2016

Memory forensic data recovery utilising RAM cooling methods

Kedar Gupta
Auckland University of Technology

Alastair Nisbet
Auckland University of Technology

DOI: 10.4225/75/58a54cc3c64a2
Gupta, K. & Nisbet, A. (2016). **Memory forensic data recovery utilising RAM cooling methods**. In Valli, C. (Ed.). (2016). *The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia*. (pp. 11-16).

MEMORY FORENSIC DATA RECOVERY UTILISING RAM COOLING METHODS

Kedar Gupta, Alastair Nisbet
Security & Forensic Research Group, Auckland University of Technology
Auckland, New Zealand
kedargupta@msn.com, alastair.nisbet@aut.ac.nz

Abstract

Forensic investigations of digital devices is generally conducted on a seized device in a secure environment. This usually necessitates powering down the device and taking an image of the hard drive or semi-permanent storage in the case of solid state technology. Guidelines for forensic investigations of computers advise that the computer should be shut down by removing the power supply and thereby maintaining the hard disk in the state it was in whilst running. However, valuable forensic evidence often exists in the volatile memory which is lost when this process is followed. The issues of locked accounts on running computers and encrypted files present particular difficulties for forensic investigators who wish to capture a forensic image of the RAM. This research involves freezing RAM removed from a running computer so that it can later be reinserted into an unlocked computer allowing for a forensic image of the RAM to be captured. Three different methods of cooling the RAM are compared, along with varying delays in RAM reinsertion. The results provide a guideline for forensic investigators on how the issues with locked accounts and encryption may be overcome to record this valuable evidence that is otherwise lost.

Keywords
information security, RAM, forensics

INTRODUCTION

The forensic investigation of digital devices usually involves an investigator examining a cell phone, tablet of computer hard disk in a sterile environment. Guidelines for forensic investigators often advise that if a computer is running, it should be switched off at the power source to preserve the hard drive in its current state (National Institute of Justice 2008). One authoritative guide for forensic investigations suggested the need to preserve all evidence yet then suggested that power should be removed immediately from a running computer. This was corrected in a later version where a greater recognition of the value of evidence in the memory was recognised. (Association of Chief Police Officers (ACPO) 2012). Shutting down the computer using the normal method will inevitably cause data to be written to the hard drive possibly overwriting valuable forensic evidence from deleted files (Vidas 2007). Whilst this method focusses on the potential forensic evidence on a hard drive, the Random Access Memory (RAM) is often overlooked as a source of forensic evidence. RAM may contain highly valuable forensic data such as web browsing history, programs that have been recently run or werecurrently running and usernames and passwords in unencrypted form (Halderman, Schoen et al. 2009). This highly valuable and useful information will be lost the instant power is switched off to the computer (Simon and Slay 2009).

It is fairly trivial to insert a USB drive with the required software to download the contents of RAM on to an external drive for later analysis. Whilst often this is not done, the fact that RAM may contain several gigabytes of valuable forensic evidence means that evidence is lost because the forensic investigator has not considered this area to be valuable to an investigation. One problem that may arise for an investigator is that of a computer that has been locked by the user and requires a password to unlock the user account. Whilst this may not present a problem in recovering hard drive evidence, the shutting down of the computer will permanently delete the volatile evidence in memory. Another significant issue that has surfaced in recent years for forensic investigators is the increasing use of cryptographic tools to encrypt files or entire hard drives. The cryptography is generally robust enough to withstand all attempts at finding the encryption key required to unlock this evidence. A securely encrypted drive means that evidence can be seized but that it simply cannot be read rendering it useless.

This research examines the area of RAM forensics as an important source of digital forensic evidence for investigators. Methods of freezing RAM are utilised to compare the retention of data within the RAM utilising three different methods. Results are then compared so that guidelines for forensic investigators are presented allowing recovery of RAM contents using these methods.

STATE OF THE ART

The physical address space consists of all valid physical memory addresses that are readable by the CPU (Intel Corporation 2013). The Memory Management Unit (MMU) acts as an intermediary between the operating system and the memory so that any attempt at acquiring the contents of RAM will require the utilised software to overcome restrictions created by the MMU. Whilst the utilisation of address spaces may vary across architectures and operating systems, the address spaces in RAM are all potentially accessible through specialised software.

