Memory Anti-Anti Forensics in a Nutshell

Aborting the Abort Factor

Diego Fuschini
Tony Rodrigues, CISSP

www.octanelabs.net

#whoami

- Tony Rodrigues, CISSP, CFCP, Security+
- 20++ anos em TI
  - Desenvolvimento
  - Contingência
  - Segurança de Informações/Computação Forense
- Perito em DFIR
- Fundador e Pesquisador-Chefe do OctaneLabs
- Blog: http://forcomp.blogspot.com

OCTANE LABS

#whoami

- Diego Fuschini
  - Bacharel em Direito
  - Especialista em Direito e Tecnologia
  - BS Computer Forensics & Digital Investigation
- Perito em DFIR
- Coordenador de Pesquisas do OctaneLabs

OCTANE LABS

Agenda

- Computer Forensics and Memory Forensics importance
- Memory Forensics - How to
- Windows Memory in a Nutshell
- Do you remember those errors in your memory dump ?
- Abort Factor
- Attacking the Memory
- Can we revert it ?
- Aborting the Abort Factor
- Conclusions

Computer Forensics and Memory Forensics Importance

OCTANE LABS

CF - Memory Forensics Importance

- Muito tempo e dificuldade localizar malware volume de dados
  - Analise *Post Mortem*
- Facilmente derrotada por malwares (hooking) e parsing offline não usa API sistema
  - Analise *Live*
- Melhor relação esforço resultado!!
  - Análise Dump Memória

OCTANE LABS

CF - Memory Forensics Importance

- Processo realizado em apenas 2 etapas
  - Coleta da memória (Dump)
  - Análise do dump
- Consegue identificar
  - Dados não alocados (processos terminados)
  - Processos estejam ocultos

OCTANE LABS

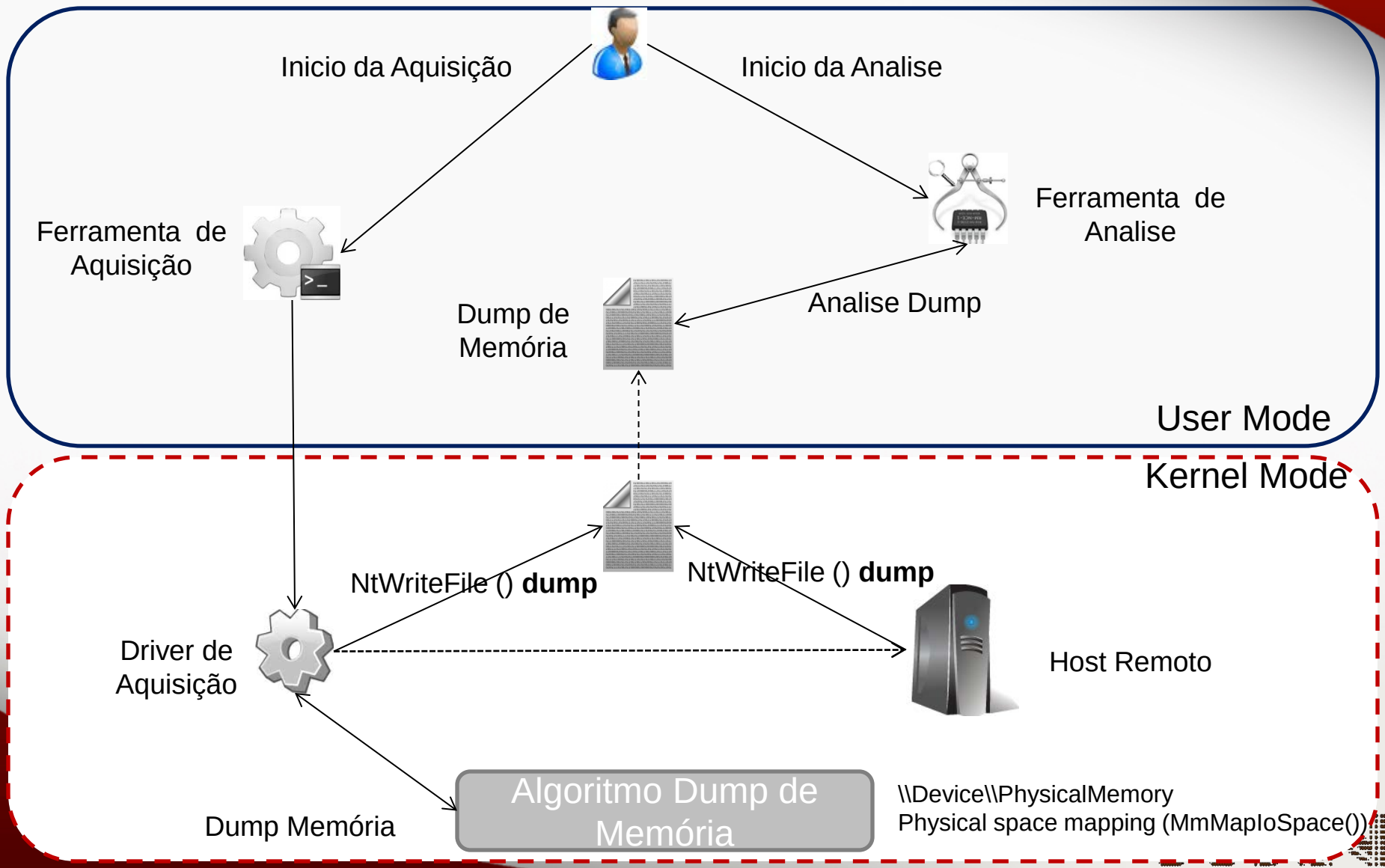
Memory Forensics – How To

OCTANE LABS

Memory Forensics – How To

- Coleta
  - MoonSols Windd (Raw e CrashDump)
  - WinEn (Raw)
  - HBGary Responder (Raw)
  - DumpIt (Raw)
- Análise
  - Volatility
  - Redline ou Memorize
  - HBGary Responder

Collecting the Memory



Volatility

- Open Source
- Versão Windows OS – XP, Vista, 7, 2003 e 2008
- Suporta Raw, Crash Dump e Hibernation
- Arquitetura Intel x86
- Trabalha com conceito de plugins

Volatility

```
root@SIFT-Workstation:/memory# vol.py -f rootkit.img psxview
Volatile Systems Volatility Framework 2.1_alpha
Offset     Name                 Pid      pslist   psscan   thrdproc
0x81666a70L winlogon.exe        896      1        1        1
0x819bc590L alg.exe             1924     1        1        1
```

