



# Finding in Windows 10 ++

Omar Sardar

Dimitar Andonov



# Omar Sardar

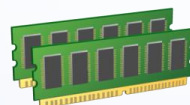
## ■ Staff Reverse Engineer @ FLARE

- Reverse engineer malware daily
- Automate reverse engineering
- Analyze **Windows Internals** for Product

## ■ Interests



 @osardar1

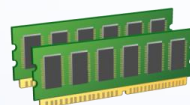


# Dimiter Andonov

- Sr. Staff Reverse Engineer @ **FLARE**
  - Reverse engineer malware daily
  - Bootkit & Rootkit analysis
  - Analyze **Windows Internals** for Product
- Interests



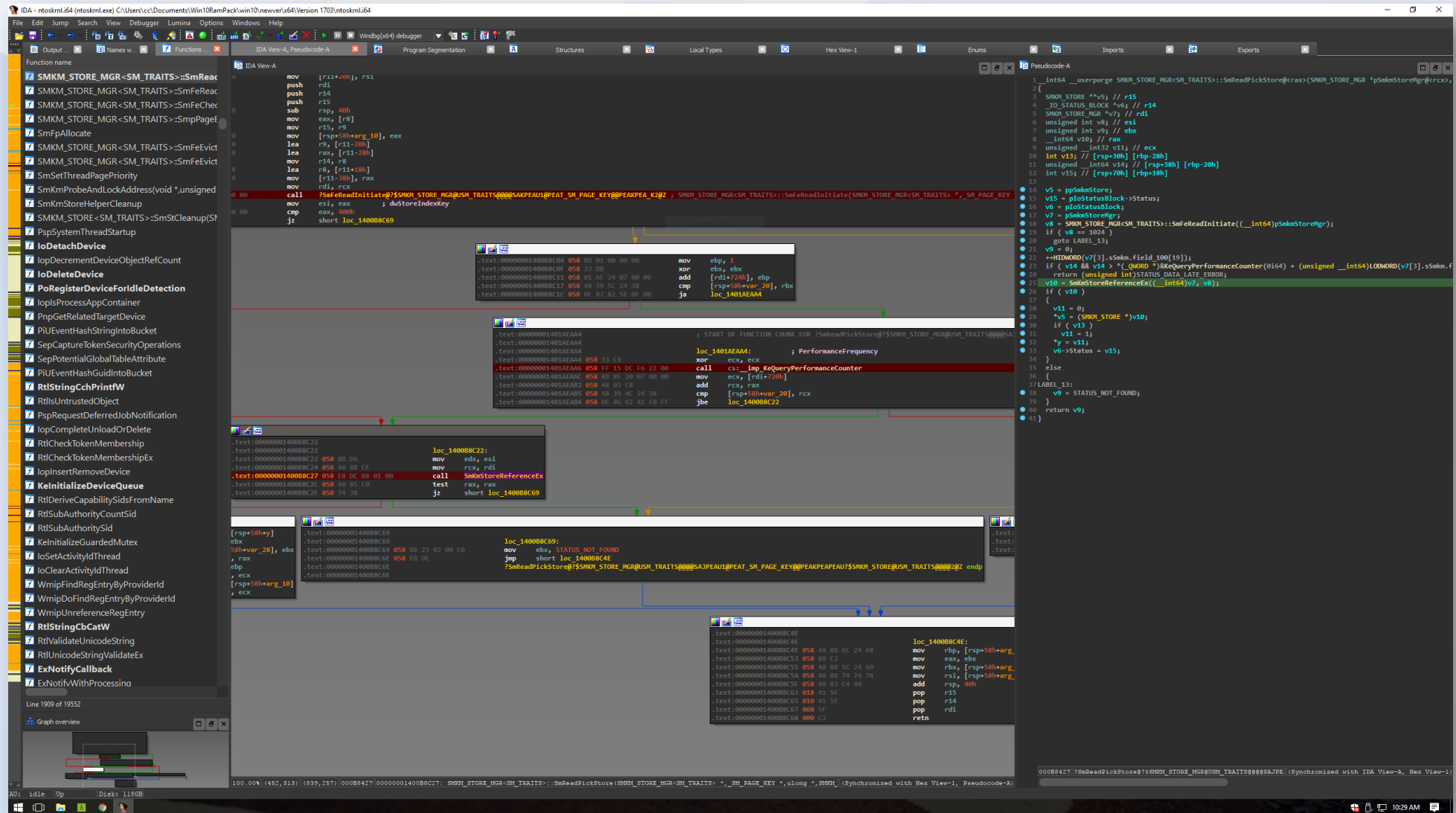
 @dandonov



# Story Time



# Obligatory IDA Screenshots



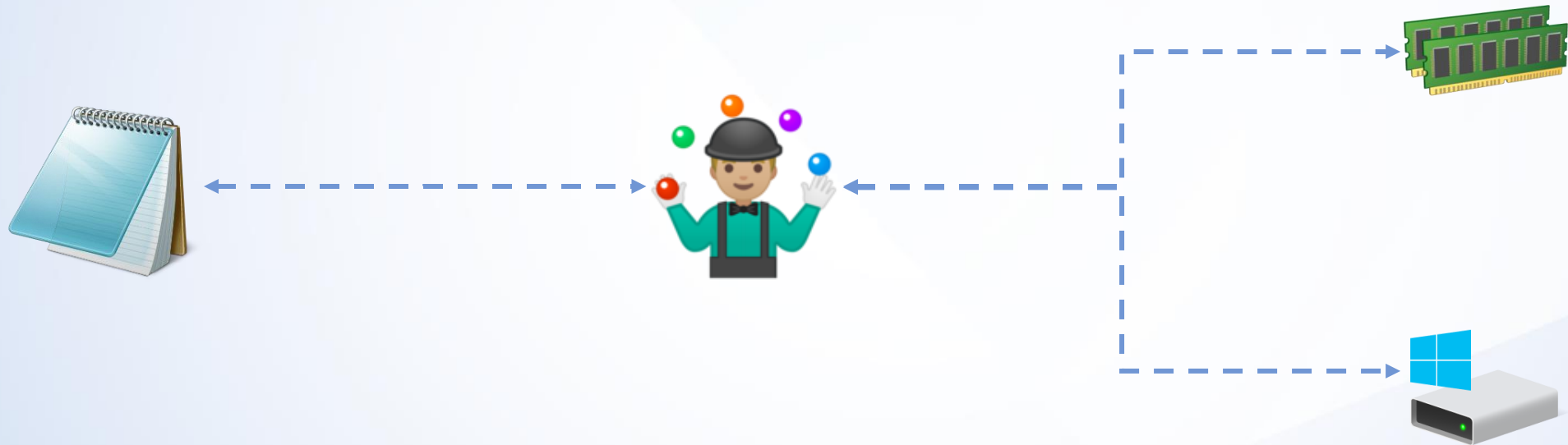
# Overview

- Memory Manager Crash Course
- Windows 10 Updates
- **Accessing Compressed Memory**
- **Automating Analysis**
- Volatility & Rekall Support
- Malware Extraction Demo
- Q&A



# Memory Manager Overview

- Provides process with **2GB to 128TB** memory
- Translates **virtual memory** to **physical memory**
- Moves data to-and-from hard drive (**paging**)
- Book-keeping





# Virtual Memory

- Windows grants a new x64 process with **8TB**
  - System doesn't have 8TB for each process
  - 8TB memory space is **virtual**
  - Data is accessed by reading from an **address**
  - **Pages** are 0x1000 bytes
  - Location of *actual* data is transparent



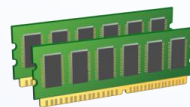
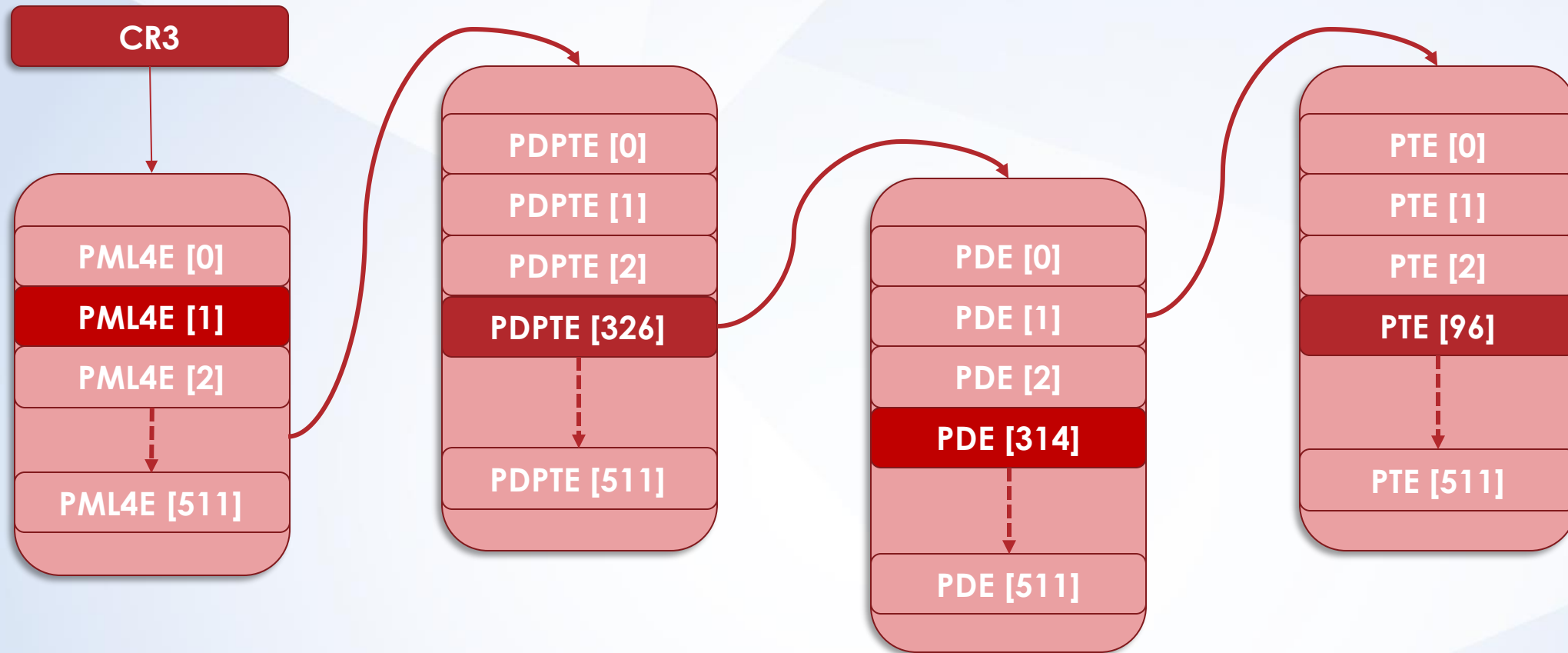


# Breaking Down a Virtual Address



- Memory address is a series of indices & offset
- Each index represents an entry in a table
- The last table contains **Page Table Entries**

# Page Tables (x64)

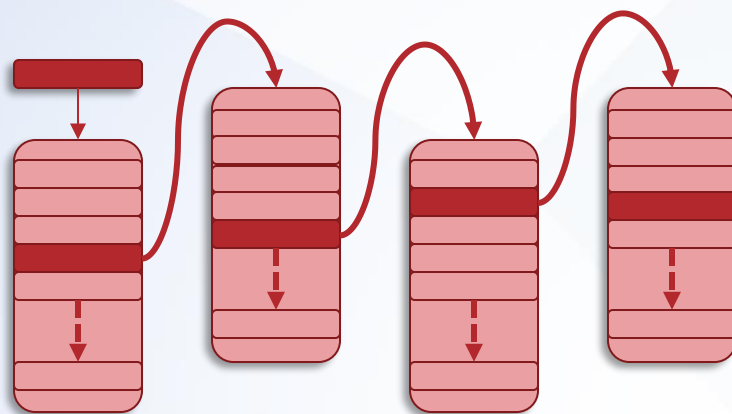


# Page Table Entries (PTEs)

```
kd> dt nt!_MMPTE*  
    ntkrnlmp!_MMPTE  
    ntkrnlmp!_MMPTE_SUBSECTION  
    ntkrnlmp!_MMPTE_HARDWARE  
    ntkrnlmp!_MMPTE_SOFTWARE  
    ntkrnlmp!_MMPTE_PROTOTYPE  
    ntkrnlmp!_MMPTE_TIMESTAMP  
    ntkrnlmp!_MMPTE_LIST  
    ntkrnlmp!_MMPTE_TRANSITION
```



# **\_MMPTE\_SOFTWARE**



Valid
PageFileReserved
PageFileAllocated
ColdPage
SwizzleBit
Protection
Prototype
Transition
<b>PageFileLow</b>
UsedPageTableEntries
ShadowStack
Unused
<b>PageFileHigh</b>

