



Reconstruction

- The purpose of having a reconstruction feature in a forensics tool is to re-create a suspect drive to show what happened during a crime or an incident.
- Another reason for duplicating a suspect drive is to create a copy for other computer investigators, who might need a fully functional copy of the drive so that they can perform their own acquisition, test, and analysis of the evidence.
- These are the sub functions of reconstruction:
 - Disk-to-disk copy
 - Image-to-disk copy
 - Partition-to-partition copy
 - Image-to-partition copy



....

- There are several ways to re-create an image of a suspect drive. Under ideal circumstances, the best and most reliable method is obtaining the same make and model drive as the suspect drive,
- If the suspect drive has been manufactured recently, locating an identical drive is fairly easy.
- A drive manufactured three months ago might be out of production and unavailable for sale, which makes locating identical older drives more difficult.



- The simplest method of duplicating a drive is using a tool that makes a direct disk-to-disk copy from the suspect drive to the target drive.
- One free tool is the **UNIX/Linux dd** command, but it has a major **disadvantage**:
- The target drive being written to must be identical to the original (suspect) drive, with the same cylinder, sector, and track count.



.....

- For a disk-to-disk copy, both hardware and software duplicators are available; hardware duplicators are the fastest way to copy data from one disk to another.
- Hardware duplicators, such as [Logicube Talon](#), [Logicube Forensic MD5](#), and [ImageMASter Solo III Forensics](#)
- Hard Drive Duplicator, adjust the target drive's geometry to match the suspect drive's cylinder, sectors, and tracks.



.....

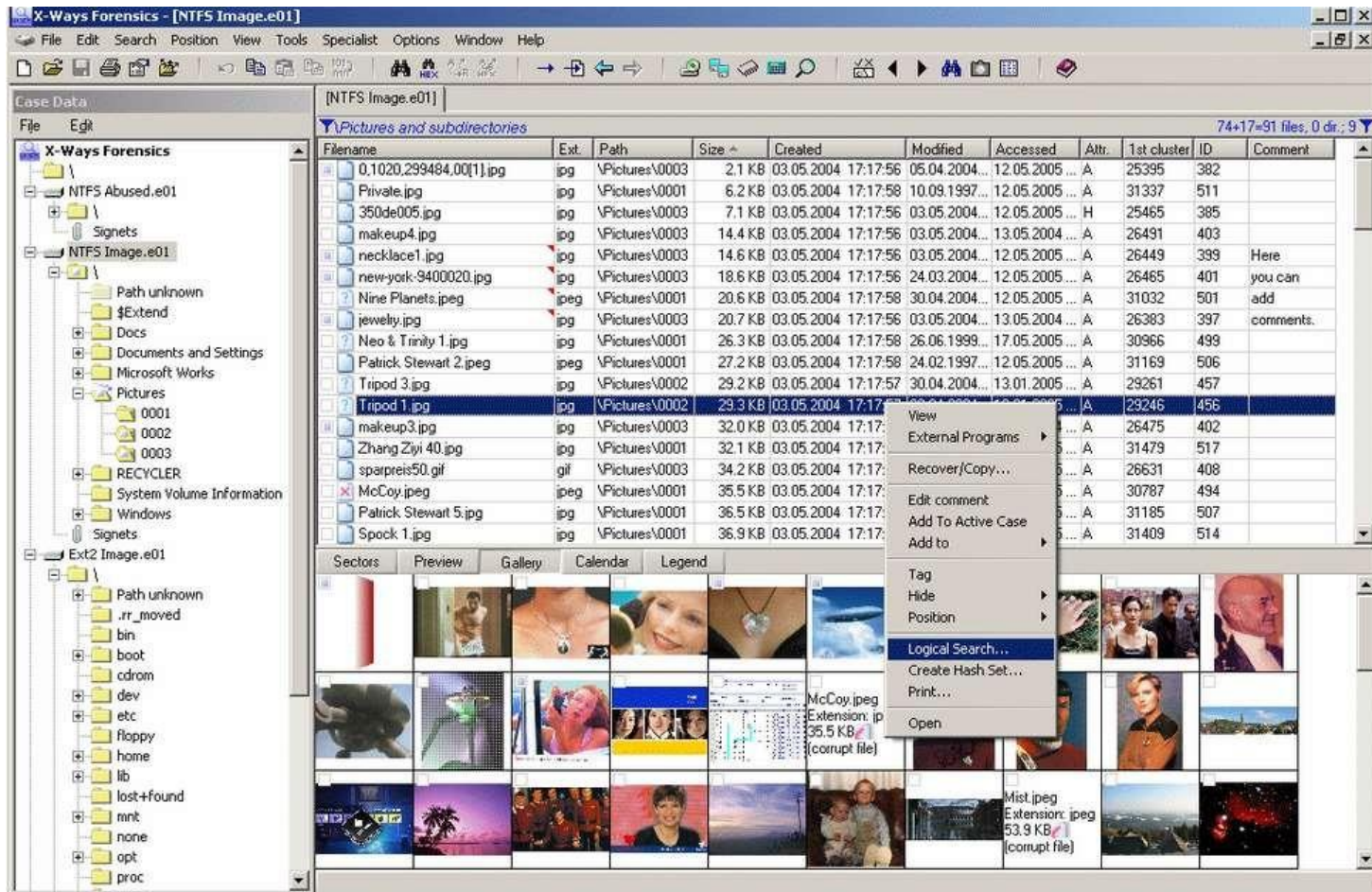
- For **image-to-disk** and image-to-partition copies, many more tools are available, but they are considerably slower in transferring data.
- The following are some tools that perform an image-to-disk copy:
 - SafeBack
 - SnapBack
 - EnCase
 - FTK Imager
 - ProDiscover
 - X-Ways Forensics



Pro discover



X-ways forensics



The screenshot displays the X-Ways Forensics interface for a file named [NTFS Image.e01]. The main window shows a list of files and directories within the image. A context menu is open over the file 'McCoy.jpeg', showing options like View, External Programs, Recover/Copy, Edit comment, Add To Active Case, Add to, Tag, Hide, Position, Logical Search, Create Hash Set, Print, and Open.

