Techniques and standards for Preservation of Data

4-1 Disk Imaging Overview

IT professionals are concern on how to prevent intrusions and attacks. But what do you do if the worst happens in spite of your security patches, firewalls, and other efforts?

Given the huge costs in downtime, lost productivity, and administrative work load that can result from an attack, we all feel happy when hackers or virus writers are caught يتم الامساك بهم and prosecuted يتم احالتهم للقضاء , but it doesn't seem to happen very often. **That's because successful criminal prosecution requires hard work, admissible evidence, which can be difficult to come by lazy investigator**. Sadly, the evidence is often contaminated يتعرض للتلوث or destroyed in the process of responding to the attack (in the same way that the water used to put out a fire sometimes causes as much damage as the fire itself).

The key point is that evidence can become inadmissible if anyone who handles it after an incident takes place does anything to change it. But simply opening a file and changes it will make it inadmissible (for example, the date of last modification may change), so how can digital evidence ever be preserved in an admissible state?

Imaging software for forensic purposes MUST use some method of verification to ensure that the copy is exactly as the original. For this reason, it is best not to use disk imaging software intended for other purposes *(such as Norton Ghost, which was made for creating cloned images to install on multiple machines, but was not designed specifically for forensic use with the emphasis on the absolute integrity of the copy).*

Forensics-based imaging systems often use a special computer that is attached to the target computer via one of its communications ports, through which the complete copy of the disk can be copied to another disk, or other electronic media. In other cases, the disk is removed from the target computer to be copied. The imaging process should be done in a way that will leave no traces (make no changes) on the target computer.

Disk Imaging characterized by:

1- **Once investigator have done forensically copy, the original disk is set aside and preserved in its current state. All examination work MUST BE DONE ON THE COPY.**
2- **The suspected computer must immediately isolated from the network and physically secured so that no one could make any changes to it between the discovery of the incident and the time the disk was imaged.**
3- **Investigator must do nothing even NOT turn the computer on or off or examine logs until the disk has been imaged.**
4- **The disk imaging should be done by a qualified forensics investigator.**

The previous steps not reflected on your abilities as an IT professional; it is because the defense attorney المحامي او الوكيل in a court trial will ask the credentials of those who performed the imaging and/or examination. More credibility will be given to the evidence if it was collected by someone who specializes in computer forensics.

More details can be fount on: https://technet.microsoft.com/en-us/library/cc512667.aspx?f=255&MSPPError=-2147217396

4-2 Acquisition and preservation مهم جدا

You cannot work with the original material, so investigator MUST create an exact Physical or Logical duplicate of it. **The creation of a forensic copy is the acquisition.**

Q What is Acquisition??.

A forensic copy is the end-product of a forensic acquisition of a computer's hard drive or other storage device. A forensic copy is also called a bit stream copy or image because it's an exact bit-for-bit copy of the original document, file, partition, graphical image, or disk. For example, all metadata, file dates, slack areas, bad sectors — everything — are the same in the image as in their original forms.

Q Why forensic copy called bit stream?

Acquisition isn't the same as copying files from one medium to another. Investigators CANNOT use a copy command because dates aren't preserved. It is essentials to make several forensic copies in case something happens to the image.

You can make a forensic copy in several ways, all requiring specialized software or hardware. **below a description for the two imaging methods**:

1- **Drive:** This means captures everything on a drive. One method of capturing or copying all data on a drive is to make a mirror image of the drive. Slight variations in definitions of a mirror image (regarding to bit stream or sector by sector) exist. A mirror image might be an exact copy of a hard drive, but not necessarily. Mirror images are meant for backup purposes. To be safe, assume that a mirror image isn't a forensic image.

2- **Sector-by-sector or bit stream:** This more advanced method starts at the beginning of a drive and makes a copy of every bit — zeros and ones— to the end of the drive without any deleting or modifying the contents of the evidence. The file slack and unallocated file space that often contain deleted files. **This method creates a forensic image of the e-evidence.**

http://www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643

4-3 Write Blockers Tools

Write blockers Tools are devices and/or software that allow acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents. They do this by allowing read commands to pass but blocking write commands or functions. Write blocker permits تسمح read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can **GUARANTEE** the protection of the data chain of custody.

There are two ways to build a write-blocker: the blocker can allow all commands to pass from the computer to the drive except for those that are on a particular list. Alternatively, the blocker can specifically block the write commands and let everything else through.

Write blockers may also include drive protection which will limit the speed of a drive attached to the write blocker tools. Drives that run at higher speed work harder (the head moves back and forth more often due to read errors). This added protection could allow drives to be read at the slower modes.

There are two types of Hardware Write Blockers, Native and Tailgate. A Native device uses the same interface for both in and out, for example a IDE to IDE write block. A Tailgate device uses one interface for one side and a different one for the other.

There are both hardware and software write blockers. Some software write blockers are designed for a specific operating system. One designed for Windows will not work on Linux. Most hardware write blockers are software independent.

http://forensicswiki.org/wiki/Write_Blockers

4- 4 Software versus hardware write blockers

Software and hardware write blockers do the same job. They prevent writes to the original storage media. THE MAIN DIFFERENCE between the two types is that software type is installed on a forensic computer workstation, whereas hardware write blockers have write blocking software installed on a controller chip inside a portable physical device.

