MACINTOSH FORENSIC ANALYSIS USING OS X

GSEC Practical Version 1.4b

Peter Hawkins

Introduction

Computer forensic analysis is a method of studying and acquiring digital evidence in a manner that ensures the data's integrity. The duty to perform such an analysis often falls upon a police officer in his quest to gather valuable evidence of a crime. Sometimes, however, system administrators and security professionals are required to partake in such functions when they suspect that someone has tampered with their system. The ability to do a proper analysis using sound forensic practices that are accepted in a court of law, opens the door to the possibility of pursuing criminal or civil action against the perpetrator. The purpose of this paper is to describe sound forensic techniques as they pertain to the Macintosh. In order to accomplish this task, I must first describe basic forensic techniques that apply to all computer systems. Then I will provide a brief history of the various Macintosh models and operating systems, as each one can provide some intriguing problems. Finally, I will follow this up with a specific outline of how to perform the proper analysis of a Macintosh computer system using an OS X based system as the analysis machine. The result of this paper will be a useful reference to those people who may be required to perform a computer forensic analysis on a Macintosh.

Basic Forensic Techniques

In order for evidence to be admissible in a court of law, it is important that it not be modified in any way. This is a fundamental rule that applies to all types of evidence. If one were to acquire a gun that was used in a crime, it is relatively difficult to modify the physical nature of this form of evidence. Computer evidence, however, is very easily modified. In fact, due to the sheer complexity of computer systems, one often does not even realize that the data on a hard drive has been changed. On windows systems, for example, when one boots the computer, last access dates and times will be modified, and recycle bins will be added to new devices. Similarly, the Macintosh tries to mount all devices it sees on boot-up, which changes the last access dates and times of certain files. The safest way to prevent any modification of data is to make a mirror image of the hard drive you wish to examine, and then perform your analysis on the copy(1). This way, the original drive is never modified. There are numerous ways to do this, which I will elaborate on later in this report. Once you have your mirror image, you are free to start your analysis, without fear of altering the original data (obviously the original is kept intact in a secure place where very few people have access to it, and those that do could testify in court that they did not modify it in any way). It is important to mention that all your actions must be very well documented. It is easy to start off your analysis in a haphazard manner thinking that you are never going to find anything. If you do find something and you call the police, you may be told that they can no longer use the evidence because it has been tainted, or control has not been maintained and documented. In order for the police to be able to use evidence, they must be able to track its movements. Everyone who has been in contact with the evidence may be required to testify in court describing his or her actions. If you have not controlled

access to the evidence, and have not documented your actions clearly, your discovery of the "smoking gun" may be useless.

When you start your analysis of the suspect computer, it is important that you know where on the hard drive you could find evidence. There are three basic areas on the hard drive where evidence could be discovered: active files, unallocated space, and slack space (there are others, such as the HPA- Host Protected Area, which require an extremely advanced user to utilize, and thus is beyond the scope of this report). Active files are self explanatory, but one should be aware that some are hidden. Unallocated space is basically the usable sectors of a hard drive that are no longer assigned to a file. Slack space is "The data storage space that exists from the end of the file to the end of the last cluster assigned to the file" (New Technologies, Inc. October 4, 2000) (2).

If you decide to boot a computer using your mirror image, you are going to run into problems. First of all, when you boot, various files are modified so you could lose valuable evidence that is located in slack and unallocated space. Secondly, unless you connect another device to the system, your tools will be limited to whatever was already on the suspect drive. Booting the system with your mirror image can be performed at the very end of your analysis if you wish to see exactly how the system looked in its native environment. If you do this, I would recommend that you place your image into the suspect computer (disconnecting the suspect hard drive of course) so that when you boot, all the preinstalled drivers will match the hardware.

