Document Name		
Document Title	Forensic Disk Imaging Report	
Project	Forensic Investigation of Digital Objects (FIDO)	
Author(s)	Gareth Knight	
Date	30 June 2011	
Access	☑ Project and JISC internal	☑ General dissemination

Document History			
Version	**Date**	**Author**	**Comments**
0.1	03 May 2011	Gareth Knight	First version
1.0	30 June 2011	Gareth Knight	Added references

Catalogue Information	
Title	Forensic Disk Imaging Report
Creator	Gareth Knight
Keywords	Forensic imaging, fido, disk image, dd, disk clone, digital preservation, acquisition
Description	The report examines the principles and practices associated with forensic disk imaging
Publisher	King's College London
Contributor	
Date	2011-06-30
Language	En-gb
Rights	Creative Commons Attribution-NonCommercial-ShareAlike 2.0 UK: England & Wales

Report purpose

The Forensic Investigation of Digital Objects (FIDO) project investigated the application of digital forensics within the working practices of a UK HE archive. The project demonstrated the value of adopting tools and techniques developed for the emerging digital forensics field, while building upon the long-standing archival theory archival and digital curation approaches. The report examines the principles and practices associated with forensic disk imaging

Introduction

Acquisition is commonly defined as the act of obtaining possession or control of an object. For an archive handling physical records, acquisition may involve several activities associated within negotiating for and transporting a box of papers or other items. For a forensic investigator, acquisition is commonly used to refer to the process of taking control of a digital device and obtaining all information possible (Grobler, 2010). The challenge for an investigator is to acquire digital information in a manner that maintains the context of its creation, while avoiding actions that will result in it being modified, corrupted, or lost. For digital information stored on live computer systems the process of capturing data in a 'forensically-sound' manner is particularly challenging, since in many circumstances, the process of accessing the machine media, either through booting from it or accessing it through file manager software, may result in the access software making some change to the underlying data.

When performing a forensic investigation, it is common for investigators to make an exact copy of the digital media and store it as a disk image prior to performing analysis. By producing a duplicate of the forensic object, they may ensure that they do not irretrievably damage or destroy the only copy of the digital information that they seek to identify and analyse. This report outlines the role of data imaging within a forensic and other environments, the encoding formats that may be used to store data the software tools that may be used for data capture, and describes a set of procedures that the archivist should follow to capture digital media in a forensically-sound manner.

What is a disk image?

A disk image is a set of one or more files that, in combination, contain the content and structure of a mass storage device, such as magnetic (e.g. 3.5" floppy, hard disk), optical (e.g. CD, DVD), or solid state (USB storage, SD card) media. The type of information encoded in a disk image will vary, dependent upon the capabilities of the disk image format and configuration of the software tool. Imaging software may be configured to capture a bit copy of the disk (including information such as partition table, file allocation tables and data partitions), or to capture used data space only. The former is considered to be the most preferable approach by forensic analysts, since it will capture the exact state of the disk, including hidden and deleted data that is managed by the operating system, but invisible to the end user.

A large number of encoding formats exist capable of storing media within a file. Many encoding formats have been designed for the storage of specific types of media, e.g. ADF and IPF have been developed with consideration of the peculiarities of the Amiga disk format, while other formats exist that are capable of storing a diverse range of generic media, e.g. the "raw" DD format.

Purposes for which disk imaging is used

Disk imaging is commonly performed by a number of communities for several purposes:

- *Media Preservation:* Media imaging is commonly used within the digital preservation community to preserve software applications/games originally stored and distributed

upon tapes, floppy disks and other media during the last 40 years. The image file may be subsequently stored and accessed using emulators or other software tools.

- *Digital Forensics:* A branch of forensic science concerned with the acquisition and analysis of material held on digital devices, often in relation to a crime.

- *Data backup and recovery:* Backup of digital data, such as that held on a live server, for restoration in the event that the original data is damaged or lost. For the backup of entire systems, it often requires less effort to create an image or mirror of an entire disk, which can be transferred offsite for storage.

- *Data distribution:* Software developers, such as Apple and Microsoft, increasingly package software tools and updates as disk images, embedded within an executable file, which are installed on the user's machine.

Motivations for disk imaging in the forensic & archival community

Several reasons may be identified for choosing to capture a complete image of physical media, as opposed to simply copying the files. These are dependent upon the discipline in which the investigator is working and the purpose for which they intend to use the data. Disk imaging is commonly performed in the IT industry as a method of data backup, in order to enable quick restoration in the event of media failure (1) or data transfer (2), while the forensic community use it as a basis for analysis (3,4). The case for disk imaging in the digital archives community is less defined, but may incorporate elements from the digital forensic and digital preservation world, providing a source object that can be analysed in order to gain an understanding of the data creator (5).