The layout of the physical address space in RAM is finalised upon completion of the copying of firmware code from ROM to RAM (Salihun 2012). Once this is complete, the RAM is ready for use by the operating system. Some forensic guidelines suggest photographing a computer screen and then switching the computer off at the power supply but forensic investigators are often aware of the valuable evidence contained in RAM and suggest performing a memory dump prior to powering off the system (Ligh, Case et al. 2014). Whilst a memory dump of RAM should provide all contents of RAM, it is possible that memory smear may occur because of the time taken to acquire the RAM contents (Vömel and Freiling 2012). Memory smear occurs when memory is copied from RAM to a physical media and during this process some errors occur because of the time taken for the acquisition. This results in minor differences between the RAM contents and the RAM image so that whilst a 100% match of the contents is hoped for, often the image falls slightly below a 100% match.

To overcome this problem, a hardware-based approach using a Firewire connection can be utilised which provides more direct access to RAM, decreasing the error rate to the point that often a 100% match can be achieved (Huebner, Bem et al. 2007). If the Firewire approach is not feasible and the computer is running a Windows operating system, then 2 other methods may provide greater reliability than a memory dump (Ruff 2008). Firstly, intentionally crashing the operating system will cause the RAM contents to be copied to the hard disk meaning a forensic acquisition of the hard disk should include most, if not all of the contents of RAM. The drawback to this method on a Windows Operating System is that the same computer must be rebooted to allow memory to be rewritten to the RAM (Russinovich, Solomon et al. 2012). The second method is to utilise the hibernation feature which will copy the contents of RAM to the hard disk and then power down the computer.

Whilst Firewire may provide greater reliability in copying memory to external storage, and the other methods suggested may provide sufficient integrity of the data for Windows Operating Systems, the forensic investigator may be in a position where these options are not available. Additionally, these options won't work if the computer has been locked by the user so that access to the RAM is not available. This problem is common and whilst asking for the password may be an option, a legally savvy suspect will likely refuse to give the password. Furthermore, full disk encryption is becoming more commonplace with freely available software such as TrueCrypt that will encrypt all files on a disk rendering them unreadable unless the password is disclosed that will decrypt the files. One issue that may also present to investigators during the memory acquisition phase is a deliberate attempt to corrupt the contents of memory if a memory dump is attempted. Specialised software designed to corrupt the memory can be created and will run when the memory is dumped from the operating system (Milkovic 2012). This can be overcome if the anti-forensic can be disabled or the RAM can be removed and inserted into another, similar but clean computer.

In 2016, an experiment was run in freezing RAM using freezing spray (Bauer, Gruhn & Freiling, 2016). In this experiment the RAM was cooled insitu with the computer running. The focus on the experiments was to demonstrate the recovery of the data and how it could be unscrambled to produce an original image or file. Unlike the current experiments, it did not utilise cooling with liquid nitrogen or ice and so has a different focus than this research.

The following section describes the experiments in cooling RAM so that the forensic investigator can remove the ram yet maintain the integrity of the data for a sufficient period of time to permit forensic analysis of the contents.

EXPERIMENTAL DESIGN

The problem for forensic investigators of locked user accounts means that RAM cannot be examined because an unlocked computer is required to examine and download RAM. The computer is locked by the user selecting 'ctrl alt delete' which then requires that same user's password to be entered to unlock the computer. What is

therefore required from a forensic investigator is the ability to remove RAM from a locked computer without losing the integrity of the digital contents and to either place the RAM into an identical computer or to reboot the suspect computer into a state where it is not locked. The RAM can then be inserted into the unlocked computer and a memory dump performed. The first stage in the experiments was to boot a laptop computer to the Windows 7 operating system. This system was chosen as it remains one of the most common operating systems in organisations and for home users. Six actions were then performed to provide data in the 1 GB RAM that would be useful in an investigation.

Those actions were:

1. Log on to Windows 7 with the administrator username and password.
2. Open a text file and copied text to the clipboard.
3. Started an Apache HTTP web server and MySQL database.
4. Unlocked a TrueCrypt file container and opened several files from the container.
5. Executed several commands using a DOS prompt.
6. Launched a web browser and logged into a Facebook account.

The process for calculating the percentage of data recovered was to take an image of the RAM and then to lock the account on the computer. The power button was then held down to halt power to the motherboard and the RAM removed at the same time where it was immediately put through the cooling process. Once the full experiment was completed and a RAM image obtained, this image was then compared to the prior image and the percentage of data recovered calculated.

Whilst this gives an accurate percentage of the data recovered, it does so at a macro level so that if parts of files are recovered or even parts of passwords, this is not obvious from the percentages that are recovered. To ascertain at a micro level, a more manual examination is required and in the case of recovered passwords this was done to ensure that a full password or encryption key has been recovered. The parameters for the test bed are shown in table 1:

Table 1: Testbed Setup

Item	**Description**
RAM	1GB DDR3
Error Correction?	Non Error Correction RAM
CPU	Samsung 2.4GHz

The experiments with freezing RAM to recover its contents began with a baseline to compare the results against. The baseline simply involved removing RAM from a computer and inserting the RAM into the now unlocked and rebooted computer. The minimum time between removal of the RAM and insertion into the computer was 10 minutes, allowing ample time for the investigator to reboot the machine to a usable state.

