20. Цінові пропозиції на вживану техніку на колісному та гусеничному ходу [Електронний ресурс]. — Режим доступу: http://www.inter-serwis.com
21. Цінові пропозиції на вживану техніку на колісному та гусеничному ходу [Електронний ресурс]. — Режим доступу: http://www.adstechnic.pl
22. Цінові пропозиції на вживану техніку на колісному та гусеничному ходу [Електронний ресурс]. — Режим доступу: http://www.machinery24.pl
23. Цінові пропозиції на вживану техніку на колісному та гусеничному ходу [Електронний ресурс]. — Режим доступу: http://www.sztaplarka.pl
24. Цінові пропозиції на вживану техніку на колісному та гусеничному ходу [Електронний ресурс]. — Режим доступу: http://www.crm.nl
25. Цінові пропозиції на вживану техніку на колісному та гусеничному ходу [Електронний ресурс]. — Режим доступу: http://www.edelmanntruck.ch
26. Цінові пропозиції на вживану техніку на колісному та гусеничному ходу [Електронний ресурс]. — Режим доступу: http://www.europe-camions.com
27. Цінові пропозиції на вживану техніку на колісному та гусеничному ходу [Електронний ресурс]. — Режим доступу: http://epaper.truckmarket.de
28. Цінові пропозиції на вживану техніку на колісному та гусеничному ходу [Електронний ресурс]. — Режим доступу: http://eu.ironplanet.com

Резюме

В статье приведена классификация специальной техники, рассмотрена база оценки и порядок определения стоимости, методические подходы к оценке специальной техники и их основные положения, приведен алгоритм определения рыночной стоимости специальной техники.

Resume

The article presents classification of special equipment, based on the assessment and the procedure for determining the value and methodological approaches to the assessment of special machines and their basic principles, the algorithm for determining the market value of the special equipment.

УДК 343.98:681.3

В.О. Чумаченко, провідний судовий експерт

Київський НДІ судових експертиз

РЕКОМЕНДАЦІЇ ТА ДЕЯКІ ТЕХНІЧНІ ПІДХОДИ З ОТРИМАННЯ ОБРАЗУ ДАНИХ ОПЕРАТИВНОЇ ПАМ'ЯТІ ПЕРСОНАЛЬНОЇ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ МАШИНИ (ПЕОМ)

Аналіз та вивчення вмісту оперативної пам'яті є важливим технічним заходом для розуміння всіх попередніх дій на ПЕОМ. Оперативна пам'ять може містити, як частину ініційованих програмним забезпеченням певних процесів так і даних про видалення файлів, відкритих сесій, ключів для криптографічних перетворень тощо. Дана стаття надає рекомендації та практичні приклади з отримання образу даних оперативної пам'яті ПЕОМ.

В останній час у практиці судово-експертного дослідження за спеціальностями 10.9 "Дослідження комп'ютерної техніки та програмних продуктів" та 10.17 "Дослідження телекомунікаційних систем (обладнання) та засобів" все частіше трапляються випадки криптографічного захисту інформації, що містять вкрай важливі дані для вирішення питань експертизи та у деяких категоріях справ — встановлюють істинні обставини чи наслідки. Крім того зустрічаються питання, щодо наявних даних про відправлені та отримані повідомлення в соціальних мережах та чатах.

За архітектурою створення та функціонування програмного забезпечення, відомо, що під час ініціалізації (запуск) програмного забезпечення, виділяється в оперативно-запам'ятовуючому пристрої ПЕОМ (далі за текстом — оперативна пам'ять) певний адресний простір пам'яті. В зазначеному адресному просторі, програмне забезпечення, що знаходиться в запущеному стані зберігає відповідні параметри, ключі та іншу інформацію. Особливо слід пам'ятати, що дані в оперативно-запам'ятовуючому пристрої присутні лише у процесі функціонування ПЕОМ (включеному живленні) та після вимкнення живлення та перезавантаження операційної системи повністю знищуються. За такими обставинами вкрай важливі дані у тому числі ключі для можливості розкриття зашифрованої інформації будуть знищені на завжди.