1 Creation of a backup copy of data, protecting against media failure or corruption to the original disk, which may have financial, legal or cultural repercussions (general)
2 Enable access and use of data in hardware and software environments other than that for which it was created and used (general)
3 Enable analysis of digital evidence, while avoiding the risk that processes will result in inadvertent, unrecoverable change to the only copy (forensic)
4 Enable analysis using methods and tools that are not possible/available in the original environment (forensic)
5 Capture and preserve more information by and about creators than previously possible (Kirschenbaum, Ovenden & Redwine, 2010, p56) (archival)

Disk imaging procedures

There is considerable discussion in the computing industry on the most effective strategies for backup and storage of data[1]. These are applicable to all types of data backup, irrespective of the motivations for its performance or the level – file or media – at which it is applied.

- *Atomic image:* A disk image created through the performance of a full backup of a drive. An atomic image[2] may be characterised by its independence, it is a standalone artefact that is not dependent upon other image types, such as incremental or differential images, to be accessed. A forensic investigator will generate an atomic image when they are running disk imaging software on a drive for the first time.

[1] See http://www.backup.info/difference-between-full-differential-and-incremental-backup and http://iosafe.com/blog/tips/types-of-computer-backups/ for discussion on this topic from a system management perspective
[2] The term has been coined by the author to distinguish it from differential and incremental images which are described at http://blog.laplink.com/tag/forensic-imaging/

- *Differential image*: A differential image contains changes that have been made since the first disk image was created only. Differential imaging is performed by comparing the previously generated disk image to the source disk and identifying files that have been created, updated, or deleted since the initial imaging process. A differential image may be deleted if a new differential image is created. Differential imaging has the advantage of being quicker to perform than a full backup and requires less storage space in comparison to the creation of two or more atomic images. It also requires less effort to merge with an atomic image in comparison to incremental images, since there will be only two files in total (atomic + differential image). However, it is unlikely that the combined image (atomic+differential) will be considered to have forensic value, due to the increased likelihood that the merging activity will have resulted in change occurring to the original disk image. In addition, since differential analysis is typically performed at the file level, it is likely that it will miss deleted or corrupted data that can only be extracted through carving.

- *Incremental Image:* an incremental image contains changes that have been made to the disk, similar to the differential image. The key difference between the performance of differential and incremental disk imaging is the number of images that will be produced. Whereas only one differential disk image will exist, multiple incremental images may exist that each contains changes that have occurred since the last incremental update was performed. To produce a combined image, an analyst must load the disk image originally created and incorporate each incremental update in turn. Similar to differential imaging, incremental imaging has the advantage of being quicker to perform than a full backup and requires less storage than multiple atomic images. However, similar to differential images, the evidential value of data captured using this method is likely to be lower and the process of performing an analysis of incremental changes may have resulted in deleted or corrupted information being overlooked.

In the digital forensic realm, the performance of a full backup and subsequent storage as an atomic disk image is the preferred method of data acquisition, for a number of reasons. Most notably is the desire for simplicity, the merging of a full + differential or incremental backup increases the potential risk that unexpected change will occur which, if discovered, may damage the case established in court. Second, there is a technological factor – differential and incremental analysis is performed at the file-level, which ignores other data held on the disk. Finally, the procedures applied in the digital forensic realm must also be considered. Forensic analysis in the legal profession is typically performed upon confiscated equipment that will not be reused, rather than equipment that undergoes ongoing use and maintenance. Therefore, there is less incentive to develop differential/incremental imaging capable of performing analysis at the bit level.

Format Overview

A diverse range of imaging formats exist that are used within the digital forensic community. The proprietary EnCase Evidence and Expert Witness Compression Format are considered to be the de-facto imaging formats within the forensic community, with a smaller number of investigators storing data using the Advanced Forensic Format (AFF) and Raw/DD. In addition, there are also a number of application-specific formats maintained by specific software developers. Examples include the ILook Investigator IDIF, IRBF, and IEIF Formats, ProDiscover image file format, PyFlag's sgzip Format, Rapid Action Imaging Device (RAID) format and Safeback format, while a small number of open and well documented formats exist

The following section explores the advantages and disadvantages of the three forensic formats most commonly used within the digital forensic community. All three are well documented and well supported within open source and commercial disk imaging tools.

Raw (DD) image

Raw or Raw/DD is a type of disk image created by the DD Unix command and other software tools. Raw images contain a bit-by-bit copy of a source device, without any attempt made to identify or interpret the filesystem or files held on the disk. As a result, it is a misnomer to describe Raw as a disk imaging format.