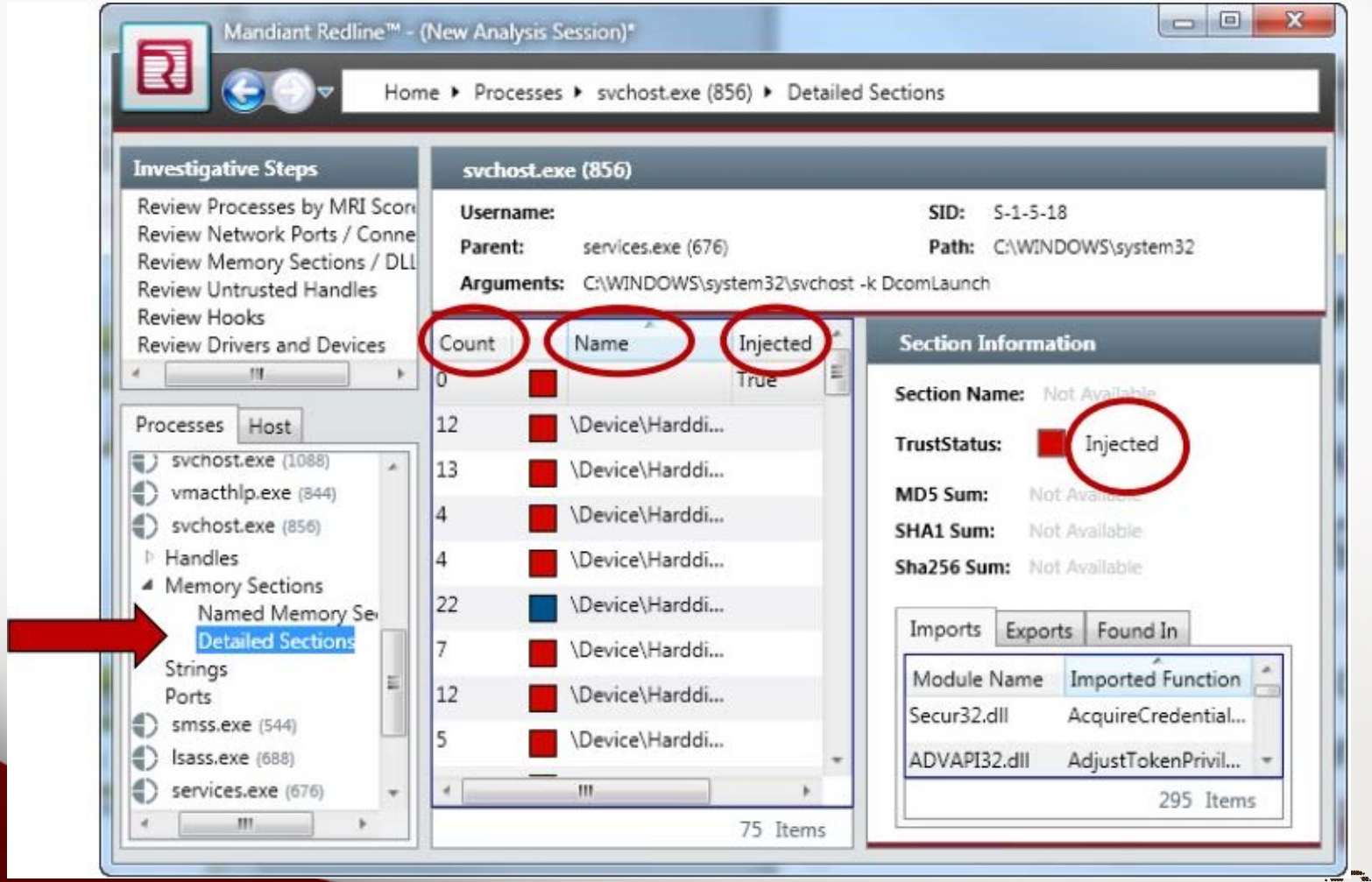
Name	Pid	pslist	psscan	thrdproc
svchost.exe	1608	0	1	1

```
0x8169bda0L svchost.exe         1188     1        1        1
0x815eb270L svchost.exe         1320     1        1        1
0x81ab1a20L services.exe        940      1        1        1
0x81617600L explorer.exe        1288     1        1        1
0x81655798L vmtoolsd.exe        308      1        1        1
0x81a385a0L smss.exe            824      1        1        1
0x819887f0L spoolsv.exe         1824     1        1        1
0x81651da0L VMUpgradeHelper     580      1        1        1
0x819922c0L svchost.exe         1608     0        1        1
0x8169d700L VMwareTray.exe      1228     1        1        1
0x815ed020L VMwareUser.exe      1484     1        1        1
0x81a55d78L vmacthlp.exe        1104     1        1        1
```

Redline

- Desenvolvido pela Mandiant
  - Foco na análise dos processos
- Versão Windows OS - todas
- Suporta apenas Raw
- Duas arquiteturas x86 e AMD64
- Trabalha três conceitos
  - Malware Risk Index
  - IoC (Indicators of Compromise)
  - MemD5 (whitelist)

Redline

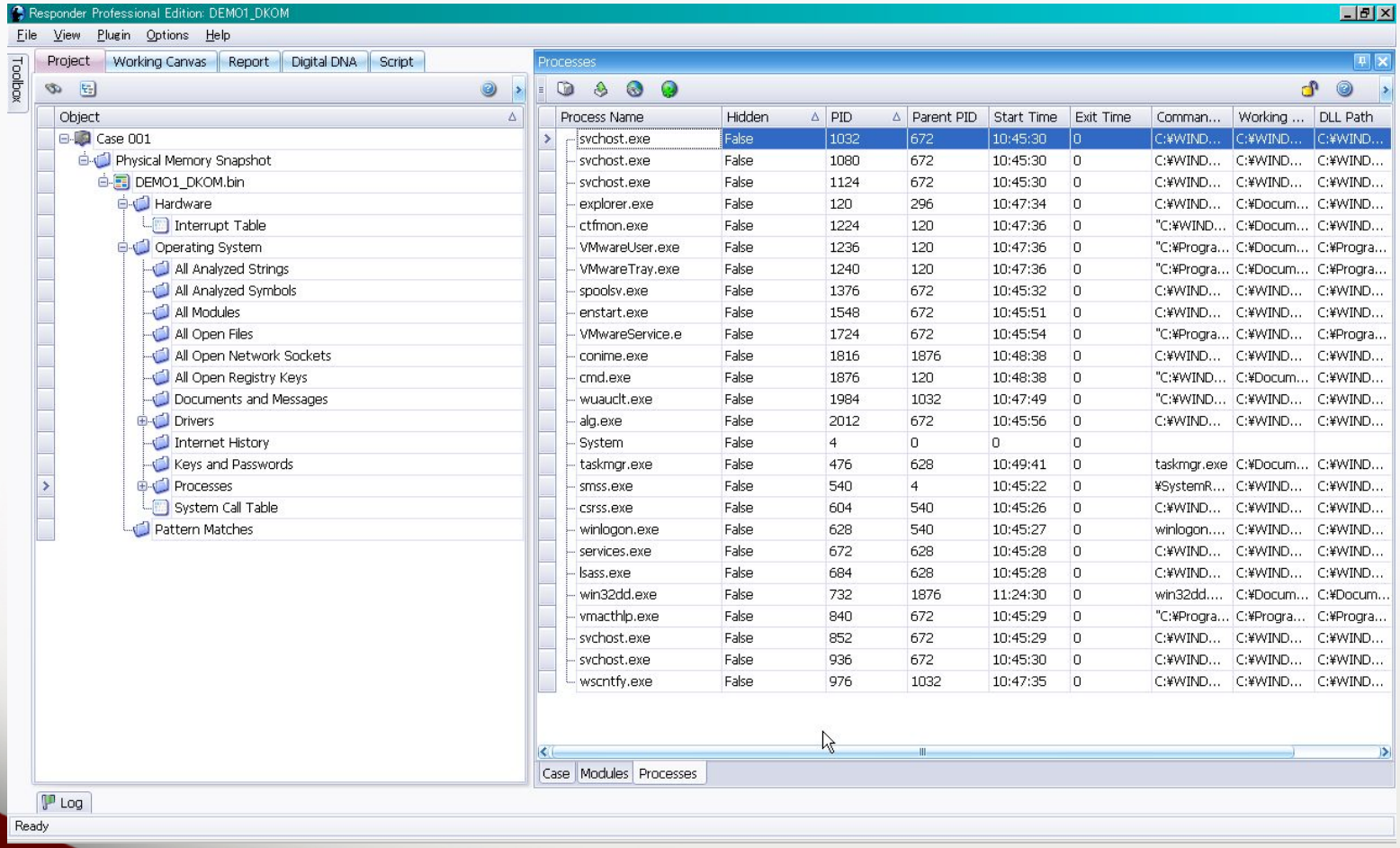

Mandiant Redline™ - (New Analysis Session)*
Home ▸ Processes ▸ svchost.exe (856) ▸ Detailed Sections
Investigative Steps
Review Processes by MRI Scor
Review Network Ports / Conne
Review Memory Sections / DLL
Review Untrusted Handles
Review Hooks
Review Drivers and Devices
Processes
Host
svchost.exe (1088)
vmacthlp.exe (844)
svchost.exe (856)
Handles
Memory Sections
Named Memory Se
Detailed Sections
Strings
Ports
smss.exe (544)
lsass.exe (688)
services.exe (676)
svchost.exe (856)
Username:
SID: S-1-5-18
Parent: services.exe (676)
Path: C:\WINDOWS\system32
Arguments: C:\WINDOWS\system32\svchost -k DcomLaunch
Count
Name
Injected
0
True
12 \Device\Harddi...
13 \Device\Harddi...
4 \Device\Harddi...
4 \Device\Harddi...
22 \Device\Harddi...
7 \Device\Harddi...
12 \Device\Harddi...
5 \Device\Harddi...
75 Items
Section Information
Section Name: Not Available
TrustStatus: Injected
MD5 Sum: Not Available
SHA1 Sum: Not Available
Sha256 Sum: Not Available
Imports
Exports
Found In
Module Name
Imported Function
Secur32.dll AcquireCredential...
ADVAPI32.dll AdjustTokenPrivil...
295 Items


Memory
Forensics

HBGary Responder

- Desenvolvido pela HBGary
- Versão Windows OS – Todas
- Suporta apenas Raw
- Duas arquiteturas x86 e AMD64
- Trabalha com dois conceitos
  - Digital DNA
  - Code Graphing

