Восстановление адресного пространства процесса в Windows 10

Тарасова П.М., 4 курс СПбГУ,
Научный руководитель: Губанов Ю.А.
Научный консультант: Тимофеев Н.М.
Рецензент: Мухаматулин М. С.

Область применения

Компьютерная криминалистика:

- Персональные компьютеры
  - Жесткие диски
  - Оперативная память
- Мобильные телефоны
- Другие электронные устройства

Существующие решения

- Volatility Framework (Python)
  + Windows XP — Windows 10
  + Широкая функциональность
  - Ручной ввод версии и битности системы

- PTFinder (Perl)
  - Windows 2000 — Windows Vista
  - Последнее обновление в ноябре 2007

Цель

Разработка и внедрение подсистемы для восстановления виртуального адресного пространства процесса приложения из образа оперативной памяти Windows 10 x86 PAE

Задачи

- Изучить структуры памяти Windows 10 x86 PAE
- Разработать метод восстановления адресного пространства процесса Windows 10 x86 PAE
- Реализовать предложенный метод в продукте Belkasoft Evidence Center
- Провести тестирование

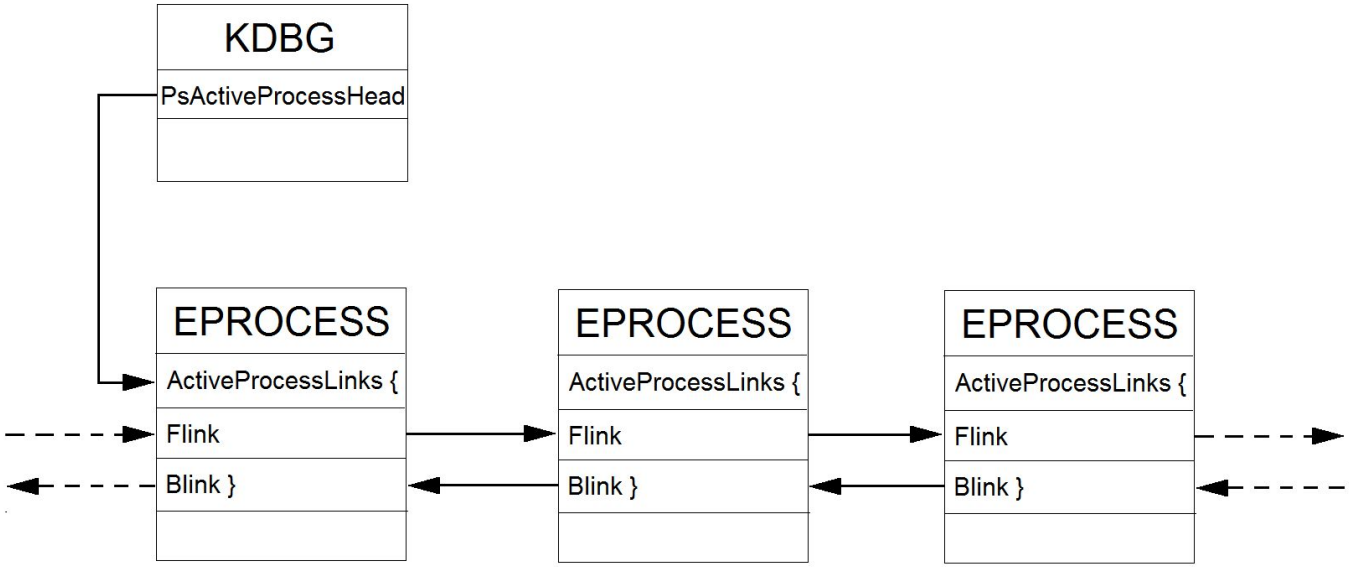
Структура EPROCESS в Windows 10

```
lkd> dt nt!_eprocess
   +0x000 Pcb               : _KPROCESS
   +0x0a8 ProcessLock       : _EX_PUSH_LOCK
   +0x0ac RundownProtect    : _EX_RUNDOWN_REF
   +0x0b0 VdmObjects        : Ptr32 Void
   +0x0b4 UniqueProcessId   : Ptr32 Void
   +0x0b8 ActiveProcessLinks : _LIST_ENTRY
...
   +0x11c Win32Process      : Ptr32 Void
   +0x120 Job               : Ptr32 _EJOB
...
   +0x140 OwnerProcessId    : Uint4B
   +0x144 Peb               : Ptr32 _PEB
   +0x148 Session           : Ptr32 _MM_SESSION_SPACE
...
   +0x28c VadRoot           : _RTL_AVL_TREE
   +0x290 VadHint           : Ptr32 Void
   +0x294 VadCount          : Uint4B
   +0x298 VadPhysicalPages  : Uint4B
   +0x29c VadPhysicalPagesLimit : Uint4B
...
   +0x330 SequenceNumber    : Uint8B
   +0x338 CreateInterruptTime : Uint8B
   +0x340 CreateUnbiasedInterruptTime : Uint8B
```