A common criticism of DD, which may serve as an argument against use of Raw in a forensic environment, is the lack of metadata support. It is not possible to store acquisition information, such as who performed the disk imaging, when it was performed, or technical details of the capture process. To address these concerns, a number of derivatives, such as dcfldd and dccidd have been created which calculate hash values (MD5, SHA-1, SHA-256) for data being copied and store them as a separate file to accompany the disk image.

Table 1: A Checklist of Preservation Consideration for the Raw (DD) format

Positive	*Negative*
Captures data from device as-is, including allocated and unallocated sectors, making it useful for forensic acquisition	No support for embedded metadata or fixity values (several tools store metadata as a separate file alongside raw file)
Device and platform agnostic, enabling it to be used to acquire data held any mounted device, irrespective of whether the underlying file system can be understood	Ability to acquire raw disk image can lead many users to be overconfident in its capabilities, potentially resulting in some information being lost or corruption. Acquisition is dependent upon the functionality of the capture device. Errors may be encountered when attempting to capture from media intended for use with custom hardware.
Ubiquitous support as a result of the inclusion of DD in all Unix-derived/influenced operating systems. Widespread support for raw disk in range of software tools, including those in use for digital forensic	
Capable of storing image of semi-working disks, omitting damaged sections, if disk can be connected and used.	

Advanced Forensic Format (AFF)

The Advanced Forensics Format (AFF) is an extensible open format for the storage of disk images and related forensic metadata. It was developed by Simson Garfinkel and Basis Technology. The AFF format is comprised of two layers: a Data-Storage layer that contains the disk information, and a Disk Representation layer that may be used to associate metadata with specific segments of the disk image. Three variations of AFF exist:

1 *AFF:* A single image file that contains disk segments and accompanying metadata. Uncompressed AFF files are slightly larger than the disks that have been imaged. The large (4GB+) file size may cause difficulties when attempting to store disk images in some file systems, such as FAT32 (as used in Windows 9x by default and optional in later versions) and ISO8601.

2 AFD: An AFF disk image stored as multiple files in a single directory. The maximum size of each AFF may be configured by the user. AFD directories are commonly labelled with the extension .afd.

3 *AFM:* One or more raw/DD disk images with accompanying AFF annotations stored in a separate AFF XML file. The variation is intended for use with analysis tools that support the raw format, without losing the ability to store additional metadata

Forensic metadata, stored internal to the AFF or as a separate file, may refer to the disk as a whole and/or individual segments. For example, metadata may refer to acquisition date, segment size (segsize), disk image size (imagesize), MD5/SHA1 fixity value, as well as reference to bad and blank sectors.

Table 2: A Checklist of Preservation Consideration for the Advanced Forensics Format

Positive	*Negative*
Images may be held in a single file or distributed across multiple files	Less support that raw/DD format
No limitations upon file size	Recovery from damaged EWF files is reported to be difficult, requiring detailed knowledge of the file format[3]
Capable of storing any forensic metadata required by investigator	The AFF default compression page size of 16 MB can impose significant overhead when accessing NTFS Master File Tables (MFT)[4]
May be compressed to reduce storage space (or uncompressed)	The Table of Contents specified in the AFF1 specification is not used and, as a result, the header for each segment must be read when the AFF image is opened. This may increase the time taken to open a large file by an estimated 10-30 seconds[5]
Markers for “bad” sectors	
Produced image file smaller than EVF	

An ‘AFF4’ specification was published in 2009 which constitutes a redesign and revision of AFF to enable large corpuses of disk images to be managed and used. The AFF4 specification uses RDF specify attributes about objects – segments of a data image, enabling different types of evidence to be linked and analysed. Support for the specification within forensic tools is currently limited, but is likely to increase in the future through integration of LibAFF4[6].

Expert Witness Forensics (EWF)

Expert Witness Forensics EWF) is a proprietary disk image format used by Guidance Software in the EnCase software tool. The format is derived from ASR Data's Expert Witness Compression Format, while offering some refinements and enhancements in its design. It is widely considered to be the de facto standard for forensic disk images[7], due to the popularity of EnCase within the law enforcement community. It is also supported by a number of open source tools, via the LibEWF library.

Evidence files are composed of three segments

1 *Case Info header:* the header contains metadata on the date and time of acquisition, an examiner's name, notes on the acquisition, and an optional password.
2 *Bitstream:* The bitstream of the disk that has been acquired. The bitstream is interlaced with checksums (Adler32) for every block of 64 x 512 byte sectors (32 KiB).

[3] http://www.forensicswiki.org/wiki/AFF4
[4] http://simson.net/clips/academic/2009.DFRWS.AFF4.pdf
[5] http://simson.net/clips/academic/2009.DFRWS.AFF4.pdf
[6] http://www.forensicswiki.org/wiki/LibAFF4 and http://code.google.com/p/aff4/
[7] http://www.forensicswiki.org/wiki/Encase_image_file_format

3 *Footer:* The footer contains an MD5 hash for the entire bitstream.