The surface temperature of the RAM was measured at 35 degrees centigrade. As expected, the contents of RAM were deleted upon removal so that no usable forensic evidence could be recovered using this method.

Table 2 shows the experimental setup for the RAM utilising three different cooling methods. The ambient temperature of the RAM before cooling was 35° degrees centigrade.

Table 2: RAM Freezing Experimental Steps

Method	Time Delay	Temperature Cooled degrees C
Liquid Nitrogen	10mins, 1 hr, 2hrs	-196
Freezing Spray	10 mins	-40
ICE	10 mins	10

The next step was to utilise liquid nitrogen to freeze the RAM. This has been attempted by previous researchers with good results. The RAM was removed from the running but locked computer and immediately submerged in liquid nitrogen, almost instantly freezing the RAM and it was hoped that the contents would therefore remain. The surface temperature of the RAM was measured at -196 degrees centigrade. The experiment was repeated a number of times with varying longer delays in removing the RAM from the liquid nitrogen to see of entropy of the contents occurred. The experiment was then repeated but with a spray of freezing compressed air rather than liquid nitrogen. The freezing by compressed air was a simple process and could easily be performed by a forensic investigator in the field as opposed to the practicality of carrying liquid nitrogen to an investigation scene. The surface temperature of the RAM was measured at -40 degrees centigrade. Finally, the third stage involved removing the RAM, placing it in an anti-static bag and burying it in ice cubes for 10 minutes. The surface temperature was measured at 10 degrees centigrade just immediately after removing it from the ice. Once cooled, the RAM was then reinserted into the same computer and the computer booted from a USB stick with DumpIT, a Linux memory dumping software programme installed on the stick which creates an image of the RAM. In the initial boot stages, the software immediately dumped the contents of the RAM onto a storage area on the USB stick where it remained for later analysis. The results of the RAM cooling are described below.

RESULTS

The purpose of the experiments was to ascertain whether freezing RAM with compressed air or ice would provide forensic evidence from the RAM that could be utilised in an investigation. It was ascertained that removing RAM and reinserting it 10 minutes later led to almost all contents being deleted. The liquid nitrogen provided results that led to almost a complete recovery of the RAM but was not practical for a forensic investigation in the field. Therefore, the freezing spray and submergence in ice were of particular interest as these methods are both feasible for an investigator. A can of freezing spray is easily obtainable for negligible cost and ice may be available if a forensic investigator has no freezing spray readably available. The following table shows the results in percentage of data recovered from RAM after 10 minutes.

Table 3: Percentage of forensic data recovered

Method	Temperature degrees Celsius	Percentage Recovered
No cooling	35	0.2%
Liquid Nitrogen	-196	99.81%
Freezing Spray	-40	96.45%
Ice	10	99.71%

The results indicated that whilst liquid nitrogen performed the best, submerging the RAM in ice was a very close second best with only 0.1% less data recovered. Freezing spray, whilst the most practical for a forensic investigator to carry in their toolkit, results in 96.45% data recovered. Whilst this result is significant, the 3.3% data not recovered compared to ice may be vital evidence that would be lost when choosing this method. Next, the results for submerging the RAM in liquid nitrogen were extended from previous experiments by allowing

for a much greater delay in submerging the RAM and removing it from the liquid nitrogen. The purpose of these further experiments were to simulate a forensic investigator who is equipped with a container of liquid nitrogen who may be able to simple drop the RAM into the container but may require a sterile and safe environment equipped with protective clothing to remove the RAM from the nitrogen. The time delay was therefore extended from 10 minutes to 1 hour and then repeated for a delay of 2.5 hours. The results are shown in table 4.

Table 4: Time delay with liquid nitrogen

Time delay	Percentage Recovered	Difference
10 minutes	99.81%	
1 hour	98.84%	-0.97%
2.5 hours	93.95%	-4.89%

It is clear from table 4 that even at -196% Celsius data is lost from RAM if there is a delay in reinserting the RAM into an unlocked computer. A delay of 1 hour results in a loss of over 1% more data than by utilising a freezing spray. If a delay of 2.5 hours occurs, then the loss exceeds the freezing spray by 2.5%. A delay of 1 hour may be unrealistic in many scenarios where the submergence of RAM would be followed by seizing of the computer and related activities, meaning that returning to a safely equipped laboratory may well take longer than 60 minutes. The delay of 2.5 hours is more realistic and shows a significant loss of valuable data. The rather low loss of 0.29% of data with ice indicates that this is the preferred method. It shows that loss of data is minimal and it is a very safe method, although somewhat cumbersome for the forensic investigator in the field. The preferred method may be to carry a can of compressed air as this is simple and fairly safe, but the forensic investigator must bear in mind that approximately 3.55% of data will be lost with a delay of only 10 minutes.

