ПОЛУЧЕНИЕ КРИМИНАЛИСТИЧЕСКОЙ КОПИИ ОПЕРАТИВНОЙ ПАМЯТИ НИЗКОУРОВНЕВЫМ МЕТОДОМ

Е.Е. Шабала, А.Е. Фролов
Алтайский государственный университет, г. Барнаул

Оперативная память запущенного компьютера (ПК) может содержать информацию, необходимую для проведения компьютерной криминалистической экспертизы, в том числе, данные, без которых дальнейшее проведение экспертизы невозможно — ключи шифрования дисков с данными. Поэтому получение образа оперативной памяти при проведении изъятия компьютерной техники во время оперативно-розыскных мероприятий является приоритетной задачей на данном этапе развития информационных технологий, когда большинство устройств являются зашифрованными. Основными методами извлечения образа оперативной памяти являются: программный метод (ПО, запускаемое в клиентской системе) [1], низкоуровневый (ПО, запускаемое вне операционной системы) [2], использование программно-аппаратных уязвимостей [3].

При получении образа оперативной памяти, в случае, если устройство (ПК) зашифровано, не могут быть использованы другие методы, кроме низкоуровневых, т.к. запуск программных методов не возможен, в отсутствии доступа к пользовательскому окружению изымаемого ПК. Также не могут быть использованы методы, связанные с использованием уязвимостей, т.к. их использование нарушает правовые нормы, установленные законодательством Российской Федерации [4]. На рынке специализированного программного обеспечения не предоставлено решений, реализующих функционал получения образа оперативной памяти низкоуровневым методом как в коммерческом варианте, так и в свободном. Данный факт делает актуальной задачу разработки собственной реализации данных методов.

Авторами данной работы предложен новый метод получения побитовой копии оперативной памяти без использования операционной системы, разработано программное обеспечение, реализующее данный функционал.

Для получения образа оперативной памяти предлагается специальная методика, позволяющая покинуть пользовательское окружение без потери данных, произвести перезагрузку и передать управление разработанному низкоуровневому ПО. Для реализации методики необходимо выполнить ряд действий:

1. Выполнить перезагрузку изымаемого ПК одним из двух методов [5]: холодный (Cold) и горячий (Hot). Холодная перезагрузка выполняется с помощью кратковременного сброса питания (кнопки reset). Под горячей перезагрузкой понимается перезагрузка устройства без приостановки питания, выполненная штатными средствами установленной операционной системы (ОС). При горячей перезагрузке устройства производится частичная очистка оперативной памяти [6], обеспечиваемая штатными средствами защиты используемой операционной системы. В связи с этим, в большинстве случаев необходимо использовать холодную перезагрузку. На Рис. 1 отображено количественное различие между восстановленными данными из снятого образа оперативной памяти с одного и того же устройства с использованием двух предложенных методов. Измерение проводилось путем многократного заполнения памяти ПК различными данными и приложениями, в т.ч. описанными в Таблица 1, и осуществлением перезагрузки двумя методами. Для снятия образа оперативной памяти использовалась реализация предложенной низкоуровневой методики, описанной далее. Использование метода холодной перезагрузки дает значительный прирост в объеме восстановленных из образа данных [6].

Проблема горячей перезагрузки состоит в том, что средства завершения работы ОС останавливают запущенные сервисы и процессы, выгружая их из оперативной

памяти, а занятые ими области в памяти намеренно затираются случайными данными. Данный механизм обеспечивает защиту критически важных данных ОС. В Таблице 1 указано, данные каких сервисов и программ могут быть извлечены из снятого образа оперативной памяти ОС Windows [6], после горячей и холодной перезагрузки соответственно. В Таблице 2 представлено сравнение сервисов и приложений, которые могут быть извлечены из снятого образа оперативной памяти в ОС семейства Linux соответственно после холодной и горячей перезагрузки [1].