HBGary Responder



Windows Memory in a Nutshell

OCTANE LABS

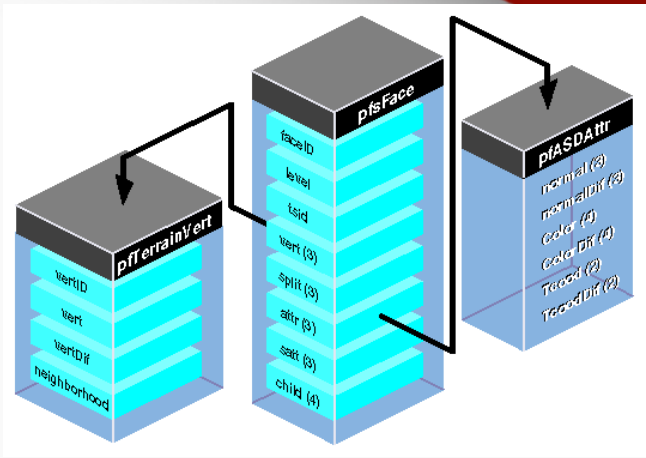
Warning

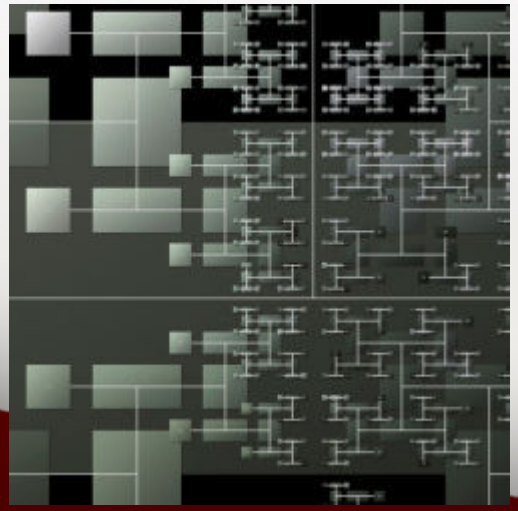
As estruturas da memória podem variar conforme versão Service Pack, bem como versão do Sistema Operacional

