Mac RAM Analysis

Written by

Catherine Stamm

The Senator Patrick Leahy Center for Digital Investigation

Champlain College

July 17, 2012

Contents

1 Introduction

1.1 Research Problem

Over the years, Apple computers have become quite popular and have risen to the top as one of the most purchased computers in the world. With an increase in the amount of Macs being bought, there is an increase in the potential misuse of the devices. Over the past 10 years, there has been an increasing need for the capture of RAM on computers. The majority of tools capable of doing this are made for Windows operating systems. Apple's license makes access to its live memory fairly difficult. For a while, Mac Memory Reader was the leading tool used to obtain RAM from a Mac. Since RAM analysis of a Mac is so restricted, it is important to understand how to use Mac Memory Reader and other tools like it, such as the month old software from Mandiant – Mac Memoryze.

1.2 Field of Research

For this project, two different RAM dump tools were used; Mac Memory Reader and Mandiant's Mac Memoryze. A MacBook pro was provided to the LCDI and was imaged and wiped using Raptor 2.0 and FTK. After the Snow Leopard operating system was reinstalled, the MacBook was used to generate data to be captured in RAM. The first analysis was done using Mac Memory Reader and then the MacBook was cleaned with CCleaner. After this, more data was created and was then captured by Mac Memoryze. The results were analyzed and then compared to each other to decide if one software was capable of capturing more information than the other.

1.3 Research Questions

- Are login passwords captured?
- Is there evidence of files/emails that were deleted?
- Are programs running in the background noted?
- Are any downloads captured?
- Is data still captured after using CCleaner?
- Was any data information obtained that wasn't created by the user?
- Do both tools acquire the same data?
    - Which one is better?

1.4 Contributions

Until recently, there were hardly any tools used to acquire RAM from a Mac. Mac Memory Reader is relatively new and Mac Memoryze is only a month old. These tools will become more prominent in the forensic world, so it is necessary to understand how to use them, what their capabilities are, and where to find relevant data after the acquisition.

1.5 Report Overview

This report will outline the process taken to perform the research. The first test was done with Mac Memory Reader. The data generated for this test was different than that of the tests done with Mac Memoryze. Most of the data captured from Mac Memory Reader was deleted and came from applications that were no longer

running. The data from Mac Memoryze had less deleted items and the applications they occurred on were running while the RAM was being captured. Once both captures were taken, the data generated for the second test with Mac Memoryze was also captured with Mac Memory Reader in order to compare the results accurately.

2 Literature Review

Not much research has been done on this topic. Apple has put many restrictions on their products, making the process of acquiring RAM very limited. Since Mac Memory Reader was the first and probably most useful way of capturing RAM, the articles read for the purpose of this research are focused on this tool. The white paper most helpful to this project was *Mac OS Forensics How-To: Simple RAM Acquisition and Analysis with Mac Memory Reader* by Ishmael Valenzuela.

This paper shows what commands are needed to capture RAM using Mac Memory Reader. This tool works through the Terminal and according to this paper, the commands are easy to implement. When it came time to implement the commands outlined in the paper, they did not work as they were supposed to. It took a while to figure out the correct commands, but once that was done, using Mac Memory Reader was as simple as the author suggested.

A blog post by Nick Furneaux on Mac RAM dumps was also pretty useful for this research. The commands in his blog were more accurate than the white paper's and helped in the figuring out of how to use Mac Memory Reader. He mentions that Memoryze does not work, as it is only for Windows operating systems, but as of June 2012 that is no longer the case. Because Mac Memoryze is so new, little to no research or information was found on the subject. Luckily, the interface is incredibly easy to use and could be performed by someone with no computer experience at all.

3 Methodology and Methods

A used MacBook Pro was obtained for this research. The hard drive was wiped with Raptor 2.0 and then Snow Leopard 10.6.3 was installed. After that, the MacBook was imaged with FTK Imager. I did this by connecting the MacBook to my workstation with a firewire cable. Once this all was finished, the user account LCDIram was created. Applications were opened, websites were visited, emails were sent, downloads were made and much more was done in order to create enough data that would be found in RAM.

3.1 Tools

Raptor 2.0 – http://forwarddiscovery.com/Raptor/

WinHex 16.5 – http://www.x-ways.net/winhex/

Mac Memory Reader – http://cybermarshal.com/index.php/cyber-marshal-utilities/mac-memory-reader

Mac Memoryze - http://www.mandiant.com/resources/download/mac-memoryze-1.0trade

3.2 Overarching Methodology

Once logged on to the LCDIram account, Activity Monitor was run to see what was already running. The unnecessary processes, (iTunes Helper, Chess, PGP Engine, Finder) were ended so that they would not be

capturing in the RAM acquisition. Next, using the Mail application, I logged on to the email account macram620@gmail.com. The account was set up using the Mail application and then an email saying “this is email number one” was sent to catstamm60@gmail.com. Next an email was sent to catstamm60 that said “delete me please!”. This email was deleted from Sent mail and was then deleted from the Trash.

Two Drafts were then created that said “this is draft number one” and “this is draft number two”. Draft number one was saved as a Draft and draft number two was deleted. An email was then received by macram620 from catstamm60 that said “hello how are you”. This email was opened using the Mail application and was deleted. The Mail application was then exited.