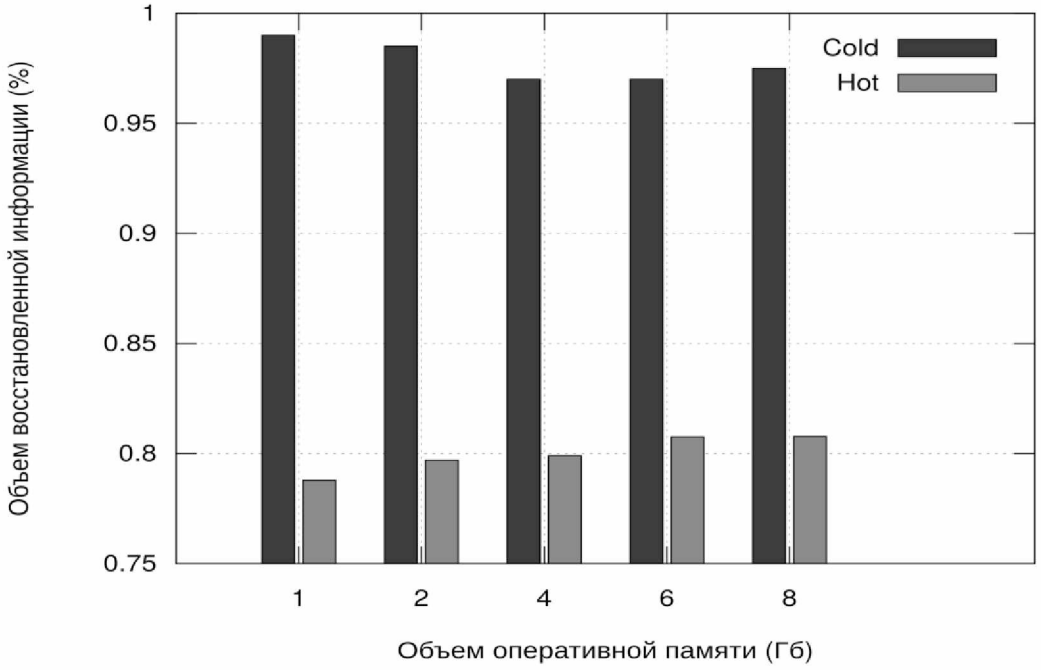

Рисунок 1 - Объем восстановленных из образа ОЗУ данных после перезагрузки методами Cold и Hot

Таблица 1. Возможности извлечения данных из образа ОЗУ полученных различными методами в ОС Windows

№	Сервис/Приложение/Данные	Горячая перезагрузка	Холодная перезагрузка
1	Bitlocker секретный ключ шифрования	Перезаписан случайными данными	Может быть обнаружен (в т.ч. в открытом виде)
2	MS SQL базы данных	Стираются заголовки, не возможно восстановить	Обнаруживаются частичные данные
3	Реестр Windows	Извлекается в неизменном виде	Извлекается в неизменном виде
4	Крипто контейнеры TrueCrypt (VeraCrypt)	Не возможно обнаружить	Возможно обнаружить ключ шифрования в обфусцированном виде, а также следы крипто-контейнеров
5	Интернет-сессии	Обнаруживаются частичные данные	Обнаруживаются более полные данные
6	Документы, изображения, открытые файлы	Частично, часто поврежденные	Частично, меньшая степень повреждения
7	Список запущенных	Могут быть обнаружены,	Обнаруживается полный их

№	Сервис/Приложение/Данные	Горячая перезагрузка	Холодная перезагрузка
	процессов и области их памяти	за исключением затертых	список, области памяти могут быть повреждены
8	Другие	Обнаруживается большинство, за исключением закрытых средствами ОС	Обнаруживаются все находящиеся в оперативной памяти до перезагрузки

Таблица 2.Возможности извлечения данных из образа ОЗУ, полученных различными методами в ОС Linux

№	Сервис/Приложение/Данные	Горячая перезагрузка	Холодная перезагрузка
1	LUKS+dm_crypt секретный ключ шифрования	Перезаписан случайными данными	Может быть обнаружен (в т.ч. в открытом виде)
2	Базы данных MySQL	Обнаруживаются частичные данные	Обнаруживаются частичные данные
3	Крипто контейнеры TrueCrypt (VeraCrypt)	Невозможно обнаружить	Возможно обнаружить ключ шифрования в обфусцированном виде, а также следы крипто-контейнеров
4	Список запущенных процессов и области их памяти	Невозможно обнаружить	Обнаруживается частичный список, области памяти могут быть повреждены
5	Интернет-сессии	Обнаруживаются частичные данные	Обнаруживаются более полные данные
6	Документы, изображения, открытые файлы	Частично, часто поврежденные	В полной мере, если не использовался SWAP файл
7	Другие	Большая часть не обнаруживается	Обнаруживается большая часть