Іншими словами, під час слідчих дій, вимкнувши живленням ПЕОМ, не виконавши технічних заходів із зняття образу оперативної пам'яті, назавжди будуть знищені такі вкрай важливі дані:

- останні повідомлення в соціальних мережах;
- зникнуть на завжди ключі якими зашифровані крипто контейнери або окремі логічні розділи;
- назавжди буде втрачено перелік Інтернет ресурсів, які у приватному режимі відвідував користувач ПЕОМ;
- також без можливості відновлення будуть втрачені інші дані.

Таким чином, для отримання та можливості подальшого експертного аналізу зазначених даних, необхідно на етапі слідчих дії (можливо із залученням експертів) отримати образ оперативної пам'яті ПЕОМ.

Які ж саме дані можливо знайти в образі оперативної пам'яті, в рамках проведення комп'ютерно-технічної експертизи. В оперативній пам'яті ПЕОМ можливо знайти відповіді на ряд важливих питань експертизи. Наприклад: ключі, які використовувались для криптографічного захисту. В оперативній пам'яті містяться останні повідомлення,

отримані та відправлені через соціальні мережі; коментарі, що залишені на форумах; повідомлення, що передавались з використанням програмного забезпечення обміну короткими повідомленнями або "чату" що інтегровані в комп'ютерні ігри. Також в оперативній пам'яті можливо знайти назву останніх завантажених файлів. В оперативній пам'яті ПЕОМ деякий час зберігаються сторінки із зображенням з ВЕБ-сайтів — навіть якщо вони переглядались в "приватному режимі". Крім того доступна велика кількість даних операційної системи та прикладного програмного забезпечення, а саме дані "реєстру", розпаковані та розшифровані версії захищених програм, дані з IP-адресами відкритих з'єднань. Слід звернути особливу увагу, що дані з відкритих з'єднаннями надають можливість у більш точній ідентифікації шкідливого програмного забезпечення.

Враховуючи вище наведену інформацію, а також аргументи у доцільності отримання образу оперативної пам'яті на етапі слідчих дій розглянемо рекомендації та приклади технічних заходів по створенню (отриманні) образів оперативної пам'яті.

Орієнтовно, створення образу оперативної пам'яті займає від 5 до 15 хвилин. Технічний інструментар для виконання зазначеного заходу — мінімальний, достатньо мати будь-який USB-накопичувач, але не менше за об'ємом оперативної пам'яті, а також спеціальну безкоштовну програмну утиліту LiveRAMCaptureвід виробника Belkasoft її можливо завантажити з офіційного сайту http://ru.belkasoft.com/ru/memory-dump/.

Зазначена утиліта не потребує інсталяції, необхідно лише розмістити на USB-накопичувачі і запустити її враховуючи розрядності системи 32-х чи 64-х. Сама процедура створення образу оперативної пам'яті не потребує спеціальних знань, необхідно лише вибрати директорії для зберігання образу, тобто директорію на підготовленому USB-накопичувачі, можливо навіть в тому з якого запускається LiveRAMCapture та натиснути "Capture".

Однак, якщо звернути увагу, зазначений метод отримання образу оперативної пам'яті може використовуватись для операційних систем сімейства Microsoft Windows. Яким же чином можливо отримати образи оперативної пам'яті з інших операційних систем? Відповідь на зазначене питання можливо знайти через метод "гарячого" перезавантаження із запуском ПЕОМ в Live-режимі.

Одним із варіантів, отримання образу оперативної пам'яті є використання спеціального дистрибутиву Ubuntu CyberPack (IRF) 1.0,

який містить мінімальний набір компонентів, а саме, тільке ті, що необхідні для отримання (вилучення) даних з оперативної пам'яті. Звісно відсутній графічний інтерфейс, а таким чином всі дії необхідно виконувати в режимі командної строки, а як наслідок на відміну від першого методу, для виконання зазначених технічних дій необхідно володіти більш високим навиками роботи на ПЕОМ та розуміти структуру представлення апаратних та програмних засобів в Unix-подібних операційних системах.