Методы поиска процессов по структурам

- Метод списков (smss.exe, csrss.exe)
- Сигнатурный метод
- Метод с использованием структуры Kernel Processor Control Region (KPCR)

Метод списков (smss.exe, csrss.exe)



Сигнатурный метод

- DISPATCHER_HEADER (KPROCESS)
  - Type
  - Size

- ThreadListHead (EPROCESS)
  - Flink
  - Blink

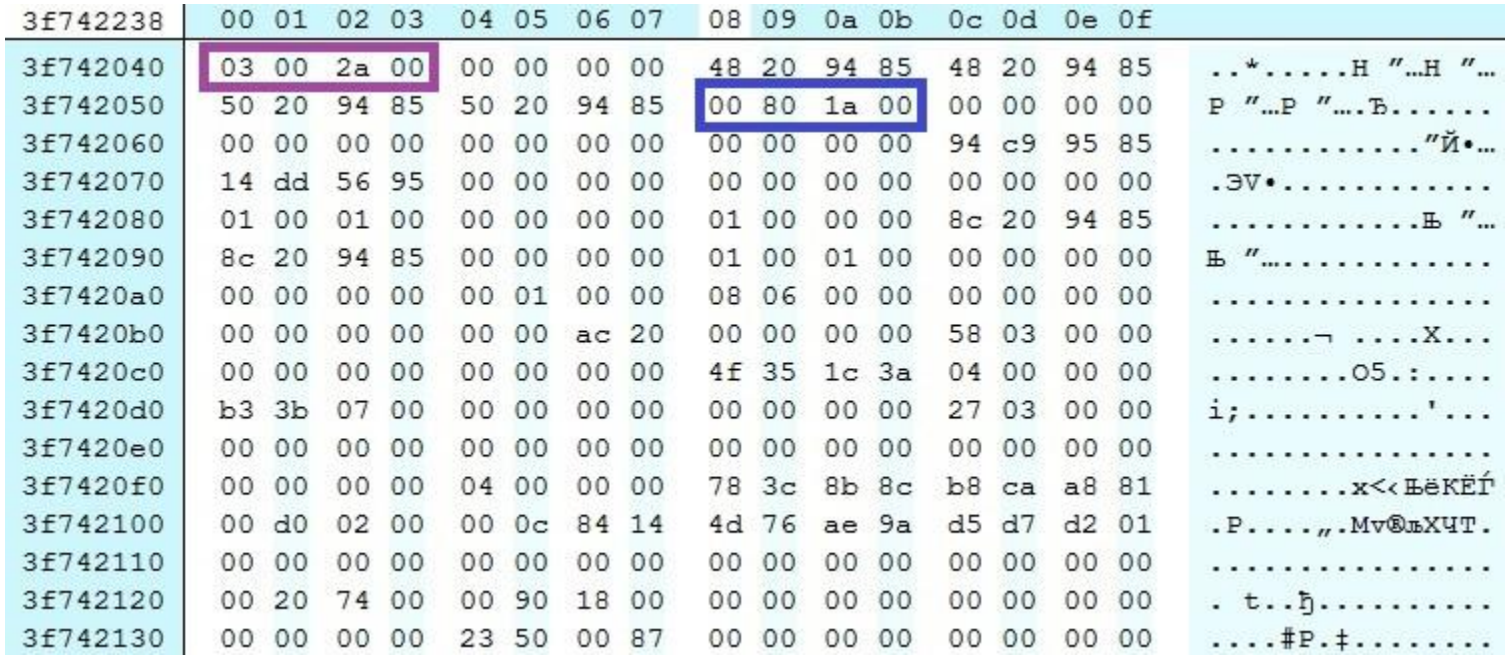
KPCR-метод

- Kernel Processor Region Control Block (KPCR)
  - KdVersionBlock
    - PsActiveProcessHead