Перезагрузка изымаемого устройства несет за собой риск потери информации, в случае, если в прошивке модуля BIOS (UEFI) содержится модуль защиты оперативной памяти от атаки холодной перезагрузки. Было протестировано 27 персональных компьютеров [6], с датой производства материнской платы от 2001 г. до 2018 г. Только одно устройство из 27 было оснащено защитным механизмом: устройство с материнской платой P5K, датой производства январь 2008 г., прошивка BIOS v 1201. Данный факт говорит о не распространённости модулей защиты, однако случай его наличия так же необходимо рассмотреть.

Авторами работы было произведено исследование зависимости процента сохранности данных в памяти ОЗУ при отключении питания в зависимости от времени. В тестировании принимало участие 10 персональных компьютеров с различными типами ОЗУ: 1x ddr1, 3x ddr2, 3x ddr3, 3x ddr4. Тестирование проводилось методикой переполнения оперативной памяти устройства с последующей холодной перезагрузкой с указанной задержкой. При этом перед перезагрузкой создавался образ оперативной памяти с помощью программных средств. После перезагрузки происходил запуск с подготовленного специального носителя (flash-накопитель с USB интерфейсом), на котором было установлено

разработанное ПО. Впоследствии путем сопоставления двух образов высчитывался процент сохранности данных (Рисунок 2.). В исследовании не бралось во внимание потенциальное различие в механизмах получения образа оперативной памяти, а именно не возможность получения программными методами доступа к памяти защищенных процессов (MS SQL, BitLocker), соответственно полученные данные отражают только потери, обусловленные отсутствием питания на чипах оперативной памяти.

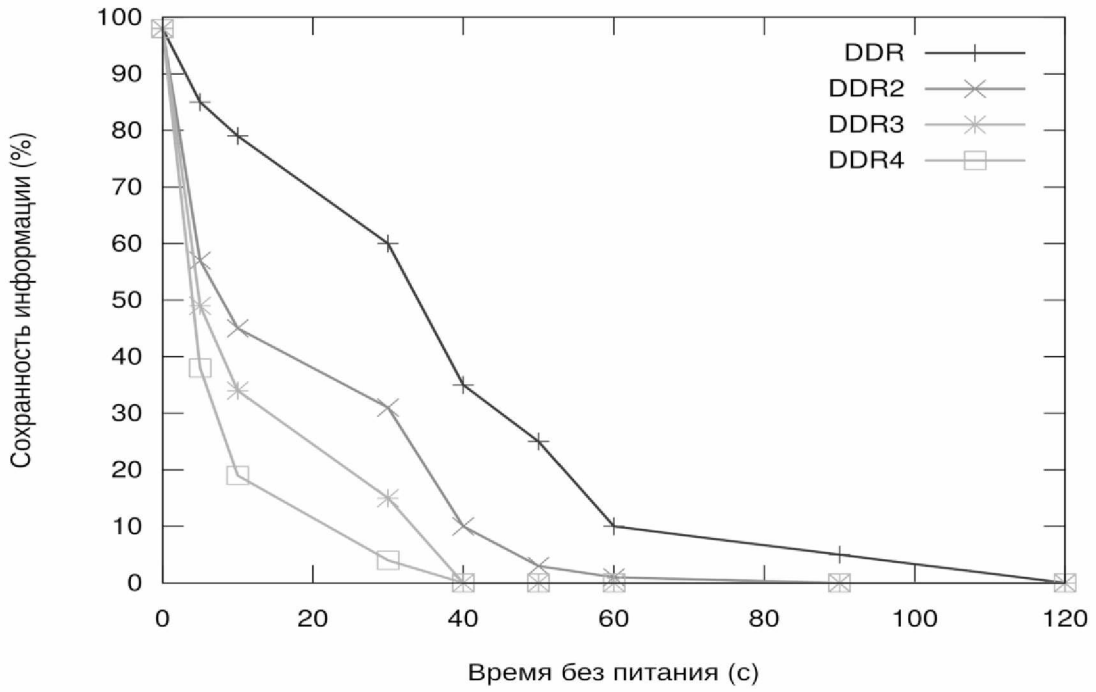

Рисунок 2 - Сохранность данных ОЗУ в зависимости от времени без питания по типу памяти