H. W Pro

1. It is not reliant on an underlying operating system.
2. Is easier to explain and generally makes more “sense” to non-technical people.

3. Clear visual indication of function through physical lights/switches.
4. Generally provides built in interfaces to a number of storage devices (IDE, SATA, etc.).
5. Appears to be more accepted in the general forensics community.

H. W Con

1. An additional piece of kit to carry around with you.
2. An additional piece of hardware that needs to be maintained and could fail.
3. Generally restricted to the available storage interfaces built into the device (additional interfaces cannot be added).

S. W Pro

1. The software write blocker is directly installed on your image acquisition workstation and additional hardware is not necessary (lightens the load, one less thing to fail, etc).
2. Generally able to use any interface available on your imaging workstation (and any interface that could be added down the road)
3. Prevents an additional purchase when a new storage interface is needed.

S. W Con

1. Can be more difficult to explain to a non-technical person and thus more difficult to explain that the write blocker is actually functioning, if challenged. (Reliant on underlying and complex hardware and/or software (i.e. operating systems).
2. **The possibility of failure through updates, upgrades, etc.**

https://www.cru-inc.com/data-protection-topics/write-blockers/

http://dereknewton.com/2010/05/write-blockers-hardware-vs-software/

4-5 Rules for Imaging Drive

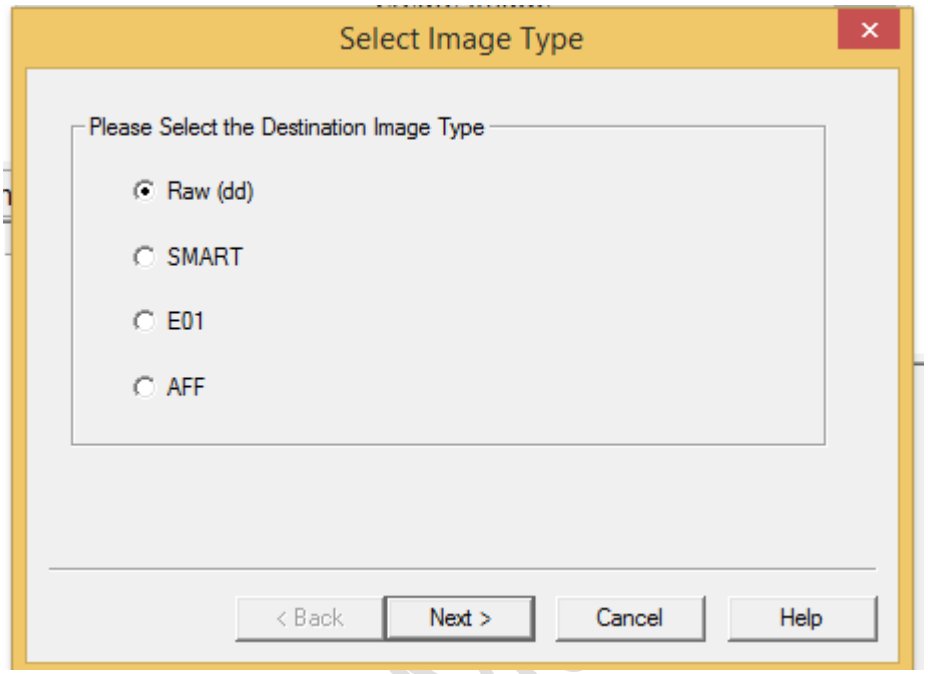
1. **Make 2 copies of the original media, fisrt copy becomes the working copy and the second copy is a ibrary / control copy.**
2. **Verify the integrity of the copies to the original.**
3. **The working copy is used for the analysis.**
4. **The library copy is stored for the event that the working copy becomes corrupted.**
5. **If performing a drive to drive imaging (not an image file) use clean media to copy to.**
6. **Verify the integrity of all images!**

4-6 Verifying Acquired Images

Hash function is used to ensure integrity by create a "fingerprint" of the data. The acquired المستحصلة image is verified by using the SHA-1 or MD5 hash functions. At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state.

Q Why media need to be hashed?

4-7 Types of Acquired images



1- Raw Image Format (dd)

The RAW Image Format is used to store a disk or volume image Contents. The RAW Image Format is basically a bit-for-bit copy of the RAW data of either the disk or the volume, without any additions or deletions.

There is no metadata (Metadata is data about data) **stored in RAW Image Format files. However sometimes the metadata is stored in additional files.**

DD **sometimes called GNU dd, is the oldest imaging tool still used. Although it is functional and requires only minimal resources to run, it lacks فيها شيء من الضعف some of the useful features found in more modern imagers such as: 1- metadata gathering 2- error correction 3- piecewise hashing and 4- a user-friendly interface**.