Враховуючи можливі складності під час використання Ubuntu CyberPack (IRF) 1.0 розглянемо у деталях зазначений метод отримання даних з оперативної пам'яті.

Перш за все необхідно пам'ятати, що використання зазначеного методу має ряд переваг і недоліків.

Переваги:

- використання Live-дистрибутива надає можливість проводити дії не залежно від типу операційної системи;
- відсутня необхідність додатково використовувати придбані засоби комунікації та спеціалізовані пристрої.

Недоліки:

- вміст оперативної пам'яті буде не повним — частина буде перезаписана даними, необхідними для завантаження Ubuntu CyberPack (орієнтовано 125 Мб).

Зауваження:

- другої можливості в отриманні вмісту оперативної пам'яті не буде — є тільки одна спроба. Після перезавантаження більшість даних оперативної пам'яті будуть перезаписані;
- необхідно підготуватися (записати образ Ubuntu CyberPack на оптичний чи USB носій) та розуміти, що під час завантаження BIOS, необхідно вибрати завантаження з CD/DVD-приводу або USB, після чого почнеться завантаження Live-дистрибутива (Ubuntu CyberPack).

І так, почнемо:

Перезавантажимо ПЕОМ.

Важливо: перезавантаження ні в якому випадку не повинно бути холодним (через натискання кнопки "ресет" або вимкненням живленням), а лише — перезавантаження має бути виконано засобами операційної системи (наприклад: натисканням кнопок Ctrl-Alt-Del або вибрати пункт "Перезавантаження" в операційній системі), зазначений метод прийнято називати "гарячий".

Рис. 1

Після завантаження дистрибутива Ubuntu CyberPack спеціалісту/експерту доступна командна строчка Linux та інформація для запуску окремих пакетів (рис. 1).

Важливо: зрозуміло, що образ вмісту оперативної пам'яті необхідно перемістити на зовнішній накопичувач, а для цього необхідно виконати спеціальну процедуру "монтування" зовнішнього пристрою (флеш або ін.). Обов'язково необхідно до початку "монтування" провести процедуру форматування зовнішнього накопичувача у файлову систему типу ext3 або ext4. Після форматування необхідно приєднати зовнішній носій до USB.

Для визначення, який ідентифікатор присвоєний зовнішньому носієві, необхідно після його приєднання до ПЕОМ завантаженого через використання Live-дистрибутивом Ubuntu CyberPack виконати наступну команду:

dmesg | tail (команда виводить на екран інформацію з буфера повідомлень ядра. Нас цікавить останній запис).

Результат на прикладі виконання команди dmesg | tail:

[16091.995428] sd 9:0:0:0: Attached scsi generic sg2 type 0

[16091.995996] sd 9:0:0:0: [sda] 32096120 512-byte logical blocks: (16.4 GB/15.3 GiB)

[16091.998192] sd 9:0:0:0: [sda] Write Protect is off

[16091.998205] sd 9:0:0:0: [sda] Mode Sense: 0b 00 00 08

[16091.999433] sd 9:0:0:0: [sda] No Caching mode page found

[16091.999447] sd 9:0:0:0: [sda] Assuming drive cache: write through

[16092.003486] sd 9:0:0:0: [sda] No Caching mode page found

[16092.003495] sd 9:0:0:0: [sda] Assuming drive cache: write through

[16092.004251] sdb: sdb1

("sdb" — це присвоєний значення зовнішньому носію).

Далі необхідно створити папку в яку буде "монтуватись" зовнішній носій. Наприклад: mkdir /media/flash. В подальшому необхідно "монтувати" логічний розділ зовнішнього носія в створену папку:

```
----
mount /dev/sdb1/ /media/flash
----
```

У разі вдалого “монтування” доступ до зовнішнього носія з’явиться в директорії /media/flash у іншому випадку з’явитись повідомлення про помилку. У разі помилки необхідно виконати інструкцію, що буде наведена в повідомлені про помилку.

Таким чином вважаємо, що всі необхідні технічні процеси виконано і можливо здійснити процедуру отримання даних з оперативної пам’яті.