С уменьшением техпроцесса происходит снижение устойчивости чипов оперативной памяти к обесточиванию, обусловленное изменением в конструкции чипов, повышающих требованию к обеспечению питанием. Данный факт делает снятие образа оперативной памяти на защищенном устройстве технически сложной задачей, т.к. практически исключает успешность восстановления данных из образа. Возникает необходимость в повышении устойчивости к обесточиванию, что может быть обеспечено благодаря снижению температуры на чипах памяти до температуры кипения жидкого азота [2].

В случае, когда известно, что изымаемый компьютер имеет в BIOS (UEFI) модуль защиты оперативной памяти от атаки холодной перезагрузки, нет возможности применить холодную перезагрузку. Соответственно, необходимо применить горячую перезагрузку, что как указывалось ранее, накладывает ограничения на получаемый в результате снятия образа результат. Полученный образ оперативной памяти может не отвечать критерию целостности и соответственно, из него не могут быть извлечены полезные данные. В зависимости от производителя памяти наблюдается различная устойчивость к отключению питания в рамках одного типа памяти (Рис. 3).

2. Произвести загрузку со специального носителя, на который установлено разработанное авторами программное обеспечение, реализующие низкоуровневое побитовое копирование информации из оперативной памяти на внутреннюю память носителя. Основой для носителя информации является flash-накопитель с USB интерфейсом.

Структура памяти специального носителя (Рисунок 4) представляет собой таблицу совокупность специальных разделов памяти. Перед произведением разметки памяти все ее ячейки «зануляются», далее в начальные сектора устанавливается Master Boot Record (MBR). Создается разделом размером 1 Мб с файловой системой fat-16. Выбор данной файловой системы обусловлен особенностями реализации загрузчика syslinux, отвечающего за запуск разработанного ПО. В данный раздел производится установка специальным образом скомпилированного дистрибутива syslinux и исполняемого файла, представляющего собой разработанное ПО, скомпилированное в исполняемый формат .c32.