Evidence files may be a maximum of 2GB in size, to enable them to be stored on file systems that define file size limitations. A 2GB+ disk image is stored as multiple files within a directory and assigned a naming convention that indicates the processing order (e.g. name.E01, name.E02, name.E03, etc.).

The format restricts the type and quantity of metadata that can be associated with an image. However, an Extended EWF (EWF-X) specification defined by the libewf[8] project defines a new header and (digest) hash section encoded as XML. The EWF-X E01 files are reportedly compatible with EnCase and an increasing number of third party tools.

Table 3: A Checklist of Preservation Consideration for the EnCase Evidence

Positive	*Negative*
Images may be held in a single (2GB or under) file or distributed across multiple files	Less support that raw/DD format
De facto format with widespread support in a range of commercial and open source tools	Disk image files produced by the software are reportedly larger than AFF.
May be compressed to reduce storage space (or stored uncompressed) Support for embedded metadata providing basic information on the data acquisition and composition Supports block-by-block checksums enabling the investigator to determine the sector that has been corrupted, limiting the damage that data corruption can cause to an investigation by demonstrating that the evidential value of other sectors has been maintained.	

Selecting a disk imaging format for the FIDO project

All of the disk image formats examined are capable of holding a bit-by-bit copy of digital media. In order to determine the format that is appropriate to the needs of the investigation, it is necessary to determine a set of criteria that includes other factors. Previous work in this area has focus upon different issues. Garfinkel, Malan, Stevens & Pham (2006), for example, considered extensibility, licence status (non-proprietary vs. proprietary), and support for compression and data location as three factors that required consideration. For the analysis of disk image formats performed for the FIDO project, the author was influenced by selection criteria used to select file formats for storage of still images, sound, video and other types of content (Todd, 2009), defining eight factors for evaluation:

1 *Adoption* – the extent to which the format is in widespread use within the forensic community and elsewhere.

2 *Software independence* - the extent to which the format is independent of specific support from hardware and software

3 *Disclosure* – the extent to which the file format specification is in the public domain;

[8] http://sourceforge.net/projects/libewf/

4 *Metadata support* – the extent to which descriptive information is supported in extractable form within the format.

5 *Licence status:* The licence associated with the format, which may affect the degree of disclosure and adoption.

6 *Level of fixity analysis supported:* The level at which a fixity check can be performed upon the data image. Forensic literature refers to fixity checks being performed at three levels – a fixity check of the data image as a whole, check on individual files within the data image, and for each segment or chunk of data within the image.

7 *Support for split files:* The ability to split a large disk image into smaller sections of an arbitrary size for storage on disc or other media

8 *Compression support:* The ability to compress the data image to reduce storage space. Compression support is useful but it not considered mandatory that the format provide built-in support, since it will take longer to locate data on a compressed file.

On the basis of the investigation, the project selected the Advanced Forensic Format (AFF) as the preferred format in which to acquire disk images.

Name	*Adoption*	*Software independence*	*Disclosure*	*MD support*	*Licence status*	*Level of fixity analysis supported:*	*Support for split files*	*Compression support*
Raw/DD	Widespread support	Supported by wide range of software tools and libraries	N/A – not a format	No, but can store AFF XML or other MD in a separate file	N/A	Data image only (via XML file)[9]	No, but, as with all files, can be split into smaller chunks using 3rd party tools	No, but can compress separately using ZIP, TGZ or algorithm
AFF	Widespread support	Supported by wide range of forensic tools and libraries	Public specification	Yes. Internal & external	Open	Unknown – supports Data image, but uncertain if supports segment-by-segment[10]	Yes	Yes
EWF	Widespread support	Supported by wide range of forensic tools and libraries	Proprietary, but documented	Yes. Internal & external	Commercial	Data image + segment-by-segment[11]	Yes, up to 2GB	Yes

Table 4: Assessment criteria for forensic image formats

[9] Necessary functionality may be provided by a third party tool. However, the 'format' has not been designed to support or store such analysis.
[10] File-level metadata may be gathered using third party tools
[11] File-level metadata may be gathered using third party tools

Data Imaging Tools

A large number of software tools exist, for a range of operating system, which may be used by a forensic investigator to acquire digital media and store it as an image file. Many of these are intended for data backup and create a copy of files that active on disk, omitting deleted files stored in unallocated space. In performing the investigation, the author trialled the use of several tools, evaluating them on the basis of functionality (support for the selected data image format, metadata support, fixity generation and verification, and ease of use).