The recommended method of performing a forensic computer analysis is to use another computer as your analysis machine. Basically you boot your analysis computer (using your trusted operating system) with the mirror image connected. Your analysis machine can be any type of computer running any type of operating system. The only requirement is that your forensic tools (software) be compatible with the mirror image's file format. It is usually preferable for you to use an analysis machine that uses the same operating and file system (you can usually use a more recent version of operating system to analyze an older version as they tend to be backwards compatible). There are forensic software tools that are designed to operate on one system, but can analyze multiple file systems. For example, EnCase forensic software (3) runs on windows systems, but can recognize "FAT12, FAT16, FAT32, NTFS, Linux, UNIX, Macintosh, CD-ROM and DVD-R" (4) file systems. Ideally when you connect the mirror image to your analysis machine, it will be connected via some form of hardware write protect device such as Fastbloc (5) or Fireblocker (6) that prevent any modification to an IDE drive (SCSI drives have a built in jumper which allows you to write protect them). If such a device is not available to you, and since you are working with an image and not the original, you may choose to connect the image directly to your analysis machine, acknowledging the fact that you may lose some evidence (depends on the operating system, basic DOS should not alter the image drive under most circumstances, but most other operating systems will). Since you are not booting with the image, however, the risk of losing some evidence is very small since the changes to the drive will be limited. Do not forget that modification to the image is tolerable since it is only copy of our evidence drive. Our only concern is with the evidence, which if it is overwritten, will

not be discovered since we will never actually touch the original drive again. In order to keep the risk of modifying the image to a minimum, you should run some form of software hard drive lock as soon as the system is booted.

Once you have access to the image on your analysis machine, you can start searching. I recommend that you go through all the file folders one by one to familiarize yourself with the suspect system. Deleted files must be recuperated if you are not using forensic software like ilook (7) or EnCase, which shows these files automatically. In my experience, approximately 95% of the evidence will be located in active files. Once this is done, you should perform keyword searches on the entire drive. This will help you discover evidence in slack and unallocated space. You must document every item you find by, in the case of active files, noting the full path and filename. In the case of slack or unallocated space, you should document the information found, and in which sector on the drive. Armed with this information, you will dramatically increase the chances of police involvement, and possible criminal or civil charges.

The Qwerky Mac

Many of the basic forensic techniques apply to the Macintosh, however, various models and operating systems present challenging obstacles. Steven Jobs and Steven Wosniac created the first Apple computer in 1976(8). It wasn't until 1986, however, with the introduction of the Apple IIgs, that apple included the first hard drive in their machines(9). This is important since prior to this model there is little point in analyzing a Mac for evidence. Most early Macintosh hard drives were SCSI, which can complicate matters. The biggest problem with the early Macintosh systems, however, was gaining access to the hard drive, since, in some cases, special tools were required to open the box. In these circumstances, a forensic analysis could be performed by booting the system with a SCSI Zip drive containing your operating system, and your analysis and back-up tools. One would plug in the SCSI Zip and press and hold the Command, Option, Shift and Delete keys while powering up. This procedure caused the Macintosh to check the SCSI chain in reverse order (starting at ID 7 and working towards ID 0, instead of the normal 0 to 7) until it found a bootable system folder. Since the Zip drive would be set to SCSI ID 6, this would be the drive from which the system would boot (ID 7 is reserved for the Macintosh CPU). The suspect drive would still be mounted, so one could apply a software write-lock to minimize alterations. This is not ideal, but one has little choice when you cannot access the hard drive. Fortunately the more modern Macs make it extremely easy to access the internal components. The G3 was first introduced in 1997 and it allows for easy access to the hard drive.

Another issue with the Macintosh is the operating system. The Macintosh operating system is now divided into two types: Classic OS and OS X. OS X is the latest operating system offered by Macintosh (version 10.2 aka Jaguar) and will only function on G3 systems and later. So if you image a pre G3 system, you will not be able to boot it (you can still mount it though) on your G4 analysis machine. But, as was mentioned earlier, the necessity to boot a system with your image is minimal. It is important to note

that since not all systems will run all operating systems, and since you may need to boot the computer with a Zip drive containing your trusted operating system and tools, it is important that you know which models of Macintosh will operate on which version of operating system(10).

