

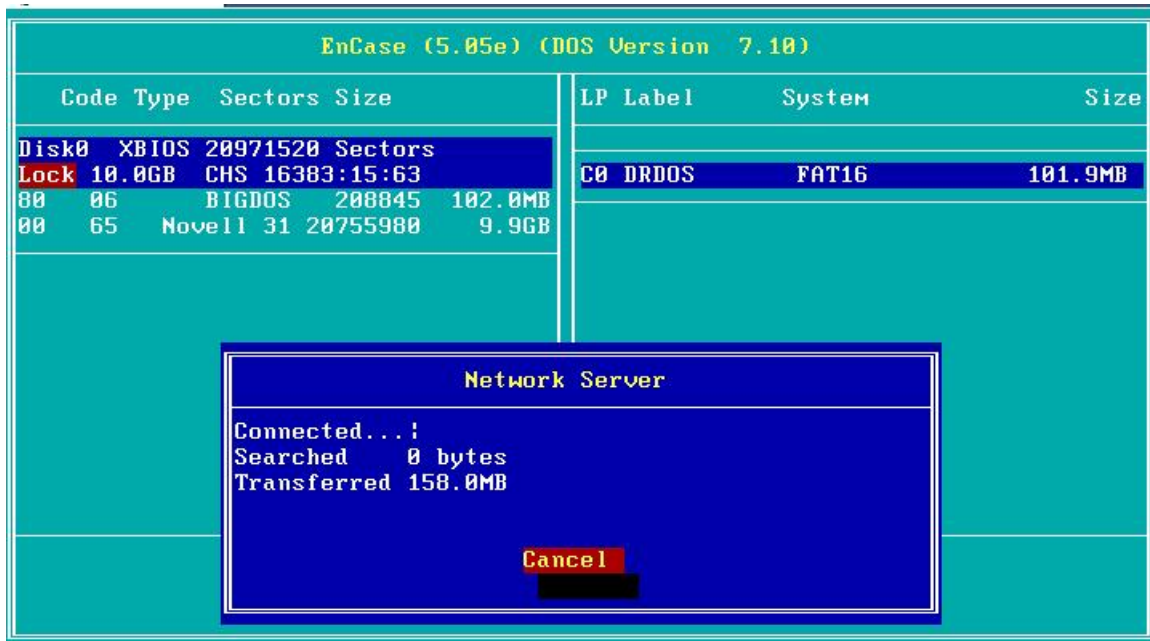
Novell Netware Advanced Investigation Challenges

Introduction

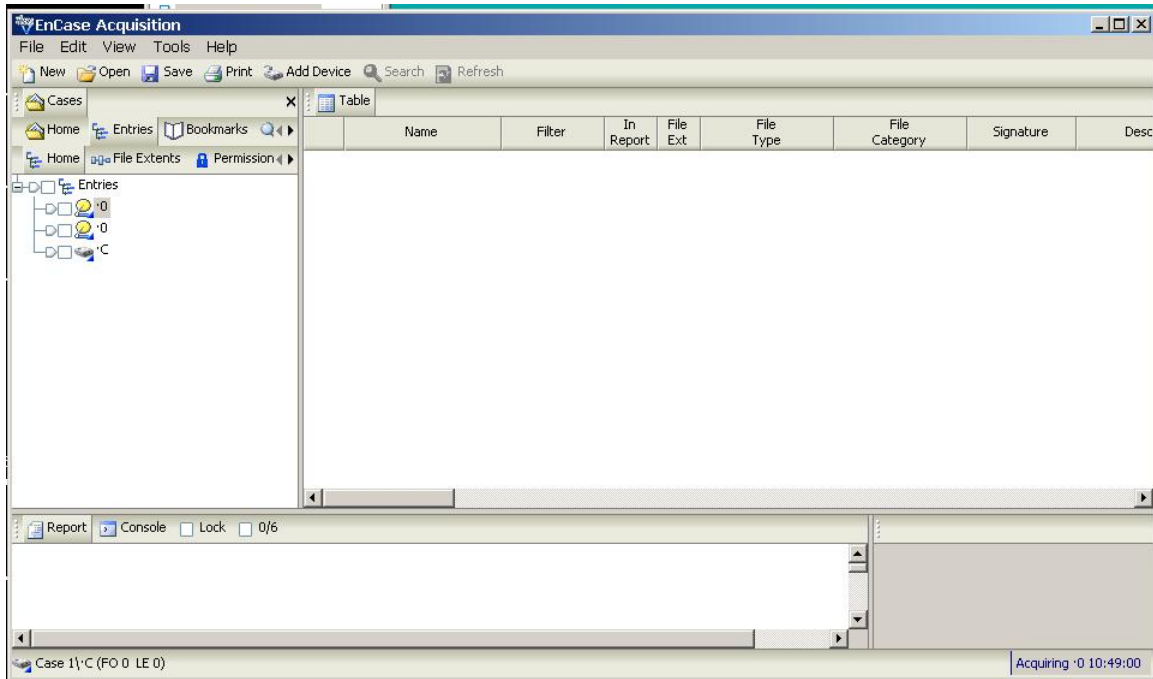
This paper will introduce users to the challenges and problems associated with advanced forensics investigations on Novell Netware servers and will acquaint users with the need for a greater understanding in the industry on the Novell Netware platform. During the research portion of this article several different tactics and forensics programs were tested in an attempt to provide some type of advanced investigation catalyst for Novell Netware.