# \_MMPTE\_SOFTWARE Example

0: kd> !pte 24d026d0000

PXE at FFFFB359ACD66020  
contains 8A00000040015867  
pfn 40015 ---DA--UW-V

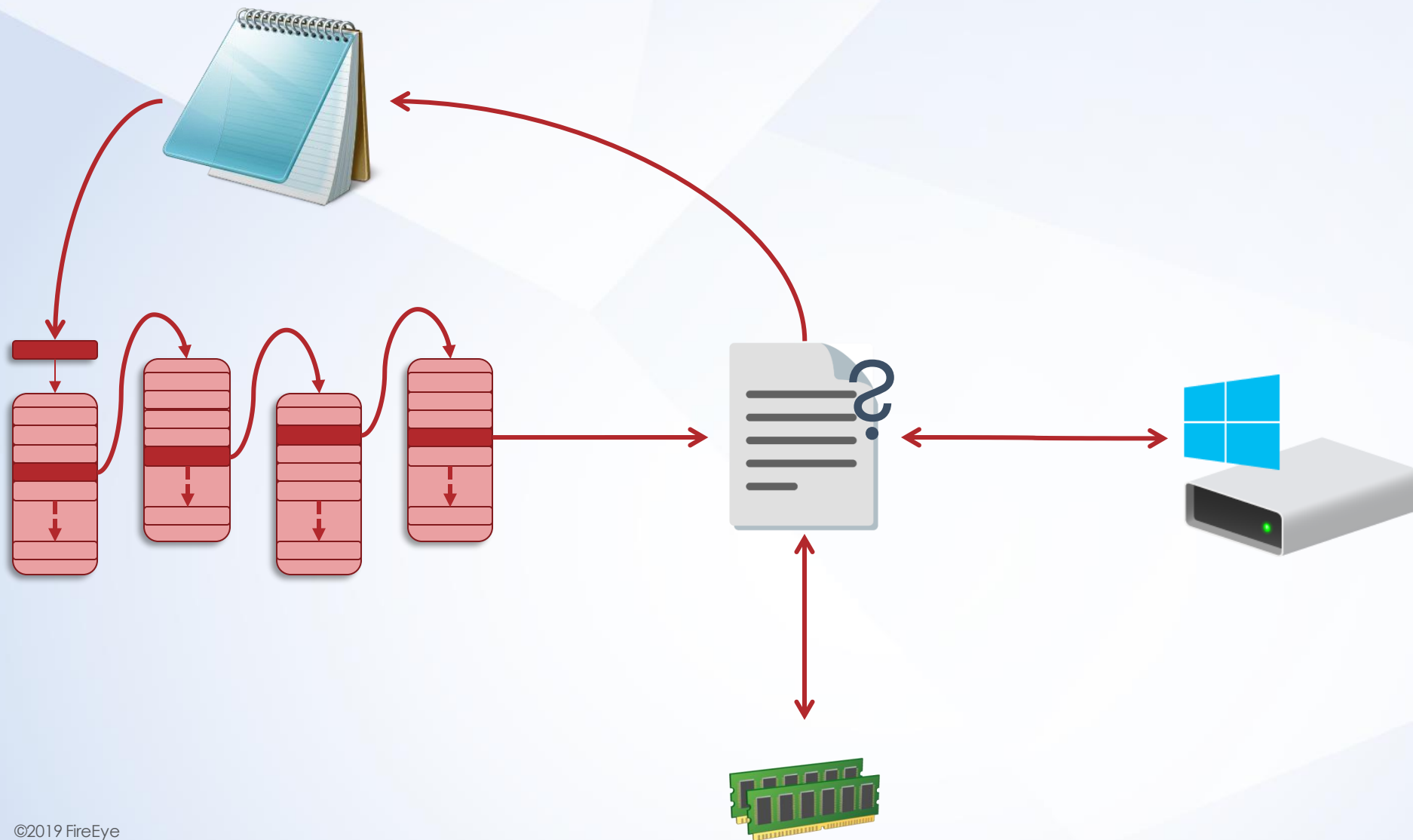
VA 0000024d026d0000  
PPE at FFFFB359ACC049A0 contains 0A00000040016867  
pfn 40016 ---DA--UWEV

PDE at FFFFB35980934098  
contains 0A00000074C22867  
pfn 74c22 ---DA--UWEV




PTE at FFFFB30126813680  
contains 00017A4D00002094  
not valid  
PageFile: 2  
Offset: 17a4d  
Protect: 4 - ReadWrite



# Demand-Paging Model



# Case for Compression

- Accessing data from a hard drive is 
- Accessing data from RAM is 
- Modern operating systems **compress memory** 
  - Allows for more data to be stored in RAM
  - Highly parallelizable operation
  - Flexible kernel deployment



# Mystery Pagefile

0: kd> !vm

Page File: \??\C:\pagefile.sys

Current:	1179648 Kb	Free Space:	1177968 Kb
----------	------------	-------------	------------

Minimum:	1179648 Kb	Maximum:	5168508 Kb
----------	------------	----------	------------

Page File: \??\C:\swapfile.sys

Current:	16384 Kb	Free Space:	16376 Kb
----------	----------	-------------	----------

Minimum:	16384 Kb	Maximum:	3144940 Kb
----------	----------	----------	------------

No Name for Paging File

Current:	7265136 Kb	Free Space:	6435008 Kb
----------	------------	-------------	------------

Minimum:	7265136 Kb	Maximum:	7265136 Kb
----------	------------	----------	------------





# MMPAGING\_FILE

- Structure used to represent traditional pagefiles
- Now supports Virtual Stores
- Check **VirtualStorePageFile** for confirmation
- Array of pagefiles located at **nt!MmPagingFile** 🥲






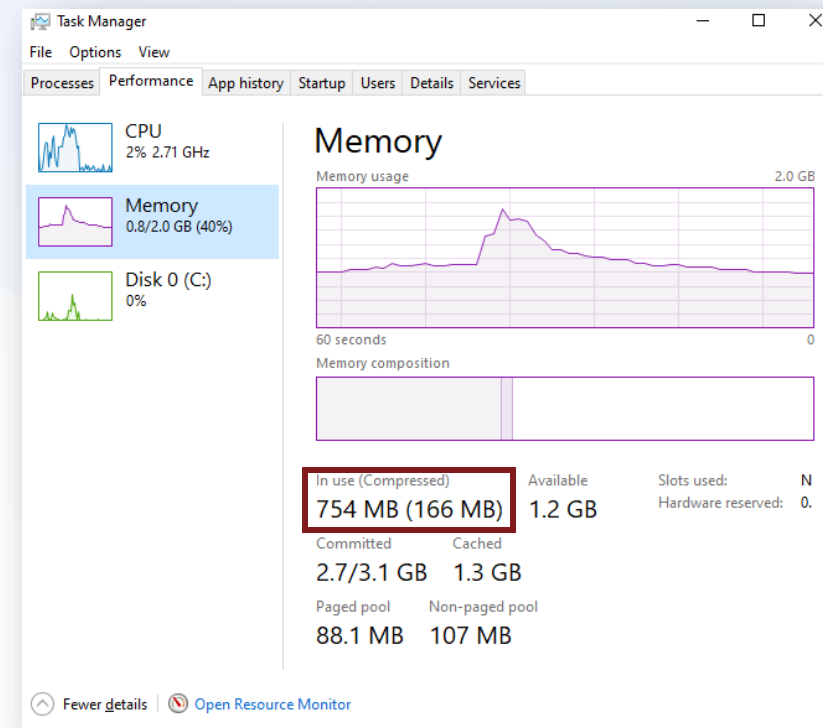
# Store Manager

- Storage allocation & content tracking
- Encryption & compression 
- Add, retrieve, or remove data
- Each **store page** is represented by a key 
- **Supports memory compression**

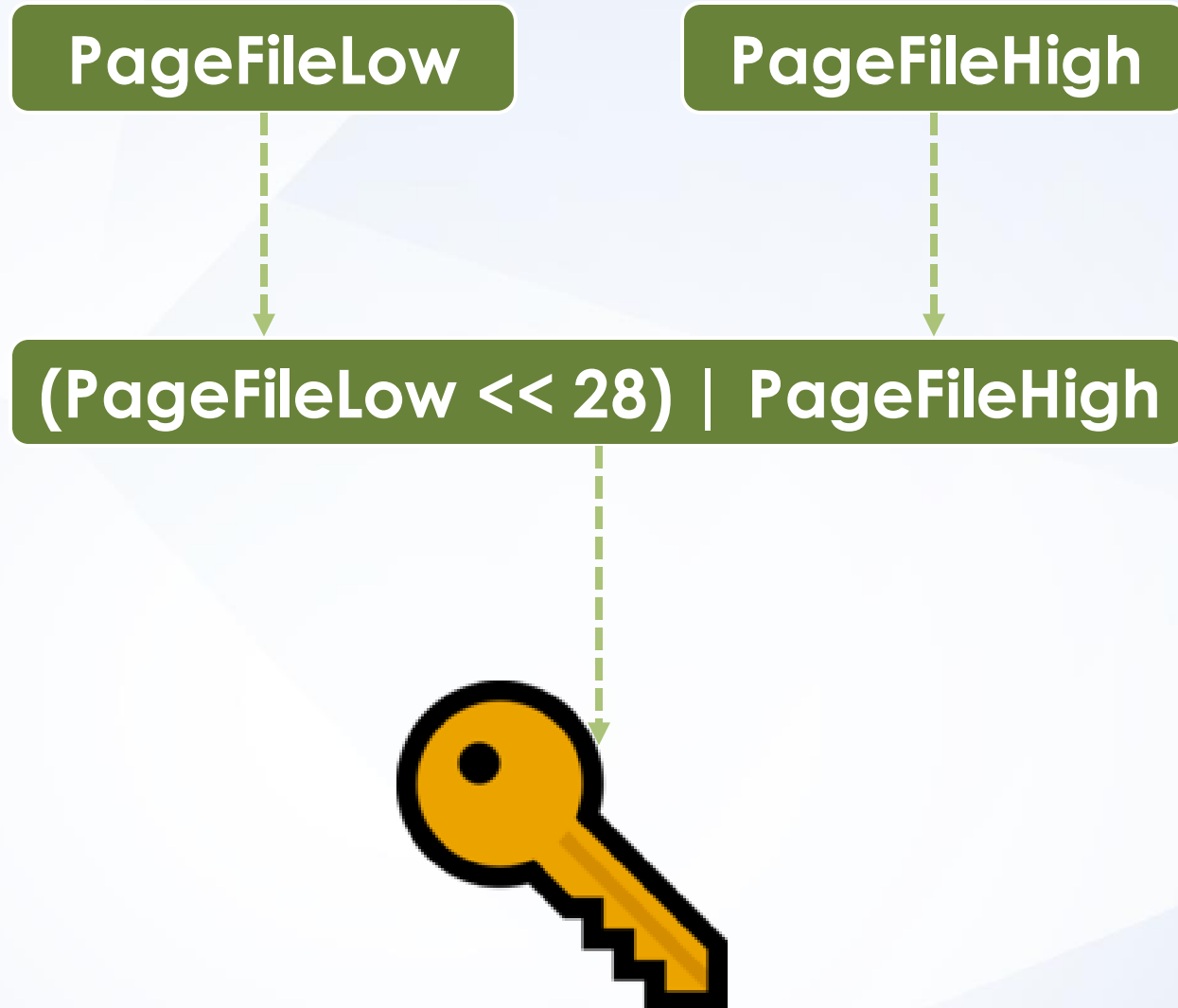
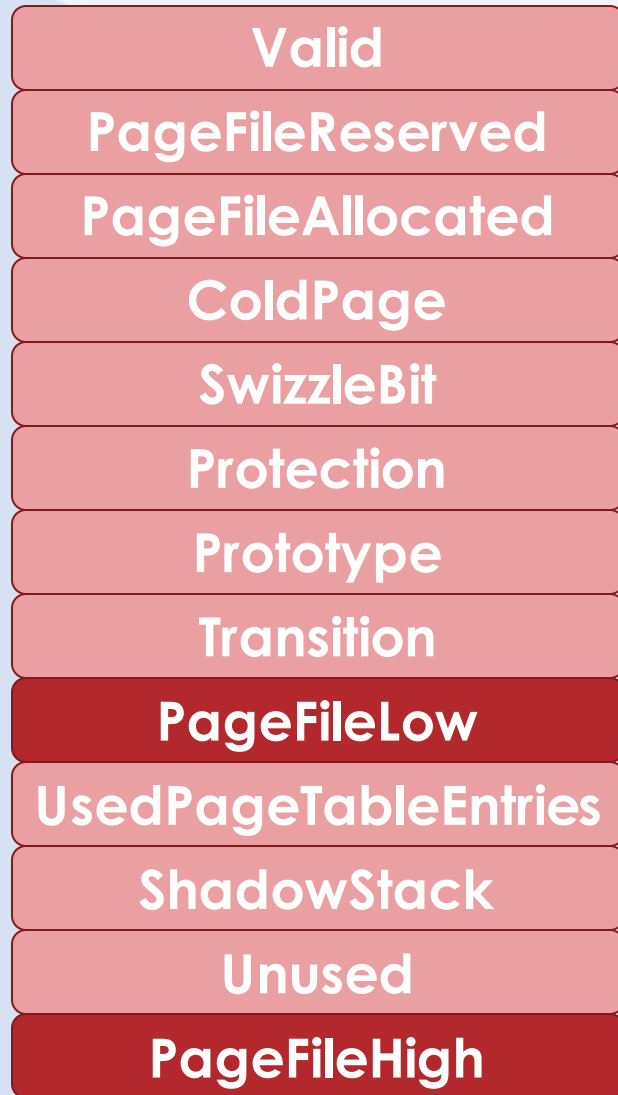


