УДК 004

Ляшенко Владислав Александрович
бакалавр,
Липницкий Александр Алексеевич
бакалавр,
Пак Максим Александрович
бакалавр,
НИЯУ «МИФИ»,
Коркин Игорь Юрьевич
кандидат технических наук, инженер ООО «Вентра»,
Быковский Павел Сергеевич
бакалавр, МГТУ им. Н.Э. Баумана
(Москва, Россия)

АНАЛИЗ СПОСОБОВ ПОЛУЧЕНИЯ КОПИИ ОПЕРАТИВНОЙ ПАМЯТИ КОМПЬЮТЕРА ПОД УПРАВЛЕНИЕМ MAC OS

Аннотация. *Цель работы: определение перспективных способов получения копии оперативной памяти компьютера под управлением Mac OS.*

Метод: сравнение существующих способов получения копии памяти.

В результате работы определен оптимальный способ снятия дампа оперативной памяти компьютера Mac OS, выявлены их достоинства и недостатки. Получение копии оперативной памяти является важной задачей в компьютерной криминалистике, к сожалению, существующие способы обладают рядом недостатков и ограничений. Представленные в данной работе классификация и анализ позволяют выявить перспективные способы получения копии памяти. Также в работе представлены предложения по дальнейшему усовершенствованию существующих средств.

Ключевые слова: *Mac OS, компьютерная криминалистика, копия памяти, оперативная память, безопасность операционных систем, вредоносное ПО.*

Lyashenko Vladislav Aleksandrovich
bachelor's degree,
Alexander Lipnitsky Alekseevich
bachelor's degree,
Pak Maxim Alexandrovich
bachelor's degree
MEPhI,
Korkin Igor Yurievich
candidate of technical Sciences, engineer of Ventra LLC,
Bykovsky Pavel Sergeevich
bachelor's degree
Bauman Moscow state technical University
(Moscow, Russia)

ANALYSIS OF WAYS TO GET A COPY OF THE RAM OF A COMPUTER RUNNING MAC OS

Abstract. *Purpose: to determine promising ways to obtain a copy of the RAM*

of a computer running Mac OS.

Method: compare existing methods for getting a copy of memory.

As a result of the work, the optimal method of removal is determined dump of Mac OS RAM, their advantages and disadvantages are revealed.

Getting a copy of RAM is an important task in computer forensics, unfortunately, the existing methods have a number of disadvantages and limitations. The classification and analysis presented in this paper allow us to identify promising ways to obtain a copy of memory. The paper also presents proposals for further improvement of existing tools.

***Keywords**: Mac OS, computer forensics, memory copy, RAM, operating system security, malware.*

ВВЕДЕНИЕ.

В настоящее время активно растет количество вредоносного программного обеспечения [1]. Злоумышленники постоянно находят какие-либо уязвимости в программном обеспечении, сетевых механизмах передачи информации, а также в глубинках операционных систем. В настоящее время наиболее распространены три вида операционных систем: Windows, Mac OS, Linux. Каждая из перечисленных операционных систем имеет свои достоинства и недостатки, злоумышленники используют найденные недостатки операционных систем и используют их в своих целях. Настоящая статья посвящена исследованию способов получения копии оперативной памяти Mac OS для расследования киберпреступлений. Согласно [2] доля компьютеров под управлением Mac OS в мире составляет 13.22 %. Данный показатель занимает вторую по популярности строчку среди используемых в персональных компьютерах операционных систем. Стоит отметить, что популярность операционной системы, рассматриваемой в настоящей статье набирает популярность. В России, например, за последние 10 лет доля компьютеров под управлением Mac OS выросла в 21 раз. [2] Популярность лидера по количеству использований – ОС Windows при этом упала на 13 % за последнее десятилетие. [2]

1 Способы получения копии оперативной памяти

Получить копию оперативной памяти компьютера под управлением Mac OS можно с помощью как программных так и аппаратных средств. В этом разделе будет проведен анализ этих способов и выбран способ для получения копии оперативной памяти.

1.1 Аппаратный способ получения копии оперативной памяти

Авторы [3] описывают способы получения копии оперативной памяти, основанные на применении PCI-шины. Rutkowska J. в своей статье [4] описывает способ, основанный на перепрограммировании северного моста, благодаря чему становится возможным скрытие областей физической памяти.