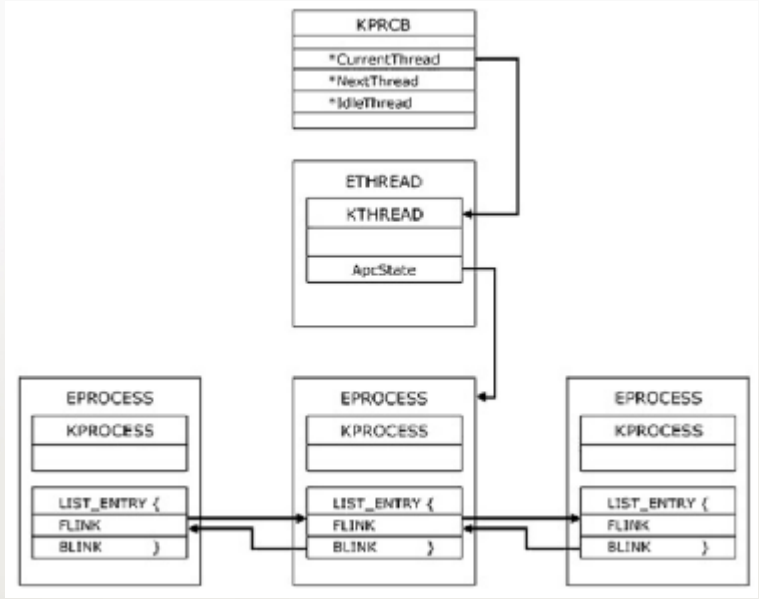
OCTANE LABS

Windows Memory

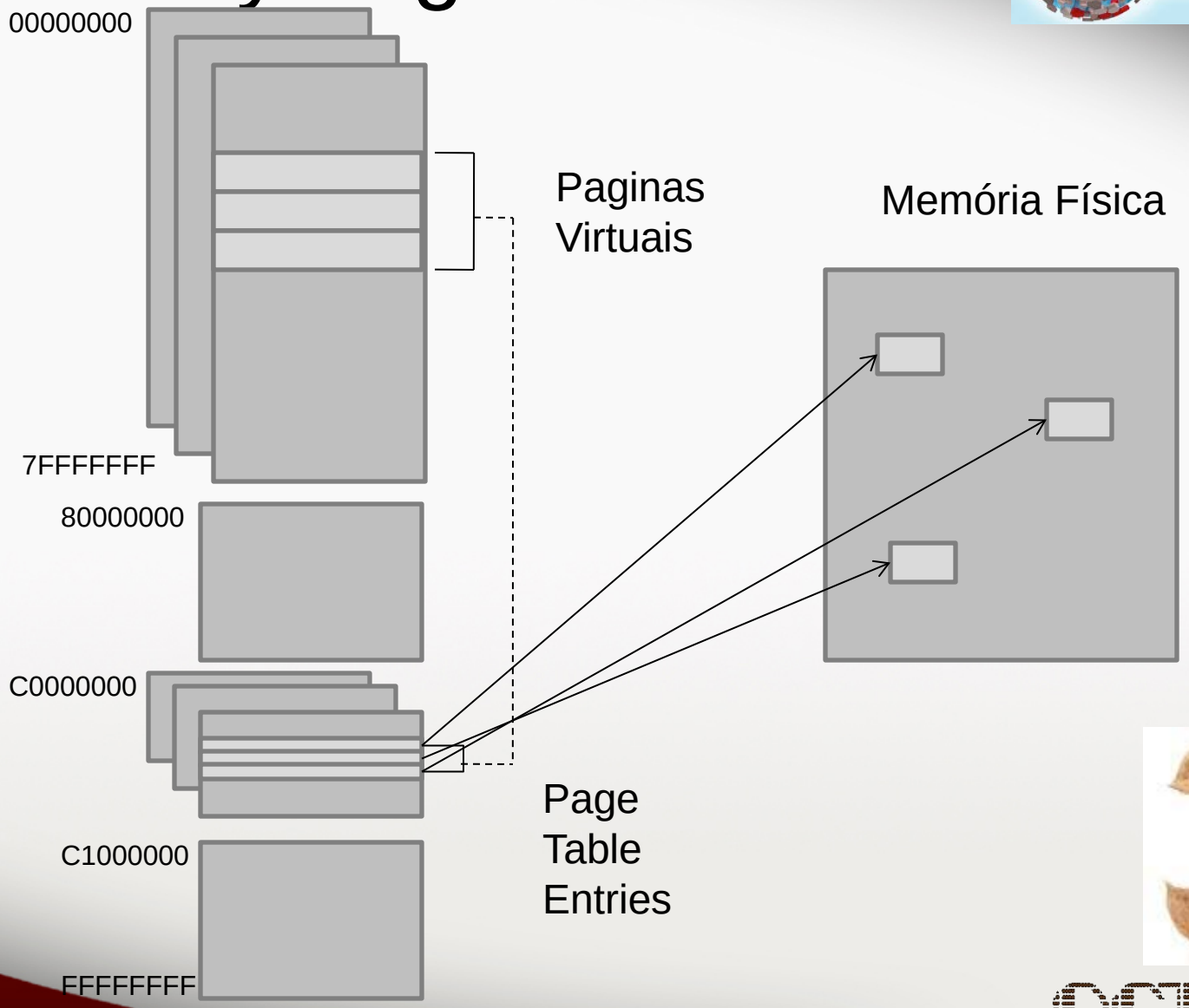
Um conjunto de bytes



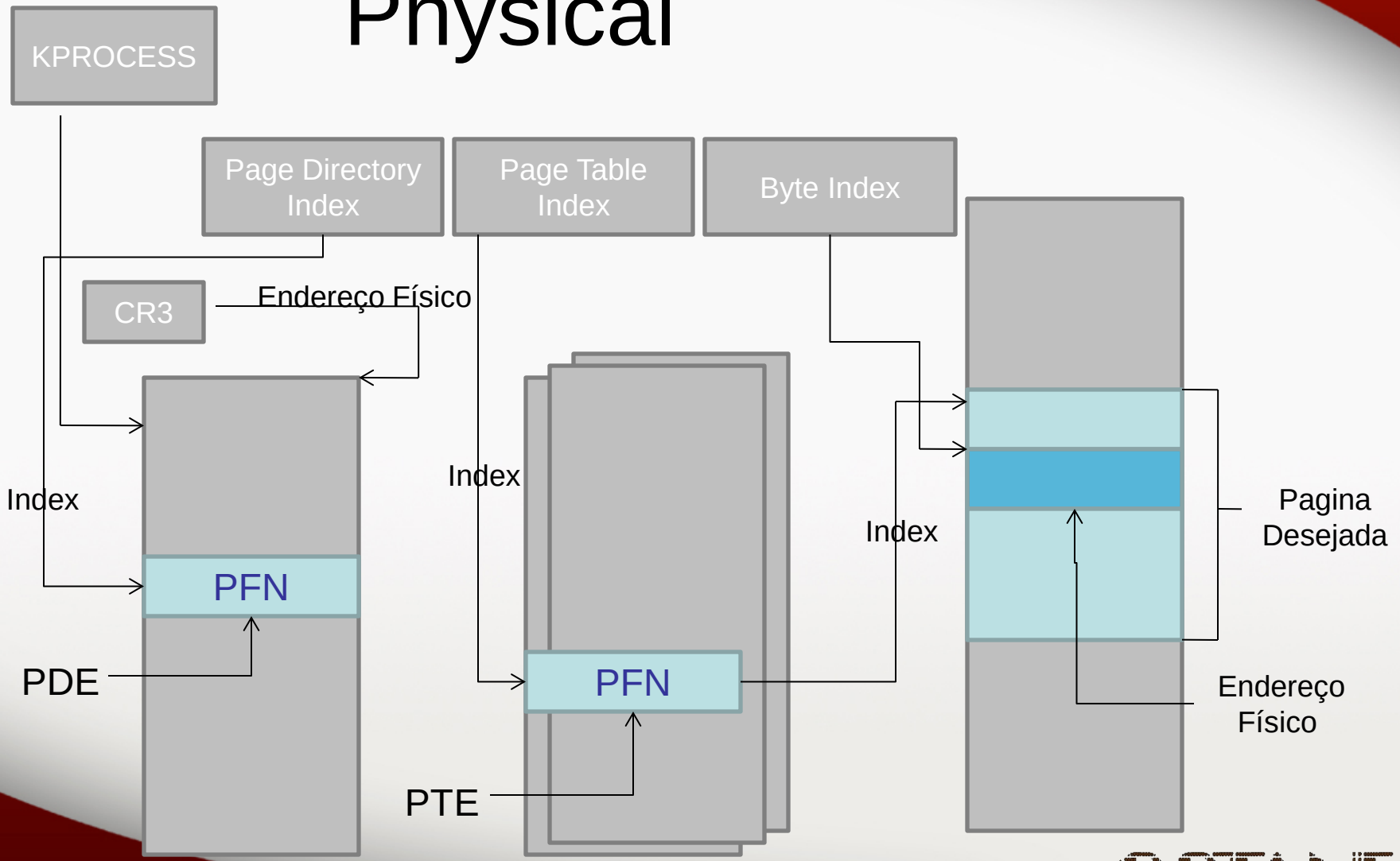




Memory Organization

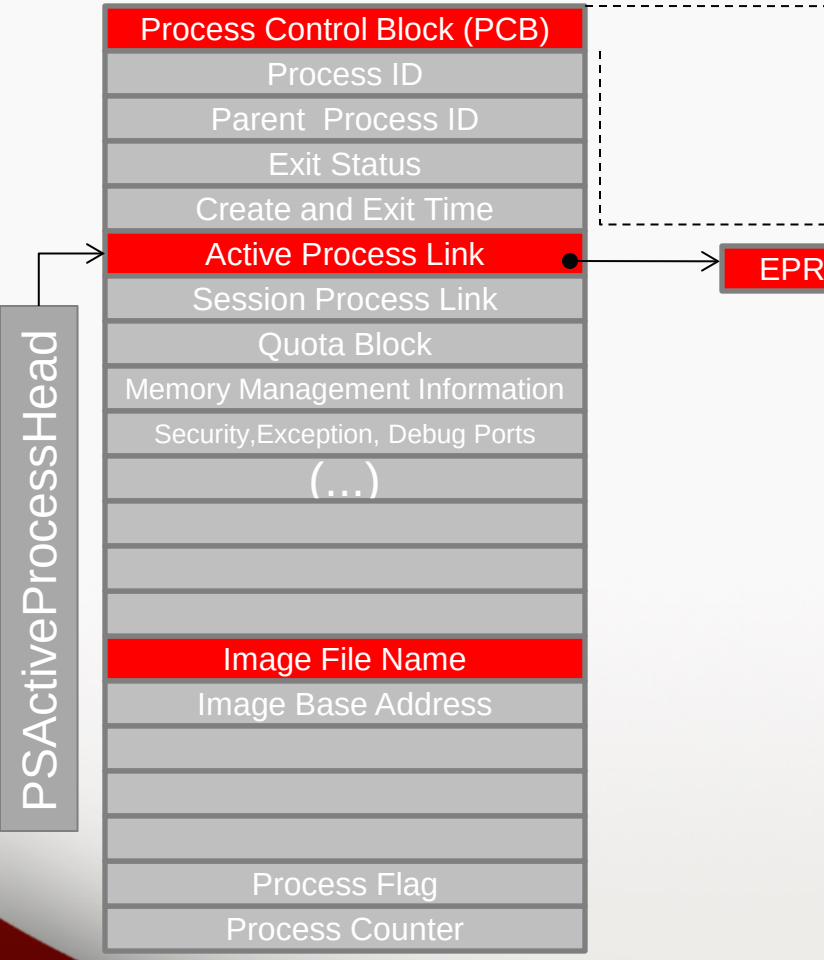


Translation of Virtual to Physical

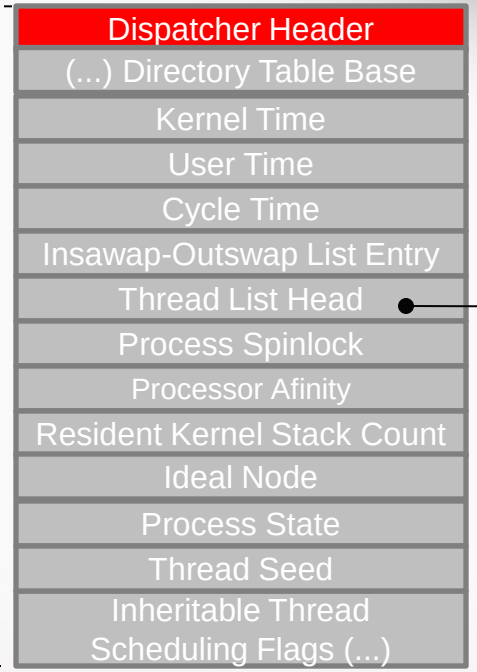


Existem outros modelos de endereçamento como o PAE e 64 bits

Important Structures

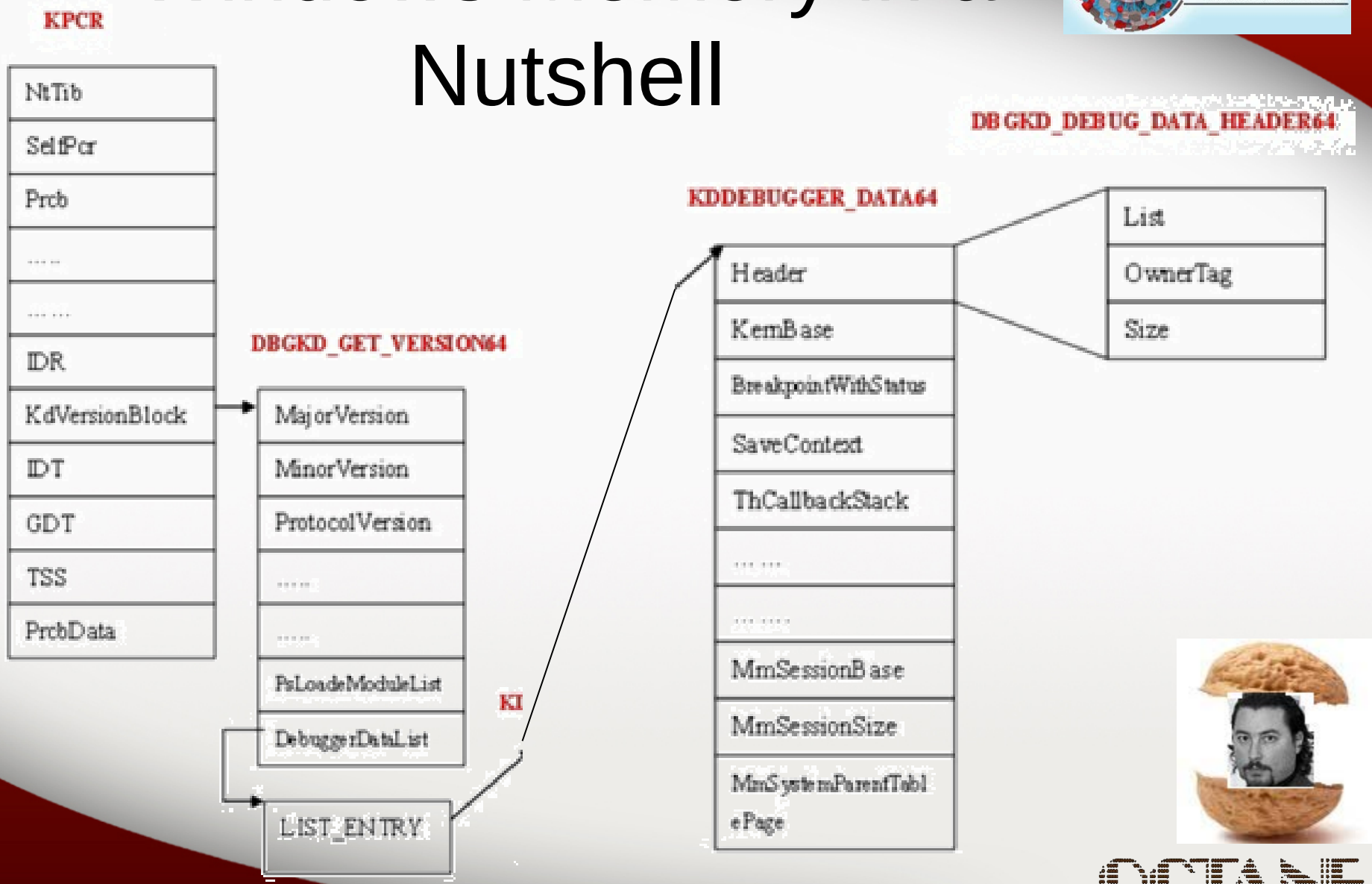


Estrutura EPROCESS



Estrutura KPROCESS

Windows Memory in a Nutshell



OCTANE LABS

Do you remember those errors in your memory dump ?!?