The next step was to use Safari. The website buzzfeed.com was visited and the first link, Cool Pranks 4 Cats, was clicked on. Nytimes.com was also visited and was bookmarked. The next website was facebook.com and was also bookmarked. The account testiphone51412@gmail.com was used to log in. While trying to post a Profile picture to Facebook, I was prompted to install Flash Player, which was downloaded at 9:25 AM. Once this was done, a picture was taken using Photo Booth and was set as the Facebook profile picture. A video was then taken within Facebook and was posted as a status. Facebook was then deleted as a bookmark.

Cool Pranks 4 Cats and nytimes.com was cleared from Safari’s web history and then Twitter was logged on to using the account testiphone51412. A Tweet was posted that said “good morning!” and Ellen Degeneres’ tweet “I’m at the beach” was retweeted. Next, the word “walrus” was Google searched and the first link, which was to Wikipedia, was clicked on. The Google search history was cleared and Flash Player was deleted from the download history. Safari was then closed.

The application Text Edit was open and “goldfish are really cool” was written and saved as goldfish.rtf. “175 lakeside avenue Burlington” was written in a new Text Edit document and was closed without saving.

Mac provides a Dictionary application which was opened and the word “onomatopoeia” was searched for. The application was then closed.

Next, the Sticky Note application was open. “Remember the milk please” was written and left unsaved on the Desktop. Another Sticky Note was written that said “pick up car” and was closed without saving.

Using the iCal application, the event “maine” was made for 1:30 AM on Friday June 29th. The event “4th of july get together” for 12 AM on Wednesday was made and was then deleted. The iCal application was closed after this.

The Calculator was opened and 2 + 2 was input, then the calculator was closed.

Next, the Address book was open and the contacts Cat Stamm, Alex, and Sarah were created along with telephone numbers. Cat Stamm was deleted and the address book was closed.

The Terminal was opened, the directory was changed using cd /Users and was then closed.

A screen shot with the name “screen shot 2012-06-29 at 9.48.50” was taken and then deleted. Photo Booth was used to take a picture called “photo on 2012-06-29 at 9.49” and a video was taken a minute later using the same application. The video was deleted and Photo Booth was closed.

The next application used was iChat. The account xcatstamm was used to log on to AOL Instant Messenger, as the made up MACram60 account was not working through the application. A chat was started with the robot SmarterChild saying “hello”. The automatic response from SmarterChild was “my brain is retired”. The chat itself was closed, as well as the iChat application.

iTunes was opened and the Store was visited. The account testiphone51412 was used to log in to the iTunes store and then “Free on iTunes” was clicked on. The song “Primadonna” by Marina and the Diamonds was downloaded, played for a few seconds, and deleted at 9:57 AM. iTunes was then closed.

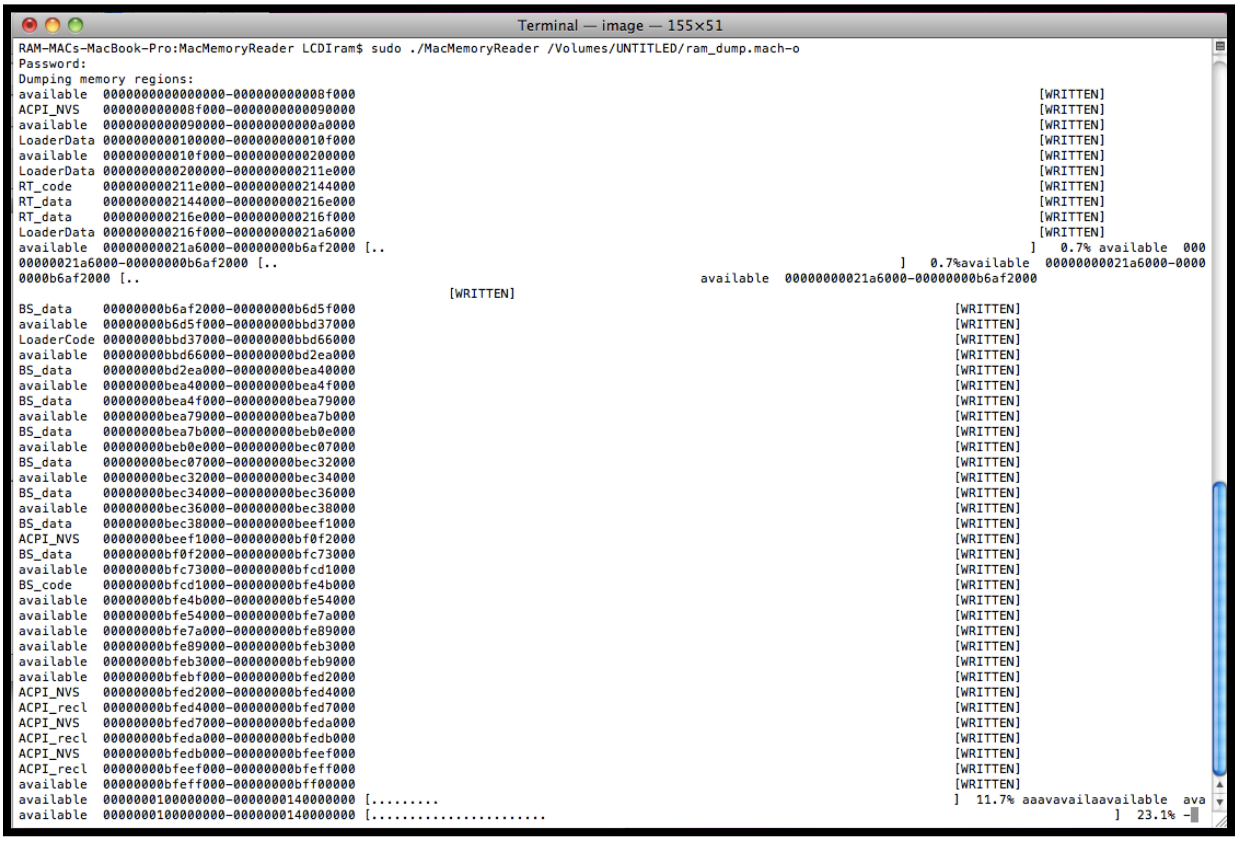
Next, the Trash was opened, completely emptied, and then closed.