# Virtual Store

- Created by the **Store Manager**
- **XPRESS** Compression Format 
- Pages stored in **MemCompression**
- 1 Page  : 1 Key 



# Store Manager Page Key (ALG0)



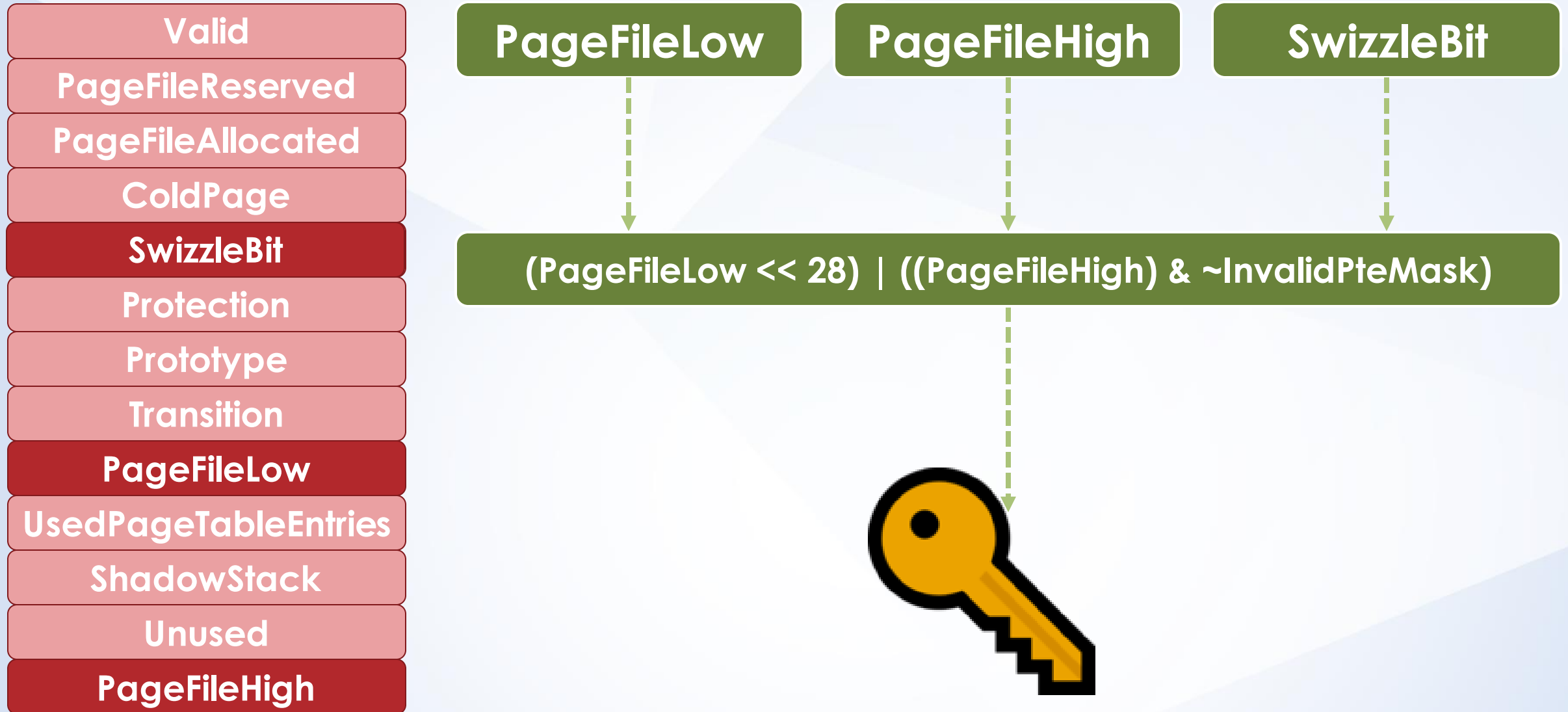
# SM\_PAGE\_KEY (ALGO)

```
PTE at FFFFB30126813680  
contains 00017A4D00002094  
not valid  
PageFile: 2  
Offset: 17a4d  
Protect: 4 - ReadWrite
```



20017A4D

# Store Manager Page Key (ALG1)





# SM\_PAGE\_KEY (ALG1)

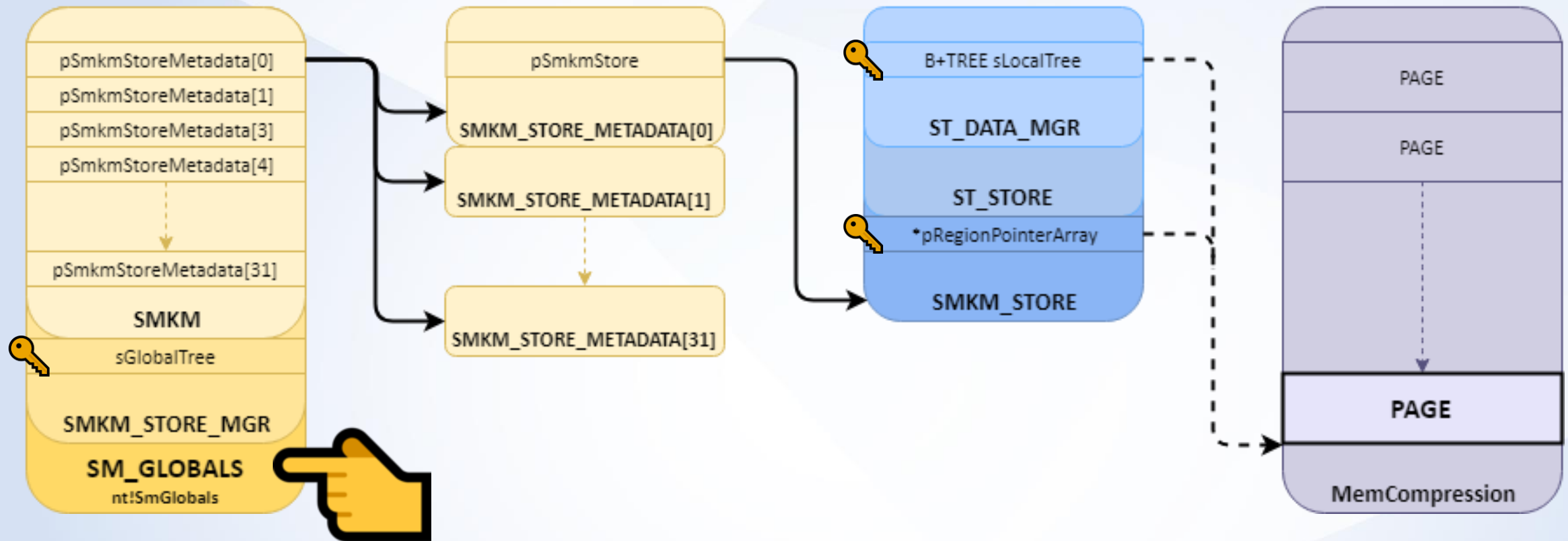
```
PTE at FFFF920149DF9B80  
contains 00026EDF00002084  
not valid  
PageFile: 2  
Offset: 24edf  
Protect: 4 - ReadWrite
```



20024EDF

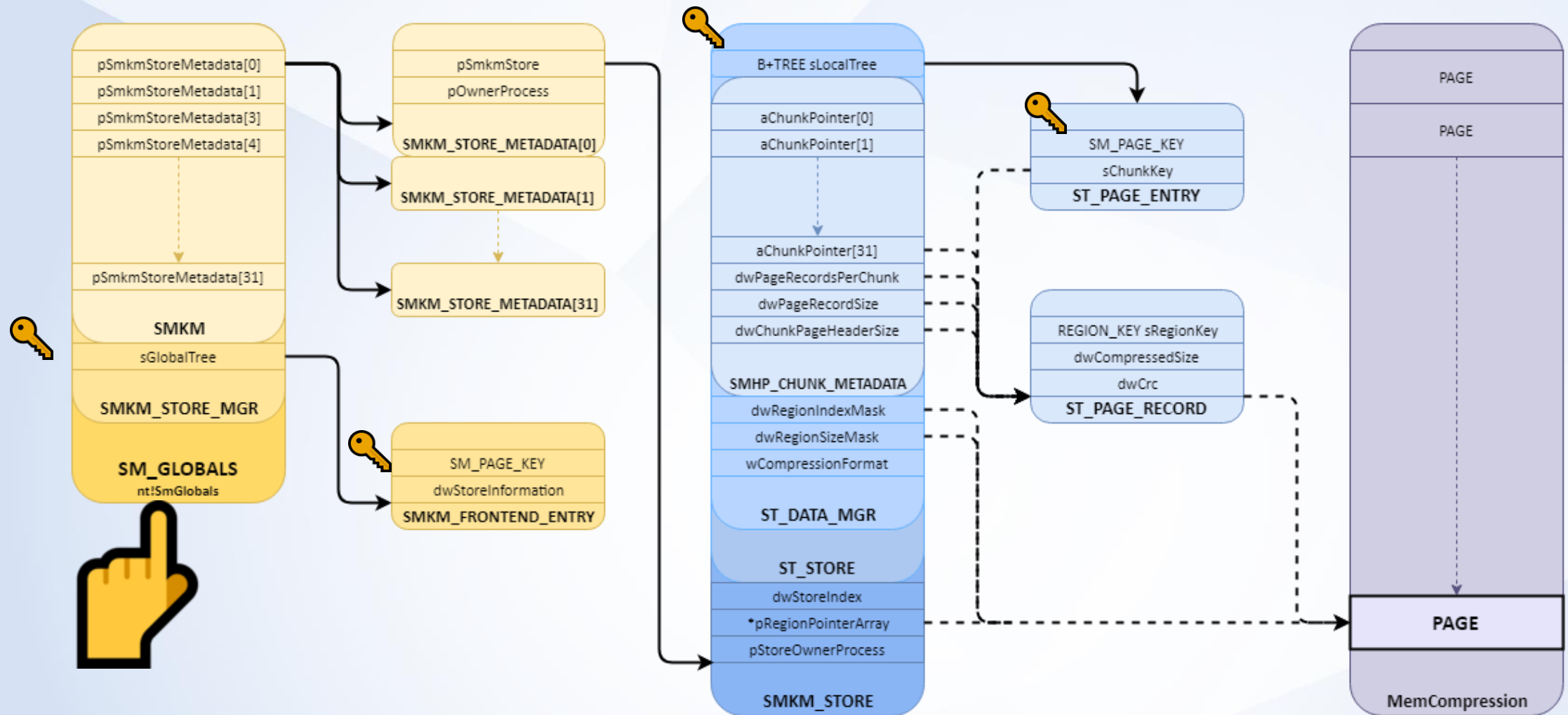
# Dude, Where's my Page?