OCTANE LABS

```
0>volatility-2.0.exe -f d:\Forense\Imagens\imgmem_atacado_abortfactor.dat pslist

Volatile Systems Volatility Framework 2.0
No suitable address space mapping found
Tried to open image as:
 WindowsHiberFileSpace32: No base Address Space
 WindowsCrashDumpSpace32: No base Address Space
 JKIA32PagedMemory: No base Address Space
 JKIA32PagedMemoryPae: No base Address Space
 IA32PagedMemoryPae: Module disabled
 IA32PagedMemory: Module disabled
 WindowsHiberFileSpace32: No xpress signature found
 WindowsCrashDumpSpace32: Header signature invalid
 JKIA32PagedMemory: No valid DTB found
 JKIA32PagedMemoryPae: No valid DTB found
 IA32PagedMemoryPae: Module disabled
 IA32PagedMemory: Module disabled
 FileAddressSpace: Must be first Address Space
```

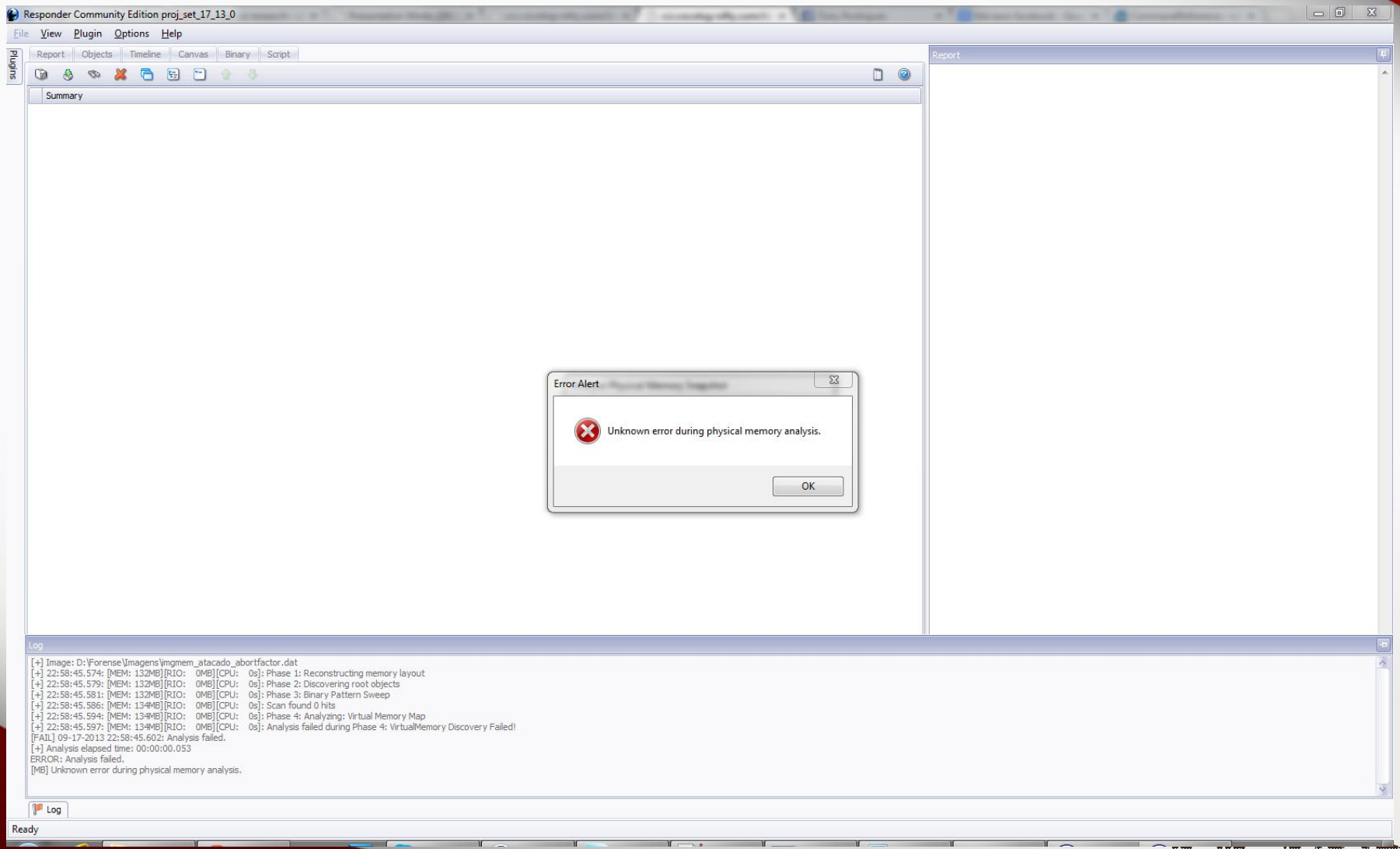
☹☹

```
D:\Forense\Imagens>volatility -f imgmem_atacado_abortfactor.dat imageinfo
Volatile Systems Volatility Framework 2.2
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with no
profile)
                     AS Layer1 : FileAddressSpace (D:\Forense\Imagens\imgmem_ata
cado_abortfactor.dat)
                      PAE type : No PAE

D:\Forense\Imagens>
```

☹☹☹


Responder Community Edition proj_set_17_13_0
File View Plugin Options Help
Plugins
Report Objects Timeline Canvas Binary Script
Summary
Report
Error Alert
Unknown error during physical memory analysis.
OK
Log
[+] Image: D:\Forense\Imagens\jmgmem_atacado_abortfactor.dat
[+] 22:58:45.574: [MEM: 132MB][RIO: 0MB][CPU: 0s]: Phase 1: Reconstructing memory layout
[+] 22:58:45.579: [MEM: 132MB][RIO: 0MB][CPU: 0s]: Phase 2: Discovering root objects
[+] 22:58:45.581: [MEM: 132MB][RIO: 0MB][CPU: 0s]: Phase 3: Binary Pattern Sweep
[+] 22:58:45.586: [MEM: 134MB][RIO: 0MB][CPU: 0s]: Scan found 0 hits
[+] 22:58:45.594: [MEM: 134MB][RIO: 0MB][CPU: 0s]: Phase 4: Analyzing: Virtual Memory Map
[+] 22:58:45.597: [MEM: 134MB][RIO: 0MB][CPU: 0s]: Analysis failed during Phase 4: VirtualMemory Discovery Failed!
[FAIL] 09-17-2013 22:58:45.602: Analysis failed.
[+] Analysis elapsed time: 00:00:00.053
ERROR: Analysis failed.
[MB] Unknown error during physical memory analysis.
Log
Ready

Abort Factor

OCTANE LABS

Abort Factor Attack

- O ataque é **contra a análise**
- Baseado na modificação de **um byte** em alguns lugares específicos (Abort Factor)
- Implementado em código que executa **no nível do Kernel**
- **Busca inviabilizar as ferramentas de análise**

Abort Factor Attack

- Ataque é realizado sobre operações críticas
  - Tradução do endereçamento virtual do kernel space
  - Identificação da arquitetura e Sistema Operacional
  - Obtenção de Objetos do Kernel
- Não pode dar BSOD !

