Examination of 60 GB Hard Drive

I am the Director of IT and Senior Forensic Consultant at In2itive Technologies in Portland, Oregon. In2itive Technologies is a company that specializes in Computer Forensics and Electronic Discovery. I have 7 years experience in the computer forensic field, and have handled numerous cases ranging from simple data recovery to investigations concerning litigation in billion dollar lawsuits, involving both civil and criminal investigations. My training and certifications include the following: EnCase Certified Examiner (EnCE); EnCase Intermediate Analysis and Reporting; EnCase Advanced Analysis and Reporting; AccessData Forensic ToolKit BootCamp; AccessData Forensic ToolKit Windows Forensics; CompTIA A+ Computer Technician (CompTIA A+); Microsoft Certified Systems Engineer (MSCE); Microsoft Certified Systems Administrator (MCSA); and Sun Java Certified Programmer (SJP).

I was requested to perform a forensic examination of a 60 GB hard drive to ascertain the email usage pattern of Max Zweizig. This 60 GB hard drive is reported to have been used by Max Zweizig as a replacement hard drive for a 120 GB hard drive that is reported to have failed in May of 2003. I used the EnCase forensic software to create a forensic image of the 60 GB hard drive on April 10, 2009, using a hardware write blocker, to prevent any changes of data to the hard drive.

The examination of the 60 GB hard drive included both searching active email files and searching the Unallocated Space for any email fragments to provide a pattern of Max Zweizig's usage of the 60 GB hard drive for his email traffic. This search did not reveal any email fragments that could be connected to Max Zweizig having used the 60 GB hard drive as his email computer.

Additionally, the 60 GB hard drive was analyzed to determine if there were any records of deleted email container files, namely Outlook PST files or Outlook Express DBX files used by Max Zweizig. No records were found that could have been used by Max Zweizig prior to his returning the computer to NorthWest Direct. The oldest email container that could be identified and possibly recovered from the 60 GB hard drive was created on November 13, 2003. See 60 GB Hard Drive Exhibit 1.

It is my conclusion that there is no indication in Allocated or Unallocated spaces that the 60 GB hard drive was used by Max Zweizig for sending and receiving emails.

On May 20, 2010, I received a hard drive containing a forensic image of the 60 GB hard drive from Steve Williams. I was informed that this image had been previously thought destroyed but an intensive search for the drive containing the image was conducted and the image was subsequently discovered. Being cognizant of the uncertain history of the older 60 GB drive image, I approached the older image with skepticism until able to show if it were the same drive and it was still a viable image.

As background for my conclusions regarding the older image, the EnCase software developed by Guidance Software is the leading forensic software in use by corporations, government and law enforcement and is accepted by the judicial system. EnCase is used to create forensic images and allow

Exhibit 8
Page 1

investigation of those forensic images as if the actual hard drive or media were being accessed. The creation of the forensic image by EnCase is an exact bit by bit mirror image of the hard drive or media that also allows access to all areas of the hard drive or media.

During the creation of a forensic image by EnCase, two different types of verification events take place. The first verification process is a CRC (Cyclical Redundancy Check) that is performed, by default, on every 64 sectors of the hard drive. The CRC is a numerical value (hash) of the contents of each 64 sector block and can have over 4 billion different values. During any subsequent validation process, the CRC is re-calculated and compared to the original CRC value to ensure the contents of that particular 64 sector block has not changed. If during the validation process a CRC value deviates from the original CRC value assigned for that 64 sector block, an error message is displayed by EnCase identifying the particular 64 sector block that is affected.

The second verification process is a MD5 (Message Digest 5) hash value of the entire contents of the image generated. As the EnCase image of the hard drive is a bit by bit mirror image of the hard drive, the MD5 is in essence, a hash of the entire original media. This can be attested to by the fact that if two images of the same hard drive are created, and no changes occurred to the hard drive between the two imaging processes, the MD5 hash value will be exactly the same for both images. This would also hold true for the CRC values generated during the imaging processes. For perspective, the MD5 hash is generated across the entire hard drive and the number of possible values is 2^{128}, resulting in 340 billion billion billion billion (34 undecillion) possible variations.

The importance of the CRC and MD5 values contained within the verification process becomes paramount during an investigation when multiple people or even multiple sites need access to the forensic images. Because the EnCase image is encapsulated into its own proprietary file format, the image can be transported, copied and even transmitted over the Internet without affecting the integrity of the forensic image. To verify the integrity of the forensic image, a validation process is run which verifies each CRC and the MD5 hash. If any values do not match the original CRC or MD5 value, an error message is generated informing the forensic specialist that the integrity of the image has been compromised.

The encapsulation of the forensic image into a proprietary file format prevents the intermingling of data contained on a hard drive where the image is being created. While it is good forensic practice to always use a clean hard drive that has been "scrubbed" of all previous data, use of an "unscrubbed", or "dirty" hard drive will have no affect on the EnCase forensic image created. By isolating the forensic image in its own format, any underlying data that may exist on the hard drive where the forensic image is being created is prevented from making any changes or affecting the forensic images created. This can again be verified by the creation of two images from the same hard drive. If one is created to a "dirty" hard drive, it will have the same CRC and MD5 hash values as the exact same hard drive imaged to a "clean" hard drive. This encapsulation feature is utilized by every law enforcement forensic laboratory that must allow access to forensic images by multiple specialists involved in investigations involving the same forensic image. The forensic image will be placed on a forensic server that cannot be "scrubbed" each

Exhibit 8
Page 2

time a forensic image is placed on the server, and the image shared out to those that need access. In addition, multiple forensic images from multiple unrelated cases will be stored on the same forensic server and the encapsulation feature prevents one image from affecting another.