Windows 8, 10 — динамический виртуальный адрес KPCR
Windows 10 — KdVersionBlock (null)

Поиск структур EPROCESS

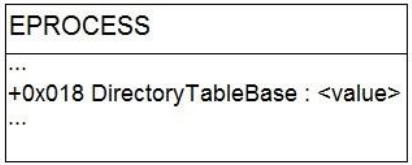
DISPATCHER_HEADER (Type, Size)



3f742238	00 01 02 03	04 05 06 07	08 09 0a 0b	0c 0d 0e 0f	
3f742040	03 00 2a 00	00 00 00 00	48 20 94 85	48 20 94 85	..*.....H ”…H ”…
3f742050	50 20 94 85	50 20 94 85	00 80 1a 00	00 00 00 00	P ”…P ”….Ъ.....
3f742060	00 00 00 00	00 00 00 00	00 00 00 00	94 c9 95 85	............”Й•…
3f742070	14 dd 56 95	00 00 00 00	00 00 00 00	00 00 00 00	.ЭV•............
3f742080	01 00 01 00	00 00 00 00	01 00 00 00	8c 20 94 85	............Њ ”…
3f742090	8c 20 94 85	00 00 00 00	01 00 01 00	00 00 00 00	Њ ”…............
3f7420a0	00 00 00 00	00 01 00 00	08 06 00 00	00 00 00 00	....
3f7420b0	00 00 00 00	00 00 ac 20	00 00 00 00	58 03 00 00	......¬ ....X...
3f7420c0	00 00 00 00	00 00 00 00	4f 35 1c 3a	04 00 00 00	........O5.:....
3f7420d0	b3 3b 07 00	00 00 00 00	00 00 00 00	27 03 00 00	i;..........'...
3f7420e0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	....
3f7420f0	00 00 00 00	04 00 00 00	78 3c 8b 8c	b8 ca a8 81	........x<‹ЊёКЁЃ
3f742100	00 d0 02 00	00 0c 84 14	4d 76 ae 9a	d5 d7 d2 01	.Р....„.Mv®љХЧТ.
3f742110	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	....
3f742120	00 20 74 00	00 90 18 00	00 00 00 00	00 00 00 00	. t..ђ..........
3f742130	00 00 00 00	23 50 00 87	00 00 00 00	00 00 00 00	....#P.‡........

Получение адресного пространства процесса

Получение адресного пространства процесса [1]



Получение адресного пространства процесса [2]

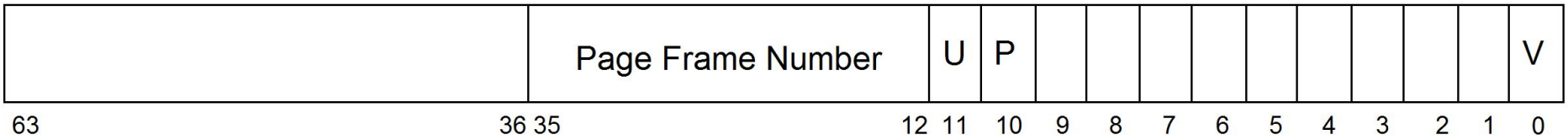
Получение адресного пространства процесса [3]

Получение адресного пространства процесса [4]