A USB drive with an iPhone forensics report and Mac Memory Reader on it was put in to the Mac and showed up on the desktop at 10:02. Mac Memory Reader was then put on to the desktop.

At this point, the test was complete and all that needed to be done was capturing the RAM.

Mac Memory Reader was run using the following steps:

1. Open Terminal
2. Change directories to where Mac Memory Reader is located
   cd /Users/LCDIram/Desktop/MacMemoryReader
3. Run Memory Reader as root and point it to where you want the dump to be saved
   sudo ./MacMemoryReader /Volumes/Untitled/ram_dump.mach-o
4. Enter the account password associated with logging in to the Mac computer, if there is one
5. Mac Memory Reader will begin to dump the memory regions



Once the dump was complete, the USB drive was ejected from the MacBook and was connected to Workstation 3. CCleaner was downloaded on to the MacBook and was used to delete passwords, index.dat files, internet history, temporary files, cache, log files, and much more. The Mac was then shut down and turned back on 5 minutes later.

The next thing on the outline was to generate similar data to have captured with Mac Memoryze. The first step was to open the Mail application. An email from MACram60@gmail.com saying “super secret” was sent to catstamm60@gmail.com. Another email was sent to catstamm60 that said “don’t read this” and then it was deleted from Sent mail and from Trash. Any emails in MACram60’s Inbox folder were deleted as well. A Draft saying “june 29 2012” was created and saved. Another Draft saying “meet me on south willard” was saved and then deleted.

The MacBook lost connection to the Student wireless network, so a personal Droid Bionic was used as a hotspot. The application used was Foxfi. The SSID of this new network coming from the Bionic was Droid 428 and the password to connect was foxfi428.

Still using the Mail application on the MacBook, an email was opened from catstamm60 that said “im busy today” and then it was deleted. The Mail application was minimized, not closed or logged out of.

Safari was opened and the websites nhl.com, stumbleupon.com tdbank.com twitter.com and facebook.com were all visited. Nhl.com and tdbank.com were bookmarked. The bookmark for tdbank.com was deleted and then stumbleupon.com was cleared from the internet history.

Facebook was logged on to using the account testiphone51412@gmail.com and a status was written that said “this is my first status”. The status “facebook is fun” was also written, but was then deleted.

Twitter was visited next and was logged on to using the same account as above. A tweet saying “twitter is awesome” was written, but was not posted.

A Google search was then made for the word “skydive” and the first link was clicked on, which was to Wikipedia.

Google.com/mac was visited and Chrome was downloaded to the MacBook. Safari was then minimized.

Using Google Chrome, youtube.com was visited and then Chrome was closed.

The Text Edit application was open and “top secret message” was written which was saved as message.rtf. This document was then deleted. “Take out the trash, fix the door, buy a dresser” was written in Text Edit and was minimized without saving.

The Dictionary application was used to look up the word “frivolous” and was then minimized.

Sticky Note was used to write “call mom” and was left unsaved on the Desktop. “Pick up laundry” was also written using Sticky Note and was saved as laundry.rtf, but was then deleted.

Next, the application iCal was used to create an event for Saturday June 30 at 12:00 PM with the title "camping". Another event was created for Saturday July 14 at 4:45 PM that said "Waterboro". This event was deleted and then iCal was minimized.

The Calculator was open and 3 + 3 was input, then the calculator was minimized.

Using the Address Book, the contacts Gina, Mom, and Amy were created, along with telephone numbers. The contact for Mom was deleted and the Address Book was minimized.

Next, the Terminal was open and the directory was changed using cd /Users/LCDIram/Desktop/ to see if the commands would be captured in RAM.

A screen shot named "screen shot 2012-06-29 at 11.24.54" was taken and kept on the desktop. Photo Booth was then used to take a picture which was named "photo on 2012-06-29 at 11.25.14" and was deleted. A video was taken using the same application which was name "movie on 2012-06-29 at 11.27" and then Photo Booth was minimized.