Name	Description	Useful Functionality	Supported formats	Licence	Requirements	Access method[12]
Dc3dd[13]	Enhanced version of dd developed at the DoD Cyber Crime Center for use in forensic investigation. Supports several features not found in dd	[1] On-the-fly hashing with multiple algorithms (MD5, SHA-1, SHA-256, & SHA-512) [2] Verify mode [3] Progress indicator [4] Improved logging	Raw	GNU GPL	Linux, and other Unix compatibles	CLI & GUI[14]
dcfldd	Enhanced version of GNU dd with features useful for forensics and security.	[1] On-the-fly hashing [2] Verify destination is bit copy of source [3] Output to multiple files/disks at same time. [4] Split output to multiple files [5] Improved logging	Raw	GNU GPL	Windows, Linux, and other Unix compatibles	CLI
FTK Imager[15]	A commercial tool for capturing and opening image files	[1] MD5 verification [2] Support for multiple output formats	Raw, EWF, SMART	Commercial [free to use]	Windows	GUI[16]
Guymager[17]	Forensic imager that focuses	[1] MD support (case	Raw, EWF (via	GNU GPL	Linux	GUI

[12] E.g. Command Line Interface (CLI), Graphical User Interface (GUI)
[13] See http://sourceforge.net/projects/dc3dd/ for further information
[14] AIR is an optional GUI for DD and DC3DD http://sourceforge.net/apps/mediawiki/air-imager/index.php?title=Main_Page
[15] See http://accessdata.com/support/adownloads#FTKImager
[16] See http://computer-forensics.sans.org/blog/2009/06/18/forensics-101-acquiring-an-image-with-ftk-imager/ for tutorial on usage
[17] See http://guymager.sourceforge.net/

	upon ease-of-use[18]	no, evidence no, examiner, description, notes) [2] MD5/SH-256 calculation [3] Verification of source & destination [4] Option to split file by size	libawf), AFF			
OSFClone	A bootable disk copying/imaging tool that may be used to capture a disk/partition and store it as a file.	[1] Ability to capture disk image using different formats [2] Metadata support (stores DD metadata as separate file)	Raw, EWF, AFF	GNU GPL	Tiny Core Linux, Perl AFF, AFFLIB, libewf	Text-based menus

Table 5: Data imaging software

The command line tools were considered too difficult to use by non-technical staff, requiring some understanding of the disk configuration. FTKImager, GuyMager and OSFClone proved to be the easiest to use, requiring little understanding of the disk itself. Of these, OSFClone was the preferred option: it contains an basic Linux operating system and copy software, enabling it to be used without having to boot from the drive to be captured; is able to mount an NTFS disk as read/write by default, without the need for further configuration; and is relatively simple to configure. Further information on the use of the tool is provided below.

In subsequent stages of the project we will work with archivists to trial the use of FTK Imager and OSFClone to determine their preferred choice.

[18] The author was able to image whole drives, but was unable to determine how to image partitions using the tool

Disk Imaging Procedures

Configuring the machine to boot from CD-ROM

To load the disk imaging software it will be necessary to configure the machine to boot from CD-ROM.

Switch on the machine and examine the messages onscreen to determine how you may enter the BIOS. The following table provides suggestions for how you may enter the BIOS on different machine types.

Computer type	*Key combination*
Most computers	Delete key <Del>
Dell computer	<F2> on newer desktop machines or <Ctrl>+<Alt>+<Enter> on older machines
Dell laptop[19]	<Fn>+<F1> or <Fn>+<Esc>

- Locate the option to alter the boot priority and alter the setting to ensure that CD-ROM is set as the first option/has greater priority over the hard disk.
- Return to the main menu (usually achieved by pressing Escape)
- Navigate to the 'Save and Exit' option and press ENTER.

Booting OSForensics

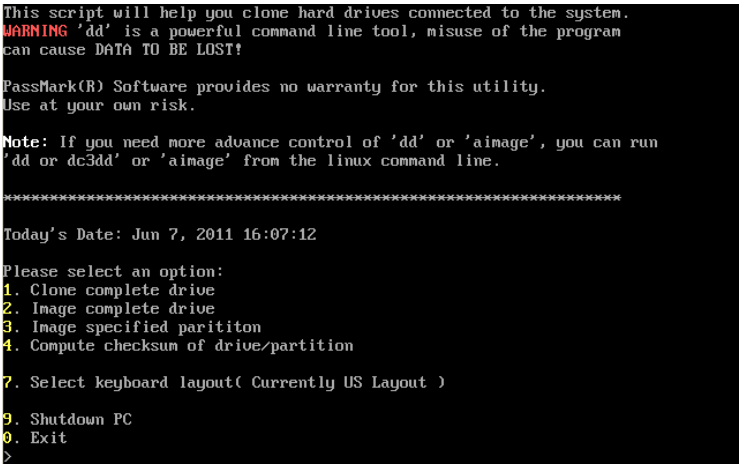
Things to check before powering on the machine

- Ensure that you have configured the BIOS to boot from CD-ROM (or USB if you're booting OSFMount from USB stick)
- Ensure that the device to which you will save data (e.g. an external hard disk, or USB stick) is connected before powering on the machine.