Encase 5

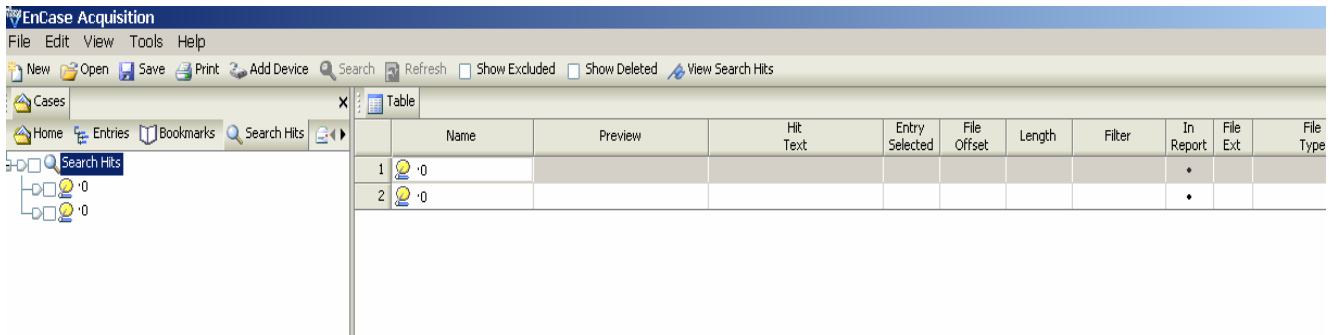
All of encases features and advertisements indicated that support for Novell maybe possible, and during the acquisition of the file from the DOS bootable version of encase, the program did indeed show the format of the Netware partition as NETWARE31, indicating some native support for the Netware file system, however when imported into the encase 5 program there was no way of browsing through the files located on the server, therefore unable to complete the investigation.



Encase Acquiring the Netware Image from DOS bootable disk



Drives Imported into Encase



Search Box is grayed, no file listing

Upon further investigation it is discovered that Novell file systems are not supported on encase