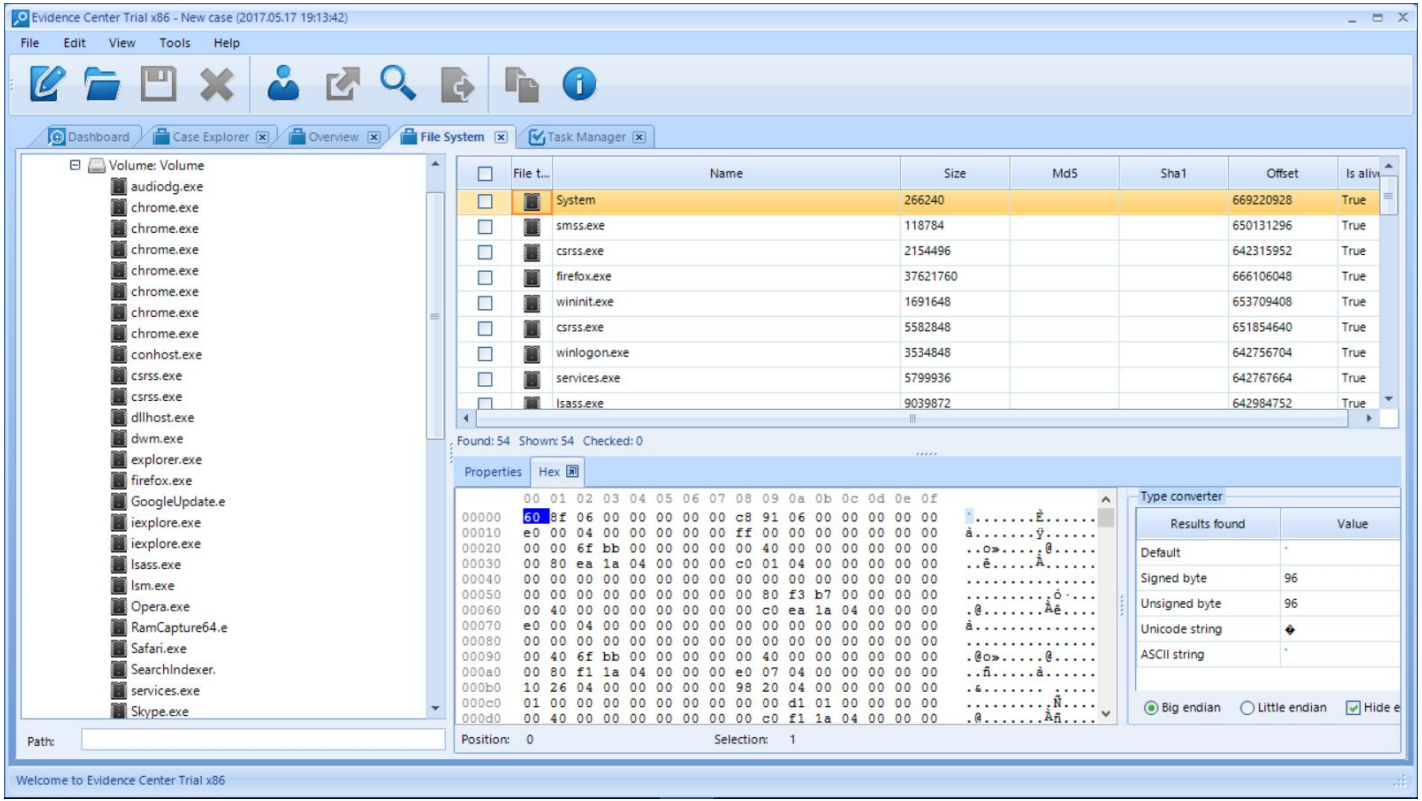
Получение адресного пространства процесса [5]

Виды недействительных записей

- Pagefile
- Demand Zero
- Transition
- Zero
- Prototype



Интеграция


Evidence Center Trial x86 - New case (2017.05.17 19:13:42)
File Edit View Tools Help
Dashboard Case Explorer Overview File System Task Manager
Volume: Volume
audiodg.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
conhost.exe
csrss.exe
csrss.exe
dllhost.exe
dwm.exe
explorer.exe
firefox.exe
GoogleUpdate.e
iexplore.exe
iexplore.exe
lsass.exe
lsm.exe
Opera.exe
RamCapture64.e
Safari.exe
SearchIndexer.
services.exe
Skype.exe
Path:
File t... Name Size Md5 Sha1 Offset Is alive
System 266240 669220928 True
smss.exe 118784 650131296 True
csrss.exe 2154496 642315952 True
firefox.exe 37621760 666106048 True
wininit.exe 1691648 653709408 True
csrss.exe 5582848 651854640 True
winlogon.exe 3534848 642756704 True
services.exe 5799936 642767664 True
lsass.exe 9039872 642984752 True
Found: 54 Shown: 54 Checked: 0
Properties Hex
Type converter
Results found Value
Default
Signed byte 96
Unsigned byte 96
Unicode string
ASCII string
Big endian Little endian Hide e
Position: 0 Selection: 1
Welcome to Evidence Center Trial x86

Заключение

- Найдены устойчивые сигнатуры для поиска процессов в Windows 10 x86 PAE
- Разработан метод восстановления адресного пространства процесса Windows 10 x86 PAE
- Реализован предложенный метод в продукте Belkasoft Evidence Center
- Проведено тестирование на пяти образах памяти