The Specifics of Macintosh Forensic Analysis

Macintosh OS X is an amazing operating system for forensic analysis. It allows you to boot from your forensic drive and not mount, and therefore not modify, any other drive connected to it. However, it still permits you to image unmounted systems. OS X gives you all the power of Unix commands, such as dd, in its Open BSD Darwin terminal. OS X is completely different than Classic OS, but it is still backwards compatible. For the aforementioned reasons, I think it makes a perfect operating system for an analysis machine catering to the Macintosh (this design could image any hard drive containing any filing system, but since the forensic tools currently available only work with Macintosh systems, it is limited to the analysis of the Mac).

In preparation of the possibility of having to perform a forensic analysis on a Macintosh, one must configure their analysis machine. I recommend that your analysis machine be a G4 laptop (portability is necessary in order to conveniently locate it to the suspect computer) running OS X Jaguar. In order to ensure that all attached drives are not mounted every time you boot the system, you have to remove the autodiskmount feature in OS X. To accomplish this task, you need to modify the MacOSX: System:Library:StartupItems:Disks:Disks file by commenting out the line containing the "/sbin/autodiskmount -va" command (this is done by placing a # in the first position of the line). Here is a printout of what the "Disks" file looks like:

```
#!/bin/sh

##
# Local filesystems
##

. /etc/rc.common

StartService ()
{
   if [ ! -f /var/db/volinfo.database ]; then Uninitialized_VSDB=-YES-; fi

   ConsoleMessage "Checking disks"
#   /sbin/autodiskmount -va

   if [ "${Uninitialized_VSDB:=-NO-}" = "-YES-" ]; then vsdbutil -i; fi
}
```

```
StopService ()
{
   return 0;
}

RestartService ()
{
   return 0;
}

RunService "$1"
```

Notice the "#" that was placed in front of "/sbin/autodiskmount –va". In its current state, the Macintosh computer containing this "Disks" file will only mount the drive from which it boots. In order to make this modification, you will have to be logged in as root. It is important to mention that your forensic system disk does not necessarily have to be the internal laptop hard drive. I use a very large (120GB) external hard drive in a firewire enclosure as my forensic drive. This is convenient because, since no other drive will be mounted due to the removal of the autodiskmount feature, this will be the only drive available to which one can copy the forensic image.

It is also a good idea to modify your ENV firmware to perform a multiboot every time you start the computer (the multiboot option can be selected each time you boot by holding the shift key while powering up, but by modifying the ENV firmware, it is done automatically). The multiboot is basically a boot manager that scans all connected drives looking for blessed system folders, and gives you the option from which partition and drive to boot. This does not modify the connected drives in any way. In order to modify the ENV firmware, you must power on your computer while pressing and holding the Command, Option, "F" key, and "O" key. Then you type in "setenv boot-command multi-boot" followed by the enter key. Then to exit, you can type multi-boot and you will be sent to the boot selection window. From now on, your computer will give you the option from which system folder to boot (this can easily be reversed by entering the ENV firmware again and typing "setenv boot-command mac-boot"). By always using the multi-boot feature, you will be confident that when you attach the suspect drive, it will not be mounted.

You should create a user account called "Analysis" on your system. Give this user normal user rights, and not admin rights. This is important because when you create your image of the suspect's hard drive, you will be logged in as root. Therefore, the image you create will automatically be read only for all other users. So once your image had been created, you will log in as "Analysis" and therefore will not be able to modify it in any way. It is important that you keep the "desktop" of your Analysis account completely free of any links, files or folders. This is because, when you mount your suspect drive image, everything that was on his desktop, will now appear on your desktop. In order to easily differentiate between the two, it is best to have nothing at all on your desktop thus eliminating any possible confusion.

The last step in the preparation of your analysis machine is to ensure that you have the necessary forensic software installed. Some of the software comes with OS X, such as the dd command and file search capabilities. However, there are other, third party software that are useful when performing your analysis. Basically you need:

1. A program that allows you to view and peruse all active files, including those that are hidden. I would suggest Canopener by Abbott Systems Inc.(11), which is now available for OS X.