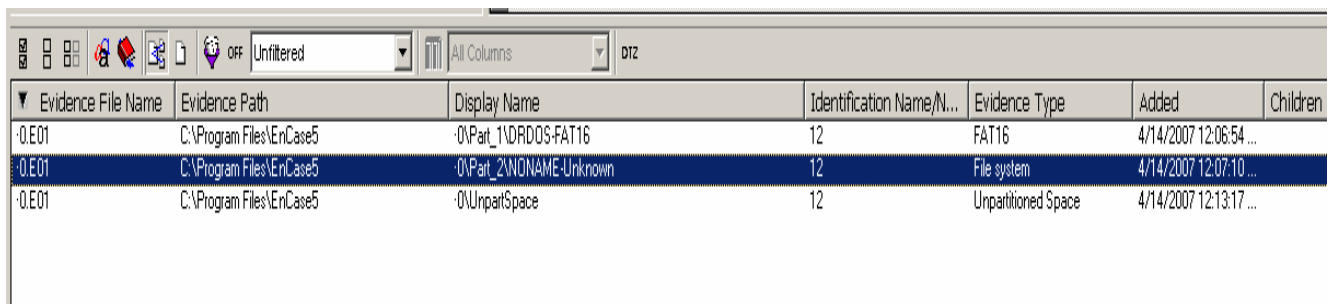
EnCase Virtual File System*

- ◆ Mounts evidence at the cases, case, device, volume, or folder level as a read-only network share. (It appears as a network share to the local operating system but the share is not available to other users over the network).
- ◆ VFS provides an easy platform for information or evidence review in a read-only state outside of the EnCase environment.
- ◆ Provides an intuitive platform for evidence to be reviewed by case agents/investigators, opposition experts, prosecutors and defense counsel.
- ◆ Files contain the same file system artifacts as contained in EnCase, including all allocated files, deleted files, internal system files as well as alternate data streams and unallocated space.
- ◆ Once mounted, the read-only media is available to any native application, including Windows Explorer and third-party Windows applications or computer forensic tools such as file carving utilities, virus checkers, spyware detectors, trojan detectors, steganography detectors, word indexers, undelete software and encryption detection software.
- ◆ Review evidence with non-EnCase users.
- ◆ File Systems supported: DOS (FAT 12/16/32, NTFS), Linux (EXT2, EXT3, Reiser), UNIX (Solaris UFS), Macintosh (HFS, HFS+), BSD (FFS), CD/DVD (Joliet, ISO 9660, UDF, DVD) and Palm (Palm OS).
- ◆ Easily mounts Windows RAIDS, Dynamics Disks rebuilt by EnCase and drives compressed or encrypted by NTFS.

Netware Not Supported

FTK: Forensics Toolkit

FTK (the latest version at the time of this publication 1.70.1) fared slightly better than the encase system when presented with the same image, the ftk program recognized both partitions the first being the DOS bootable partition the second being the Netware file system



The screenshot shows the FTK interface with a table of evidence partitions. The table has columns for Evidence File Name, Evidence Path, Display Name, Identification Name/N..., Evidence Type, Added, and Children. The data is as follows:

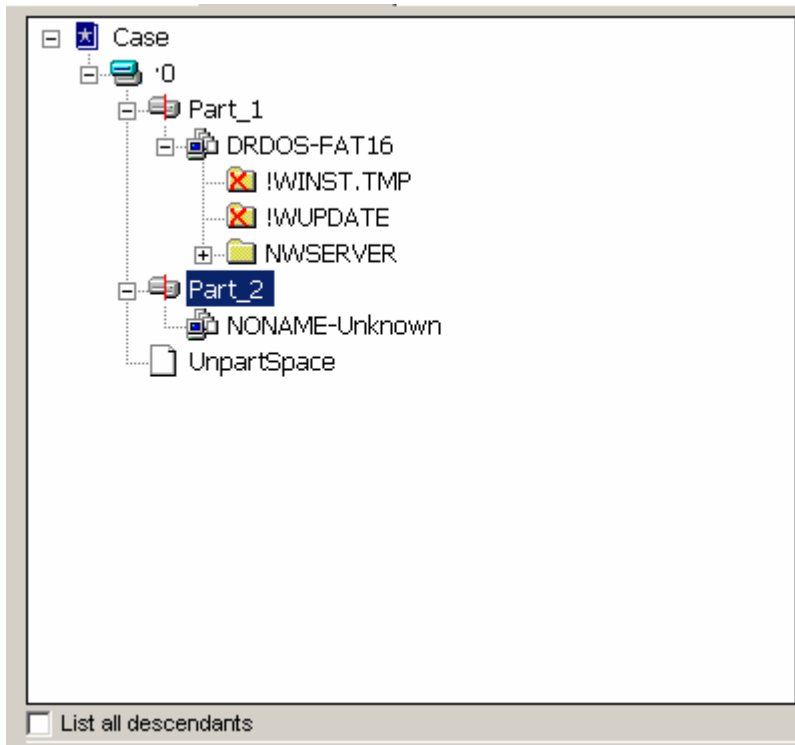
Evidence File Name	Evidence Path	Display Name	Identification Name/N...	Evidence Type	Added	Children
0.E01	C:\Program Files\Encase5	0\Part_1\DRDOS-FAT16	12	FAT16	4/14/2007 12:06:54 ...	
0.E01	C:\Program Files\Encase5	0\Part_2\NDNAME-Unknown	12	File system	4/14/2007 12:07:10 ...	
0.E01	C:\Program Files\Encase5	0\UnpartSpace	12	Unpartitioned Space	4/14/2007 12:13:17 ...	

Evidence Partition summary in FTK

The FTK program then scanned the image for questionable files

Evidence Items		File Status		File Category	
Evidence Items:	3	KFF Alert Files:	0	Documents:	23
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	1069	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	0
Unchecked Items:	1069	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	154	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	3
Filtered In:	1069	Duplicate Items:	40	Archives:	0
Filtered Out:	0	OLE Subitems:	0	Folders:	8
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	421
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	614

However it quickly became apparent that FTK would not be scanning the Novell partition, and was only scanning the bootable C Drive of the system



FTK Explore Dialog, indicating the “unknown” Network file system

Both of the main forensics suites (encase and FTK) were unable to properly investigate a Netware image, therefore it is necessary to use certified Novell programs like the filer and on track to properly investigate the server, although FTK did properly identify and catalog the operating system partition of the server, this is of little use as this partition isn't directly accessible to the Netware users.