Авторы статьи [5] предлагают замораживать энергозависимую память, чтобы в дальнейшем извлечь ее с носителей и анализировать. Однако, такой подход неудобен и дается всего один шанс на получение копии памяти.

Несмотря на то, что аппаратные методы устойчивы к распространенным способам скрытия областей физической памяти, они применимы только в лабораторных условиях [6].

1.2 Программные способы получения копии оперативной памяти

Изначально компания Apple разрешала программному обеспечению получать данные физической памяти через блочное устройство /dev/mem, виртуальное адресное пространство ядра было доступно через устройство /dev/kmem. На версиях Mac OS старше 10.6 эта возможность была отключена. В данном разделе будут рассмотрены средства, позволяющие получить копию оперативной памяти компьютера Mac OS с использованием программного подхода.

1.2.1 Mac Memory Reader

Mac Memory Reader [7] — это программа командной строки для получения копии содержимого физической оперативной памяти на компьютере Mac OS, позволяющая собирать информацию о нестабильном состоянии до выключения машины. Результаты хранятся либо в двоичном файле Mach-O, либо в файле «сырого» формата для последующего анализа исследователем. Программа ищет диапазоны оперативной памяти путем разбора загрузочных аргументов ядра. Mac Memory Reader предоставляется бесплатно, но имеет закрытый исходный код. Он выполняется непосредственно на 32 и 64-разрядных целевых машинах под управлением Mac OS 10.4 — 10.8 и требует PowerPC G4 или более поздней версии или любого процессора Intel. Mac Memory Reader позволяет получать копию оперативной памяти как пользовательского пространства, так и пространства ядра. Включает в себя модуль расширения ядра, который позволяет вернуть блочное устройство /dev/mem, которое было убрано компанией Apple в Mac OS 10.6. Так же пользователю после загрузки в память ядра расширения становится доступно блочное устройство /dev/pmap, которое содержит информацию о диапазонах физической памяти.

При использовании данного средства в первую очередь необходимо получить смещения и размеры объектов в оперативной памяти с помощью считывания информации из /dev/pmap. Далее можно получать копию памяти, используя блочное устройство /dev/mem. Mac Memory Reader по умолчанию сохраняет копию памяти в формате Mach-O, смещения будут необходимы при анализе копии оперативной памяти с таким расширением.

На рисунке 1 представлен скриншот примера работы Mac Memory Reader.

```
$ sudo ./MacMemoryReader mem.dmp
No kernel file specified, using '/mach_kernel'
Dumping memory regions:
available  0000000000000000 (568.00 KB)                              [WRITTEN]
available  0000000000090000 (64.00 KB)                               [WRITTEN]
available  0000000000100000 (511.00 MB)                              [WRITTEN]
available  0000000020200000 (199.00 MB)                              [WRITTEN]
LoaderData 000000002c900000 (76.00 KB)                               [WRITTEN]
available  000000002c913000 (948.00 KB)                              [WRITTEN]
LoaderData 000000002ca00000 (5.26 MB)                                [WRITTEN]
available  000000002cf42000 (760.00 KB)                              [WRITTEN]
LoaderData 000000002d000000 (35.21 MB)                               [WRITTEN]
RT_data    000000002f336000 (336.00 KB)                              [WRITTEN]
RT_code    000000002f38a000 (196.00 KB)                              [WRITTEN]
LoaderData 000000002f3bb000 (232.00 KB)                              [WRITTEN]
available  000000002f3f5000 (268.06 MB)                              [WRITTEN]
available  0000000040005000 (1.15 GB)                                [WRITTEN]
BS_data    0000000089d0f000 (84.00 KB)                               [WRITTEN]
available  0000000089d24000 (4.12 MB)                                [WRITTEN]
[snip]
Reported physical memory: 8589934592 bytes (8.00 GB)
Statistics for each physical memory segment type:
 reserved: 6 segments, 46727168 bytes (44.56 MB)--assigned to unreadable device
 LoaderCode: 2 segments, 516096 bytes (504.00 KB) -- WRITTEN
 LoaderData: 35 segments, 42881024 bytes (40.89 MB) -- WRITTEN
 BS_code: 83 segments, 2093056 bytes (2.00 MB) -- WRITTEN
 BS_data: 109 segments, 43204608 bytes (41.20 MB) -- WRITTEN
 RT_code: 1 segment, 200704 bytes (196.00 KB) -- WRITTEN
 RT_data: 1 segment, 344064 bytes (336.00 KB) -- WRITTEN
 available: 20 segments, 8436510720 bytes (7.86 GB) -- WRITTEN
 ACPI_recl: 1 segment, 155648 bytes (152.00 KB) -- WRITTEN
 ACPI_NVS: 1 segment, 262144 bytes (256.00 KB) -- WRITTEN
 MemMapIO: 3 segments, 217088 bytes (212.00 KB) -- assigned to unreadable device
Total memory written: 8526168064 bytes (7.94 GB)
Total memory assigned to unreadable devices \
      (not written): 46944256 bytes (44.77 MB)
Reported memory not in the physical memory map: 16822272 bytes (16.04 MB)
```