Filename	Ext.	Path	Size	Created	Modified	Accessed	Attr.	1st cluster	ID	Comment
0.1020.299484.00[1].jpg	jpg	\Pictures\0003	2.1 KB	03.05.2004 17:17:56	05.04.2004...	12.05.2005...	A	25395	382	
Private.jpg	jpg	\Pictures\0001	6.2 KB	03.05.2004 17:17:58	10.09.1997...	12.05.2005...	A	31337	511	
350de005.jpg	jpg	\Pictures\0003	7.1 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005...	H	25465	385	
makeup4.jpg	jpg	\Pictures\0003	14.4 KB	03.05.2004 17:17:56	03.05.2004...	13.05.2004...	A	26491	403	
necklace1.jpg	jpg	\Pictures\0003	14.6 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005...	A	26449	399	Here
new-york-9400020.jpg	jpg	\Pictures\0003	18.6 KB	03.05.2004 17:17:56	24.03.2004...	12.05.2005...	A	26465	401	you can
Nine Planets.jpeg	jpeg	\Pictures\0001	20.6 KB	03.05.2004 17:17:58	30.04.2004...	12.05.2005...	A	31032	501	add
jewelry.jpg	jpg	\Pictures\0003	20.7 KB	03.05.2004 17:17:56	03.05.2004...	13.05.2004...	A	26383	397	comments.
Neo & Trinity 1.jpg	jpg	\Pictures\0001	26.3 KB	03.05.2004 17:17:58	26.06.1999...	17.05.2005...	A	30966	499	
Patrick Stewart 2.jpeg	jpeg	\Pictures\0001	27.2 KB	03.05.2004 17:17:58	24.02.1997...	12.05.2005...	A	31169	506	
Tripod 3.jpg	jpg	\Pictures\0002	29.2 KB	03.05.2004 17:17:57	30.04.2004...	13.01.2005...	A	29261	457	
Tripod 1.jpg	jpg	\Pictures\0002	29.3 KB	03.05.2004 17:17:57	30.04.2004...	13.01.2005...	A	29246	456	
makeup3.jpg	jpg	\Pictures\0003	32.0 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005...	A	26475	402	
Zhang Ziyi 40.jpg	jpg	\Pictures\0001	32.1 KB	03.05.2004 17:17:58	03.05.2004...	12.05.2005...	A	31479	517	
sarpreis50.gif	gif	\Pictures\0003	34.2 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005...	A	26631	408	
McCoy.jpeg	jpeg	\Pictures\0001	35.5 KB	03.05.2004 17:17:58	03.05.2004...	12.05.2005...	A	30787	494	
Patrick Stewart 5.jpg	jpg	\Pictures\0001	36.5 KB	03.05.2004 17:17:58	03.05.2004...	12.05.2005...	A	31185	507	
Spock 1.jpg	jpg	\Pictures\0001	36.9 KB	03.05.2004 17:17:58	03.05.2004...	12.05.2005...	A	31409	514	



X-ways forensics

- Superior, fast disk imaging with intelligent compression options
- Ability to read and write .e01 evidence files (a.k.a. EnCase images), optionally with real encryption (256-bit AES, i.e. not mere "password protection")
- Ability to create skeleton images, cleansed images, and snippet images ([details](#))
- Ability to copy relevant files to [evidence file containers](#), where they retain almost all their original file system metadata, as a means to selectively acquire data in the first place or to exchange selected files with investigators, prosecution, lawyers, etc.
- Complete case management.
- Ability to tag files and add notable files to the case report. Ability to enter comments about files for inclusion in the report or for filtering.
- Support for multiple examiners in cases, where X-Ways Forensics distinguishes between different users based on their Windows accounts. Users may work with the same case at different times or at the same time and keep their results (search hits, comments, report table associations, tagmarks, viewed files, excluded files, attached files) separate, or shares them if desired.
- Case reports can be imported and further processed by any other application that understands HTML, such as MS Word
- CSS (cascading style sheets) supported for case report format definitions
- Automated activity logging (audit logs)
- Write protection to ensure data authenticity
- Keeps you posted about the progress of automatic processing via a drive on the same network or via e-mail while you are not at your workplace
- Remote analysis capability for drives in network can be added optionally ([details](#))
- Additional support for the filesystems HFS, HFS+/HFSJ/HFSX, ReiserFS, Reiser4, XFS, many variants of UFS1 and UFS2
- Ability to include files from all volume shadow copies in the analysis (but exclude duplicates), filter for such files, find the snapshot properties, etc.
- Often finds much more traces of deleting files than competing programs, thanks to superior analysis of file system data structures, including \$LogFile in NTFS, .journal in Ext3/Ext4
- The basis for a listed file is practically just a mouse click away. Easily navigate to the file system data structure where it is defined, e.g. FILE record, index record, \$LogFile, volume shadow copy, FAT directory entry, Ext* inode, containing file if embedded etc.
- Supported partitioning types: MBR, GPT (GUID partitioning), Apple, Windows dynamic disks (both MBR and GPT style), LVM2 (both MBR and GPT style), and unpartitioned (Superfloppy)
- Very powerful main memory analysis for local RAM or memory dumps of Windows 2000, XP, Vista, 2003 Server, 2008 Server,