2. A program that allows you to search the entire physical hard drive for key words, including slack space and unallocated space. For this, I would recommend Expert Witness by ASR Data(12). It is considered OS X savvy, which means it is OS 9 native, but will operate well in OS X. I have tried the latest version 3.9.4 and it works very well under OS X. Another, less expensive option would be RescueTXT by Abbott Systems Inc.(13).

3. A program that can recuperate deleted files. I suggest Norton SystemWorks 2.0 for Macintosh (14). This product contains Norton Unerase, which will recuperate deleted files. It also contains anti-virus software, which is important to protect you from being infected by the suspect files. One more useful program SystemWorks contains is Norton Disk Editor. This is a very powerful piece of software that allows you to analyze all parts of a hard drive sector by sector.

4. Programs that allow you to view a wide range of file formats. CanOpener can view a great many file types. If this doesn't work, you can try Graphic Converter by Lemke Software (15). It can import 160 graphic file formats and export 45.

I would recommend that you create links to these tools on your task bar for easy access. This will also allow you to keep your desktop free of links.

Step by Step

Now that our analysis machine is prepared, we can focus on a step-by-step procedure explaining how to safely analyze a Macintosh computer system.

1. Document your actions and all the pertinent details of the suspect computer. This includes noting why you need to perform a computer analysis, the type of computer and all its components, the names of the individuals who had access to the computer and its specific physical location.

2. Create an image of the suspect hard drive. This is done by removing the hard drive from the suspect computer and placing it into a firewire hard drive enclosure. Plug the firewire enclosure into your analysis machine and power up. At the multi-boot screen, make sure you choose your forensic boot partition. If

you choose the suspect drive by accident, you will modify the data on it, so be careful at this point! Once your forensic system has booted, log on as root. You will only see one drive in the upper right hand corner of your screen; this will be your forensic system. Recall that you modified the autodiskmount line in your "Disks" file so that only the system partition you chose mounted. Since the suspect drive partitions did not mount, they were not modified in any way. At this point you will want to open a terminal window (the terminal program is located in MacOSX:Applications:Utilities:Terminal). Now you are at a Unix type command line. Type the command "pdisk", and then "L". This will give you a listing of all the drives currently connected to the system. You need to determine what drive number has been assigned to the suspect drive. It is important that you be familiar with your own system in order to be able to differentiate it from the suspect system (e.g. unique partition names, number of partitions, size of partitions, size of drive, etc…). Lets say that the suspect drive was "rdisk1", then you simply write this number down in your notes, and exit the pdisk program by typing "q". Now you are again at the command line, and we are ready to image the suspect hard drive. The command to use to create the image is the "dd" command (if you type "man dd", you will get a detailed explanation of how to use it). The syntax is as follows: dd if="path of the input file" of="path of the output file". There are many other variables that allow you to image only parts of a drive, but we want the whole thing, so they do not concern us. It is important to note that Unix/Linux treats drives as files. So our input file will be the path to our suspect drive : "/dev/rdisk1". Our output file will be the image file we wish to create (it is a good idea to give it a meaningful name that connects it uniquely to the suspect drive, perhaps the name of the sole user, or the serial number of the hard drive), such as "/Users/Shared/hdr-sn1234567.dmg". So our final command will look like: **dd if="/dev/rdisk1" of="/Users/Shared/hdr- sn1234567.dmg"**. Once the image is done, you should remove the comment from the autodiskmount line of your "Disks" file, so that when you reboot, you will have access to all drives and partitions (this is because you will be removing the suspect drive and will want to mount the image file you just created which is not possible if you have commented out the autodiskmount line). Turn the computer off, and disconnect the suspect hard drive. Place the hard drive in a safe place where access to it is controlled (e.g. Locked in a locker). At a later date, should you so desire, you can use the same dd command in reverse to write your image file back to another hard drive (it can be bigger, but not smaller) so that you can boot the suspect system to see exactly what your suspect was seeing.