Possible Abort Factors

Tool	Virtual Address Translation in Kernel Space	Guessing OS version and Architecture	Getting Kernel Objects
Volatility Framework	2 factors: _DISPATCHER_ HEADER and ImageFileName (PsIdleProcess)	1 factor: _DBGKD_DEBUG_ DATA_HEADER64	2 factors: _DBGKD_DEBUG_ DATA_HEADER64 and PsActiveProcessHead
Mandiant Memoryze	4 factors: _DISPATCHER_ HEADER, PoolTag, Flags and ImageFileName (PsInitialSystem Process)	2 factors: _DISPATCHER_ HEADER and offset value of ImageFileName (PsInitialSystem Process)	None
HBGary Responder	None	1 factor: OperatingSystem Version of kernel header	1 factor: ImageFileName (PsInitialSystem Process)

Attacking the Memory

OCTANE LABS

Attacking the Memory

- Rootkit
  - Altera o abort factor
    - Apenas 1 byte alterado em cada
    - Não pode dar BSOD*
  - Logo no momento da carga do rootkit
- Durante a análise, teremos:
  - Impossibilidade de achar o SO
  - Erro nas operações

- No PoC realizado a máquina ficou ligada por 15 dias consecutivos sem dar BSOD

Code is the wild

Windows XP

```
      mov eax,[eax + 0xC] // _KPRCB->IdleThread
      mov eax,[eax + 0x44]// _KTHREAD->ApcState.Process
      //mov eax,[eax + 0x150]// _KTHREAD->Process
      mov IdleProcess,eax
      }
  return IdleProcess;
}

void * GetNtMajorVersion()
{
  void * ptrNtMajorVersion;

  KeSetSystemAffinityThread(1); // select 1st processor
  _asm {
    mov eax, fs:[0x1C]  // SelfPCR
      mov eax, [eax + 0x34] // _KPCR->KdVersionBlock
      mov eax, [eax + 0x10] // _DBGKD_GET_VERSION64->KernBase
      add eax, 0x120 // PE.MajorOperatingSystemVersion
      mov ptrNtMajorVersion, eax
      }
  KeRevertToUserAffinityThread();

  return ptrNtMajorVersion;
}

void PatchDispatcherHeaderSize(PEPROCESS ep)
{
  DWORD dispatch_size_addr;

  dispatch_size_addr = (DWORD)ep + DISPATCHER_HEADER_SIZE_OFFSET;
```

Windows 7

```
  return IdleProcess;
}

void * GetNtMajorVersion()
{
  void * ptrNtMajorVersion;

  KeSetSystemAffinityThread(1); // select 1st processor
  _asm {
    mov eax, fs:[0x1C]  // SelfPCR
      mov eax, [eax + 0x34] // _KPCR->KdVersionBlock
      mov eax, [eax + 0x10] // _DBGKD_GET_VERSION64->KernBase
      add eax, 0x2B8 // PE.MajorOperatingSystemVersion
      mov ptrNtMajorVersion, eax
      }
  KeRevertToUserAffinityThread();

  return ptrNtMajorVersion;
}

void PatchDispatcherHeaderSize(PEPROCESS ep)
{
  DWORD dispatch_size_addr;

  dispatch_size_addr = (DWORD)ep + DISPATCHER_HEADER_SIZE_OFFSET;
  DbgPrintEx(DPFLTR_IHVDRIVER_ID, DPFLTR_ERROR_LEVEL,
            "Patching one byte to Size in _DISPATCHER_HEADER at 0x%08x\n", dispatch_size_addr);
  memset((void *)dispatch_size_addr, 0, 1);
}
```

Usage

- Malwares
  - Esconder os vestígios na memória
  - Evitar ou atrasar a análise do dump
- Auto-defesa maliciosa
  - Usuário malicioso pode usar na própria máquina
  - Evitar vestígios de atividades ilícitas

Can we revert it?

Presenting ....

OctaneLabs

Phosfosol

Indicium in Veritas

OCTANE LABS

Aborting the Abort Factor

- Fato
  - Abort Factor inviabiliza todas as 3 ferramentas de análise
- Anti-Abort Factor
  - Fazendo funcionar para ao menos uma das ferramentas
- Volatility é o alvo
  - Permite indicar DTB e Profile

OCTANE LABS

How ?

- Principalmente
  - Localizando o DTB do Kernel
  - Inferindo o profile correto
- Foco em estruturas de kernel intactas e correlação
  - Não atacadas por opção
  - Não atacadas por impossibilidade
  - Correlação entre os vestígios

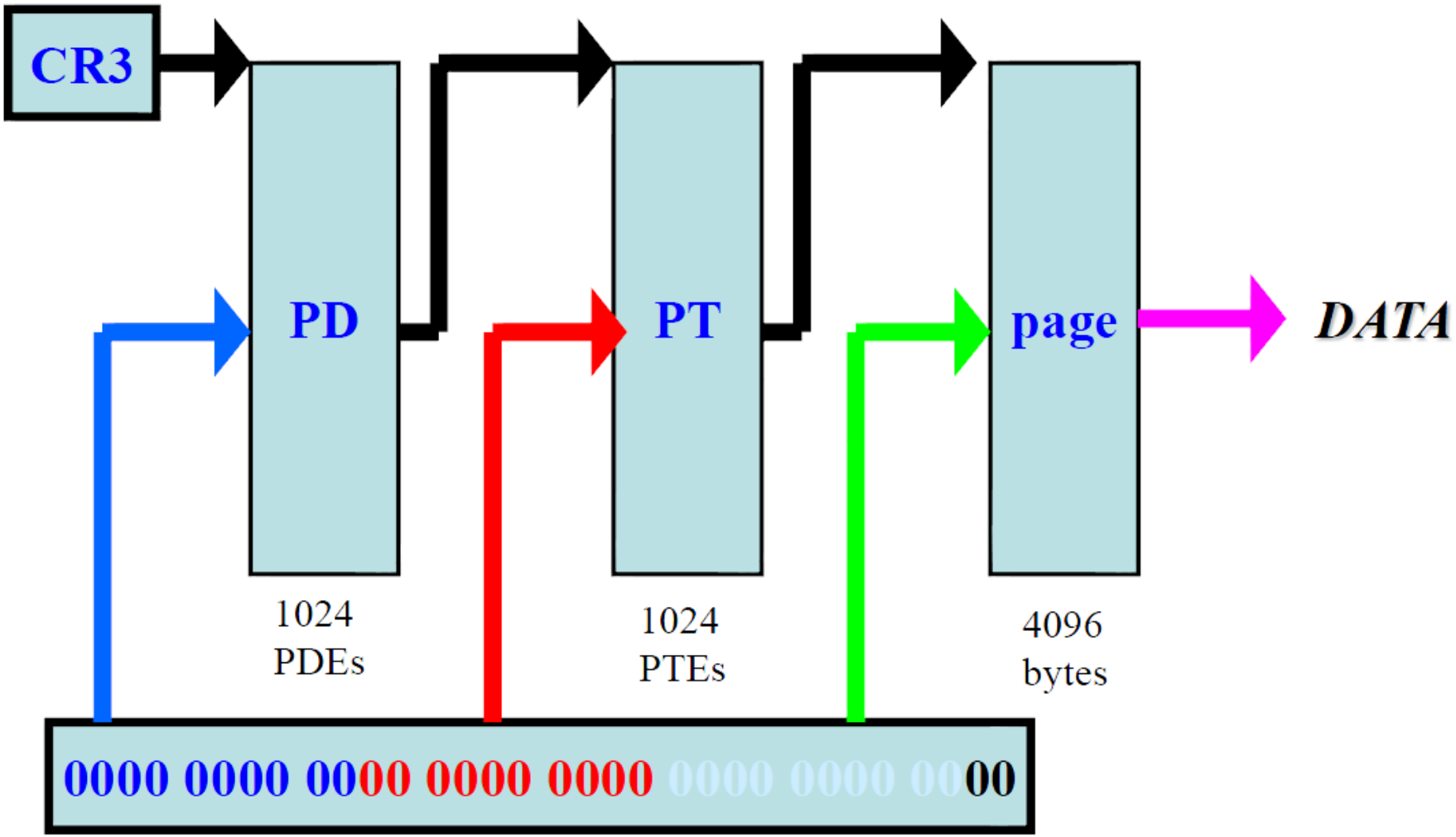
Non-Attacked Strutures

- Poc somente explora 3 Abort Factors
  - Código pronto. Copy&Paste
  - Os 3 explorados já cumprem o objetivo
- Outros podem ser mais complicados
  - Pelo menos em um primeiro momento
- Estruturas mapeadas
  - Eprocess do IDLE
  - _DBGKD_DEBUG_DATA_HEADER64 (KDBG)

