





- 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 ImageMASSter 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 imageto-disk copy:
- SafeBack
- SnapBack
- EnCase
- FTK Imager
- ProDiscover
- X-Ways Forensics





Pro discover

ile Action View Tools Help
Project Report Add Remove Content View Images Disks Registry View EventLog View Search Search Results Content Search Results Content Search Results Content Search Results Content Activity Search Theremet Activity Search Donk show this dalog in the future Dent cancel Help

19SB502 /Cyber Forensics /Unit 2/ RAJKUMAR.K.K / AP/ ECE / SNSCE





FTk imager

Ele View Mode Help 🕼 🚳 🗣 📣 🍘 🖓 🖬 🖬 🕼 🚙 🚙 📟 🔞 🍕 🗋 🗃 🗐	86	100 100 8	
vidence Tree	×	File List	
		Name SBoot SI30 SLogFile	Size Type Date Modified 8 Regular File 27-11-2012 8:5 23 NUTCH dex All 20-2-2014 7:16: File 27-11-2012 8:5
		SMFT SMFTMirr	4 Regular File 27-11-2012 8:5 1 Regular File 27-11-2012 8:5 2 Participant File 27-11-2012 8:5
Config.Mai C		00000090 00 00 0 000000a0 00 00 1 000000b0 05 00 0 000000c0 48 04 9	00 38 00 01 00 <td< td=""></td<>
Hex Value Interpreter	×		2 67 7C CC CD 01-00 40 00 00 00 00 00 00 00 K··g¦ÍÍ··@····· 0 00 00 00 00 00-06 00 00 00 00 00 00 00 00 00 00 00 00 0
Type Size Value signed integer 1-8 unsigned integer 1-8 FILETIME (UTC) 8 DOS date 2 DOS time 2 time_t (UTC) 4 Hex Value Interpreter	1	0000100 80 00 0 0000110 00 00 0 0000120 40 00 0 0000130 00 04 40 0000140 32 C0 2 0000140 32 C0 2 0000160 C8 00 9 0000160 11 00 44 00000170 17 00 0 0000160 01 00 80 0 0000100 87 FF FF 00000100 FF FF F	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$

19SB502 /Cyber Forensics /Unit 2/ RAJKUMAR.K.K / AP/ ECE / SNSCE





X-ways forensics

se Data	[NTFS Image.e01]											
File Edit	ThPictures and subdirectories 74+17=91 files, 0 dr.; 9 T											
	Filename	Ext	Path	Size +	Created	Modified	Accessed	Attr.	1st cluster	and a first state of the local division of t	Comment	
- <u>Čii \</u>	0.1020,299484,00(1).jpg	ipg	\Pictures\0003		03.05.2004 17:17:56				25395	382		_
MTFS Abused.e01	Private.jpg	ipg	\Pictures\0001		03.05.2004 17:17:58				31337	511		_
ф <u>ф</u> /	350de005.jpg	ipg	\Pictures\0003		03.05.2004 17:17:56		1		25465	385		
Gignets	🗆 🧾 makeup4.jpg	ipg	\Pictures\0003		03.05.2004 17:17:56				26491	403		
NTFS Image.e01	💷 🛄 necklace1.jpg	ipg	\Pictures\0003		03.05.2004 17:17:56	for the second second second	and a state of the		26449	1676 101	lere	
P 🙆 \	💷 🔄 new-yark-9400020.jpg	ipg	\Pictures\0003		03.05.2004 17:17:56				26465		ou can	
	I III III Nine Planets.jpeg				03.05.2004 17:17:58				31032	22.01	dd	
Docs	ieweliy.jpg	ipg	\Pictures\0003		03.05.2004 17:17:56				26383		omments.	
Documents and Settings	Neo & Trinity 1.jpg	ipg	\Pictures\0001		03.05.2004 17:17:58				30966	499		
Microsoft Works	Patrick Stewart 2.jpeg	ipeg	\Pictures\0001		03.05.2004 17:17:58				31169	506		
Pictures	Tripod 3.jpg	ipg	\Pictures\0002		03.05.2004 17:17:57	30.04.2004	13.01.2005	A	29261	457		
0001	C 7 Tripod 1.jpg	ipg	Pictures\0002	An entry of the second second	03.05.2004 17:17	View	1	A	and the design of the local division of the	456		
	💷 📄 makeup3.jpg	ipg	\Pictures\0003	32.0 KB	03.05.2004 17:17:	External Proc	warme +	A	26475	402		
	🗆 🔄 Zhang Ziyi 40.jpg	ipg	\Pictures\0001	32.1 KB	03.05.2004 17:17:	Excernaring	i and	A	31479	517		
E- RECYCLER	🗆 🧾 sparpreis50.gif	gif	\Pictures\0003	34.2 KB	03.05.2004 17:17:	Recover/Cop	iy þ	A	26631	408		
- System Volume Information	McCoy.jpeg	ipeg	\Pictures\0001	35.5 KB	03.05.2004 17:17:	Edit comment	. 1	A	30787	494		
😟 🚞 Windows	Patrick Stewart 5.jpg	ipg	\Pictures\0001	36.5 KB	03.05.2004 17:17:	Add To Activ		A	31185	507		
- 🗍 Signets	🗆 📄 Spock 1.jpg	ipg	\Pictures\0001	36,9 KB	03.05.2004 17:17:	Add to	o caso	A	31409	514		
Ext2 Image.e01	Sectors Preview Gallen	C.	alendar Lege	nd		MOGICO						-
			annua cogo		101	Tag		17	1	1000	-	-
🗉 🚞 Path unknown		- 10	- alle	No.		Hide		-	AR	a Comercia	2t	
.rr_moved		Sur			Contraction of the local division of the loc	Position		12	Construction of the		A	
bin		*	-	A CON		Logical Searc	5				12	
🗈 🛄 boot				-		Create Hash		1				
cdrom		a.		Dear		Print	Joten		()			
🕀 📃 dev 🚽		180			McCoy.jpeg	PERRAN					_	
E etc					Extension: jp	Open			ales.	the state		
		1200		110	(corrupt file)	100 M			4.7	1.000	(Participation)	
🕀 🦲 home 🕀 🛄 lib	I send the	and the second second		paret.	74.54	10.0	N N		REAL PROPERTY		_	
lest+found			AL	and stationers where	-		t dist in s -		-	No. of Concession, Name		
e		The second				No mail	Mist.jpeg Extension:	ipeq	-			
none		1 Mary		Section -		Contraction of the local division of the loc	53.9 KB	1999 B	and the set	1.5		
Inone		10 I.S.		1	UNITE OF THE OWNER		[corrupt file		100 40	-		

19SB502 /Cyber Forensics /Unit 2/ RAJKUMAR.K.K / AP/ ECE / SNSCE





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 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,