DD is a command line program that uses several obscure command line arguments to control the imaging process. Because some of these flags are similar and, if confused can destroy the source media, users should be careful when running this program. The program generates raw image files which can be read by many other programs.

http://www.forensicswiki.org/wiki/Dd

2- SMART (EnCase)

SMART is a software utility for Linux designed by the original authors of Expert Witness (now sold under the name of EnCase), **can store disk images as pure bit streams (compressed or uncompressed)** and also in ASR Data's Expert Witness Compression Format. **Images stored in the latest format can be stored as a single file or in multiple segment files, each of which consist of a standard 13-byte header followed by a series of sections, each of type "header", "volume", "table", "next", or "done". Each section includes its type string, a 64-bit offset to the next section, its 64-bit size, padding, and a CRC, in addition to actual data or comments, if aplicable.**

3- AFF

The Advanced Forensics Format (AFF) is an extensible open format for the storage of disk images and related forensic metadata

AFFv3 Extensions

The original AFF format is a single file that contains segments with drive data and metadata. Its contents can be compressed, but it can be quite large as the data on modern hard disks often reach 100GB or more in size. AFFv3 supported three file extensions -–– AFF, AFD and AFM –-- and provided a tool to easily convert between the variations.

For ease of transfer, large AFF files can be broken into multiple AFD format files.

The AFM format stores the metadata in an AFF file, and the disk data in a separate raw file. This format allows analysis tools that support the raw format to access the data, but without losing the metadata.

For more details about prevoius vesion found on:

https://www.loc.gov/preservation/digital/formats/fdd/fdd000412.shtml

4- E01 File? مهمة جدا

The E01 (Encase Image File Format) file keeps backup of various types of acquired digital evidences that includes disk imaging, storing of logical files, etc. When an investigator (or a Forensic Expert) uses Encase to create a backup of data available in the hard disk, a bit stream of the data is produced. This procedure is known as Disk Imaging. **The basic theory behind the relation between the Encase and E01 image file format is that, while creating images of the data available on the hard disk, Encase divides the complete data into 640 MB of data chunks. Due to this division of data at 640 MB, multiple data files, storing hard disk information are created. The most peculiar feature الصفة الغريبة او المميزة of these files is that the name of the files remains the same (as named by the user) whereas the file extension changes.**

For example, if the very first chunk of 640 MB is created with the name "S01.E01", the next 640 MB chunks will be named as "S01.E02", followed by "S01.E03", "S01.E04", "S01.E05" and so on.

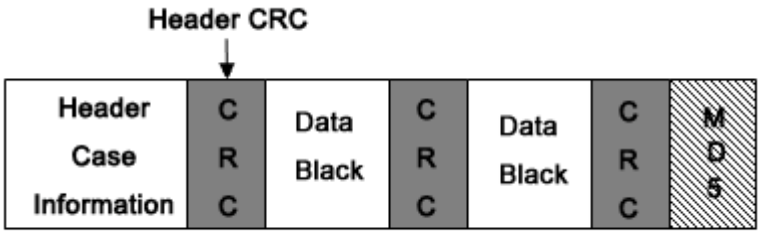
Note: - *In spite of the fact that the file extension gets changed after*

crossing a limit of 640 MB (i.e E01, E02, E03, E04 and so on), the internal structure of the file remains absolutely intact سليم

Structure of E01 File: -

The e01 image file format is prefixed with a "Case Info" header, After every block of 64 sectors (512 KB) i.e. 32 KB. It is interlaced متشابكة with CRCs (Cyclic Redundancy Check). The footer of the E01 file contains an MD5 hash value of the entire imaged data.

Header: - The header portion of the e01 encase image file basically contains the **"Case Information"**. At the time of the disk imaging, this information includes:-



1. Name of the Person (or the Investigator)
2. Case Name (in relevance to the actual case)
3. Description of media (the configuration, etc. of the hard disk from which the data are being collected)
4. Date/time information (when the encase image file was done)
5. The version of the Encase Software being used

The operating system on which Encase Software is currently running (i.e. the operating system installed on the acquired device)

CRC (Cyclic Redundancy Check): - CRC is an acronym for Cyclic Redundancy Check. CRC is an error – detection code used by the Encase in E01 files to check for any accidental changes in the original data. CRC

is basically a hash function. A CRC code for each data block is created by the software at the beginning of the acquisition and stored. Later, when that particular data block is scanned, the CRC code of the resultant e01 encase image is calculated again. If the new calculated CRC code and the previously stored CRC matches, then the data block is error – free else, some data error has occurred. CRC checksum is interlaced at every 32 KB notch of data.

Data Blocks: - The E01 file (Encase Image File) contains data chunks. In these, data chunks, the data is divided into blocks of 32 KB and CRC checksums are embedded between every data block, to check for the occurrence of any kind of error.

Footer: - The footer portion of the E01 image file format contains an MD5 value of the entire message stream available in that particular file. This MD5 hash value of the raw image file can be checked and compared with, the MD5 value of the same image file created by any other third party tool. If both the MD5 values match, then no modification has been made in the original disc image file. Otherwise, the file has been tampered or modified.

This E01 file is a very important source of disk imaging and has now become a very peculiar and advantageous medium for forensic investigators to backup the data available on a hard disk that may later be examined and analyzed.

http://www.forensicsware.com/blog/e01-file-format.html