---

dd if=/dev/fmem of=/media/flash/ram.mem bs=1k count=’head -1 /proc/meminfo | awk ’{print $2}’ ’

(dd — утиліта створення образу

“if=/dev/fmem” — джерело даних оперативної пам’яті

“of=/media/flash/ram.mem” — запис в файл “ram.mem” в папку /flash, яка фактично є зовнішнім накопичуваче

“bs=1K” — розмір блока інформації — 1 Kb

“count=’head -1 /proc/meminfo | awk ’{print $2}’’ — об’єм оперативної пам’яті)

У результаті вдалого виконання команду, ми повинні отримати повідомлення, що схоже на рис. 2.

(521453568 bytes (521 MB) copied — об’єм скопійованих даних

“158.405 s” — час виконання процедури копіювання

“3.3 MB/s” — швидкість копіювання даних)

У подальшому командою umount /media/flash необхідно “демонтувати” зовнішній накопичувач та разом з ПЕОМ надати його на дослідження до спеціалізованої експертної установи, яка згідно ЗУ “Про судову експертизу” визначена суб’єктом судово-експертної діяльності.

Зустрічаються випадки, особливо під час слідчих дій, коли на вхід в ПЕОМ встановлений пароль. І як відомо, розповсюджені методи обходу паролю потребують перезавантаження ПЕОМ, а як наслідок дані з оперативної пам’яті будуть частково, а можливо і в цілому втрачені.

```
root@ubuntu:/tmp# dd if=/dev/fmem of=/tmp/ram-image.mem bs=1K count=`head -1 /pr
oc/meminfo | awk '{print $2}'`
509232+0 records in
509232+0 records out
521453568 bytes (521 MB) copied, 158.405 s, 3.3 MB/s
root@ubuntu:/tmp# _
```

Рис. 2

Необхідно звернути особливу увагу, якщо є інформація про наявність криптографічного захисту сектору завантаження, у разі перезавантаження ПЕОМ, відновити доступ навіть до даних на жорстких дисках буде не можливо. В такому випадку (коли на вхід в ПЕОМ встановлений пароль) можливо використати методику, що описана австрійськими дослідниками. Якщо подивитись з боку апаратного забезпечення ПЕОМ в більшості сучасних ПЕОМ є мінімум один порт IEEE 1394, відомий також під назвою FireWire або i.LINK. Стандарт FireWire описує можливість прямого доступу в оперативну пам'ять ПЕОМ через канал DMA. Таким чином, фактично існує можливість створити копію даних оперативної пам'яті.

Тобто, для цього, необхідно з'єднати робочий ПЕОМ експерта/спеціаліста з ПЕОМ (обов'язково у робочому стані), який заблокований на вхід паролем звичайним FireWire кабелем. Та на робочому ПЕОМ експерта/спеціаліст з використанням спеціалізованого програмного забезпечення наприклад: Inception (завантажити можливо з https://github.com/carmaa/inception) завантажити вміст оперативної пам'яті із заблокованого ПЕОМ на ПЕОМ експерта/спеціаліста.

Обов'язково у разі отримання образу оперативної памяті з декількох ПЕОМ необхідно чітко провести ідентифікацію файлів образів з ПЕОМ, іншими словами вказати з якого саме ПЕОМ отримано той чи інший образ оперативної пам'яті.

Список використаної літератури

1. Belkasoft. — [Електронний ресурс]. — Режим доступуhttp://ru.belkasoft.com/ru/memory-dump/
2. GitHub. — [Електронний ресурс]. — Режим доступу: https://github.com/carmaa/inception

Резюме

Анализ и изучение содержимого оперативной памяти является важнейшем техническим процессом для понимания всех предыдущих действий пользователем ПК. Оперативная память может содержать, как часть инициированных программным обеспечением определенных процессов, так и данные про удаленные файлы, открытые сессии, ключи криптографического кодирования и т.д. В данной статье рассмотрены рекомендации и практические примеры по созданию образа/копии данных с оперативной памяти ПК.

Summary

Examination of RAM contents is crucial for understanding processes that happened on PC. RAM contents could have both code of programs and data about file deletion, opened sessions, encryption keys etc. The following article provides recommendations and examples of RAM acquiring.