W10.1607+



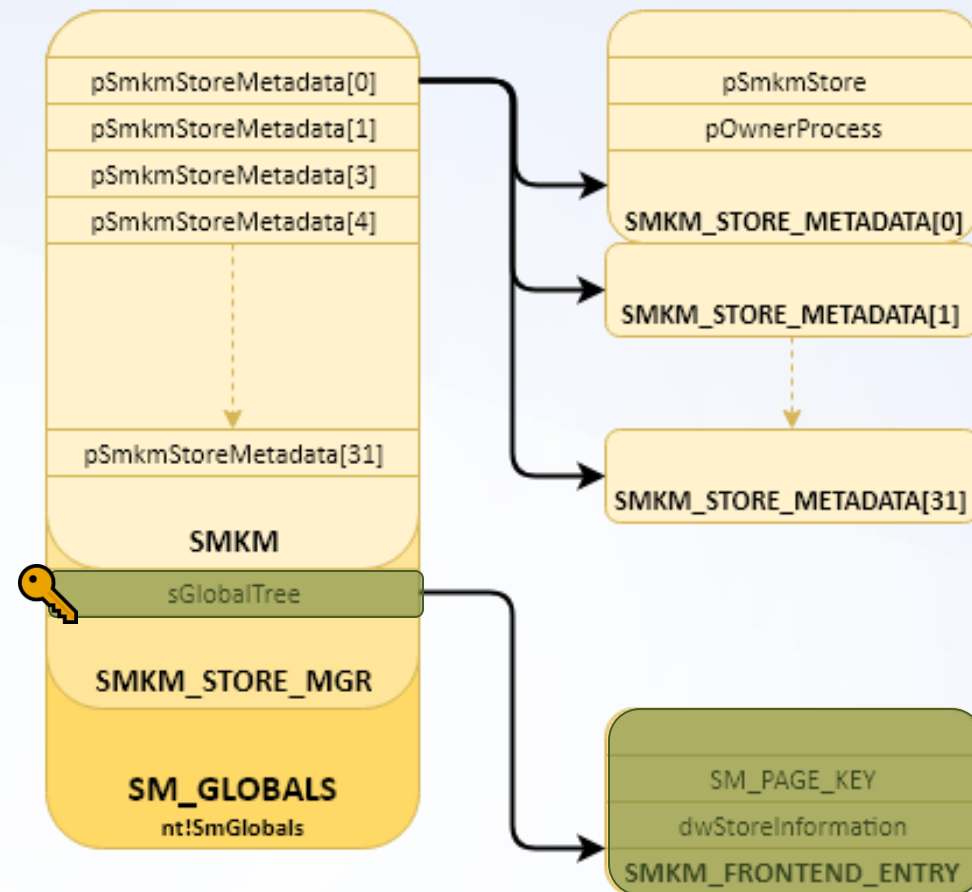
# Navigating the Store Manager

W10.1607+

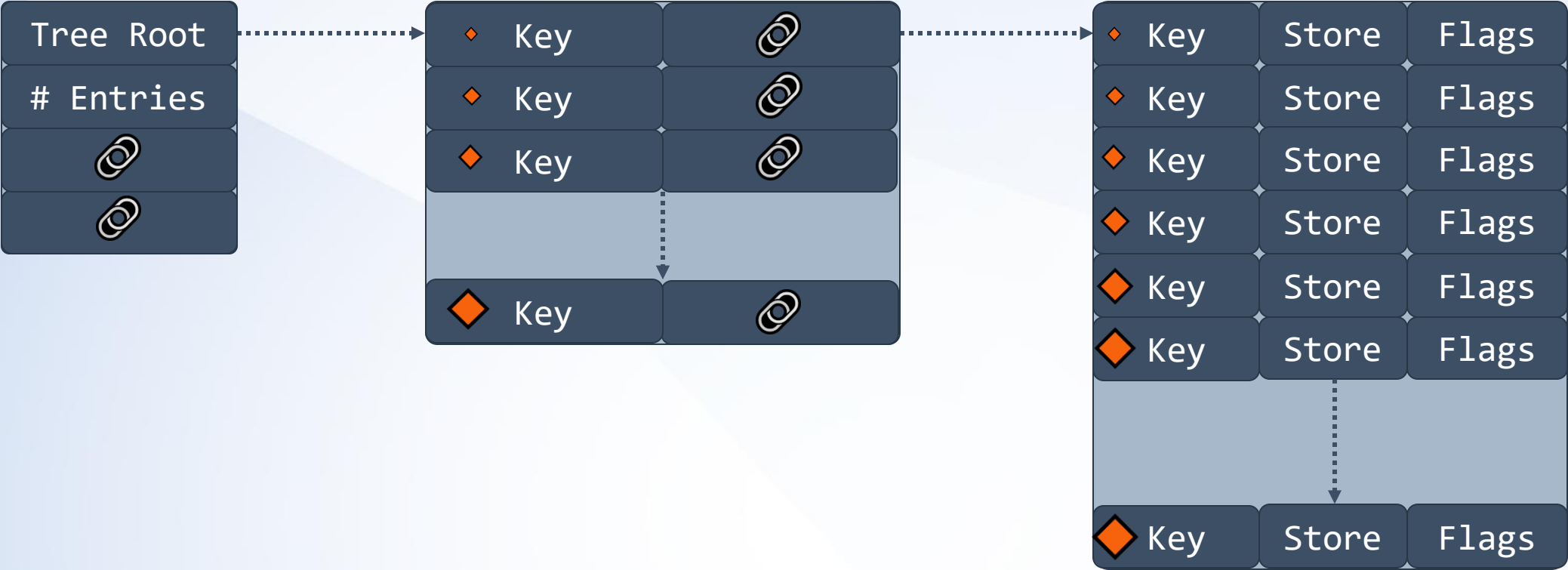


# Finding Your Store

- Journey begins at **nt!SmGlobals**
- Calculate **SM\_PAGE\_KEY**
- Search **B+TREE** for key
- Determine store containing key



# B+TREE Layout



# Traversing a B+TREE



a4163000
62,720

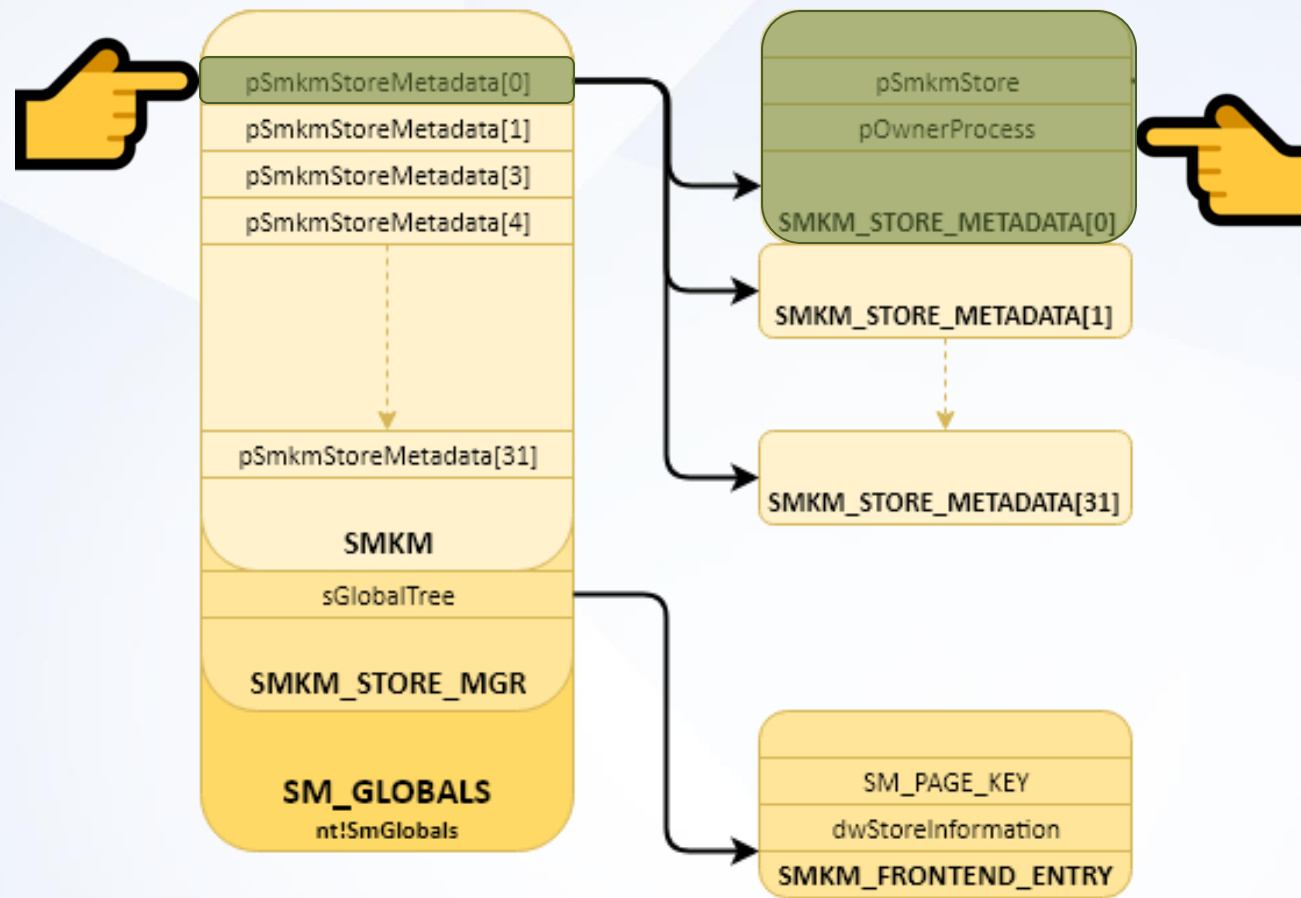
000200a2	a415d000
2001a210	a5c01000
2001c460	a875f000
2001e6bc	a2546000

2001a210	0000	3
2001ac16	0000	3
2001b687	0000	3
2001b688	0000	3
2001b689	0000	3
2001b68f	0000	
2001b691	0000	3



2001B68F

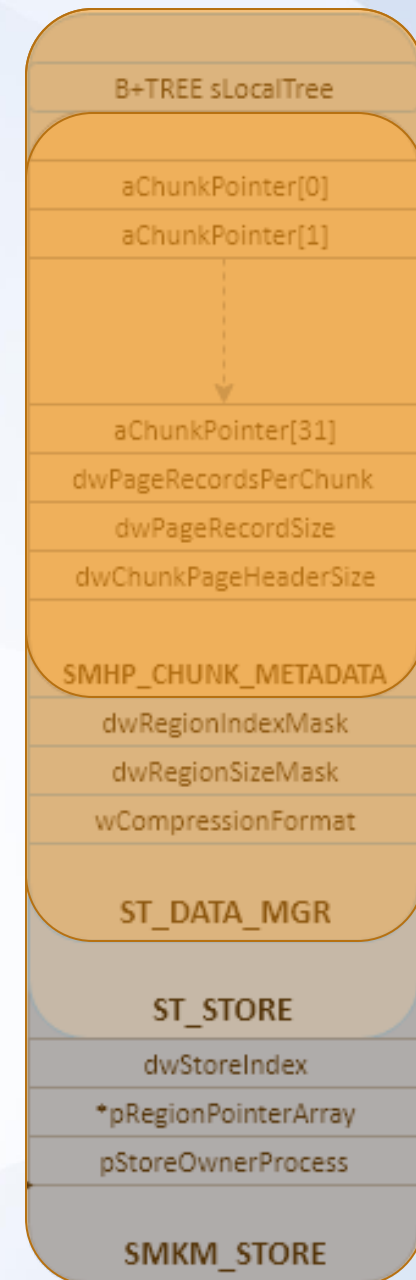
# Finding Your Store






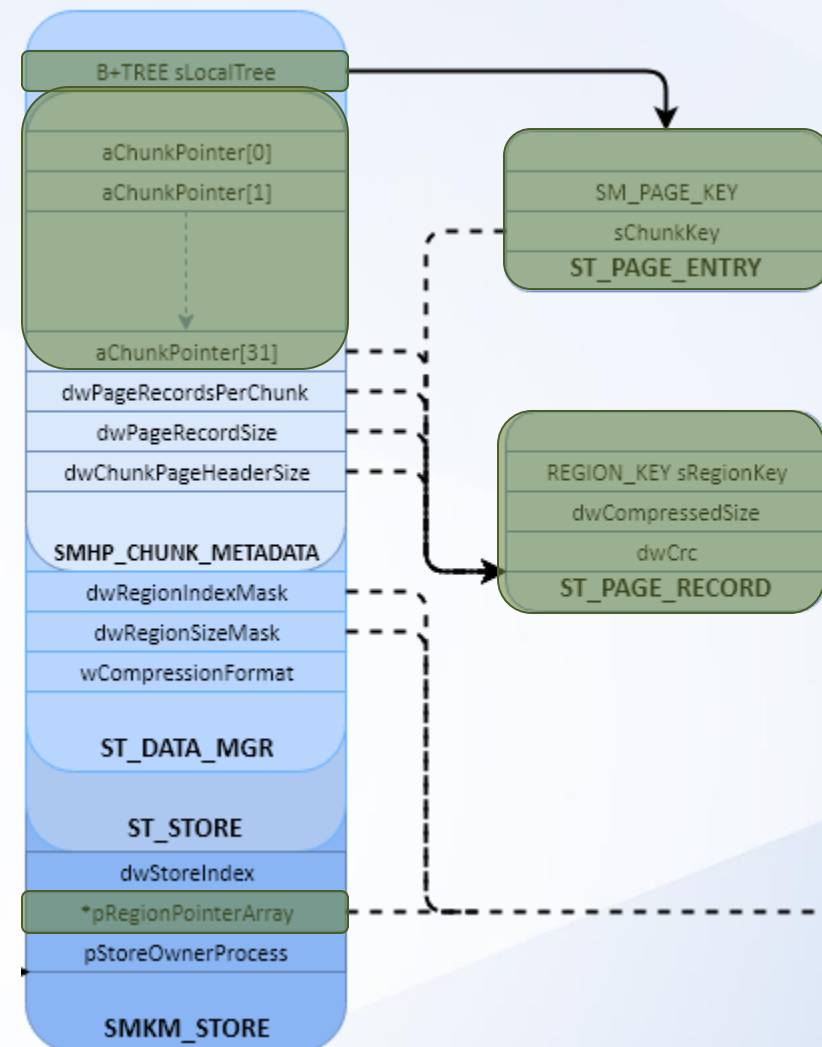
# SMKM\_STORE & Family 🧑👩👧

- Store-specific structures
  - All information leads to locating a page record
- SMKM\_STORE
  - Pointer to an array of pointers to regions of compressed pages
- ST\_DATA\_MGR
  - Chunk keys, compression format, region indices
- SMHP\_CHUNK\_METADATA
  - Array of chunks that contains vectors of page records



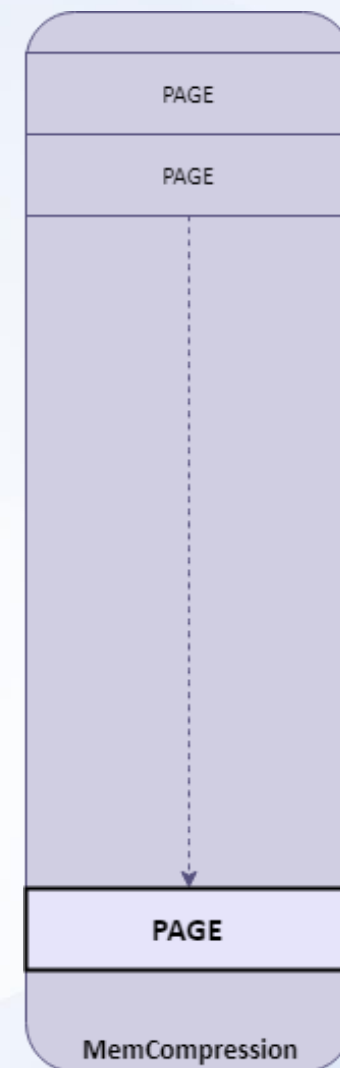
# Deriving Page Virtual Address

- Obtain **Chunk Key** from local B+TREE
- Chunks lead us to **ST\_PAGE\_RECORD**
- ST\_PAGE\_RECORD leads us to a **Region**
- Regions lead us to 

