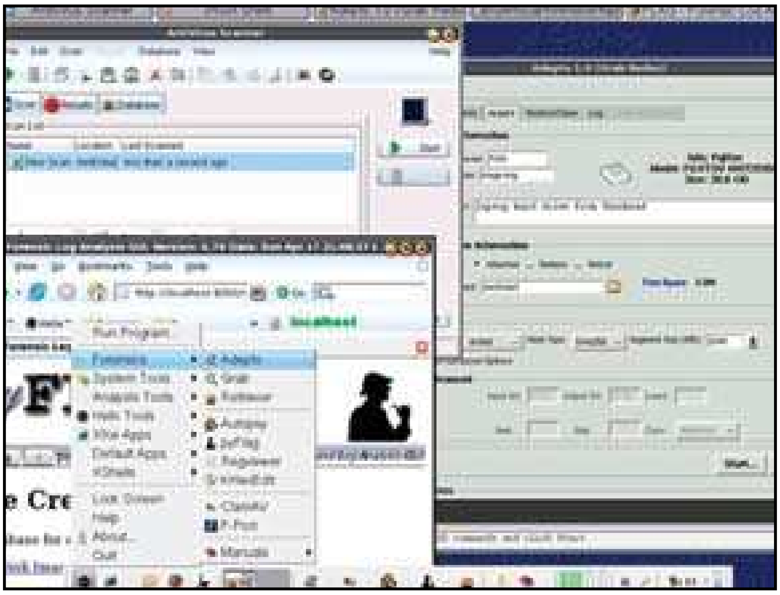
*Editor's note: these articles are from a specifically Italian perspective.*

# A Digital Forensic Report

By Nanni Bassetti

**Digital forensics in Italy has come a long way and is still developing, though barely keeping up with the technology.**



Digital forensics, applied to computer evidence in the crime lab, has come a long way and is still developing, though barely keeping up with the technology. Computers are everywhere – businesses cannot function without them, criminals are becoming more adept at utilizing them – and evidence of wrongdoing is stored on a variety of media – ever-larger hard disks, beloveds floppy disks, CDs and DVDs, USB flash drives, memory cards, MP3 players, mobile phones, etc.

Here in Italy, the Judicial Authorities funding and tasking the crime labs often do not succeed in keeping up with improving technologies, falling behind with tools that become obsolete all too quickly. Moreover, they often do not know how to work with the new types of evidences and media. It is hoped that in the future they will adopt a common protocol of analysis and reporting for evidence gathered from digital media.

Many Italian investigators use Open Source forensics tools because they are reliable and free. And trustworthy: entire communities of developers view and work on the publicly available source code, and this public scrutiny enables forensic acquisition tools to be free of the objection of *reasonable doubt* that the acquisition process has compromised the evidence due to unknown and perhaps untrustworthy source code, thus invalidating the investigation.

This has been a long, hard and endless topic of discussion within the digital forensics community because *reasonable doubt* is based on commercial software's *black box* model: we know the inputs and we can see the outputs, but we do not know what is going on inside – nobody can view the proprietary source code – and it could pose a legal objection in a trial, even if the commercial software is certified. With Open Source tools, anyone can view the source code, so there are inputs and outputs, but no black box hiding the forensic processes.

### Open Source

- Free
- Not always easy to use
- We know what is going on inside

### Closed Source

- Expensive
- Easier to use
- Black box: we do not know what is going on inside

## Phase 1 - Acquisition

Before acquiring the data from a seized hard disk, every doubt must be eliminated that the investigator might have contaminated or altered the contents of the disk, thus rendering the evidence useless and inadmissible. In order to accomplish this we must isolate the hard disk by either utilizing a separate machine or by booting the seized computer from an Incident Response and Forensics CD. The most popular tools are Helix, FIRE and IrItaly Live CD, which are designed to mount the hard disk in read-only mode, keeping the drive and its data forensically sound. In this case we will used Helix 1.7.

Our investigation is tasked with uncovering evidence of money-laundering associated with a phishing/fraud operation. We will search through e-mail, documents, internet browsing, etc. Let's acquire some data.

### 10:00 am – Isolate the seized hard disk

Open the case of the seized computer and detach the power connector from the hard disk. Switch on the computer, enter into the BIOS and check the clock of the BIOS and the Boot sequence. Set it up to boot from CD-Rom, switch off the computer and switch on it again (the hard disk is still detached) in order to test that the computer will boot from the Helix CD.

After verifying the computer is working properly from the CD shut it down. Now connect an external USB drive in order to store a copy of the original hard disk. Reconnect the power cable to the seized hard disk and reboot – always keeping a finger on the power button ready to quickly cut power if the hard disk starts accessing. The computer absolutely MUST NOT boot from the hard disk because it could write something (swap files, etc.) or delete/alter the contents of the disk – evidence destroyed.

### 10:30 am - acquire the data

Helix displays a graphical environment with several acquisition and analysis tools – Autopsy, Adepto, foremost and PyFlag – graphical tools, video tools, and the entire suite of Open Office, etc.