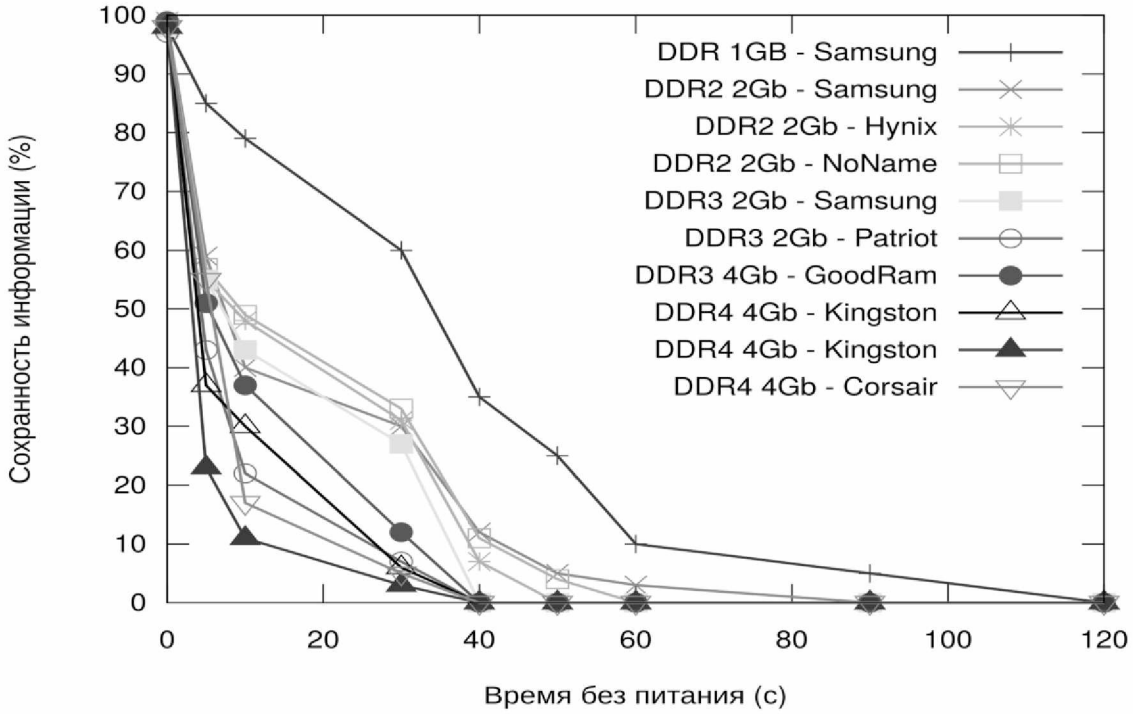

Рисунок 3. - Сохранность данных ОЗУ в зависимости от времени без питания по производителю

Переносной носитель (USB flash, HDD)			
MBR	FAT-16	VENIX-80286 (40) -> Personal Risc Boot	Множество разделов под образы памяти в рамках общей емкости переносного носителя
	SysLinux + Код программы	Образ памяти RAM	
512 B	1 MB	Объем памяти RAM	

Рисунок 4 - Структура памяти специального носителя

Оставшаяся не размеченная область памяти делится на необходимые по объему части (разделы) по следующему правилу: емкость раздела должна соответствовать или быть больше объема оперативной памяти, образ которой необходимо сделать. Количество разделов не ограниченно, их размер может быть разным, однако использоваться они могут только в порядке расположения в памяти накопителя.

Область памяти, выделенная под разделы, не подлежит форматированию, для данной области указываются лишь границы и цифровой код, указывающий на принадлежность раздела к типу «Venix 80286». Файловая система «Venix 80286» обеспечивает низкоуровневый доступ к ячейкам памяти. После запуска, разработанного ПО, происходит обнаружение разделов на носителе, выбирается первый раздел типа 40 («Venix 80286»). Перед началом создания образа, тип раздела меняется на 41 («Personal RISIC Boot»), это обеспечивает возможность многократного

использования носителя информации для извлечения образа оперативной памяти и гарантирует целостность данных на уже использованных разделах носителя.

В последствии, с помощью утилиты dd можно произвести побитовое копирования с раздела типа «Personal RISIC Boot» специального носителя, при этом случайная запись на это устройство не возможна, т.к. ОС Windows и ОС Linux не поддерживают работу с данными файловыми системами.

Предложенная методика получения образа оперативной памяти может найти применение как в работе компьютерных криминалистов, осуществляющих изъятие информации, так и при проведении компьютерной криминалистической экспертизы. Данный метод позволяет эксперту следовать как требованиям «Уголовно-процессуального кодекса Российской Федерации» [4] при изъятии образа оперативной памяти, так и положениям № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» [7] при проведении компьютерной криминалистической экспертизы. Применение данной методики может быть единственной законной возможностью для снятия образа оперативной памяти, а его открытость и распространение разработанного ПО под свободной лицензией, обеспечивает возможность внесения требуемых изменений в его код компетентными органами, для обеспечения соответствия необходимым нормативным актам [8].

Библиографический список

1. Pettersson T. Cryptographic key recovery from Linux memory dumps // Presentation, Chaos Communication Camp – 2007.
2. Halderman J.A., Schoen S., Nadia H., Clarkson W.; Paul W.; Calandrino J., Feldman J.; Appelbaum J. и др. Lest We Remember: Cold Boot Attacks on Encryption Keys // In 17th USENIX Security Symposium - 2008.
3. Maartmann-Moe Ch. Inception Metasploit integration // 2013. URL:http://www.breaknenter.org/projects/inception/.
4. "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ.
5. Carvey H. Windows Forensic Analysis DVD Toolkit // ISBN: 9780080957036 – Syngress - 2018.
6. Шабала Е.Е., Фролов А.Е. Низкоуровневый метод извлечения образа оперативной памяти для проведения компьютерной криминалистической экспертизы // Труды молодых ученых Алтайского государственного университета - №16 - 2019.
7. Федеральный закон от 31 мая 2001 г. N 73-ФЗ "О государственной судебно-экспертной деятельности в Российской Федерации".
8. Федеральный закон "Об оперативно-розыскной деятельности" от 12.08.1995 N 144-ФЗ.