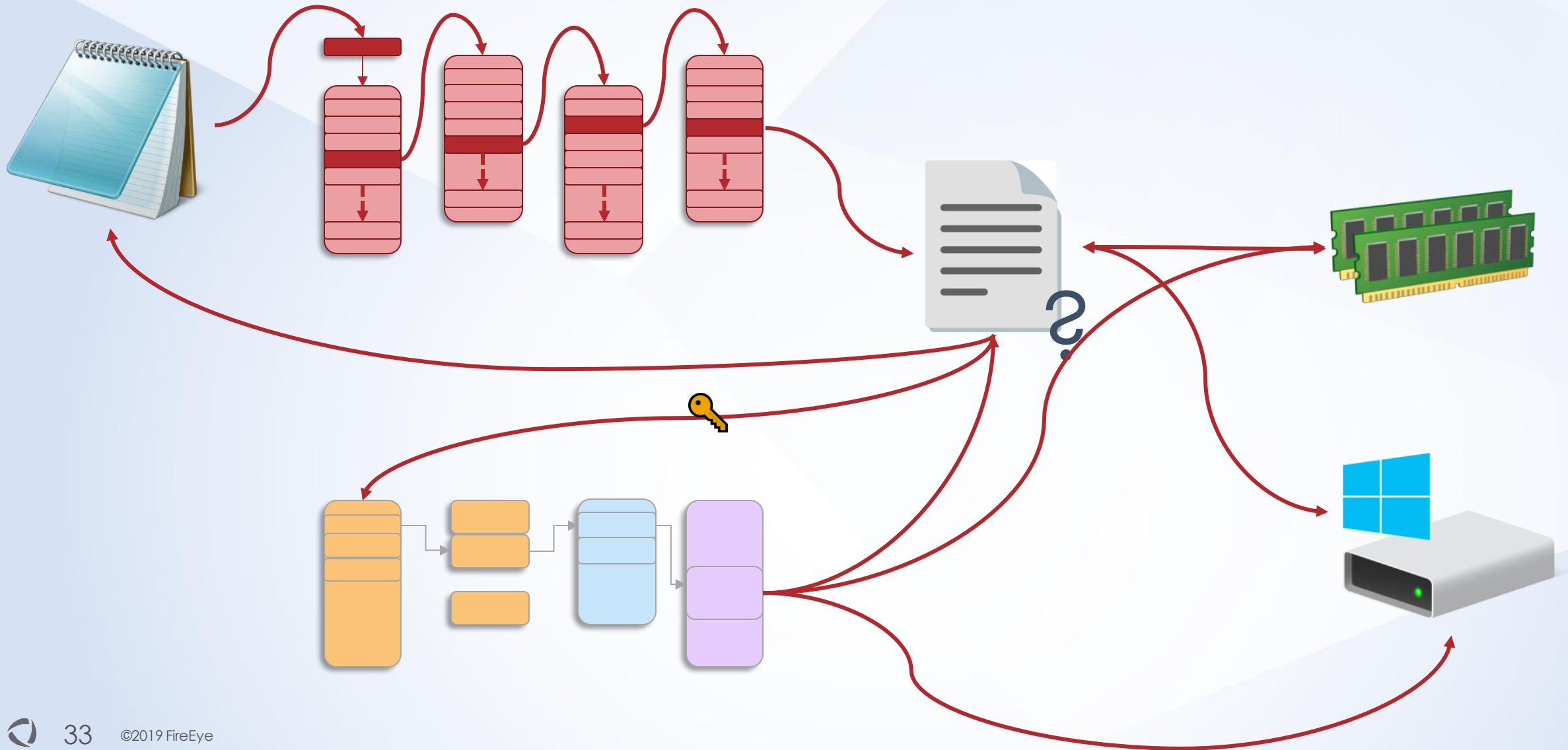


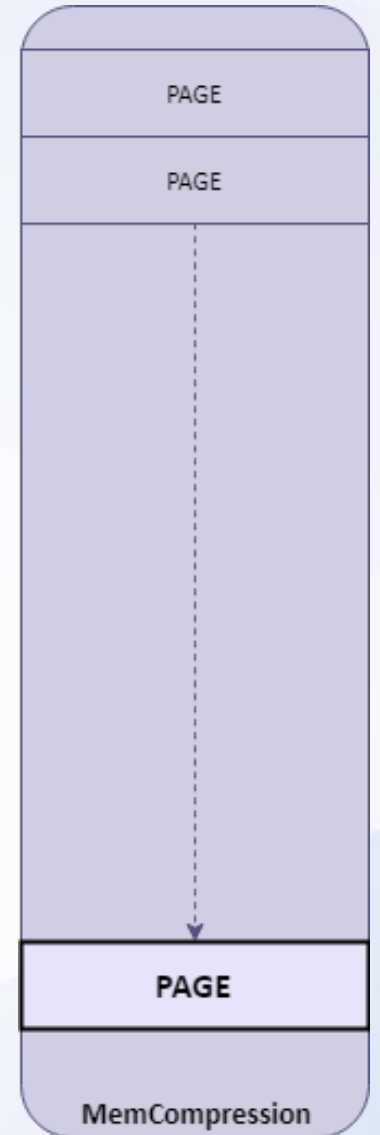
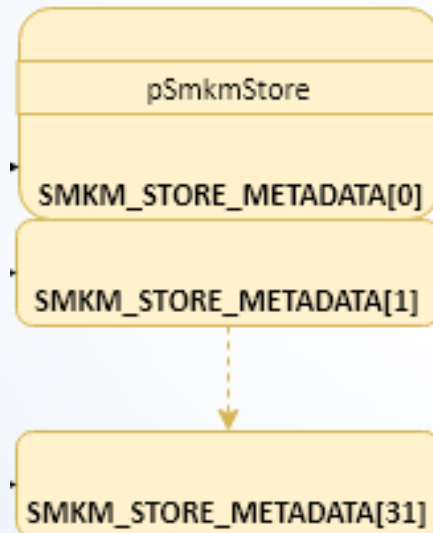
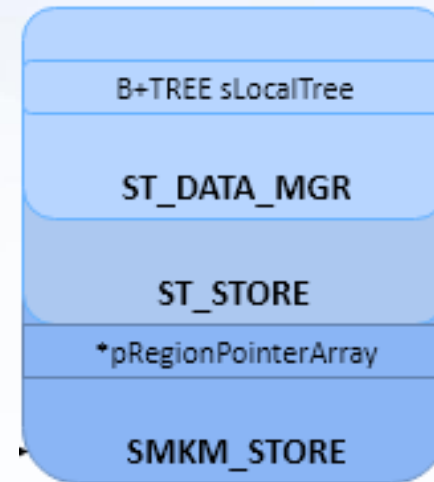
# MemCompression

- Compressed pages previously stored in System
- Storage container for all compressed data
- Minimal process
  - No PEB or user threads, NTDLL is not mapped
- Minimal threads (No TEB)
  - Page compression
  - Page read/write
  - Page swapping



# The Big Picture







# Structure Extraction Automation

Windows	10	0	17134	117
OS Name	Major	Minor	Build	Revision

- Structures change between **builds**
- Analysis effort is **~8h/kernel**
- Too many kernels
- Automated analysis desired



# FLARE-EMU

- IDA Pro ❤️ Unicorn
- Written by Tom Bennett @ **FLARE**
- Scriptable emulation framework 
- Rapid prototyping 





# FLARE-EMU

- Analyzed ~10 kernels manually
- Discovered commonalities
  - Structure locations
  - Function prototypes
  - Order of operations
  - Data usage patterns
  - Callstacks



# Automate This

```
.text:004A6A93 04C push [ebp+pWorkspace] ; pWorkspace
.text:004A6A96 050 lea ecx, [ebp+pdwFinalUncompressedSize]
.text:004A6A99 050 push ecx ; pdwFinalUncompressedSize
.text:004A6A9A 054 push eax ; dwCompressedBufferSize
.text:004A6A9B 058 movzx eax, word ptr [edi+220h]
.text:004A6AA2 058 push ebx ; pCompressedBuffer
.text:004A6AA3 05C push edx ; dwUncompressedBufferSize
.text:004A6AA4 060 push [ebp+pUncompressedBuffer] ; pUncompressedBuffer
.text:004A6AA7 064 push eax ; wCompressionFormat
.text:004A6AA8 068 call _RtlDecompressBufferEx@28 ; RtlDecompressBufferEx(x,x,x,x,x,x,x,x)
.text:004A6AAD 04C test eax, eax
.text:004A6AAF 04C js loc_547BCE
```



# FLARE-EMU

## ST\_DATA\_MGR

AaAbAcAdAeAfAgAhAiAjAkAlAmAnA  
oApAqArAsAtAuAvAwAxAyAzBaBbBc  
BdBeBfBgBhBiBjBkBlBmBnBoBpBqB  
rBsBtBuBvBwBxBzCaCbCcCdCeCf  
CgChCiCjCkClCmCnCoCpCqCrCsCtC  
uCvCwCxCyCzDaDbDcDdDeDfDgDhDi  
DjDkDlDmDnDoDpDqDrDsDtDuDvDwD  
xDyDzEaEbEcEdEeEfEgEhEiEjEkEl  
EmEnEoEpEqErEsEtEuEvEwExEyEzF  
aFbFcFdFeFfFgFhFiFjFkFlFmFnFo  
FpFqFrFsFtFuFvFwFxFyFzGaGbGcG  
dGeGfGgGhGiGjGkGlGmGnGoGpGqGr  
GsGtGuGvGwGxGyGzHaHbHcHdHeHfH  
gHhHiHjHkHlHmHnHoHpHqHrHsHtHu  
HvHwHxHyHzIaIbIcIdIeIfIgIhIiI  
jIkIlImInIoIpIqIrIsItIuIvIwIx  
IyIzJaJbJcJdJeJfJgJhJiJjJkJlJ  
mJnJoJpJqJrJsJtJuJvJwJxJyJzKa  
KbKcKdKeKfKgKhKiKjKkKlKmKnKoK  
pKqKrKsKtKuKvKwKxKyKzLaLbLcLd  
LeLflgLhLiLjLkLlLmLnLoLpLqLrL  
sLtLuLvLwLxLyLzMaMbMcMdMeMfMG




```
.text:004A6A93 04C push [ebp+pWorkspace] ; pWorkspace
.text:004A6A96 050 lea ecx, [ebp+pdwFinalUncompressedSize]
.text:004A6A99 050 push ecx ; pdwFinalUncompressedSize
.text:004A6A9A 054 push eax ; dwCompressedBufferSize
.text:004A6A9B 058 movzx eax, word ptr [edi+220h]
.text:004A6AA2 058 push ebx ; pCompressedBuffer
.text:004A6AA3 05C push edx ; dwUncompressedBufferSize
.text:004A6AA4 060 push [ebp+pUncompressedBuffer] ; pUncompressedBuffer
.text:004A6AA7 064 push eax ; wCompressionFormat
.text:004A6AA8 068 call _RtlDecompressBufferEx@28 ; RtlDecompressBufferEx(x,x,x,x,x,x,x)
.text:004A6AAD 04C test eax, eax
.text:004A6AAF 04C js loc_547BCE
```



# FLARE-EMU



0x20101000
0x1163
0x31001200
0x1423
0x20001400
 "Km"

AaAbAcAdAeAfAgAhAiAjAkAlAmAnAoApAqArAsAtAuAvAwAxAyAzBaBbBcBdBfBgBhBiBjBkBmBnBoBpBqBrBsBtBuBvBwBxBzCaCbCcCdCeCfCgChCiCjCkClCmCnCoCpCqCrCsCtCuCvCwCxCyCzDaDbDcDdDeDfDgDhDiDjDkDlDmDnDoDuDvDwDxDyDzEaEbEcEdEeEfEgEhEiEkElEmEnEoEpEqErEsEtEuEvEzFaFbFcFdFeFfFgFhFiFjFkFlFnFmFoFpFqFrFsFtFuFvFzGaGbGcGdGeGfGgGhGiGjGkGlGmGnGoGpGqGrGsGtGuGvGzHaHbHcHdHeHfHgHhHiHjHkHlHmHnHoHpHqHrHsHtHuHvHwHxHyHzIaIbIcIdIeIfIgIhIiIjIkIlImInIoIpIqIrIsItIuIvIwIxIyIzJaJbJcJdJeJfJgJhJiJjJkJlJmJnJoJpJqJrJsJtJuJvJwJxJyJzKaKbKcKdKeKfKgKhKiKjKlKnKoKpKqKrKsKtKuKvKwKzLaLbLcLdLeLfLgLhLiLjLkLlLmLnLoLpLqLrLsLtLuLvLwLxLyLzMzMbMcMdMeMfMG



# Field Offset Located

 >>>pattern.find("Km")