Using iChat, AOL Instant Messenger was logged on to using the account xcatstamm. A chat was started with SmarterChild where xcatstamm said "what's up" and SmarterChild responded with "my brain is retired". The chat was left open, as well as the iChat application.

Next, iTunes was opened, the Store was clicked on, and the account testiphone51412 was used to log on. An interview with Michael Hall from Dexter was downloaded and then iTunes was minimized.

The Trash was opened and minimized. Any contents in the Trash were not deleted.

A USB drive was plugged in to the MacBook. A folder with a Text Edit document that said "this is not for your eyes" was created and put on to the USB drive. This completed the second test for RAM dump.

Mac Memoryze was installed onto the MacBook from the USB drive and was opened. Unlike Mac Memory Reader, Mac Memoryze has a GUI instead of using commands provided through the Terminal. This tool was incredibly easy to use and took no time at all to figure out. As soon as it opened, there was a button that said Dump It! Once clicked on, the contents of RAM started to be dumped.

Once this was done, Mac Memory Reader was used to capture the same contents as Mac Memoryze for comparison.

3.3 Data Collection

The Mac RAM was analyzed twice with Mac Memory Reader and once Mac Memoryze. The first test was done with Mac Memory Reader, the second test was done using Mac Memoryze, and the third test used the same exact data as the second test, only it was captured with Mac Memory Reader. Each capture was saved to the Mac Image folder located in Z:\LCDI\Projects\Mac RAM as mach-o files.

3.4 Analysis

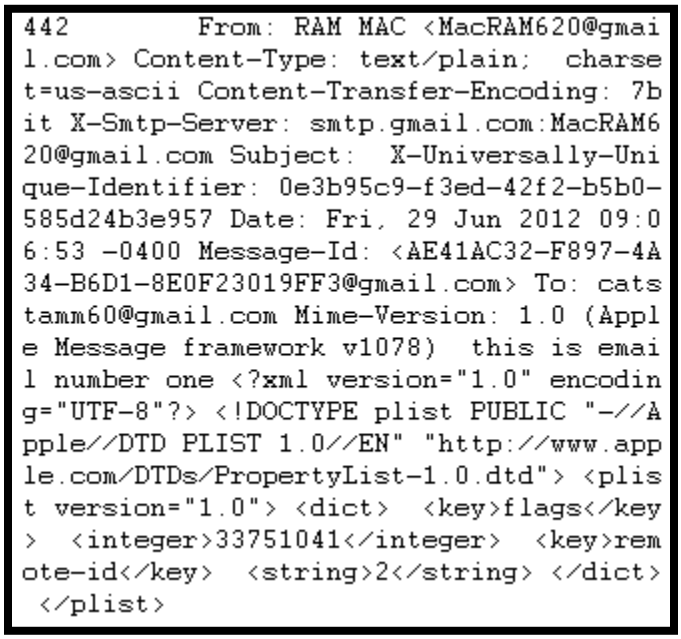
All three RAM dumps were analyzed using WinHex. The dump from Mac Memory Reader was the first to be analyzed.

4 Results

4.1 Mac Memory Reader

Mail

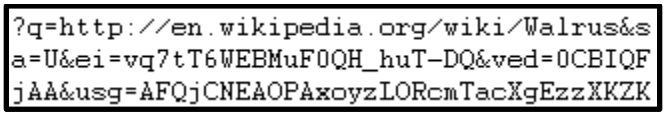
The first evidence of email on the MacBook was found at offset 1164820491. It shows who sent the email, the time and date of the email, and who was receiving the email. It shows the contents of the email as well. An example of what this looked like can be seen below.



A few offsets over, evidence of the first draft was found. It was similar to the data presented above, except the timestamps (June 29 9:10 AM) were different and the contents were “this is draft number one”. This same result came from the email sent on June 29 at 9:07 AM that said “delete me please!”. These emails were found using a keyword search in WinHex. The second draft that had the contents “this is draft number two” within it was not found. This is likely because it was never sent or saved. What was interesting is the email sent from catstamm60@gmail.com that said “hello how are you” was not found. This email was opened on the MacBook using the Mail application and was deleted, but it apparently was not captured in RAM.

Safari

At offset 1083496085, a list of the websites visited can be viewed (buzzfeed.com, twitter.com, apple.com, buzzfeed.com?/coolpranks, facebook.com, google search walrus, Wikipedia page for walrus, nhl.com/statshome, and youtube.com)



On buzzfeed.com, the link that was clicked on (Cool Pranks 4 Cats) showed up in the RAM dump. Along with this, other links from the same webpage were found. Even though they weren't clicked on, they were still captured.

At offset 668389039, nytimes.com was found as a bookmark, along with facebook.com.

Within the RAM dump, video codecs were found for Facebook. A URL to the Tes TiPhone Facebook account was found a few offsets over from this. Information about Flash Player was also found in this section. Being that this was the only indication of video codecs for Facebook, I assume this is the capture of the video that was posted as a status. Along with that, a URL of a random person's Facebook profile picture was found. No other profiles were clicked on during this test, so perhaps this was captured from the "People You May Know" section of Facebook.

When searching for the generated Twitter data, the tweet "good morning!" was found, but there was no indication that it was related to Twitter. The tweet "I'm at the beach" that was retweeted from Ellen Degeneres was not found at all. Also, both account usernames were found for Twitter and Facebook, but no passwords.