Notes:

- You may return to the main/previous menu by typing 'Q' (without quotes) and pressing ENTER.
- Press ENTER on the start-up screen to boot into OSForensics

1. Choose the drive/partition that you wish to image



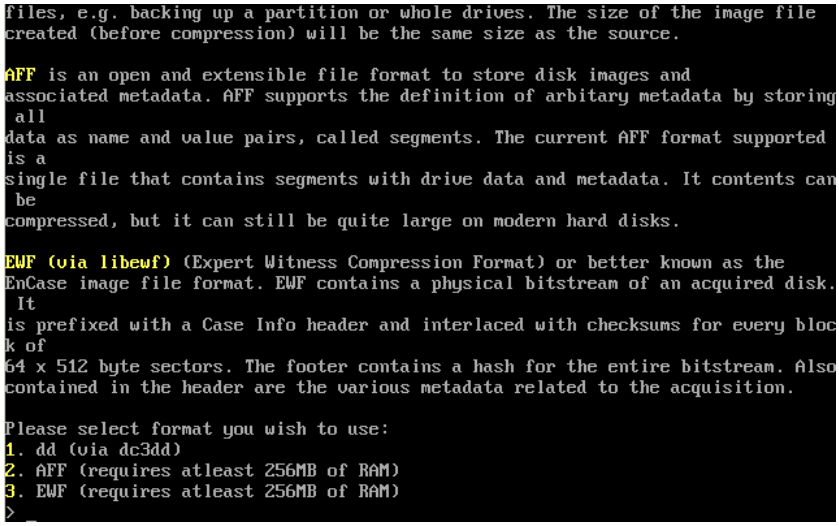
19 http://support.dell.com/support/topics/global.aspx/support/kcs/document?c=us&l=en&s=gen&docid=DSN_148562&isLegacy=true

First, choose the type of disk imaging that you wish to perform. Two options are available:

1 If you wish to create an image of the drive in its entirety, including all partitions, type '2' (without quotes) and press ENTER
2 If you wish to create an image of a single partition on a drive. The choice of this option presumes that there are multiple partitions on the disk, of which you wish to capture only one, type '3' (without quotes) and press ENTER

If in doubt, choose capture the complete drive.

2. Choose the acquisition format of the disk image

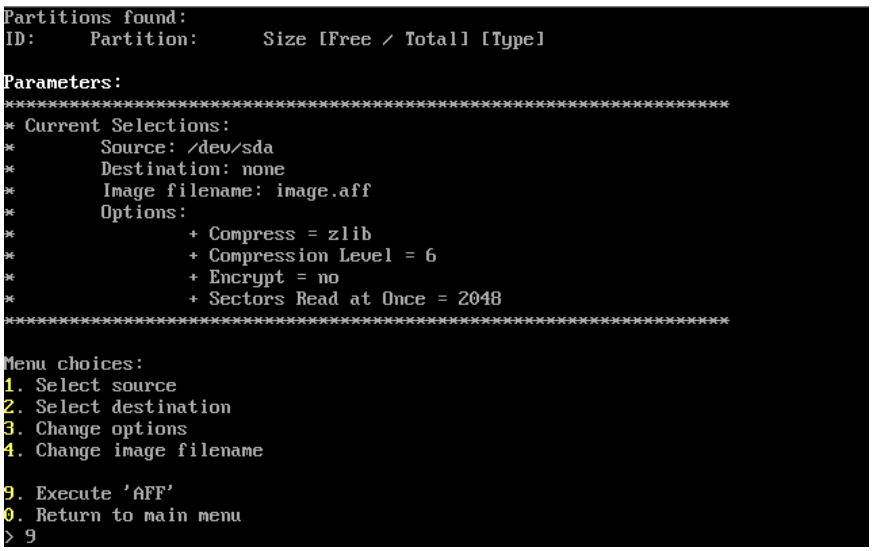


Choose the format in which you wish to store the disk/partition. The preferred format, as noted above, is AFF. Type '2' and press ENTER.

In some cases, the capture software may be unable to capture data in the preferred format. If this happens, return to this screen and choose the DD format [option 1].