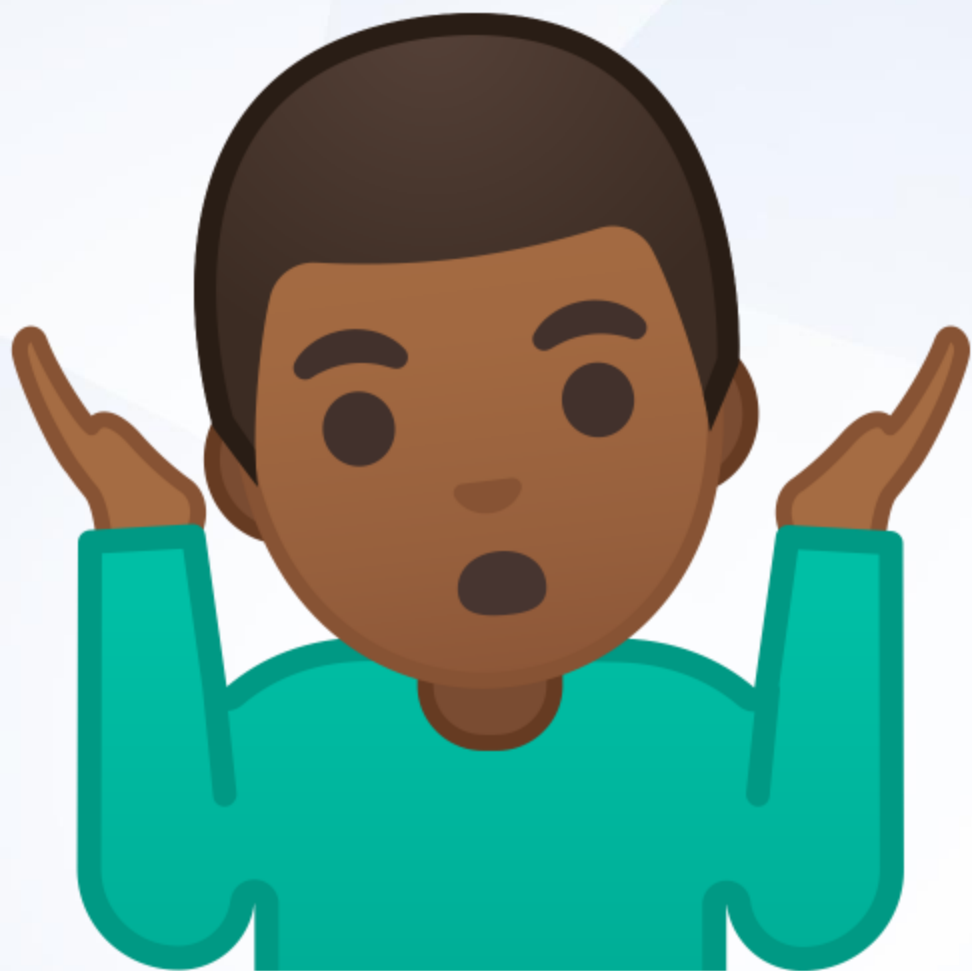
0x220

```
.text:004A6A93 04C push [ebp+pWorkspace] ; pWorkspace
.text:004A6A96 050 lea ecx, [ebp+pdwFinalUncompressedSize]
.text:004A6A99 050 push ecx ; pdwFinalUncompressedSize
.text:004A6A9A 054 push eax ; dwCompressedBufferSize
.text:004A6A9B 058 movzx eax, word ptr [edi+220h]
.text:004A6AA2 058 push ebx ; pCompressedBuffer
.text:004A6AA3 05C push edx ; dwUncompressedBufferSize
.text:004A6AA4 060 push [ebp+pUncompressedBuffer] ; pUncompressedBuffer
.text:004A6AA7 064 push eax ; wCompressionFormat
.text:004A6AA8 068 call _RtlDecompressBufferEx@28 ; RtlDecompressBufferEx(x,x,x,x,x,x,x)
.text:004A6AAD 04C test eax, eax
.text:004A6AAF 04C js loc_547BCE
```

# Rinse & Repeat

```
INFO:Magic:MAGIC.SmGlobals: 0x55a9c0  
INFO:Magic:MAGIC.MmPagingFile: 0x43e5e0
```

Python



“With **Windows 10** you're not getting data you'd expect because it's **compressed** in memory...”

- Andrew Case



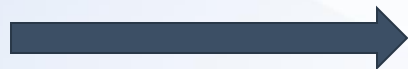
# Volatility & Rekall

- **FLARE** research integrated into plugins
  - Blaine Stancill (Volatility Lead)
  - Sebastian Vogl (Rekall Lead)



# Plugin's Baby Steps

Compressed Address



Decompressed Data



# volshell

```
In [1]: cc(pid=3676)
```

```
Current context: ram_eater.exe @ 0x9cc0d040, pid=3676, ppid=3548 DTB=0x3fffb780
```

```
In [2]: db(0x7c0000)
```

```
Memory unreadable at 007c0000
```



```
In [1]: cc(pid=3676)
```

```
Current context: ram_eater.exe @ 0x9cc0d040, pid=3676, ppid=3548 DTB=0x3fffb780
```

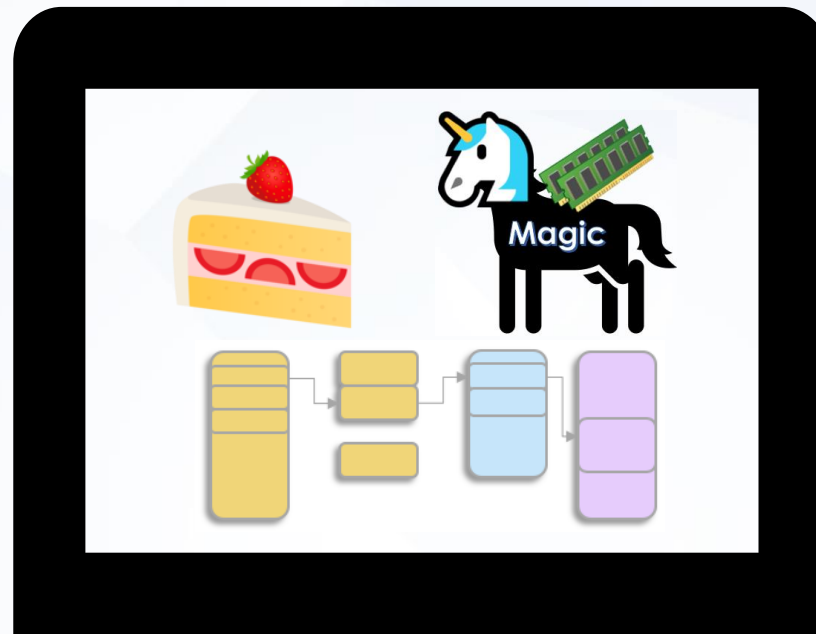
```
In [2]: db(0x7c0000)
```

```
0x007c0000  43 43 20 57 41 53 20 41 20 45 21 20 20 43 43  CC.WAS.HERE!..CC
0x007c0010  20 57 41 53 20 48 45 52 45 21 20 20 43 43 20 57  .WAS.HERE!..CC.W
0x007c0020  41 53 20 48 45 52 45 21 20 20 47 4f 54 27 45 4d  AS.HERE!..GOT'EM
0x007c0030  00 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58  .XXXXXXXXXXXXXXXXX
```



# Transparent Translation

cmdline  
cmdscan  
consoles  
crashinfo  
deskscan  
devicetree  
dlldump  
dlllist  
driverirp  
drivermodule  
driverscan  
dumpcerts  
dumpfiles



# modules

```
File
----
\SystemRoot\system32\ntoskrnl.exe
\SystemRoot\system32\hal.dll
\SystemRoot\system32\kdcom.dll
\SystemRoot\System32\drivers\msrpc.sys
\SystemRoot\System32\drivers\ksecdd.sys
\SystemRoot\System32\drivers\werkernel.sys
\SystemRoot\System32\drivers\tm.sys
\SystemRoot\system32\PSHED.dll
\SystemRoot\system32\BOOTVID.dll
\SystemRoot\System32\drivers\clipspace.sys
\SystemRoot\System32\drivers\cmimcext.sys
\SystemRoot\System32\drivers\ntosextd.sys
\SystemRoot\System32\drivers\cng.sys
```

```
File
----
\SystemRoot\system32\ntoskrnl.exe
\SystemRoot\system32\hal.dll
\SystemRoot\system32\kdcom.dll
\SystemRoot\system32\mcupdate_GenuineIntel.dll
\SystemRoot\System32\drivers\msrpc.sys
\SystemRoot\System32\drivers\ksecdd.sys
\SystemRoot\System32\drivers\werkernel.sys
\SystemRoot\System32\drivers\CLFS.SYS
\SystemRoot\System32\drivers\tm.sys
\SystemRoot\system32\PSHED.dll
\SystemRoot\system32\BOOTVID.dll
\SystemRoot\System32\drivers\FLTMGR.SYS
\SystemRoot\System32\drivers\clipspace.sys
\SystemRoot\System32\drivers\cmimcext.sys
\SystemRoot\System32\drivers\ntosextd.sys
\SystemRoot\system32\CI.dll
\SystemRoot\System32\drivers\cng.sys
```

# dlllist -p 2444

\*\*\*\*\*

SearchIndexer. pid: 2444

Command line : C:\Windows\system32\SearchIndexer.exe /Embedding

Base	Size	LoadCount	LoadTime	Path
0x00007ff655ec0000	0xea000	0xffff	2019-03-29 11:57:22 UTC+0000	C:\Windows\system32\SearchIndexer.exe
0x00007ffea9c20000	0x1db000	0xffff	2019-03-29 11:57:22 UTC+0000	C:\Windows\SYSTEM32\ntdll.dll
0x00007ffea96c0000	0xae000	0xffff	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\KERNEL32.DLL
0x00007ffea6ee0000	0x249000	0xffff	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\KERNELBASE.dll
0x00007ffea8ec0000	0x9d000	0x6	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\msvcrt.dll
0x00007ffea8670000	0x2f9000	0x6	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\combase.dll
0x00007ffea6cd0000	0xf6000	0x6	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\ucrtbase.dll
0x00007ffea98e0000	0x125000	0x6	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\RPCRT4.dll
0x00007ffea6dd0000	0x6a000	0x6	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\bcryptPrimitives.dll
0x00007ffea85c0000	0xaa000	0x6	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\shcore.dll
0x00007ffea9a50000	0xbf000	0x6	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\OLEAUT32.dll
0x00007ffea6e40000	0x9a000	0x6	2019-03-29 11:57:22 UTC+0000	C:\Windows\System32\msvcp_win.dll

# driverscan

Service Key	Name	Driver Name
acpiex	acpiex	\Driver\acpiex
CNG		\Driver\CNG
Wdf01000		\Driver\Wdf01000
cdrom	cdrom	\Driver\cdrom
WudfPf	WudfPf	\Driver\WudfPf
\Driver\PnpManager	PnpManager	\Driver\PnpManager
\Driver\DeviceApi	DeviceApi	\Driver\DeviceApi
\Driver\S...reDevice	Softw...vice	\Driver\SoftwareDevice
	WMIxWDM	\Driver\WMIxWDM
	ACPI_HAL	\Driver\ACPI_HAL
vm3dmp	vm3dmp	\Driver\vm3dmp
DXGKrnl		\Driver\DXGKrnl
FileCrypt	FileCrypt	\FileSystem\FileCrypt
Null	Null	\Driver\Null
vmrawdsk		\Driver\vmrawdsk
Beep	Beep	\Driver\Beep
BasicDisplay	BasicDisplay	\Driver\BasicDisplay
BasicRender		\Driver\BasicRender
AFD		\Driver\AFD
ws2ifsl	ws2ifsl	\Driver\ws2ifsl
Npfs		\FileSystem\Npfs
Msfs	Msfs	\FileSystem\Msfs
tdx	tdx	\Driver\tdx
NetBT		\Driver\NetBT

Service Key	Name	Driver Name
acpiex	acpiex	\Driver\acpiex
CNG	CNG	\Driver\CNG
Wdf01000	Wdf01000	\Driver\Wdf01000
cdrom	cdrom	\Driver\cdrom
WudfPf	WudfPf	\Driver\WudfPf
\Driver\PnpManager	PnpManager	\Driver\PnpManager
\Driver\DeviceApi	DeviceApi	\Driver\DeviceApi
\Driver\S...reDevice	Softw...vice	\Driver\SoftwareDevice
\Driver\WMIxWDM	WMIxWDM	\Driver\WMIxWDM
\Driver\ACPI_HAL	ACPI_HAL	\Driver\ACPI_HAL
vm3dmp	vm3dmp	\Driver\vm3dmp
DXGKrnl	DXGKrnl	\Driver\DXGKrnl
FileCrypt	FileCrypt	\FileSystem\FileCrypt
Null	Null	\Driver\Null
vmrawdsk	vmrawdsk	\Driver\vmrawdsk
Beep	Beep	\Driver\Beep
BasicDisplay	BasicDisplay	\Driver\BasicDisplay
BasicRender	BasicRender	\Driver\BasicRender
AFD	AFD	\Driver\AFD
ws2ifsl	ws2ifsl	\Driver\ws2ifsl
Npfs	Npfs	\FileSystem\Npfs
Msfs	Msfs	\FileSystem\Msfs
tdx	tdx	\Driver\tdx
NetBT	NetBT	\Driver\NetBT