Рисунок 1. Пример работы Mac Memory Reader

Mac Memory Reader сообщает пользователю, что компьютер имеет 8 ГБ оперативной памяти. Последние 3 строки вывода говорят, что было записано 7,94 Гб оперативной памяти; 44,77 Мб памяти были нечитаемыми, 16,04 Мб существуют, но не были в фактической физической памяти. В сумме получается 7,99 Гб, если бы это число сильно отличалось от 8 Гб, это могло бы говорить о том, что ядро было подвергнуто модификации и возвращает неверные диапазоны памяти.

1.2.2 Mac Memoryze

Mac Memoryze [8] — еще одна программа командной строки для получения памяти из систем под управлением Mac OS версий 10.6 – 10 на 32 и 64-разрядных процессорах Intel. Формат копии оперативной памяти, предоставляемый данным средством, поддерживается Volatility Framework. В настоящий момент, нет информации о том, когда и будут ли вообще поддерживаться системы старше версии 10.8. Ниже, на рисунке 2, приведен пример использования Mac Memoryze в системе 10.8.

```
$ sudo./macmemoryze dump -f 10.8.dump
INFO: loading driver...
INFO: opening /dev/mem...
INFO: dumping memory to [/Users/a/10.8.dump]
INFO: dumping 4290871296-bytes [4092-MB]
INFO: dumping [4290871296-bytes:4092-MB]
100%
INFO: dumping complete
INFO: unloading driver...
```

Рисунок 2. Пример использования Mac Memorize

Затем можно проанализировать 10.8.dump файл с использованием Volatility. При использовании данного средства имеет место быть смазывание страниц оперативной памяти.

1.2.3 OSXPmem

OSXPmem [9] — это программа командной строки от Google с открытым исходным кодом для получения копии оперативной памяти. На момент написания настоящей работы программа позволяет получить копию оперативной памяти у компьютеров под управлением Mac OS от версии 10.6 до версии 10.14.6 включительно. Авторы программы исключили возможность получать копию оперативной памяти в компьютерах с 32 битной архитектурой. По умолчанию OSXPmem записывает копию памяти в файл формата «ELF», но средство позволяет выбрать так же «Mach-o» формат или необработанный «raw». OSXPmem, как и Mac Memory Reader, позволяет получать копию оперативной памяти уровня ядра и уровня пользователя. После загрузки драйвера ядра, который поставляется вместе с OSXPmem, становится доступно блочное устройство «/dev/pmem» из которого можно получить копию оперативной памяти компьютера.

На рисунке 3 изображен пример работы OSXPmem.

```
$ sudo./osxpmem mem.dump
[0000000000000000 - 0000000000001000] ACPI Memory NVS [WRITTEN]
[0000000000001000 - 000000000000a0000] Conventional    [WRITTEN]
[0000000000100000 - 000000002f700000] Conventional     [WRITTEN]
[000000002f700000 - 000000002f713000] Loader Data      [WRITTEN]
[000000002f713000 - 000000002f800000] Conventional     [WRITTEN]
[000000002f800000 - 000000002fd3e000] Loader Data      [WRITTEN]
[000000002fd3e000 - 000000002fe00000] Conventional     [WRITTEN]
[000000002fe00000 - 000000003137f000] Loader Data      [WRITTEN]
[000000003137f000 - 0000000003138a000] RTS Code        [WRITTEN]
[0000000003138a000 - 0000000003138f000] RTS Code       [WRITTEN]
[0000000003138f000 - 0000000031392000] RTS Code        [WRITTEN]
[0000000031392000 - 00000000313b2000] RTS Code         [WRITTEN]
[00000000313b2000 - 00000000313fc000] RTS Data         [WRITTEN]
[00000000313fc000 - 0000000031402000] RTS Data         [WRITTEN]
[0000000031402000 - 0000000031433000] Loader Data      [WRITTEN]
[0000000031433000 - 000000007db20000] Conventional     [WRITTEN]
[000000007db20000 - 000000007db9c000] Loader Code      [WRITTEN]
[000000007db9c000 - 000000007dc57000] Conventional     [WRITTEN]
[000000007dc57000 - 000000007dc90000] BS Data          [WRITTEN]
<snip>
Acquired 524192 pages (2147090432 bytes)
Size of physical address space: 4290871296 bytes (71 segments)
Successfully wrote elf image of memory to mem.dump
Kernel directory table base: 0x000000195c5000
```