As for the Google search of the word "walrus", the search query was found at offset 589892880 and the Wikipedia article on walrus' was found at offset 597811200. Also, a link to the Wikipedia picture of a walrus was found.

Downloads

An indication that Flash Player was installed as an application was found as well. Offset 523858485 shows Flash Player was being installed as a result of Facebook [http/%2F%2Fwww.facebook.com%2Fl.php?u=http%253A%252F%252Fget.adobe.com%252Fflashplayer&h=4AQHvMf80.webhistory]. About 570 offsets over from that, evidence of where the Flash Player was downloaded from was found.

The song downloaded from iTunes (Primadonna) was also found, but as a temp file [/Users/LCDIram/Music/iTunes/iTunes Media/Downloads/Primadonna _ Marina and the Diamonds.tmp/]. It's repeated over and over in different sections of the RAM dump. It would be interesting to figure out why this occurred. Links to Marina and the Diamonds' Twitter and Facebook pages were also found, although they were not available on iTunes.

Text Edit

The first instance of the text document "goldfish.rtf" is found at offset 618441876. There is no evidence of what program was used to create it, when it was created, or what its contents are. It's not until offset 687172448 that "goldfish.rtf" is associated with Text Edit [com.apple.TextEdit.plist]. The contents of "goldfish.rtf" are found at offset 1385034054. There is no timestamp or any information that the message "goldfish are really cool" is in fact saved as "goldfish.rtf". I only know this to be true because I created it.

As for the text document that had the message "175 lakeside avenue Burlington" written, there was no evidence of this document existing. This message was not found in the RAM dump, possibly because it was never saved, but interestingly enough at offset 561131540 "unsaved text edit document.rtf" was found. Being that the "175 lakeside" message was the only message unsaved in Text Edit, it can be assumed that this is associated with "unsaved text edit document.rtf"

Dictionary
The word “onomatopoeia” that was looked up using the Dictionary application was not found at all.

Sticky Notes
The sticky note that was left unsaved on the Desktop saying “remember the milk please” was found at offset 413982760. There is nothing showing that this text document is part of the Sticky Note application. As for the “pick up car” sticky note, there is no data found for it within the RAM dump.

iCal
The event for “maine” was found at offset 686913500, but there is no information on what date or what time this event is occurring. At offset 1581051904 though, there is some information on what date the “maine” event was saved for.

Offset 1076508560 has the first instance of the “july 4th get together” event, but this section of data does not make it known that this event is part of the iCal application. Once getting to offset 1639294840, data regarding the “4th of july” event as part of the calendar was found. This event was found even though it had been deleted.

Calculator
There were a lot of 2+2 instances found throughout the RAM dump, but none seemed to associate with the Calculator application. I should have used a more random equation to definitively conclude calculator input is not captured in RAM.

Address Book
There were a few times where the contacts “sarah, alex and cat stamm” were found, but it was at offset 1182377684 that the names were found along with their telephone numbers. Although the contact for “cat stamm” was deleted, it was still found.

Terminal
Commands put into the Terminal were found at offset 1653944280. The running of Mac Memory Reader, the change in directory to /Desktop/MacMemoryReader, the name of the USB drive plugged in, and change in directory to /Users were all captured in RAM.

Photo Booth
The screen shot [screen shot 2012-06-29 9.48.50.png] that was deleted was found at offset 672369053 and showed its location of where it was saved. At offset 1050200168, we can see that this same screen was deleted, as it is in the Trash [/Users/LCDIram/.TrashScreen shot 2012-06-29 at 9.48.50 AM.png].

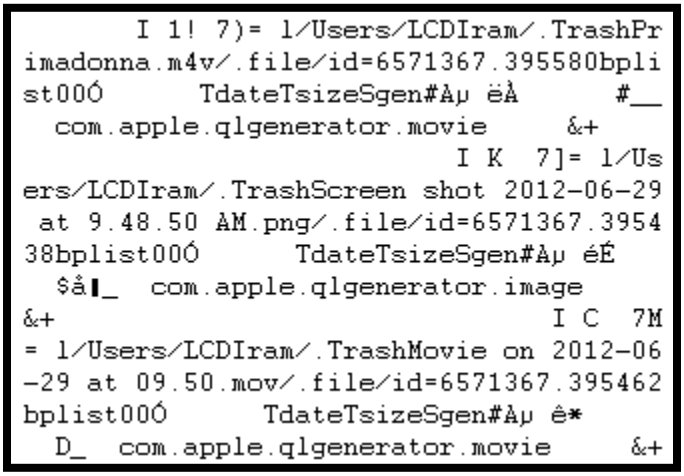
At offsest 601787840, the photo “photo on 2012-06-29 at 09.49” was found. The deleted video that was taken was only found in the Trash.

iChat
A keychain log is found at offset 487547080 that indicates the username xcatstamm was used to log on to AOL Instant Messenger. What’s really interesting is at offset 1590760880. There is a bunch of data regarding xcatstamm’s Buddy List. All contacts from this user were found in the RAM dump. The only thing that was not found was the conversation between SmarterChild and xcatstamm. This could be because the chat was closed and not minimized.

iTunes
Offset 449912840 has evidence of the downloading of the song “Primadonna” by Marina and the Diamonds. The password and username used to log on to the iTunes store was not found at all.

