tr>
<tr>
<td>4-3</td>
<td>Protection</td>
<td>Protection.</td>
</tr>
<tr>
<td>0</td>
<td>MMPTE_SOFTWARE</td>
<td>Matrix Page Table Entry Software.</td>
</tr>
</tbody>
</table>

---

Straight from the Windows NT Research Kernel Source Code!
## Windows NT Software Paging Overview

<table>
<thead>
<tr>
<th>PageFileHigh</th>
<th>Transition</th>
<th>Prototype</th>
<th>Protection</th>
<th>PageFileLow</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Software PTE
Windows NT Software Paging Overview

<table>
<thead>
<tr>
<th>PageFileHigh</th>
<th>Transition</th>
<th>Protection</th>
<th>PageFileLow</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00</td>
<td>00</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Software PTE

Demand Zero PTE
## Windows NT Software Paging Overview

<table>
<thead>
<tr>
<th>Page File High</th>
<th>Transition</th>
<th>Prototype</th>
<th>Protection</th>
<th>Page File Low</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>00</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Software PTE**

**Demand Zero PTE**

**Pagefile PTE**
## Windows NT Software Paging Overview

<table>
<thead>
<tr>
<th>PageFileHigh</th>
<th>Transition</th>
<th>Prototype</th>
<th>Protection</th>
<th>PageFileLow</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 0</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PageFileHigh</td>
<td>0 0</td>
<td></td>
<td></td>
<td>PageFileLow</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1 0</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

### Software PTE

- Demand Zero PTE
- Pagefile PTE
- Transition PTE
# Windows NT Software Paging Overview

<table>
<thead>
<tr>
<th>PageFileHigh</th>
<th>Transition</th>
<th>Prototype</th>
<th>Protection</th>
<th>PageFileLow</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- **Software PTE**
- **Demand Zero PTE**
- **Pagefile PTE**
- **Transition PTE**
- **Prototype PTE**
Outline

Introduction
  Virtual Address Translation (Refresher)
  Inferring Address Translation via Graybox Testing (Our Research)

Windows NT Page Table Entries (PTEs)
  Hardware IA32e (x64) PTEs
  Software IA32e (x64) PTEs
  Software Generic Overview

Evaluation
  Problem Cases
  Windows NT Versions

Conclusion and Future Work
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
</table>

Memory Carving  
Pagefile Carving  
Virtual Memory  
... + Pagefile
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
</table>

- **Virtual Memory**
- **Physical Memory**
- **Pagefile**

### Memory Carving
- Pagefile Carving
- Virtual Memory
- ... + Pagefile
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Pagefile</td>
<td>Mem Carving</td>
</tr>
<tr>
<td>Pagefile Carving</td>
<td>Yes</td>
<td>Maybe</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Memory Carving
Pagefile Carving
Virtual Memory

2015-05-18 | Michael Gruhn | FAU i1 | VirMA: NT
Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Pagefile</td>
<td></td>
</tr>
</tbody>
</table>

Memory Carving: No
Pagefile Carving: Yes
Virtual Memory: No
... + Pagefile

Maybe
No
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Pagefile</td>
<td>Memory Carving</td>
</tr>
<tr>
<td>Pagefile Carving</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Maybe</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Diagram:
- Virtual Memory
- Physical Memory
- Pagefile

### Notes:
- Memory Carving
- Pagefile Carving
- Virtual Memory
- ... + Pagefile
# Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Pagefile</td>
<td></td>
</tr>
</tbody>
</table>

- **Memory Carving**: Maybe
- **Pagefile Carving**: No
- **Virtual Memory**: Yes
- **... + Pagefile**: Yes
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Virtual Memory</td>
<td>Physical Memory</td>
</tr>
<tr>
<td>Pagefile</td>
<td></td>
<td>Pagefile</td>
<td></td>
</tr>
</tbody>
</table>

- **Memory Carving**: Maybe
- **Pagefile Carving**: No
- **Virtual Memory**: Yes
- **... + Pagefile**: Yes
# Evaluation: Problem Cases