Рисунок 3. Пример работы OSXPmem

Вывод OSXPmem начинается с перечисления областей, которые средство записало в файл с копией «mem.dump». Вывод заканчивается перечислением того, сколько страниц было получено, размер физического адресного пространства. Этот вывод необходим, чтобы убедиться, что вредоносное ПО и руткиты не вносили изменений в процесс получения копии оперативной памяти.

Помимо этого, возможно получение необработанной (raw) копии оперативной памяти с помощью команды «sudo dd if=/dev/pmem of=image.raw». Выполнение данной команды в терминале скопирует все содержимое оперативной памяти в файл «image.raw». Однако здесь, как и в ранее перечисленных средствах возможно «смазывание» страниц оперативной памяти.

1.2.4 Подход получения копии памяти, основанный на виртуализации

Помимо использования блочного устройства также имеет место быть подход, основанный на виртуализации. Авторы [10] [11] предлагают запустить систему в виртуальной машине, а затем остановить ее и, как результат, файл подкачки будет содержать необходимые данные (файл формата *.vmem в случае VMware). Однако, этот подход применим только если система запущена в виртуальной машине и не стоит задачи быстро получить копию памяти. Данный подход позволяет получить полную копию памяти.

В таком случае исключается возможность «смазывания» страниц памяти, поскольку пользователь не имеет возможности вносить изменения в память. Этот подход имеет недостатки, т.к. в данном случае система «замораживается» и все ее процессы приостанавливаются. Если речь идет об обычном компьютере, когда операционная система запущена без виртуализации, такой способ неприменим. Кроме того, могут возникнуть проблемы с приостановкой работающей виртуальной машины, поскольку это может повлиять на производительность и стабильность компьютера.

1.2.5 Использование двух операционных систем, для получения копии памяти одной из них

В статье [12] автор предложил использовать вторую операционную систему вместе с основной. Суть подхода основана на извлечении копии памяти первой операционной системы из второй операционной системы. Основным недостатком использования данного подхода является неудобство использования вне лабораторных условий.

1.3 Схема классификации способов получения копии памяти

На основании проведенного анализа была составлена схема классификации способов получения копии памяти. Схема представлена на рисунке 4.

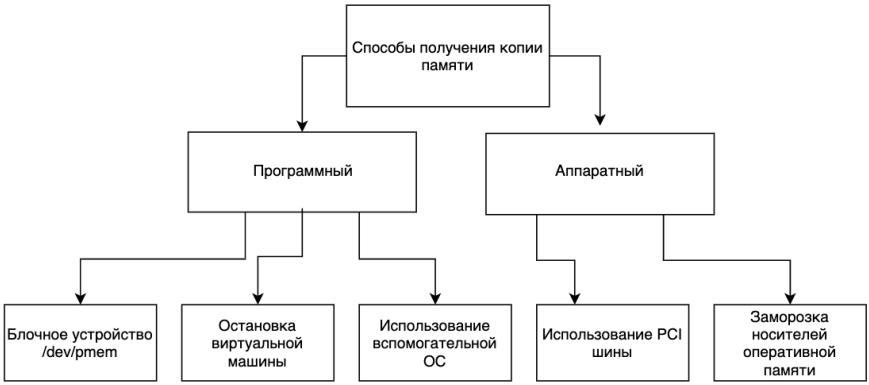

Рисунок 4. Схема классификации способов получения копии памяти

1.4 Сравнение способов получения копии памяти

Выше были рассмотрены способы и средства по получению копии оперативной памяти. Каждый подход имеет свои сильные и слабые стороны.