When I received the older 60 GB forensic image, my first action was to perform the verification process to check that the image was a valid image and had not been corrupted. This process finished with no errors generated, indicating that the image was complete and uncorrupted from its original creation.

My next actions were to attempt to verify that the older image was actually a forensic image of the same hard drive that I had created an image of on April 10, 2009. This process involved four items of comparison,

1. Both hard drive images contained the exact same number of sectors for the volume created. The number of sectors is set at the time a volume is created.

2. Both hard drive images contained the exact same number of clusters for the volume created. The number of clusters is set at the time a volume is created.

3. Both hard drive images contained Windows system files indicating that both hard drives were formatted at the exact same time, 5/12/03 at 8:34:54 AM. This time is set at the time a volume is formatted.

4. Finally, the electronic serial number from both forensic images is exactly the same, 62D40ABD40A9487. This serial number is an electronic serial number that is unique to every hard drive. The hard drive serial number is recorded during the imaging process and as such, is stored as part of the forensic image. Any attempt to change the electronic serial number would result in a verification error being generated during the verification process. No errors were generated during the verification process I performed.

Based on the above four facts, it is conclusive that the two images that I am now in possession of are valid images of the same hard drive taken at two different times.

Creating a forensic image of a hard drive is essentially a snapshot in time, in that what is imaged is the data that is present on the hard drive at the time the image is created. A unique situation is present with these two images as the same hard drive can be compared and evaluated for content and usage, separated by four years of time. The original image was created on May 5, 2005 and the second image was created on April 10, 2009.

Overall, there are 200,000 files on the two images combined. An MD5 hash analysis was performed on the files to generate a MD5 value for each file. After the MD5 hash values were generated, the results showed that 131,000 unique files were contained on the hard drives. Of those unique files, only 39,000 were unique to the older image, indicating that over a four year time frame, only 30% of the files present on the older image were different from the files present on the later image. As an MD5 hash value is generated off the contents of the file, even the adding or removal of a punctuation mark would

Exhibit 8
Page 3

make the MD5 value different. As such, the 39,000 unique files would be a combination of new files added and files being modified of a 4 year period.

Using the 30% change over four years as base, this implies that on average, 7% of the files contained on the hard drive are added or modified during any given year. Extrapolating this data to the time period between November 2003 and May 2005, this implies that 11% of the files contained on the hard drive at the time of the creation of the first forensic image had been added or modified.

An additional factor related to the overwriting of deleted data is the Slack Space. When a file is deleted and its space overwritten with new data, the original data may not be completely overwritten, leaving residual data viewable through forensic means. This Slack Space is located at the end of every new file that is smaller than the previous deleted file that was stored in the same space. As a file is saved to the hard drive, the new file overwrites any previous data that was contained in the space previously, except, if the new file is smaller than the previous file. This Slack Space is searchable and its contents can reveal file remnants including email fragments and addresses.

Based on usage percentages it is seen that this hard drive was likely used for light business purposes after being returned by Max Zweizig. Taking into account this usage and the details of what happens when a file is overwritten and the probability that all data is not overwritten, it is difficult to defend the concept that all references to Max Zweizig's email could have been eradicated within the 18 months after the computer was returned to Tim Rote. From personal experience, I have recovered deleted email fragments with indications that the email had been deleted from a personal computer five years previous, to the detriment of the original email user.

I submit that the computer was in use after being returned by Max Zweizig and that the usage was insufficient to eradicate all references to Max Zweizig's email from the hard drive in the 18 months before the first image was taken. Therefore, it is reasonable to conclude that the computer that housed this hard drive was not used by Max Zweizig for his email.

I HEREBY DECLARE THAT THE ABOVE STATEMENTS ARE TRUE TO THE BEST OF MY KNOWLEDGE AND BELIEF, AND THAT I UNDERSTAND THEY ARE MADE FOR USE AS EVIDENCE IN COURT AND ARE SUBJECT TO PENALTY FOR PERJURY.

Dated May 27, 2010

Mark Cox

Mark Cox

Exhibit 8
Page 4

Exhibit 1

Full Path	File Category	Last Accessed	File Created
C\Recovered Folders\NWT Employee\outlook.pst	Mail	08/30/08 05:40:33PM	11/13/03 12:27:18AM
C\Recovered Folders\Sent Items.dbx	Mail	06/01/07 05:07:01PM	05/13/05 05:27:57PM
C\Recovered Folders\Outbox.dbx	Mail	06/01/07 05:07:03PM	05/13/05 05:27:57PM
C\Recovered Folders\outlook.pst	Mail	11/12/08 03:09:06PM	11/29/05 05:24:28PM

Exhibit 8
Page 5