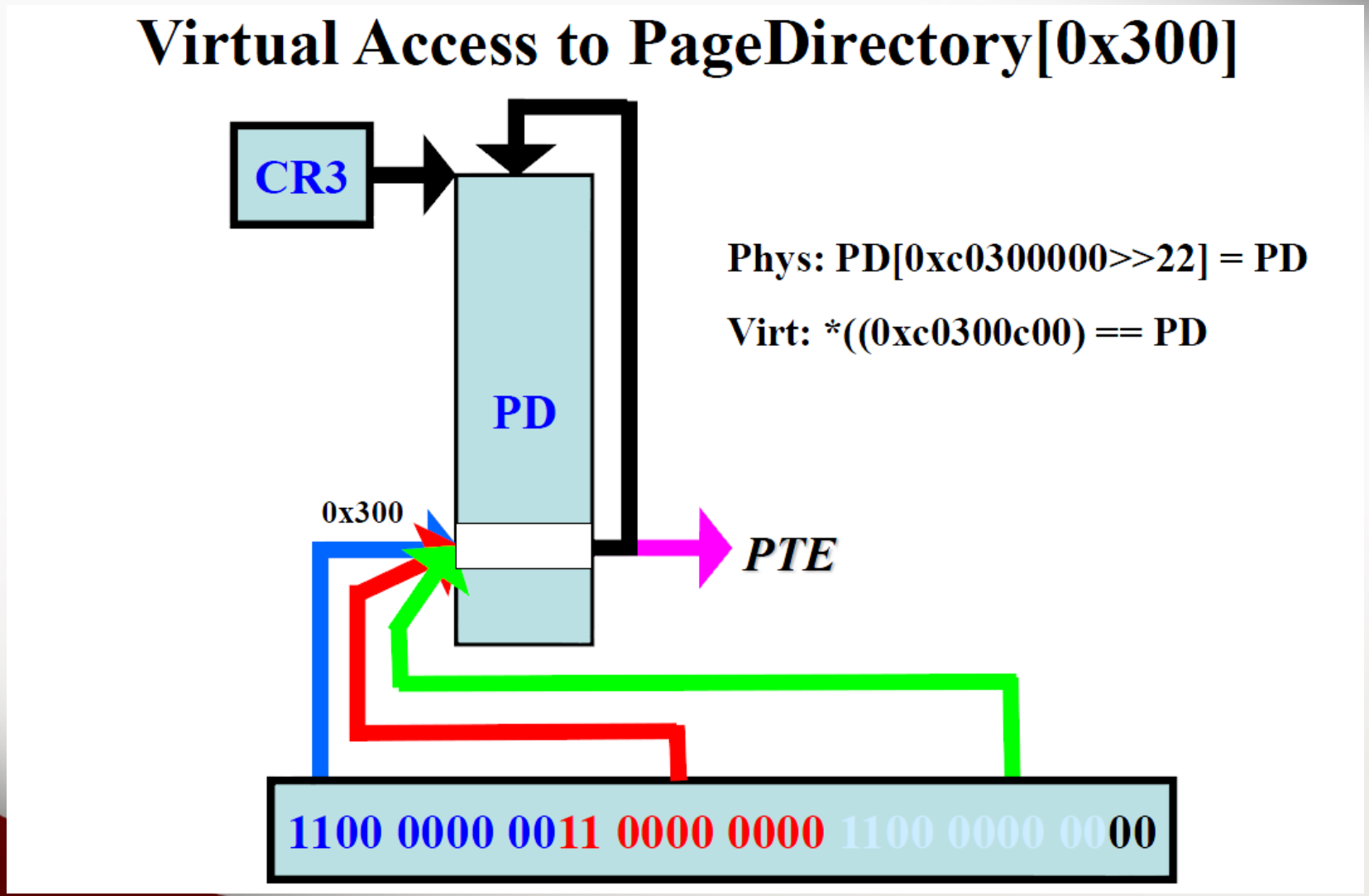
Impossible to attack

- Assinaturas baseadas em endereços
  - Endereços adulterados == BSOD
- Estruturas auto-referenciadas
  - Page Directory Table, Page Table

Self Mapping Page Tables



Self Mapping Page Tables



Phosfosol

```
0>volatility-2.0.exe -f d:\Forense\Imagens\imgmem_atacado_abortfactor.dat pslist

Volatile Systems Volatility Framework 2.0
No suitable address space mapping found
Tried to open image as:
 WindowsHiberFileSpace32: No base Address Space
 WindowsCrashDumpSpace32: No base Address Space
 JKIA32PagedMemory: No base Address Space
 JKIA32PagedMemoryPae: No base Address Space
 IA32PagedMemoryPae: Module disabled
 IA32PagedMemory: Module disabled
 WindowsHiberFileSpace32: No xpress signature found
 WindowsCrashDumpSpace32: Header signature invalid
 JKIA32PagedMemory: No valid DTB found
 JKIA32PagedMemoryPae: No valid DTB found
 IA32PagedMemoryPae: Module disabled
 IA32PagedMemory: Module disabled
 FileAddressSpace: Must be first Address Space
```

```
D:\Forense\Imagens>volatility -f imgmem_atacado_abortfactor.dat imageinfo
Volatile Systems Volatility Framework 2.2
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with no
profile)
                     AS Layer1 : FileAddressSpace (D:\Forense\Imagens\imgmem_ata
cado_abortfactor.dat)
                      PAE type : No PAE

D:\Forense\Imagens>
```

Abort Factor

Phosfosol

Vamos usar essas informações

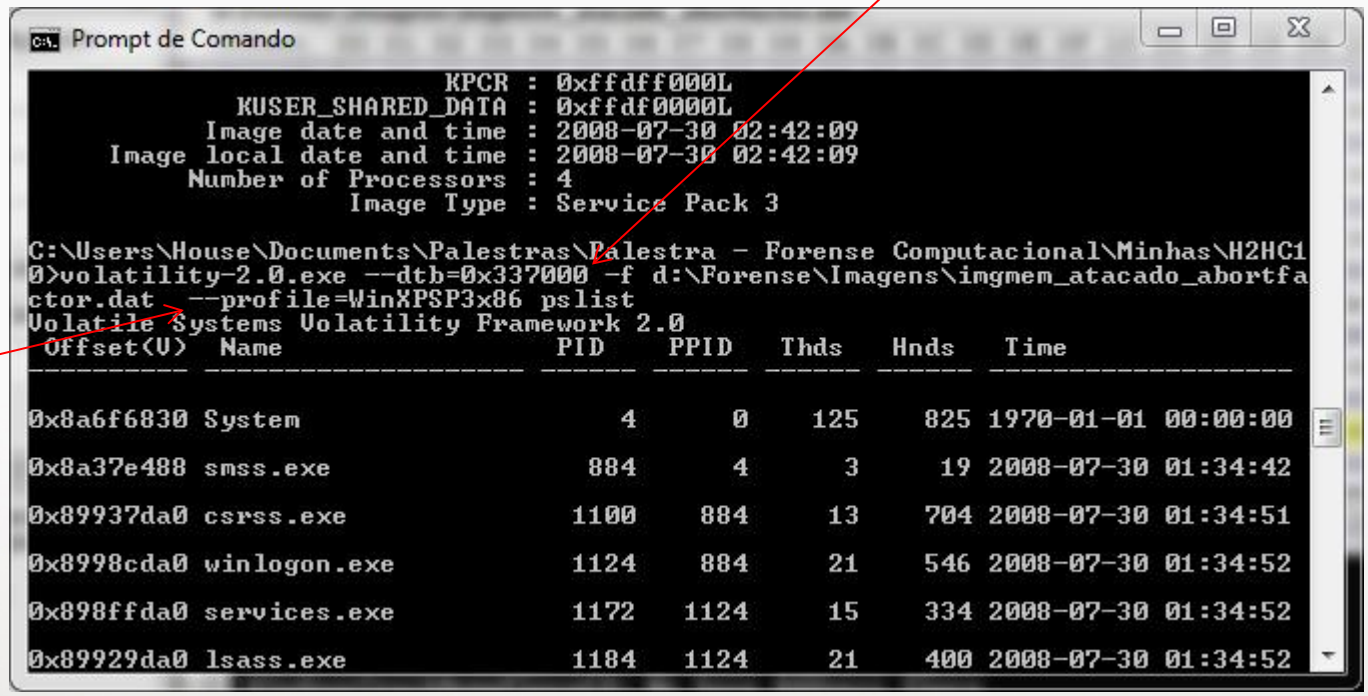
```
D:\Forense\Phosfosol>phosfosol.pl -f ..\Imagens\imgmem_atacado_abortfactor.dat
Reading offset ...  3485466624
Candidate DTB and Profile:
-------------------------
      DTB=0x337000
  PROFILE=WinXPSP2x86 -> KDBG Confirmed
     KDBG=0x54d2e0
32 bits Operational System (via KDGB)
32 bits PAE Operational System (self-ref pages)

D:\Forense\Phosfosol>
```

Phosfosol

DTB informado

Profile informado



Video - Phosfosol

What if it´s not working ?!?