## Problem Case 1
- **Virtual Memory**: Yes
- **Physical Memory**: No
- **Pagefile**: Yes
- **Memory Carving**: No
- **Pagefile Carving**: No
- **Virtual Memory Analysis + Pagefile**: Yes

## Problem Case 2
- **Virtual Memory**: Yes
- **Physical Memory**: No
- **Pagefile**: Yes
- **Memory Carving**: Maybe
- **Pagefile Carving**: No
- **Virtual Memory Analysis + Pagefile**: Yes

## Problem Case 3
- **Virtual Memory**: Yes
- **Physical Memory**: No
- **Pagefile**: Yes
- **Memory Carving**: No
- **Pagefile Carving**: No
- **Virtual Memory Analysis + Pagefile**: Yes

## Problem Case 4
- **Virtual Memory**: Yes
- **Physical Memory**: No
- **Pagefile**: Yes
- **Memory Carving**: Maybe
- **Pagefile Carving**: No
- **Virtual Memory Analysis + Pagefile**: Yes
Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Virtual Memory</td>
<td>Physical Memory</td>
</tr>
<tr>
<td>Pagefile</td>
<td>Maybe</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Memory Carving</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Pagefile Carving</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Memory</strong></td>
<td><strong>Physical Memory</strong></td>
<td><strong>Virtual Memory</strong></td>
<td><strong>Physical Memory</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pagefile</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Memory Carving
- Problem Case 1: Maybe
- Problem Case 2: No
- Problem Case 3: No
- Problem Case 4: No

### Pagefile Carving
- Problem Case 1: No
- Problem Case 2: Yes
- Problem Case 3: No
- Problem Case 4: Yes

### Virtual Memory
- Problem Case 1: Yes
- Problem Case 2: No
- Problem Case 3: Yes
- Problem Case 4: No

### ... + Pagefile
- Problem Case 1: Yes
- Problem Case 2: Yes
- Problem Case 3: No
- Problem Case 4: No
Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Virtual Memory</td>
<td>Physical Memory</td>
</tr>
<tr>
<td>Pagefile</td>
<td></td>
<td>Pagefile</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Memory Carving</th>
<th>Maybe</th>
<th>No</th>
<th>No</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pagefile Carving</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Virtual Memory</td>
<td>Physical Memory</td>
</tr>
<tr>
<td>Pagefile</td>
<td>Pagefile</td>
<td>Pagefile</td>
<td>Pagefile</td>
</tr>
</tbody>
</table>

Memory Carving: Maybe, No
Pagefile Carving: No, Yes
Virtual Memory: Yes, No
... + Pagefile: Yes, Yes, Yes
Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Virtual Memory</td>
<td>Physical Memory</td>
</tr>
<tr>
<td>Pagefile</td>
<td></td>
<td>Pagefile</td>
<td></td>
</tr>
<tr>
<td>Memory Carving</td>
<td>Maybe</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Pagefile Carving</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Carving</td>
<td>Maybe</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Pagefile Carving</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>No</td>
<td>Maybe</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Diagram

[Diagram showing memory allocation and carving for each problem case]
### Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Memory</strong></td>
<td><strong>Physical Memory</strong></td>
<td><strong>Virtual Memory</strong></td>
<td><strong>Physical Memory</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pagefile</strong></td>
<td><strong>Pagefile</strong></td>
<td><strong>Pagefile</strong></td>
<td><strong>Pagefile</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Memory Carving</th>
<th>Pagefile Carving</th>
<th>Virtual Memory</th>
<th>... + Pagefile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maybe</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>Maybe</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

2015-05-18 | Michael Gruhn | FAU i1 | VirMA: NT
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Carving</td>
<td>Maybe</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Pagefile Carving</td>
<td>No</td>
<td>Yes</td>
<td>Maybe</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2015-05-18 | Michael Gruhn | FAU i1 | VirMA: NT
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Memory</strong></td>
<td><strong>Physical Memory</strong></td>
<td><strong>Virtual Memory</strong></td>
<td><strong>Physical Memory</strong></td>
</tr>
<tr>
<td><strong>Pagefile</strong></td>
<td><strong>Pagefile</strong></td>
<td><strong>Pagefile</strong></td>
<td><strong>Pagefile</strong></td>
</tr>
</tbody>
</table>