Trash

Offset 1389329847 has information on what was located in the MacBook's Trash, as you can see below:



At offset 1050200168, other contents of Trash which had been emptied from the trash can were found. This offset shows all data deleted through the Trash which includes: the goldfish.rtf document, the video made at 9:50 AM on June 29, and number of various screen shots and pictures that were taken before the initial test was conducted and are not part of this project.

USB

At offset 8386472, there is information on the type of media that was plugged in to the MacBook as well as what partition scheme was used [Media/IOGUIDPartitionScheme/Untitled 1]. Offset 430408411 has evidence that Mac Memory Reader was stored on that USB, named Untitled 1, at some point. A few offsets from that is Untitled 1 /dev/disk2s1, which is where the USB mounted to.

Offset 686789760 has data on the iPhone Forensics.docx file that was moved from the Untitled 1 USB to the Desktop.

Other

The serial number [w8750119XA9] of the MacBook was found at offset 34334256, along with the model [MacBook Pro 3] found directly underneath the serial number.

Offset 442772050 has the "Real Name" of the MacBook [RAM MAC], which is the name used to logon to the computer. Alongside of that is the password associated with that account [RAMpassword]. This password was the only one found; none were captured from the Mail and iChat application or iTunes.

What I found to be really interesting is at offset 1083494840. It's there that all open/used utilities on the MacBook are found. It lists the Activity Monitor, Address Book, Bluetooth File Exchange, which I clicked on accident, Chess, which was clicked on just to see if it would show up, Dictionary, Utility, Photo Booth, Safari, Stickies, Text Edit, iTunes, Terminal, iCal, and Calculator. These were all the applications used during my test. I can tell that this is not just a list of applications on the MacBook (but a list of used ones) because there were plenty of other applications installed on the MacBook that were not used, and therefore would have been on this list if that were the case.

At offset 0510527040 there is some peculiar data on a student of Champlain. This students name isn't necessary to mention in this report, but I do know for a fact this person is a student here. The student's full name and title of her Workgroup was found followed by several different types of printers [HP Photosmart C4700 series, HP Deskjet F4400, EPSON Stylus Photo R260, Canon MX300 series]. Further down from this, the word "student" was found. This is the

name of Champlain's network and is also the network my MacBook Pro was connected to in order to perform the tests. Other than her name and a list of printers, nothing else on this student was found. Data on this student was gathered probably because she had sharing turned on her on laptop and the MacBook I was using picked up on it.

4.2 Mac Memoryze

Mail

The email from catstamm60 to MACram620 sent on June 29 at 10:46 AM was found at offset 1226855160. The contents of this email "super secret" were found as well. Also, the email saying "don't read this" that was sent from MACram620 to catstamm60 was found at offset 1253551687. This email was found even though it had been deleted.

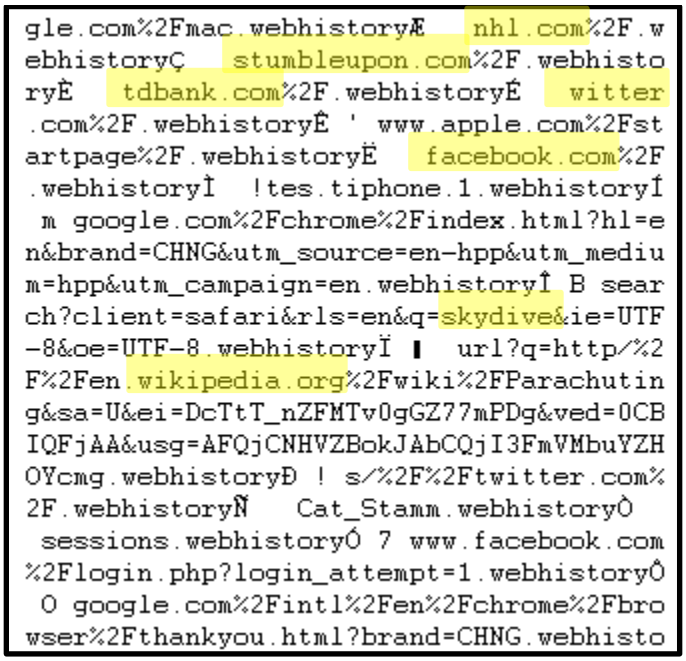
At offset 1258176514, the draft "june 29 2012" to catstamm60 was found. The deleted draft "meet me on south Willard" made at 10:52 on June 29, was found at offset 1457234171. Further down, at offset 1457234906 there is a string that says "imap://macram620@imap.gmail.com/Gmail/Trash", which indicates this email has been deleted.

The email saying "im busy today" that was created at 10:47 and was opened and then deleted at 10:52 from the MacBook was found at offset 1426622302. There was no indication that this email was deleted.

Safari

The bookmarks for tdbank.com and nhl.com are found at offset 327620180. At offset 1277710600, it is evident that tdbank.com is a bookmark. Nhl.com is not found in this section, probably because this section of data represents deleted bookmarks and nhl.com was not deleted.