В таблице 1 сравниваются программные и аппаратные способы получения копии оперативной памяти.

Таблица 1.

Сравнение способов получения копии памяти

Способ / Критерий	Блочное устройство	Остановка виртуальной машины	Использование вспомогательной ОС	Использование PCI шины	Заморозка носителей памяти
Использование вне лабораторных условий	+	–	–	–	–
Получение полной копии	+	+	+/–	+/–	+
Устойчивость ко вредоносному ПО	+/–	+/–	+	+	+

На основании данных, представленных в таблице, принято решение использовать программный способ получения копии памяти, основанный на копировании содержимого памяти из блочного устройства, предоставленного после внедрения в ядро операционной системы соответствующего расширения. В таблице 2 представлено сравнение средств получения копии оперативной памяти, основанных на использовании блочного устройства.

Таблица 2.

Сравнение средств получения копии памяти

	Поддержка всех доступных форматов	Поддержка актуальной версии Mac OC	Поддержка 64 битной архитектуры	Дальнейший анализ копии с помощью известных инструментов
Mac Memory Reader	–	–	+	+
Mac Memorize	–	–	+	+
OSXPmem	+	+	+	+

Сравнение средств проводилось по 4 критериям. В результате анализа было установлено, что OSXPmem — лучший вариант для получения копии оперативной памяти. Это средство позволяет получать копию памяти на актуальных версиях Mac OS, может работать в режиме командной строки, есть возможность использования в целях дальнейшей автоматизации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Malware Statistics 2019 [Электронный ресурс] // The Independent IT Security Institute (AV-TEST). — Режим доступа к ресурсу: https://www.av-test.org/en/statistics/malware/ (Дата обращения: 21.11.2019).
2. Desktop OS Market Share Worldwide 2019 [Электронный ресурс] //GlobalStats — Statcounter. — Режим доступа к ресурсу: https://gs.statcounter.com/ os-market-share/desktop/worldwide/#monthly-200901-201912 (Дата обращения: 14.08.2019).
3. Carrier, B.D. A hardware-based memory acquisition procedure for digital investigations [Электронный ресурс] // B.D. Carrier, J.Grand — Режим доступа к ресурсу: https://www.researchgate.net/publication/222538794_A_ hardware-based_memory_acquisition_procedure_for_digital_investigations (Дата обоащения: 11.10.2019).
4. Rutkowska, J. Beyond The CPU: Defeating Hardware Based RAM Acquisition [Электронный ресурс] //Rutkowska, J — Режим доступа к ресурсу: https://www.first.org/conference/2007/papers/rutkowska-joanna-slides.pdf (Дата обращения: 15.08.2019)
5. Получаем образ оперативной памяти [Электронный ресурс] // Habr. — Режим доступа к ресурсу: https://habr.com/ru/post/211749/ (Дата обращения: 11.10.2019).
6. Korkin, I. Y. Applying Memory Forensics To Rootkot Detection [Электронный ресурс] // I.Y. Korkin, I. Nesterov — Режим доступа к ресурсу: https://sites.google.com/site/igorkorkin/cdfsl14_korkin_paper.pdf (Дата обращения: 11.10.2019).
7. Ligh, M.H. The art of Memory Forensics [Текст] // M.H. Ligh, A. Case, J. Levy, A. Walters — Wiley. — 2014, 912 с.
8. OSXPmem Mac Memory Asquistion Tool [Электронный ресурс] // Google — Режим доступа к ресурсу: https://code.google.com/archive/p/pmem/wikis/OSXPmem.wiki (Дата обращения: 11.10.2019).

9. Carvey, H. Windows Forensic Analysis DVD Toolkit [Текст] // H. Carvey — Syngress. — 2009, 512 c.
10. Vomel, S. A survey of main memory acquisition and analysis techniques for the windows operating system [Текст] // S. Vomel, F. Freiling. — The International Journal of Digital Forensics & Incident Response — 2011.
11. Schatz, B. BodySnatcher: Towards reliable volatile memory acquisition by software [Текст] // B. Schatz — Journal Digital Investigation: The International Journal of Digital Forensics & Incident Response — 2007.