It should be noted that there are other ways to image a hard drive. One way is to use a hardware device such as SoloMasster(16), which basically allows you to mirror a hard drive onto another hard drive that is at least as large. This is a fast method to make a mirror copy, but in the Macintosh world, we still cannot mount it without modifying any of the data. The SoloMasster is very good when all you want to do is boot the suspect computer with the mirror image you created. Another method of imaging a hard drive is to use a program called Safeback(17). Safeback allows you to create an image of a hard drive onto magnetic tape, or

some other medium. The problem with this, of course, is that you have to restore it to be able to analyze the data. And once again, you would have to restore it to another hard drive, and then in turn go through the "dd" procedure in order to study it on the Mac. Each of these tools has their place, but when it comes to the Macintosh, the best method is the one described first. (Another method exists as well which is called EnCase(3). However, the image you create can only be analyzed by EnCase, which does not operate on the Macintosh platform, and thus is beyond the scope of this paper).

3. Boot your analysis machine and log into your Analysis user account (by doing this you ensure that you cannot modify the image file you just created because you do not have the appropriate rights, since you created it as root). Now you need to navigate to the image you just created and mount it by double clicking on it. You should see on your desktop, drives representing all the partitions that were on the suspect's disk drive. You are now free to peruse these drives to look for evidence.

4. The first thing you want to do is to recuperate any and all deleted files. A good tool for this is Norton Unerase. This program will go through the specified drive and pull out all the files that were deleted. It will tell you what the title of the file or directory was, its size and the odds of recovery. You should recover all deleted files you can, and save them to your hard drive. Once you have done this, you will be able to examine them with CanOpener.

5. On your task bar, click on your CanOpener icon as this will be the tool of choice for navigating through the suspect drive. One of the main features of CanOpener is that it shows you all hidden files. When you use CanOpener, you will see all active files. You can then view them quickly and easily since CanOpener can view most file types. I would recommend that you spend most of your time looking through the user files as this is the most likely place you will find evidence. By doing this, you also get a feel for the computer you are analyzing which helps you get the big picture. Don't forget to examine the undeleted files that you stored on your hard drive.

6. Once you feel that you have gotten all that you can from looking at the active files, it is time to do some keyword searches. It is important to discuss what makes a good keyword. You want your keyword to be as unique as possible so that you are not inundated with false positives. For example, if you are looking for the name "bob", you risk having a lot of false positives. One reason for this is because "bob" can easily exist in other words such as "bobsled". Another reason you could get false positives is because it is only three letters long, so it will randomly appear in garbled text more frequently. If you have no other choice but to search for "bob", you might want to try putting a space before and/or after to minimize the random garbled text results. A good tool for the Macintosh that allows you to search the entire hard drive (including slack and unallocated space) is the program Expert Witness, or RescueTXT. Expert Witness is superior in that

it allows you to search for multiple search strings at a time, however, it is only available to law enforcement. RescueTXT is a program that is actually designed to recuperate lost or deleted text fragments from your hard drive. It is far less expensive (and powerful) than Expert Witness, but it will do the job.

7. Sometimes it is important to see what images the suspect kept on his hard drive. All images contained on a hard drive can be viewed easily with a program called Graphic Converter(13). You simply drag the suspect drive onto the Graphic Converter program window, and it will pull out all the image files.

8. One of the features of mounting the suspect's image on the Macintosh is that you don't necessarily need to have the original software to view the files. Quite often you can open files using the suspect's software, with no configuration necessary. Sometimes, however, you will be required to make some minor alterations, such as importing the suspect's e-mail inbox into your e-mail program.

Conclusion

The purpose of this paper was to provide the reader with a general understanding of how to extract data from a Macintosh computer, in a manner that is forensically sound. I explained general computer forensic techniques first to give the reader an understanding of the basic principals. I then explained how the Macintosh offered some unique problems that could only be overcome with the appropriate knowledge and tools. Finally I provided a step-by-step guideline explaining how to prepare one's Macintosh computer for an analysis and how to perform it on a suspect's Macintosh hard drive.