Below shows the full internet history found at offset 1040152268, including deleted items.



The status made on Facebook that says "this is my first status" was not found at all. This is likely because it was just typed into the status bar and not actually posted. The status that was posted, "facebook is fun", and then was deleted was not found either.

As for Twitter, the tweet that was written saying "twitter is awesome!" was found at offset 1513488689. This is extremely interesting because this tweet was never posted. It was just written and then Safari was minimized. The Facebook status that was created the same way was not captured, but Twitter's was.

The Google search for “skydive” was found at offset 456907793, and the Wikipedia page associated with it was found at offset 1235512106.

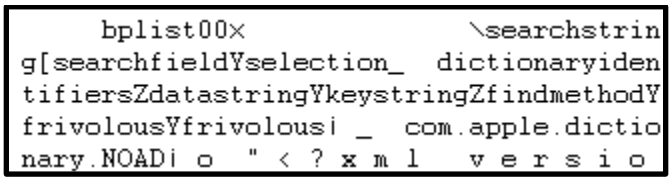
Evidence of visiting google.com/mac in order to download Google Chrome was found at offset 1773854990 [http://google.com/macGoogle} http://www.google.com/chrome/index.html]. The only website visited on Chrome was youtube.com and there was data on this found at offset

Text Edit

The only indication of the text document “top secret message” is located at offset 1632772097. There is nothing suggesting that it was created using Text Edit or that it was saved under the name “message.rtf”. A search for “message.rtf” leads to offset 1460454213, which shows /Users/LCDIram/ .Trashmessage.rtf, indicating this document has been deleted.

The text document “take out the trash, fix the door, buy a dresser” was found at offset 1693249849. It was written in Text Edit, not saved and was minimized. This was the only evidence of the document.

Dictionary



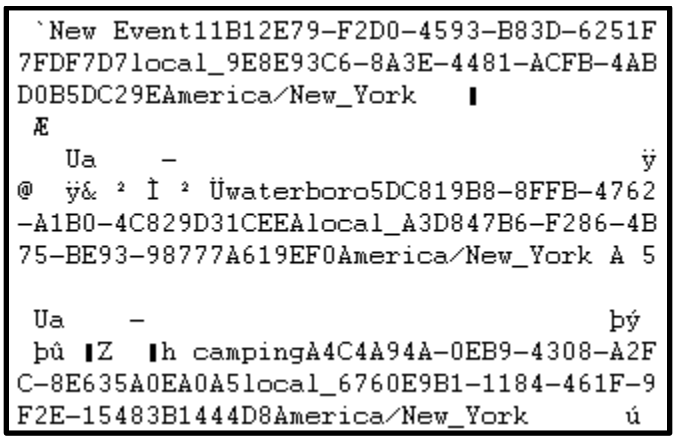
The data above is found at offset 1809750045. The word “frivolous” that was searched for using the Dictionary application was found. It probably wasn’t found in the dump from Mac Memory Reader because the Dictionary application as closed after the search. For this test, the application was minimized and therefore capable of being captured by RAM.

Stickies

The Sticky Note saying “call mom” was found at offset 1902264753. This note was left unsaved on the desktop and within the data, had .txt at the end of it. There was no indication that this document was made using the Stickies application.

The Sticky Note saved as laundry.txt that said “pick up laundry” was deleted and found at offset 1460454251. It was obvious that this file had been deleted [/Users/LCDIram/ .Trashlaundry.txt]

iCal



Offset 1146488322 has the two events, “camping” and “Waterboro”, that were created on June 29. Although the event “Waterboro” was deleted, it was found multiple times throughout the dump and I couldn’t find any indication that this event was deleted.

Calculator
Similarly to Mac Memory Reader, the equation 3+3 was found a bunch of times in the RAM dump. Most, if not all, were unrelated to the Calculator application. I should have chosen a more unique equation so that the search would have been easier.

Address book
The contacts “amy and gina” were found at offset 1221039791 along with their telephone numbers. The contact for “mom” was not found at all.

Terminal
There was no evidence of the change of directory [cd /Users/LCDIram/Desktop/] made in the Terminal.

Photo Booth
At offset 0495866640, “screen shot 2012-06-29 at 11.24.54” was found. A few offsets over from that, “movie on 2012-06-29 at 11.27.mov” was found. The photo that was deleted, “photo on 2012-06-29 at 11.25.14”, was not found anywhere; not even in the Trash.

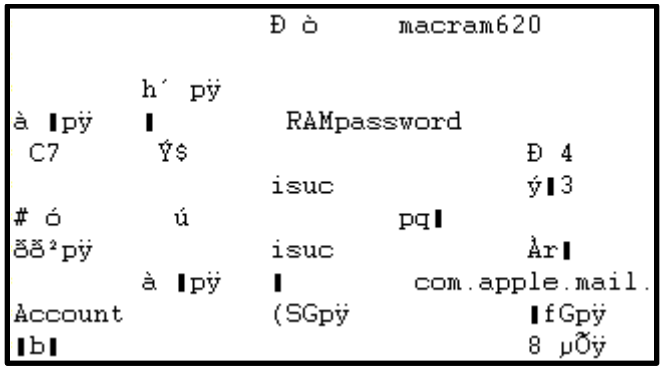
iChat
From xcatstamm’s account, the message “what’s up” was sent to SmarterChild. This message is found at offset 2135554353, but there is no indication who sent it or what application was used. Offset 0423006066 says “chat with SmarterChild” but the contents of the chat are not revealed and neither is the name of the person SmarterChild is chatting with. At offset 2185556640, the response from SmarterChild “my brain is retired” is found. There is no evidence of who this response was sent to or what instant messaging program was use. A few offsets over from that is an indication that this was sent using iChat, but that’s the extent of the information given.