The first thing to do is determine the series number and the model of hard disk:

```
hdparm - i /dev/hda
```

or run Adepto and choose *hd source*.

Next, before starting to copy, mount the external USB drive in read/write mode by running Root Terminal and writing:

```
mount - or rw /dev/sda1 /media/sda1
+ ENTER
```

This is the moment of starting the true acquisition! Launch Adepto, write the name of the investigator and case number, and then choose the source drive `/dev/hda` and the destination drive, paying attention NOT to choose `/dev/sda1` which will clone the entire hard disk. We want the *raw image* of the drive, which is easier to manage. In fact, the raw image – image.img – can be compressed, divided into pieces of various sizes while the external hard disk maintains its size. If the seized disk were cloned, the external disk would be the same size of the cloned disk.

Choose the raw image – image.img – and then, in the copy options, choose SDD (a faster version of Linux DD). Finally choose the MD5 hash in order to sign the copy digitally and to compare it with the hash of the original disk, so as to dispel every doubt that the copy is not equal, bit for bit, to the original disk.

Now press START, and prepare to wait: the average speed (with USB 2) of the copying process is 1GB per minute. Therefore, if the size of the hard disk to copy is of 80 GB, it will take 80 minutes. When

# A Security Incident

By Giuseppe Russo

Any serious security incident requires an in-depth forensic investigation to uncover criminal activity for use as evidence in court as well as to understand how the incident was perpetrated.

### Do not modify the crime scene

Prevent unauthorized personnel from tampering with the compromised system. It may be useful take photographs of papers, disks, or peripheral devices in the area and to collect any items that might contain evidence. If the system is running, DO NOT shut it down before performing a memory dump in order to retrieve any data from memory of programs still running.

### Collect the evidence

Examine the affected system and/or network. An important action here is to check the current date and time and compare it to the known standard. Make a note of the difference, if any. This could be useful in correlating file timestamps to other incident data gathered.

A this point we must prepare the system for data acquisition. See Nanni Bassetti's description of this process. When finished, secure the evidence: remove all the drives and seal them with evidence tape in antistatic bags. Date and sign the evidence tape, and secure the drives in a locked container.

Our analysis starts with determining what we are looking for, and accordingly we would check data on registers, peripheral memory and caches, memory (kernel and physical), network state, running processes, hardware data residue, memory chips, and PDA-type systems, hard disks, backup media, CD-Roms and printouts.

### Document the Chain of Custody

Each step taken must be documented with a secure Chain of Custody procedure, tracking who has been involved in handling the evidence and where it has been stored. Law enforcement officials and legal counsel are good sources for advice about how and when to collect and protect critical information.

### Prepare evidence for delivery

This involves making secure copies and documenting all the steps taken. Again, see Nanni Bassetti's description.

Digital evidence must stand up in court. Taking care to follow established procedural guidelines will ensure the evidence you gather will be not be tainted by the process of gathering it.

## About the Author

*Giuseppe Russo is Principal Engineer, Chief Technologist and Security Ambassador with Sun Microsystems, Inc. and is based in Rome, Italy. He can be reached at Giuseppe.Russo@Sun.com.*

copying is complete, Adepto verifies the hash – other 80 minutes.

### 13:30 pm – reliable copy

Adepto has finished. Click the LOG tab to see log files listing the computer's environment (cards, hard disk, CPU, etc.), the completed operations, and the comparison of the two hash codes – source and copy – that must coincide. Fortunately, they match! Save Adepto's log files to the external drive and switch off the computer.

We now have the seized computer, a reliable copy of the hard disk, and the log files describing the steps used to obtain the copy. Our steps are clear – this stage will hold up in court.

## Day 2

### 10:00 am - compressing

Before starting our analysis, we connect the external hard disk to our forensics station. If it mounts only Windows XP and the external hard disk has been formatted in EXT2 or EXT3, we will not succeed in reading it. It is useful to have the Ext2IFS software that installs drivers that allow it to read a hard disk formatted in EXT3 or EXT2 as if it were formatted NTFS or Fat. We would then be able to use all the tools of analysis and copying we usually use with MS Windows.

We have a full hard disk copy ready for investigating, but we need the hard disk image as small as possible so we can burn it to DVD-Roms in order to provide the Judicial Authority with copies. The file image.img is an 80 GB monster, so we must compress it. If the external hard disk has been formatted in EXT3, it is best to zip from Linux by gzip – even though the EXT2FSD driver for Windows allows the writing on HD EXT3 and EXT2 from Windows – because the reading and writing of large amounts of data generate reading errors after few hours, corrupting all the files generated with WinRar or Winzip. In practice the reading HD EXT3 from Windows is not perfect.

Therefore we boot from Helix and from terminal root we write:

```
gzip -N -C -9 /media/sda1/image.img /
media/sda1/zip/image.gz
```

The parameter `-N` is used to maintain the file name and timestamp equal to the original file (very important); the `-9` indicates the maximum compression factor; and `/media/sda1/image.gz` writes the data to the file `image.gz` in the directory `zip`.