For those of you who are familiar with EnCase(3), and since EnCase can analyze Macintosh formatted hard drives, you may be wondering why one would go to all the trouble to set up a Macintosh analysis machine and follow the procedures outlined in this paper. The main reason is clarity. I have used EnCase to analyze Macintosh hard drives before, and it does not represent the drive files and folders very well. As I mentioned earlier, approximately 95% of the evidence you seek will be found in active files. It is therefore very important that you be able to navigate all the active files and folders on the suspect's hard drive. EnCase will perform the string searches very well, however, once you find the file containing the string, you will not be able to view it in it's original format. From my experience, you will discover far more evidence by viewing the drive in its native environment.

I hope that system administrators and security professionals will be able to use this paper as a guideline to performing computer forensic analyses. I realize that the need for these individuals to perform such duties is somewhat limited, which is why a thorough guideline is so important. For someone who does not perform computer forensic analyses very often, it is very easy to forget (or not even realize) the importance of doing it correctly. By "doing it correctly" we open the door to the possibility of pursuing criminal and civil actions. This is a very positive option when

one's system has been hacked, or an employee has stolen important files. One might wonder why the police wouldn't be called in immediately in these cases, and the fact is that sometimes, mere suspicions are not enough to obtain police involvement. If you were to go to the police and give them evidence in support of your suspicions, you dramatically increase the chances of them assisting you.

References

1. The International Association of Computer Investigative Specialists. "Forensic Procedures" September 14, 2002. URL: http://www.cops.org/forensic_examination_procedures.htm (October 8, 2002).

2. New Technologies, Inc. "File Slack defined." October 4th, 2000. URL: http://www.forensics-intl.com/def6.html (September 19, 2002).

3. Guidance Software, Inc. "Home page" 2002. URL: http://www.encase.com (September 19, 2002).

4. Guidance Software, Inc. "Features 2.pdf." URL: http://www.encase.com/products/software/encaseforensic.shtm (September 19, 2002).

5. Guidance Software, Inc. "Fastbloc." 2002. URL: http://www.encase.com/products/hardware/fastbloc.shtm (September 19, 2002).

6. Digital Intelligence, Inc. "Fireblock, IEEE 1394 to IDE Hardware-based Write Blocker." 2001. URL: http://www.digitalintel.com/fireblock.htm (September 19, 2002).

7. Criminal Investigation, Department of Treasury. "CI's ILook Download Page." September 15, 2002. URL: http://www.ilook-forensics.org/ (September 19, 2002).

8. Apple History. "History 1976-1981." 1996-2002. URL: http://www.apple-History.com/history.html (October 4, 2002).

9. Apple History. "The Apple IIgs." 1996-2002. URL: http://www.apple-history.com/quickgallery.html?where=aIIgs.html (October 4, 2002).

10. Everymac.com, "Mac Systems" 1996-2001. URL: http://www.everymac.com/systems/index.html (October 4, 2002).

11. Abbott Systems Inc, "CanOpener Emergency access to any file!" 1997-1999. URL: http://www.abbottsystems.com/co.html (October 1, 2002).

12. ASR Data, "Expert Witness for Macintosh" URL: http://www.asrdata.com/ExpertWitness/ (October 1, 2002).

13. Abbott Systems Inc, "RescueTXT Recover text that has gone!" 1997-1999. URL: http://www.abbottsystems.com/rtxt.html (October 1, 2002).

14. Symantec, “Norton SystemWorks 2.0 For Macintosh” 1995-2002. URL: http://www.symantec.com/sabu/sysworks/mac/ (October 1, 2002).

15. Lemke Software, “About GraphicConverter”. URL: http://www.graphicconverter.net/us_gcabout.html (October 1, 2002).

16. Intelligent Computer Solutions, “Image Masster Solo Forensics Hard Drive Duplicator” URL: http://www.imagemasster.org/imagemasstersolo2for.html (October 4, 2002).

17. New Technologies Inc., “SafeBack Mirror Image Backup Software” July 15, 2002. URL: http://www.forensics-intl.com/safeback.html (October 4, 2002).