iTunes
At offset 0477625123, the interview with Michael C. Hall that was downloaded from iTunes is found. Offset 0578418360 has the location of where this interview was saved to on the MacBook [/Users/LCDIram/Music/iTunes/iTunes Media/Downloads/Interview with Michael C. Hall _ Dexter _ Dexter.tmp].

Trash
Like the data found in the Trash in the Mac Memory Reader dump, offset 1460453480 has the same information. Although CCleaner was used and the Trash was cleared multiple times, evidence of data that was generated in the first test was still found in the second test. Memoryze captured data that was also captured by Mac Memory Reader, regardless of the fact that the MacBook had CCleaner run on it to hopefully prevent this.

USB
A folder with a word document that said “this is not for your eyes” was found at offset 1763680617. This document was put on a USB drive, but the information found at this offset did not indicate that the message was part of a text document.

Other
The password for the wireless network Droid 428 is found at offset 2413555713, but there is no indication that it is a password or that it is associated with a network.
At offset 448222382, the string “home /Users/LCDIram home DirType longname RAM MAC managedUser password RAMpassword” is found. This shows the name of the account used to log in to the MacBook, as well as the password for the account.
Below shows the username and password used to sign in to the Mail application of the MacBook:



Information on the Champlain student that was found in the Mac Memory Reader dump was also found with Memoryze.

The serial number for the MacBook is found at offset 31464096, but it is not as obvious as the one found in the Mac Memory Reader dump.

Information regarding the Champlain student was also found in this dump at offset 1050893292.

5 Conclusion

After conducting all tests I wanted to do for this project, I was able to answer all of my previous questions. The login passwords used to access the MacBook account were easily captured. That is one of the known pieces of data that can be caught in RAM, so it was a successful find.

Of the 16 pieces of data deleted during both the Mac Memory Reader and Memoryze tests, 11 indications were found in RAM. With over half the deleted data captured in RAM, I would say both Mac Memory Reader and Mac Memoryze are very reliable tools to use when it comes to acquiring RAM from a Mac.

Both programs capture what applications are being run in the background of the system. The list of the open processes was fairly easy to find and in my opinion, is the most important part of the RAM dump. It's because of this list that we can identify what applications were being used at a given time and then we can figure out what direction to turn to next.

From what I can tell, both RAM dumps captured a significant amount of useful data. Almost everything that was used in my tests was found in both dumps. Downloads, emails, chats, web history, pictures, and much more were all captured, even if they were eventually deleted. Even data that was cleared with CCleaner was still found in the RAM dumps created by both programs. Aside from the data I created on the MacBook, there was information on the type of computer the dump was being run on, the wireless network the computer was connected to, applications that weren't used, and much more.

After using both these tools, it is my opinion that they are both equal when it comes to capturing RAM from a Mac system. Memoryze was a lot easier to use, but other than that it was not any different from Mac Memory Reader. My third test consisted of capturing the data made in the second test with Mac Memory Reader. So both test two and three were the same exact data except one was captured with Mac Memoryze and one was captured with Mac Memory Reader. This was done to prove which program was better, if better at all. Both dumps captured the same data. What wasn't found in one wasn't found in the other. Because of this, I can conclude that both these tools are sufficient for computer examiners looking to investigate a Mac's RAM.

6 Further Work

A lot more could be done with this project. More in depth tests could have been conducted. Looking back on it, I should have used Facebook chat to see if it would be captured. I also should have sent emails with attachments to see if those would have been captured too.

Although it would have taken more time than I would want, I should have wiped the hard drive again after the first test. In the second test, I captured data that was generated from the first test. It did not interfere with the second test; it was just redundant to look at the same data that shouldn't have been there. If I were to do this project again, I would figure out a better method of erasing the contents of the Mac besides using CCleaner. I assumed that once that was run and once the MacBook was shut down that the contents from test one found in RAM would be lost. This was not the case, and therefore to come up with more accurate results, the hard drive should have been wiped before the second test began.

7 References

Valenzuela, Ishmael. "Mac OS Forensics How-To: Simple RAM Acquisition and Analysis with Mac Memory Reader ." *Computer Forensics and Incident Response*. SANS, 28 Jan 2011. Web. Web. 29 Jun. 2012. <http://computer-forensics.sans.org/blog/2011/01/28/mac-os-forensics-howto-simple-ram-acquisition-analysis-mac-memory-reader-part-1>.

Furneaux, Nick. "Mac Ram Dumps ." *CSI Tech*. SANS, 20 Jan 2011. Web. Web. 29 Jun. 2012. <http://nickfurneaux.blogspot.com/2011/01/mac-ram-dumps.html>.