3. Select Source

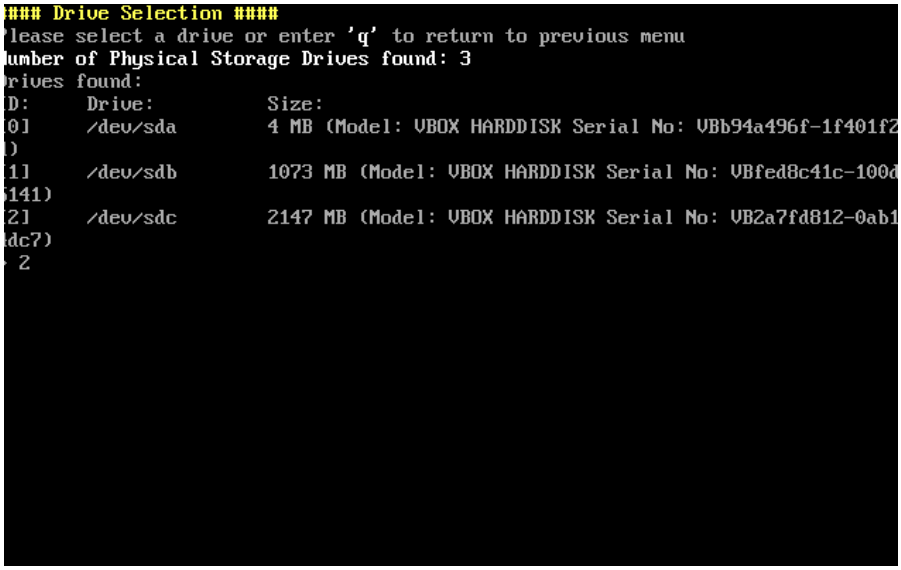
You will be presented with a new set of menus, as shown below.



Type '1' to select the source disk/partition that you wish to capture and press ENTER

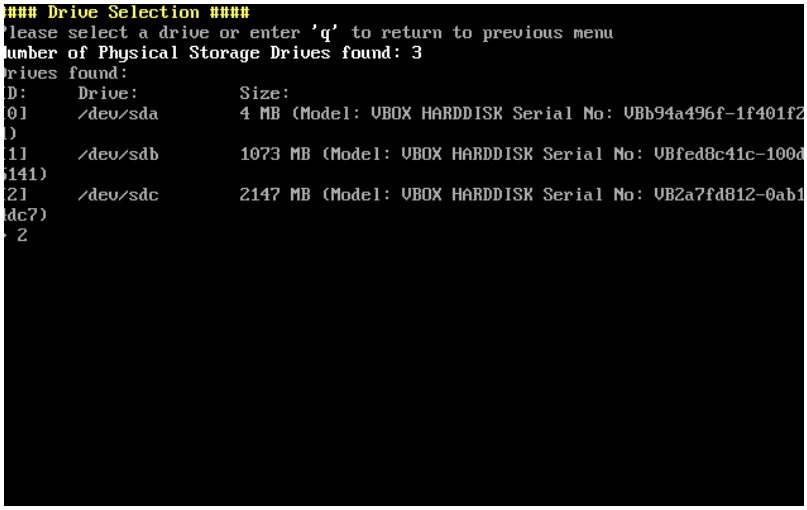
4. Drive Selection

Identify the drive or partition that you wish to capture and enter the associated number (0 indicates the first drive in the list, 1 is the second, 2 is the third, etc.). Press ENTER.



5. Select Destination

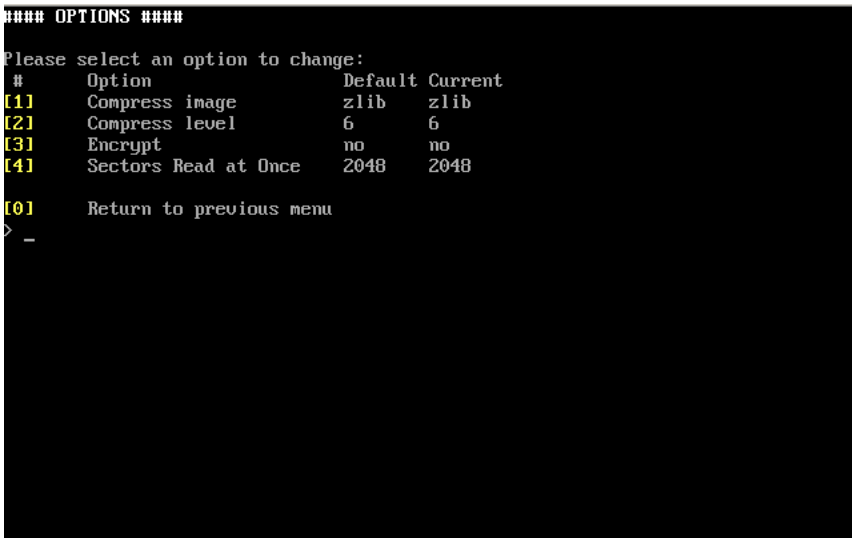
Type '2' and press ENTER to enter the 'Select Destination' menu. Choose the disk to which you wish to save the data and enter the appropriate number (0 indicates the first drive in the list, 1 is the second, 2 is the third, etc.). If you do not see the disk, ensure that it is connected and formatted correctly.