Finally, the data that was recovered from the RAM was identified. A USB drive with Linux software suitable for a RAM dump was used to store the RAM image. Among the data recovered was the expected information regarding user activities on the computer including web pages visited and processes that were started and stopped. Of particular interest was whether the TrueCrypt password could be recovered. It was found in all experiments that the 512 bit AES encryption key utilised by TrueCrypt was recovered allowing the encrypted files to be decrypted and read. This is particularly important for the forensic investigator because it is often the encrypted files that contain the most vital information for the forensic investigator. The recovery of the encryption key was possible in all experiments involving cooling of the RAM but with less than 100% of data recovered there was some luck involved. Any data that is lost may by bad luck involve the encryption key or other vital evidence and so the forensic investigator should bear this in mind when selecting which method to utilise. The greater the percentage of data recovered, the greater the likelihood that the most vital data will remain in the RAM image.

CONCLUSION

The purpose of a forensic investigation of a computer is to acquire, analyse and potentially use information in a criminal, civil or employee investigation. The more information that can be gleaned from the device, the higher the likelihood of a successful investigation. Traditional methods of preserving information from a running computer usually involve looking at the screen to ascertain running programs and then removing the power to the device to preserve the information on the hard disk. Often, the valuable forensic information in RAM is overlooked, or thought to be unobtainable because of a locked user account or encrypted files that prevent the investigator from reading the files unless the encryption key can be obtained. This is unlikely if the suspect's computer contains malicious or nefarious evidence of wrongdoing. The ability to secure the RAM image is therefore highly valuable to the forensic investigator.

This research provides evidence that RAM images can be obtained in these circumstances, and in the case of TrueCrypt encryption, the encryption key may be able to be recovered from the image of memory. This research provides a guideline for forensic investigators as to the best methods for a successful data recovery of RAM and provides evidence of the importance of time delays in the entropy of information in the case of liquid nitrogen freezing. The importance of memory forensics should not be overlooked by the forensic investigator and the

implementation of account locking or encryption of files or entire volumes does not present an insurmountable challenge to successfully acquiring a RAM image.

REFERENCES

Association of Chief Police Officers (ACPO) (2012). Good Practice Guide for Computer-Based Electronic Evidence. E-Crime Working Group.

Bauer, J. Gruhn, M. Freiling, F. (2016). "Lest we forget: Cold-boot attacks on scrambled DDR3 memory". Digital Investigation: 16, 65-74

Halderman, J. A., S. D. Schoen, et al. (2009). "Lest we remember: cold boot attacks on encryption keys." Communications of the ACM 52(5): 91-98.

Huebner, E., D. Bem, et al. (2007). "Persistent systems techniques in forensic acquisition of memory." Digital Investigation 4(3-4): 129-137.

Intel Corporation (2013). Intel 64 and IA-32 Architectures Software Developers' Manual. 3A: System Programming Guide, Part 1.

Ligh, M. H., A. Case, et al. (2014). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux and Mac Memory, Wiley.

Milkovic, L. (2012). "Defeating Windows Memory Forensics." Retrieved June 1st 2016, from https://events.cc.de/congress/2013/Fahrplan/events/5301.en.html.

National Institute of Justice (2008). Crime Scene Investigation: A Guide for First Responders. U.S. Department of Justice. Washington, DC.

Ruff, N. (2008). "Windows Memory Forensics." Journal in Computer Virology 4(2): 83-100.

Russinovich, M. E., D. A. Solomon, et al. (2012). Windows Internals, Pearson Education.

Salihun, D. (2012). Disassembly Ninjutsu Uncovered (Uncovered series), A-List Publishing.

Simon, M. and J. Slay (2009). Enhancement of Forensic Computing Investigations through Memory Forensic Techniques. International Conference on Reliability and Security, ARES Fukuoka, Japan.

Vidas, T. (2007). "The Acquisition and Analysis of Random Access Memory." Journal of Digital Forensic Practice 1(4): 315-323.

Vömel, S. and F. C. Freiling (2012). "Correctness, Atomicity and Integrety: defining criteria for forensically-sound memory acquisition." Digital Investigation 9(2): 125-137.