### 14:00 pm – hashing

The compression process has finished. We must generate the MD5 hash code of `image.gz` in order to sign the file. Every file we produce must be signed using a Hash algorithm.

> **It is always best to pursue all reasonable methods for discovering evidence.**

Since there is no practical way to calculate a particular data input that will result in a desired hash value, our copies are reliable and secure, virtually impossible to be corrupted – secure evidence, once again.

Write:

```
md5sum /media/sda1/zip/image.gz /media/
sda1/zip/md5gz.txt
```

### 15:16 pm – hashed

Md5 is calculated – 1 hour and a quarter with Centrino 760 2 Ghz. Now we can work in MS Windows and launch the Winzip for splitting the file `image.gz` (including the file `md5gz.txt`) of 44 GB. We choose the option *Fast Compression* and DVD size which generates 11 files (10 of 4.4 GB and 1 of 1 GB).

### 16:46 pm – sign the split files

The 11 files are ready to be copied, but every single file must be signed.

```
md5deep c:\dvd \ *. * md5split.txt
```

### 18:00 pm - sign the signatures

Now we sign the files of the signatures (hash codes):

```
md5sum md5split.txt md5check.txt
```

Now even if someone tampered with the files and recreated an `md5split.txt` file, the new signature of `md5split.txt` would never coincide with that one taken from `md5check.txt` (Paranoia? Just being thorough!)

Final step: burning every single file (always adding the two files `md5split.txt` and `md5check.txt`) on DVD. At 8x speed it takes 15 minutes in order to write each DVD and 15 minutes for the write verification (in this case it is advisable). The process takes 30 minutes per DVD, so the 11 files take 5

## Advertisers

| | |
|---|---|
| Auerbach Publications – www.auerbach-publications.com | 17 |
| Microsoft – www.microsoft.com | 52 |
| PGP – www.pgp.com | 5 |
| RSA – www.rsasecurity.com | 9 |
| Security Awareness Incorporated – www.securityawareness.com | 27 |
| Skyline Advanced Technology Services – www.skyline-ats.com | 25 |
| SystemExperts Corporation – www.systemexperts.com | 21 |

hours and 30 minutes to burn. Then in the immense state of paranoia that overcomes us, we sign and label each DVD by a pen. The clock strikes 23:30 and WE HAVE ENDED!

## Phase 2 - Analysis

We focus on the target that we have been commissioned to find: all the e-mail, JPGs, and other very specific types of information. We don't want to waste our time searching for useless things. We've already spent enough time just acquiring the data!

Suppose we are tasked with discovering any relationship of the suspect (owner of seized computer) with the Company X. We try to uncover e-mail or documents relating to Company X and web browser navigations to the website of Company X. In extreme cases we could search for steganography – messages hidden into the images – or encrypted information. It depends on the importance of the investigation, the nature of our suspicions, and the computer owner's profile: a computer expert? a hacker? a typical computer user? With this profile we can determine the owner's level of knowledge in the art of hiding information. In any case, in my opinion, it is always best to pursue all reasonable methods for discovering evidence.

We launch Autopsy and try the keywords that might lead back to files or fragments of files containing something pertinent to the case: Company X, IP address of the Company X, Internet website, e-mail of Company X, financial statements, bank accounts, etc. The keywords can be in ASCII format or Unicode format and even in the unallocated space.

From the outgoing references of Autopsy we can save the contents of the files as text reports. We can even mount the image with software like Mount Image Pro and then choose *copy the files* to examine with GUI software. For example, if we find the file `SentMail.dbx`, we can feed it to tools like Attachment Extractor for OE that allow visualization of e-mail messages and attachments. In any case, we can open the file's `dbx` with a text editor and analyze the headings of the e-mail in order to determine who has sent the message, etc. The attachments will be visualized with uudecode that will transform the ASCII characters forming the attachments into binary format.

## Conclusion

After exhausting the searches and discovering all we can regarding our investigation, our final steps would be:

- Deliver the DVDs with a signed sheet containing all the MD5 hash codes
- Deliver all the digital evidence found and signed with MD5 and/or SHA1
- Write a technical report on all the actions we performed and update the documents of the *chain of custody* – the paper trail tracking every step that has been taken with the evidence. It is always signed by the investigator and the police officer who brought the evidence. Our portion of the chain documents when we received the computer, who delivered it, what was done with ti: the copying the hard disk, hashing, zipping, and burning to DVDs for delivery to the prosecutors who must have the copies for official use and who must eventually must provide a copy to the defense.

The investigation is concluded and the evidence…will speak in a court of law.

## About the Author

*Nanni Bassetti is a Digital Forensics and Computer Security consultant in southeastern Italy on the Adriatic Sea. He has a Computer Science degree, many years of experience with the Italian companies and Italian privacy law. He is a member of ISSA, AIPSI and CLUSIT and can be reached at nannib@libero.it and www.nannibassetti.com*