You will be returned to the main menu once you have chosen the destination where you will save the disk image.

6. Change Options

OSFClone is configured to compress the disk by default which, although saving disk space, will result in the imaging process taking significantly longer. To disable the option, choose '3' from the menu and press ENTER. You should be presented with the following screen.



- Type ‘1’ without quotes and press ENTER.
- You will be presented with three options: 'ZLib’, ‘LZMA’ (unavailable if you have less than 1GB memory) and 'none'. Choose ‘3’ (none) and press ENTER.

7. Execute

You should now be on the disk imaging menu, as shown below.

- Review the choices that you have made under the Parameters: Current Selections box.

- If you are satisfied with the options chosen in the previous stages, type ‘9’ and press ENTER to begin the data imaging process.

Note:
The speed at which the disk will be copied will vary, dependent upon the type and speed of the source media. Experimentation has found it takes an average of 3 – 3.30 minutes (180-240 seconds) to copy each gigabyte from a SATA disk over to a USB external drive when creating an AFF image, and an average of 1.30 - 2 minutes (90-120 seconds) for each gigabyte using DD.

If, for some reason, the disk is unable to capture the disk, return to the first menu (as shown in 1) and choose the option to create a ‘DD’ image.

References

Anon. 2010a. “AFF4: Advanced Forensics Framework 4“. ForensicsWiki. 3 November 2010. Accessed June 29, 2011: http://www.forensicswiki.org/wiki/AFF4

Anon. 2010b. “Encase Image File Format”. Forensics Wiki. 17 December 2010. Accessed June 29, 2011: http://www.forensicswiki.org/wiki/Encase_image_file_format

Anon. 2011. “DC3DD”. Forensic Wiki. 21 January 2011. Accessed June 29, 2011: http://www.forensicswiki.org/wiki/Dc3dd

Cohen, M. Garfinkel, S. Schatz, B. 2009. “Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow.” *Digital Investigation 6 (2009) S57–S68*. Accessed June 29, 2011: http://simson.net/clips/academic/2009.DFRWS.AFF4.pdf

Garfinkel, S.L., Malan, D.J. Dubec, K.A, Stevens, C.C. & Pham, C. 2006. “Advanced forensic format: An open, extensible format for disk imaging”. Advances *in Digital Forensics II: FIP International Conference on Digital Forensics*, National Center for Forensic Science, Orlando, Florida, January 29-February 1, 2006, ed. Martin Olivier and Sujeet Shenoi, 17-31. New York: Springer. Accessed June 29, 2011: http://nrs.harvard.edu/urn-3:HUL.InstRepos:2829932

Grobler, M. M. 2009. “Liforac - A Model For Live Forensic Acquisition”. University of Johannesburg. Accessed June 29, 2011: http://hdl.handle.net/10210/3438

Kirschenbaum, M.G., Ovenden, R. & Redwine, G. 2010. “Digital Forensics and Born-Digital Content in Cultural Heritage Collections”. *Council on Library and Information Resources*. Accessed June 29, 2011: http://mith.umd.edu/wp-content/uploads/whitepaper_borndigital.pdf

ioSafe. 2011. “What are the Main Types of Computer Backup?”. Accessed June 29, 2011: http://iosafe.com/blog/tips/types-of-computer-backups/

Jarocki. 2009. “Forensics 101: Acquiring an Image with FTK Imager”. SANS Computer Forensics. 18 June 2009. Accessed June 29, 2011: ttp://computer-forensics.sans.org/blog/2009/06/18/forensics-101-acquiring-an-image-with-ftk-imager/ for tutorial on usage

LapLink. 2010. “Demystifying The Disk Image”. Accessed June 29, 2011: http://blog.laplink.com/tag/forensic-imaging/

Rosen, A. 2002. "Expert Witness File Format Specification". ASR Data. April 7, 2002. Accessed June 29, 2011: http://www.forensicswiki.org/wiki/File:ASR_Data%27s_Expert_Witness_Compression_Format.pdf

Todd, M. 2009. “File Formats for Preservation”. *Digital Preservation Coalition Report*. 55. Accessed June 29, 2011: http://www.dpconline.org/component/docman/doc_download/375-file-formats-for-preservation