# Idrmodules

Pid	Process
736	winlogon.exe
736	winlogon.exe
904	svchost.exe
600	dwm.exe
600	dwm.exe
600	dwm.exe
600	dwm.exe
580	svchost.exe
580	svchost.exe
980	svchost.exe
980	svchost.exe
1044	svchost.exe
1284	MsMpEng.exe
1284	MsMpEng.exe
1284	MsMpEng.exe
1284	MsMpEng.exe
1460	sihost.exe
2572	svchost.exe
2572	svchost.exe

MappedPath
\Windows\System32\user32.dll
\Windows\System32\gdi32full.dll
\Windows\System32\user32.dll
\Windows\System32\ntdll.dll
\Windows\System32\userenv.dll
\Windows\System32\sspicli.dll
\Windows\System32\bcryptprimitives.dll
\Program Files\Windows Defender\MsMpEng.exe
\Windows\System32\bcryptprimitives.dll
\Windows\System32\rpcrt4.dll
\Windows\System32\twinui.appcore.dll

MappedPath
\Windows\System32\user32.dll
\Windows\System32\sechost.dll
\Windows\System32\svchost.exe
\Windows\System32\gdi32full.dll
\Windows\System32\user32.dll
\Windows\System32\gdi32.dll
\Windows\System32\ntdll.dll
\Windows\System32\userenv.dll
\Windows\System32\sspicli.dll
\Windows\System32\KernelBase.dll
\Windows\System32\bcryptprimitives.dll
\Windows\System32\svchost.exe
\Program Files\Windows Defender\MsMpEng.exe
\ProgramData\Microsoft\Windows Defender\Definitions
\Windows\System32\bcryptprimitives.dll
\Windows\System32\rpcrt4.dll
\Windows\System32\twinui.appcore.dll
\Windows\System32\KernelBase.dll
\Windows\System32\kernel.appcore.dll



# hashdump

```
Volatility Foundation Volatility Framework 2.6.1
```

```
ERROR : volatility.debug : Unable to read hashes from registry
```

```
Volatility Foundation Volatility Framework 2.6.1
```

```
Administrator:500: : : :
```

```
Guest:501: : : :
```

```
DefaultAccount:503: : : :
```

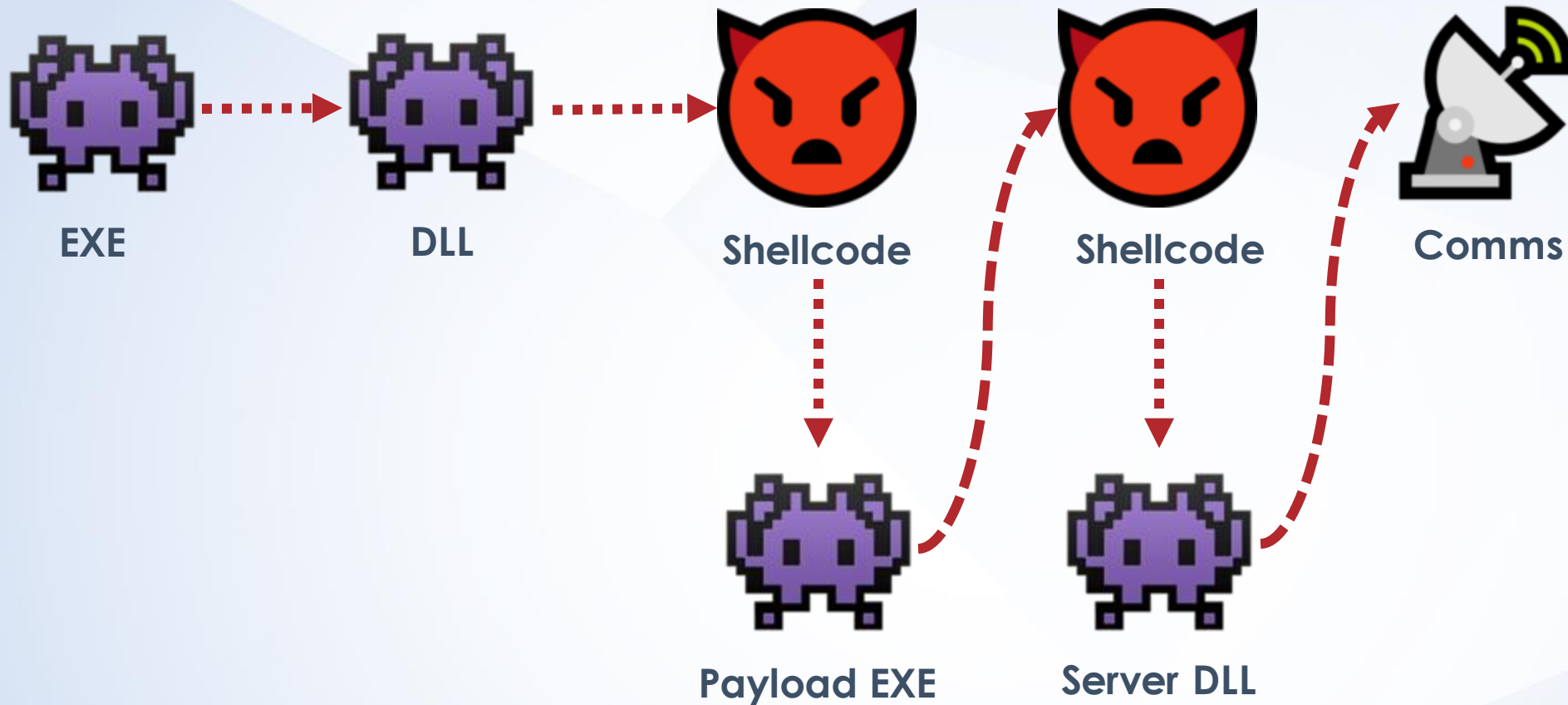
```
cc:1001: : : :
```



# Unlocked Data




# Malware Overview



# Get the Basics (imageinfo)

```
INFO      : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_17134, Win10x64_14393, Win10x64_10586, Win10x64_16299
          AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
          AS Layer2 : FileAddressSpace (/Do_Not_Scan/rampack/mw_fmtoptions/Win10_1709
          PAE type  : No PAE
                   DTB : 0x1aa000L
                   KDBG : 0xf803f894c4d0L
          Number of Processors : 2
          Image Type (Service Pack) : 0
                   KPCR for CPU 0 : 0xffffffff803f7919000L
                   KPCR for CPU 1 : 0xffffffff820021fa0000L
                   KUSER_SHARED_DATA : 0xffffffff780000000000L
          Image date and time : 2019-07-11 03:37:36 UTC+0000
          Image local date and time : 2019-07-10 20:37:36 -0700
```

# pstree

Name		Pid	PPid	Thds	Hnds	Time
0xffff99867074d5c0:csrss.exe		400	392	11	0	2019-07-09
0xffff998670b4b080:wininit.exe		480	392	2	0	2019-07-09
. 0xffff998670ba25c0:services.exe		620	480	7	0	2019-07-09
.. 0xffff9986708965c0:NisSrv.exe		2828	620	4	0	2019-07-09
.. 0xffff99866eab35c0:svchost.exe		1496	620	8	0	2019-07-09
0xffff9986721905c0:fmtoptions.exe		5684	4272	6	0	2019-07-11

# dlllist -p 5684

\*\*\*\*\*

fmtoptions.exe pid: 5684

Command line : Command line : c:\users\cc\netautocon\fmtoptions.exe 10002

Base	Size	LoadCount	LoadTime	Path
0x0000000000400000	0xe000	0xffff	2019-07-11 03:25:21 UTC+0000	c:\users\cc\netautocon\fmtoptions.exe
0x00007ffe7aa50000	0x1e0000	0xffff	2019-07-11 03:25:21 UTC+0000	C:\Windows\SYSTEM32\ntdll.dll
0x000000005e2d0000	0x51000	0xffff	2019-07-11 03:25:21 UTC+0000	C:\Windows\System32\wow64.dll
0x000000005e250000	0x76000	0x6	2019-07-11 03:25:21 UTC+0000	C:\Windows\System32\wow64win.dll
0x000000005e240000	0xa000	0x6	2019-07-11 03:25:21 UTC+0000	C:\Windows\System32\wow64cpu.dll
0x0000000000400000	0xe000	0xffff	2019-07-11 03:25:21 UTC+0000	c:\users\cc\netautocon\fmtoptions.exe
0x00000000771a0000	0x18d000	0xffff	2019-07-11 03:25:21 UTC+0000	C:\Windows\SYSTEM32\ntdll.dll
0x0000000074cb0000	0xd0000	0xffff	2019-07-11 03:25:21 UTC+0000	C:\Windows\System32\KERNEL32.DLL
0x0000000074f90000	0x1d7000	0xffff	2019-07-11 03:25:21 UTC+0000	C:\Windows\System32\KERNELBASE.dll
0x0000000073bb0000	0xa000	0x6	2019-07-11 03:25:21 UTC+0000	C:\Windows\System32\CRYPTBASE.dll
0x0000000076f30000	0x57000	0xffff	2019-07-11 03:25:21 UTC+0000	C:\Windows\System32\bcryptPrimitives.dll
0x0000000076c30000	0x43000	0x6	2019-07-11 03:25:21 UTC+0000	C:\Windows\System32\sechost.dll
0x000000006fd20000	0x5000	0x6	2019-07-11 03:25:2	c:\users\cc\netautocon\FmtOptions.dll Options.dll



# handles -p 5684 -t mutant

Offset(V)	Pid	Handle	Access	Type	Details
0xffff998671c19fc0	5684	0x188	0x1f0001	Mutant	SM0:5684:168:WilStaging_02
0xffff998670e6b060	5684	0x220	0x1f0001	Mutant	
0xffff998670c3c3d0	5684	0x228	0x1f0001	Mutant	
0xffff998671c2a2e0	5684	0x22c	0x1f0001	Mutant	
0xffff99867183be30	5684	0x230	0x1f0001	Mutant	
0xffff998672048c20	5684	0x234	0x1f0001	Mutant	
0xffff998671abb060	5684	0x238	0x1f0001	Mutant	
0xffff998671d22300	5684	0x23c	0x1f0001	Mutant	
0xffff998671e9b440	5684	0x284	0x1f0001	Mutant	CheckAndProtectProcessThread

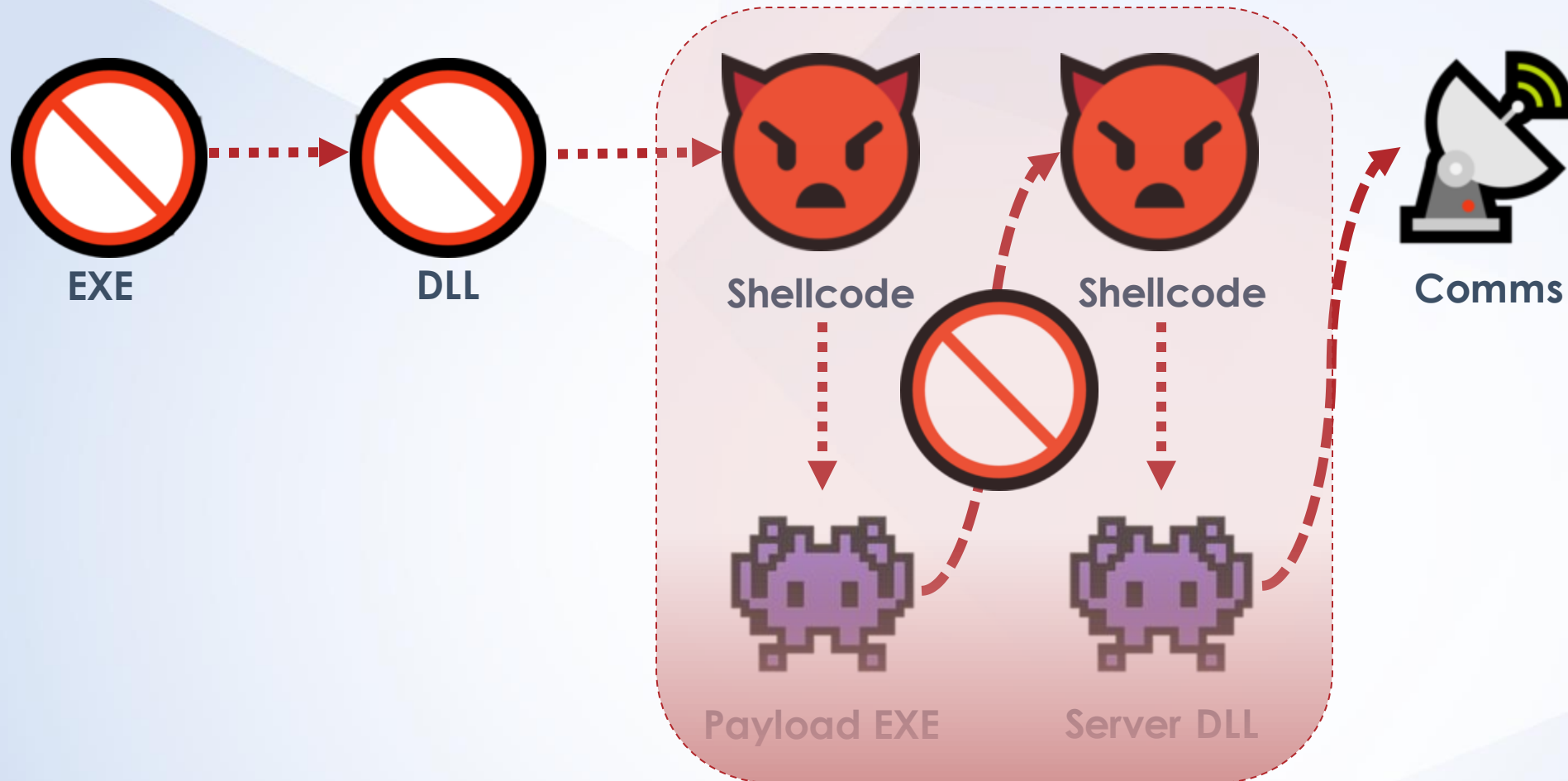
# Fails

- malfind
- handles (file)
- procdump
- dlldump
- vaddump





# Malware Overview



# handles -p 5684 -t mutant / file

Offset(V)	Pid	Handle	Access	Type	Details
0xffff998671c19fc0	5684	0x188	0x1f0001	Mutant	SM0:5684:168:WilStaging_02
0xffff998670e6b060	5684	0x220	0x1f0001	Mutant	
0xffff998670c3c3d0	5684	0x228	0x1f0001	Mutant	
0xffff998671c2a2e0	5684	0x22c	0x1f0001	Mutant	
0xffff99867183be30	5684	0x230	0x1f0001	Mutant	
0xffff998672048c20	5684	0x234	0x1f0001	Mutant	
0xffff998671abb060	5684	0x238	0x1f0001	Mutant	
0xffff998671d22300	5684	0x23c	0x1f0001	Mutant	
0xffff998671e9b440	5684	0x284	0x1f0001	Mutant	CheckAndProtectProcessThread
0xffff9986713a6160	5684	0x28c	0x1f0001	Mutant	Child-1634

