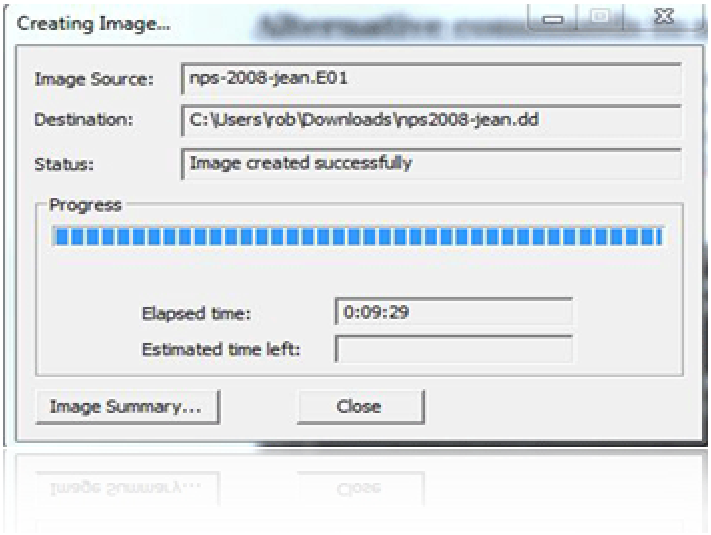
Contact Us (http://www.forensicsware.com/contact-us.html) Blog (http://www.forensicsware.com/blog.html) +1 801-895-4228

Search for a specific term

Home (http://www.forensicsware.com) » Blog (http://www.forensicsware.com/blog.html) »
E01 File Format

E01 (Encase Image File Format)

Encase Forensic is the most widely known and used forensic tool, that has been produced and launched by the Guidance Software Inc. Encase is embedded with a variety of forensic functions that include attributes such as disc imaging and preservation, absolute data recovery in the form of the bit stream, etc. In this series of humongous applications, when Encase is used for creating backup (i.e. Imaging) of hard drives, CD, USB drive, etc., a file known as "E01" is produced. This ".e01" extension file is primarily recognized as "Encase Image File Format". The E01 image file format is also known as EWF (an acronym for Expert Witness Format). The concept of the E01 encase image developed by the Encase software came into existence as a result of efficient efforts by the Guidance Software to assist forensic investigators, analysts, and forensic scientists in finding an organized and systematized data for investigation.



Creating Image...

Image Source: nps-2008-jean.E01

Destination: C:\Users\rob\Downloads\nps2008-jean.dd

Status: Image created successfully

Progress

Elapsed time: 0:09:29

Estimated time left:

What is E01 File ?

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 physical 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 the pause of 640 MB, multiple data files, storing crucial hard disk information, are created. The most peculiar feature of these files is that the name of the files remains the same (as named by the user) whereas the file extension changes.

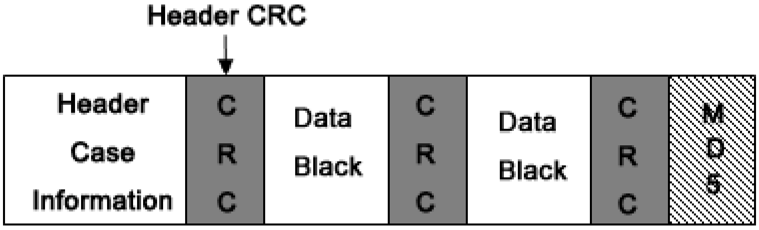
For example, if the very first chunk of 640 MB is created with the name "S01.E01", the next 640 MB chunks will be named as "S01.E02", followed by "S01.E03", "S01.E04", "S01.E05" and so on.

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.*

Structure of E01 File: -

The e01 image file format is prefixed with a "Case Info" header, After every block of 64 sectors i.e. 32 KB. It is interlaced 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, the user is required to enter these details into EnCase. This information includes: -



- Name of the Person (or the Investigator)
- Case Name (in relevance to the actual case)
- Description of media (the configuration, etc. of the hard disk from which the data are being collected)
- Date/time information (when the encase image file was done)
- 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.