### Memory Carving
- **Problem Case 1**: Maybe
- **Problem Case 2**: No
- **Problem Case 3**: No
- **Problem Case 4**: No

### Pagefile Carving
- **Problem Case 1**: No
- **Problem Case 2**: Yes
- **Problem Case 3**: Maybe
- **Problem Case 4**: Yes

### Virtual Memory
- **Problem Case 1**: Yes
- **Problem Case 2**: No
- **Problem Case 3**: No
- **Problem Case 4**: Maybe

### ... + Pagefile
- **Problem Case 1**: Yes
- **Problem Case 2**: Yes
- **Problem Case 3**: Yes
- **Problem Case 4**: Yes
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th></th>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Memory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pagefile</td>
<td>Memory Carving</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Maybe</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2015-05-18 | Michael Gruhn | FAU i1 | VirMA: NT
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Virtual Memory</td>
<td>Physical Memory</td>
</tr>
<tr>
<td>Pagefile</td>
<td></td>
<td>Pagefile</td>
<td></td>
</tr>
<tr>
<td>Memory Carving</td>
<td>Maybe</td>
<td>No</td>
<td>Maybe</td>
</tr>
<tr>
<td>Pagefile Carving</td>
<td>No</td>
<td>Yes</td>
<td>Maybe</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2015-05-18 | Michael Gruhn | FAU i1 | VirMA: NT
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Memory</td>
<td>Physical Memory</td>
<td>Physical Memory</td>
<td>Physical Memory</td>
</tr>
<tr>
<td>Pagefile</td>
<td>Pagefile</td>
<td>Pagefile</td>
<td>Pagefile</td>
</tr>
<tr>
<td>Memory Carving</td>
<td>Maybe</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Pagefile Carving</td>
<td>No</td>
<td>Yes</td>
<td>Maybe</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2015-05-18 | Michael Gruhn | FAU i1 | VirMA: NT

25(20) /28
## Evaluation: Problem Cases

<table>
<thead>
<tr>
<th></th>
<th>Problem Case 1</th>
<th>Problem Case 2</th>
<th>Problem Case 3</th>
<th>Problem Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Carving</td>
<td>Maybe</td>
<td>No</td>
<td>No</td>
<td>Maybe</td>
</tr>
<tr>
<td>Pagefile Carving</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Maybe</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Maybe</td>
</tr>
<tr>
<td>... + Pagefile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Diagram:**

- **Virtual Memory**
- **Physical Memory**
- **Pagefile**
Evaluation: Windows NT Versions

Working code for:

- Windows 7 7600 x86 (with 32 Bit Paging and/or PAE Paging)
- Windows 7 7600 x64 (with IA32e Paging)
- Windows 8.1 9600 x86 (with 32-Bit Paging and/or PAE Paging)
- Windows 8.1 9600 x64 (with IA32e Paging)
- Windows 10 9841 x86 (with PAE Paging)
- Windows 10 9841 x64 (with IA32e Paging)

1https://www1.cs.fau.de/virma/ (Warning: Research Code!)
Conclusion and Future Work

Conclusion

- Incorporated pagefile.sys into Windows memory analysis
- Graybox Testing good method to find errors in tools

Future Work

- Windows NT Prototype PTEs
- File mappings
- Shared memory
- Do this for more operating systems
- Linux
- Mac OS X (Mach Kernel)
- Combined acquisition methods for physical memory and pagefile
### Conclusion and Future Work

#### Conclusion
- Incorporated pagefile.sys into Windows memory analysis
- Graybox Testing good method to find errors in tools

#### Future Work
- Windows NT Prototype PTEs
  - File mappings
  - Shared memory
- Do this for more operating systems
  - Linux
  - Mac OS X (Mach Kernel)
- Combined acquisition methods for physical memory and pagefile
Questions?

42.