Offset(V)	Pid	Handle	Access	Type	Details
0xffff998670b8de10	5684	0x3c	0x100020	File	\Device\HarddiskVolume2\Windows
0xffff998671ac3100	5684	0x84	0x100020	File	\Device\HarddiskVolume2\Users\cc\Desktop\FmtOptions
0xffff998671d94a20	5684	0xe0	0x100001	File	\Device\CNG
0xffff9986714ba9b0	5684	0x158	0x120089	File	\Device\DeviceApi\CMapi
0xffff998671a9f080	5684	0x29c	0x120089	File	\Device\HarddiskVolume2\Windows\SysWOW64\en-US\ntdll.dll
0xffff9986710cc700	5684	0x33c	0x100080	File	\Device\Nsi

# malfind -p 5684

```
Process: fntoptions.exe Pid: 5684 Address: 0x2740000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6
```

```
0x02740000 6a 00 e8 c9 4f 58 72 8d 90 1b 10 00 00 8b c5 8b
0x02740010 c8 8b 00 39 51 04 75 f7 c7 41 04 d0 10 d2 6f c3
0x02740020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x02740030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
0x02740000 6a00          PUSH 0x0
0x02740002 e8c94f5872       CALL 0x74cc4fd0
0x02740007 8d901b100000   LEA EDX, [EAX+0x101b]
0x0274000d 8bc5          MOV EAX, EBP
0x0274000f 8bc8          MOV ECX, EAX
0x02740011 8b00          MOV EAX, [EAX]
0x02740013 395104         CMP [ECX+0x4], EDX
0x02740016 75f7          JNZ 0x274000f
0x02740018 c74104d010d26f  MOV DWORD [ECX+0x4], 0x6fd
0x0274001f c3            RET
```

```
Process: fntoptions.exe Pid: 5684 Address: 0x4090000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6
```

```
0x04090000 e8 eb 89 07 00 e8 08 84 07 00 c3 55 8b ec 51 e8
0x04090010 00 00 00 00 5a 81 ea 00 00 00 00 89 55 fc 8b 45
0x04090020 fc 59 5d c3 e8 04 00 00 00 00 6a 0b 00 58 c3 e8
0x04090030 04 00 00 00 46 83 07 00 58 8b 00 c3 e8 46 83 07
```

```
0x04090000 e8eb890700       CALL 0x41089f0
0x04090005 e808840700       CALL 0x4108412
0x0409000a c3            RET
0x0409000b 55            PUSH EBP
0x0409000c 8bec          MOV EBP, ESP
0x0409000e 51            PUSH ECX
0x0409000f e800000000       CALL 0x4090014
0x04090014 5a            POP EDX
0x04090015 81ea00000000    SUB EDX, 0x0
0x0409001b 8955fc         MOV [EBP-0x4], EDX
```



## Shellcode

# malfind -p 5684

```
Process: fmtoptions.exe Pid: 5684 Address: 0x4200000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6
```

```
0x04200000 4d 5a 90 00 03 00 00 00 ff ff 00 00
0x04200010 b8 00 00 00 00 00 00 00 00 00 00 00
0x04200020 00 00 00 00 00 00 00 00 00 00 00 00
0x04200030 00 00 00 00 00 00 00 00 d8 00 00 00
```

```
0x04200000 4d      DEC EBP
0x04200001 5a      POP EDX
0x04200002 90      NOP
```

```
MZ.....
.....@.....
.....
.....
```

```
Process: fmtoptions.exe Pid: 5684 Address: 0x10000000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6
```

```
0x10000000 4d 5a 90 00 03 00 00 00 ff ff 00 00
0x10000010 b8 00 00 00 00 00 00 00 00 00 00 00
0x10000020 00 00 00 00 00 00 00 00 00 00 00 00
0x10000030 00 00 00 00 00 00 00 00 e0 00 00 00
```

```
0x10000000 4d      DEC EBP
0x10000001 5a      POP EDX
0x10000002 90      NOP
```

```
MZ.....
.....@.....
.....
.....
```

# Server DLL Strings

```
-POST / HTTP/1.1
Accept: text/plain, */*
Accept-Language: zh-cn
Host: 192.168.29.65:80
Content-Type: multipart/form-data; boundary=-----7db372eb000e2
UContent-Length: 3693
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: JSP3/2.0.14
Date: Thu, 28 Jul 2016 02:57:44 GMT
Content-Type: image/jpeg
Content-Length: 36669
Connection: keep-alive
ETag: 8954017092536739756
Last-Modified: Thu, 28 Jul 2016 01:18:01 GMT
Expires: Fri, 28 Jul 2017 01:46:45 GMT
Age: 4
bad allocation
Connect error
Recv error
Authentic error
127.0.0.1
```



RSDS

```
e:\WorkSpace\A4\A4-3.0\A4
\SvchostServer\bin\server.pdb
server.dll
```

http\_recv

http\_send

192.168.1.55

9000

192.168.1.119

9002

127.0.0.1

9000

192.168.0.54

1080

plugin\_key.binx



# Payload Strings

```
MY_START_SELF_MODE
SANDBOX
VIRUS
MALWARE
\SAMPLE
\VIRUS
%ssample.exe
%smalware.exe
IsNativeVhdBoot
kernel32
sbiedll.dll
Wow64DisableWow64FsRedirection
Wow64RevertWow64FsRedirection
IsWow64Process
advpack
```

```
Win10
Win8
WinNT
Win2000
WinXP
Win2003
2003 R2
Vista
Win2008
Win7
2008 R2
Win2012
Win8.1
2012 R2
```

FiFaBoy

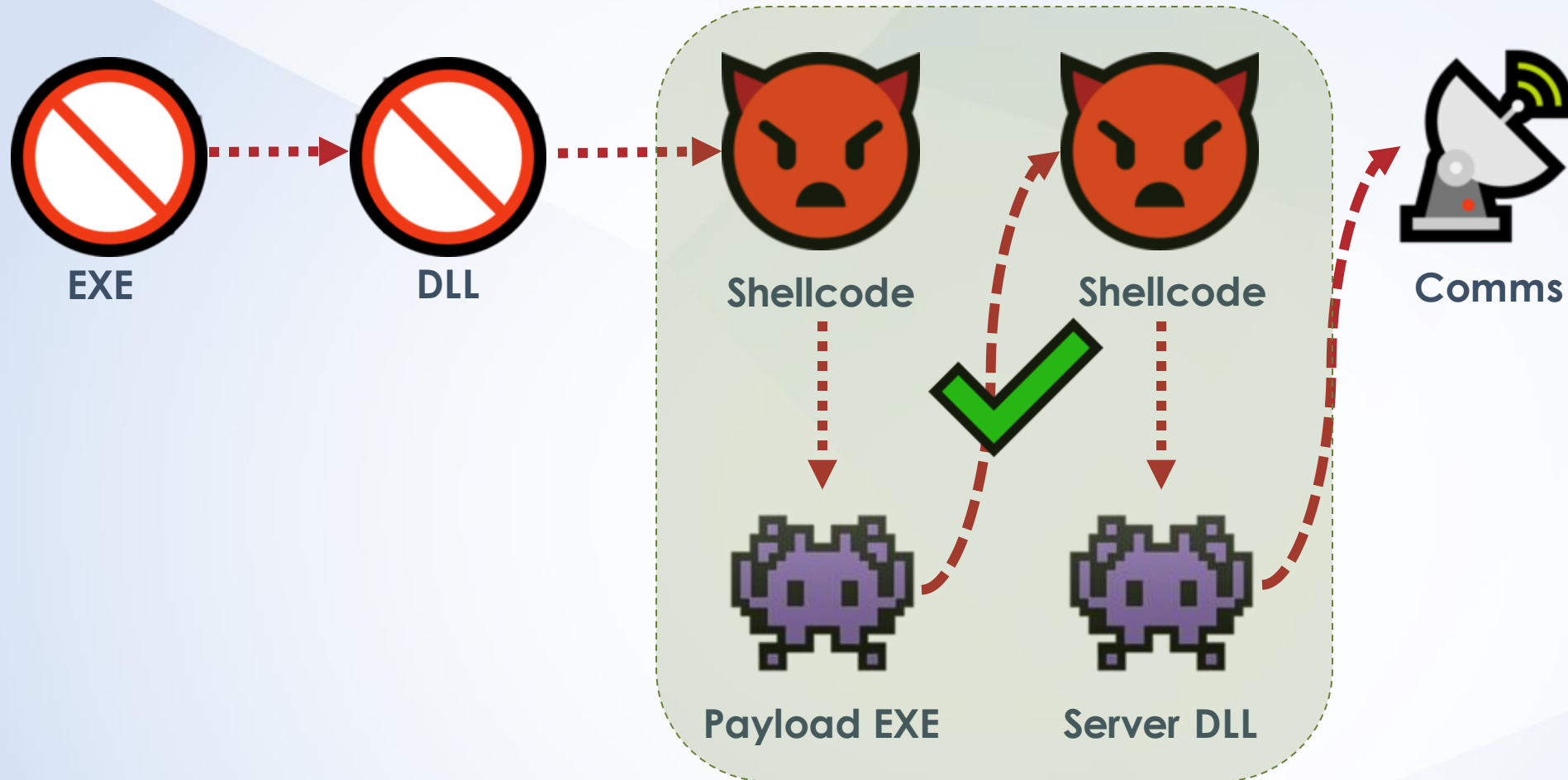
www.CeleWare.NET1-0+

fifaInternationale@hotmail.com1



```
CMD_KeepAlive 02
mythread
MY_MODULE_FILE
\net32.lib
Global\CheckAndProtectProcessThread
-CheckAndProtectProcessThread ERROR_ALREADY_
Global\Child-
```

# Malware Overview



# Enhanced Analysis



WWW.CeleWare.NET1



 Web

 Images

 Video

 News

 Shopping

Web Results

[signature-base/apt\\_ap30\\_backspace.yar at master · Neo23x0 ...](#)

[github.com](#)

Apr 13, 2015 ... \$s8 = "WWW.CeleWare.NET1" ascii. condition: filesize < 100KB and uint16(0) == 0x5A4D and 6 of them. } rule APT30\_Sample\_34 { . meta:.



# Call It a Day

```
rule APT30_Sample_33 {  
  meta:  
    description = "FireEye APT30 Report Sample - file 5eaf3deaaf2efac92c73ada82a651afe"  
    license = "https://creativecommons.org/licenses/by-nc/4.0/"  
    author = "Florian Roth"  
    reference = "https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf"  
    date = "2015/04/13"  
    hash = "72c568ee2dd75406858c0294ccfcf86ad0e390e4"  
  
  strings:  
    $s0 = "Version 4.7.3001" fullword wide  
    $s1 = "msmsgsr.exe" fullword wide  
    $s2 = "MYUSER32.dll" fullword ascii  
    $s3 = "MYADVAPI32.dll" fullword ascii  
    $s4 = "CeleWare.NET1" fullword ascii  
    $s6 = "MYMSVCRT.dll" fullword ascii  
    $s7 = "Microsoft(R) is a registered trademark of Microsoft Corporation in the" wide  
    $s8 = "WWW.CeleWare.NET1" ascii  
  
  condition:  
    filesize < 100KB and uint16(0) == 0x5A4D and 6 of them  
}
```



# The FLARE On Challenge

github.com/fireeye/flare-on.com



win10\_volatility



win10\_rekall



win10\_auto



flare-emu



**Omar Sardar** – Technical Lead (2016+)

**Claudiu Teodorescu** – Technical Lead (2016)

**Dimitar Andonov** – Windows Research (2017+)

**Blaine Stancill** – Volatility Integration (2019+)

**Sebastian Vogl** – Rekall Integration (2016+)



win10\_volatility



win10\_rekall



win10\_auto



flare-emu