Phosfosol didn´t work

- Outros Abort Factors foram usados
  - Assinatura do KDBG adulterada
  - Imagename do System ou do Idle adulterado
- Serão endereçados no upgrade do Phosfosol

Upgrade best definition

Jan Seidl v0.1 alpha

- Trava muito ao acessar partes baixas de uma tabela
- Rouba memória o tempo todo
- Performance sempre fraca

Upgrade best definition

Jan Seidl v1.0 unstable

- Performance irregular, ora roda bem, ora roda mal demais
- Bug reportado: sempre pula a segunda linha, o segundo parâmetro, etc
- Requer batom.dll instalado para rodar

Upgrade best definition

Jan Seidl v2.0 Gold Plus Advanced Protein

- Alta performance
- Uso eficiente de recursos
- Roda bem em Windows, Linux, Mac, SãoJanuOS e até mesmo no novíssimo ManéGarrinchaOS

Phosfosol Upgrade

- Uso de assinaturas fortes
  - Trabalho de Brendan Dolan-Gavitt
  - Carving baseado em campos críticos
    - BSOD se adulterados
- Suportará ataques múltiplos até mesmo de todos os Abort Factors conjugados
- Novas opções de linha de comando
  - Confirmação de ataque/abort factor
  - Reversão do ataque

Conclusions

- Abort Factor é um ataque eficiente
- Código disponível
- Phosfosol pode recuperar as informações danificadas

References

- Phosfosol
  - https://code.google.com/p/phosfosol/
- OctaneLabs
  - http://www.octanelabs.net
- Moonsols (Dumpit, Win32dd)
  - http://www.moonsols.com/
- Mandiant (Red Line, Memoryze)
  - http://www.mandiant.com/
- HBGary (Responder Community Edition)
  - http://www.hbgary.com/
- Volatility
  - https://www.volatilesystems.com/default/volatility/

References

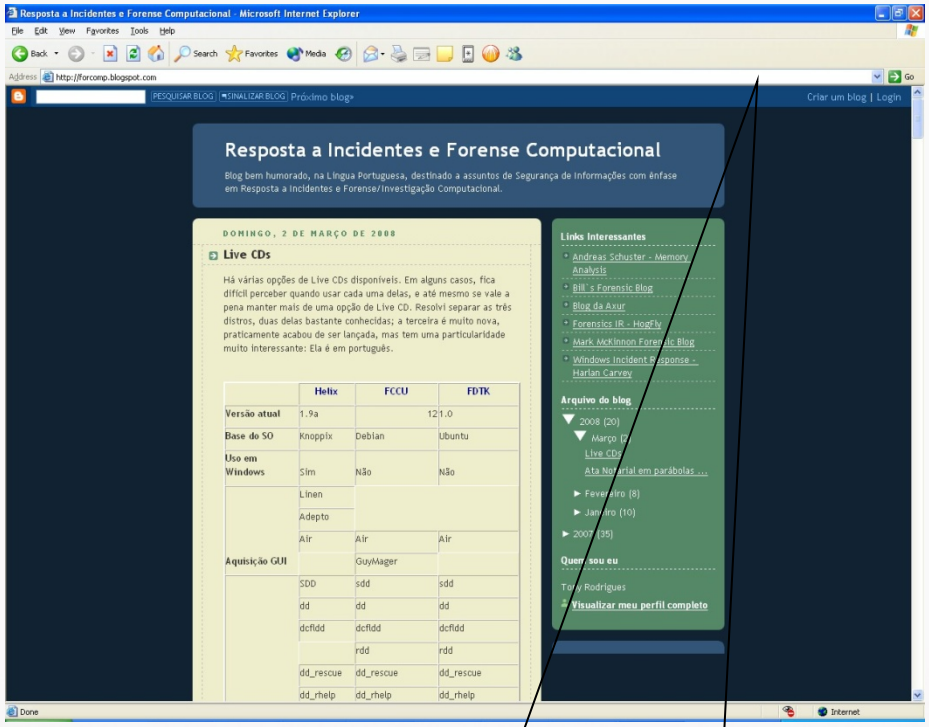
- One-byte Modification for Breaking Memory Forensic Analysis
  - https://media.blackhat.com/bh-eu-12/Haruyama/bh-eu-12-Haruyama-Memory_Forensic-Slides.pdf
- Robust Signatures for Kernel Data Structures
  - http://www.cc.gatech.edu/~brendan/ccs09_siggen.pdf
- Windows Kernel Architecture Internals
  - Dave Probert
- Windows Internals
  - Mark Russinovich, David Solomon
- Windows operating systems agnostic memory analysis
  - http://www.dfrws.org/2010/proceedings/2010-306.pdf

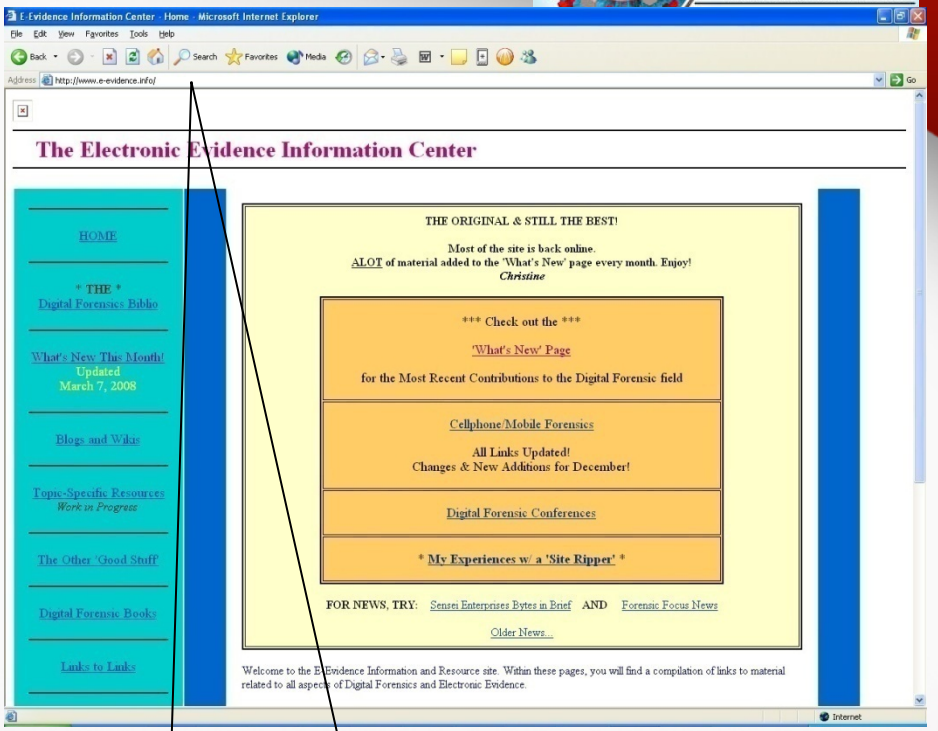
OCTANE LABS

Thanks to

- Agradecimentos do OctaneLabs
  - Aos amigos Nelson Brito e Jan Seidl ;)
  - Takahiro Haruyama san
  - Mr Brendan Dolan-Gavitt
  - Mr Matthieu Suiche

Readings





http://forcomp.blogspot.com

http://www.e-evidence.info

Octane Labs


,o888888o. ,o888888o. 8888888 8888888888 .8. b. 8 8 8888888888
. 8888 `88. 8888 `88. 8 8888 .888. 888o. 8 8 8888
,8 8888 `8b ,8 8888 `8. 8 8888 :88888. Y888888o. 8 8 8888
88 8888 `8b 88 8888 8 8888 . `88888. .`Y888888o. 8 8 8888
88 8888 88 88 8888 8 8888 .8. `88888. 8o. `Y888888o. 8 8 888888888888
88 8888 88 88 8888 8 8888 .8`8. `88888. 8`Y8o. `Y88888o8 8 8888
88 8888 ,8P 88 8888 8 8888 .8' `8. `88888. 8 `Y8o. `Y8888 8 8888
`8 8888 ,8P `8 8888 .8' 8 8888 .8' `8. `88888. 8 `Y8o. `Y8 8 8888
` 8888 ,88' 8888 ,88' 8 8888 .888888888. `88888. 8 `Y8o.` 8 8888
`8888888P' `8888888P' 8 8888.8' `8. `88888. 8 `Yo 8 888888888888
LABS

OctaneLabs

- O que é OctaneLabs ???
  - Time de Pesquisa Open Source em Computação Forense e Resposta a Incidentes

OCTANE
LABS

OctaneLabs

- Objetivos
  - Fomentar a pesquisa em Computação Forense no Brasil
  - Promover Projetos Open Source com foco em Computação Forense e Investigação Digital
  - Ministrar Treinamentos em CF
  - Consultoria, Perícia e Investigação Digital

OctaneLabs

- Projetos em andamento
  - MUFFIN
  - Byte Investigator
  - DataJuicer
  - Jardineiro
  - CORE
  - FSJuicer
- Projetos esperando por você
  - Phosfosol
  - Blitz
  - Langoliers

We Want YOU !

www.octanelabs.net
@octanelabs

Perguntas !

Obrigado !

inv.forense arroba gmail ponto com

@octanelabs

(Tony Rodrigues)

diegofuschini arroba gmail ponto com

(Diego Fuschini)