

Filesystem Review

Once a snapshot of the running system has been obtained, the next logical step is to review the files and folders for potential evidence of compromise. While this could be performed using the Windows Explorer, the responder risks altering last accessed dates and times, in addition the possibility of inadvertent data tampering. However, using Nigilant32 the responder can review the contents of the filesystem safely and without concern of data tampering.

Using the preview drive tool within Nigilant32 a first responder can gather information from multiple sources within the active system, including:

- Partition Table
- Hidden Files, Folders
- System Files, Folders
- Allocated and Unallocated Files, Folders

It is for this reason that we developed Nigilant32.

Nigilant32 is an incident response tool designed to capture as much information as possible from a running system with the smallest potential impact. Nigilant32 has been developed with Windows 2000, XP, and 2003 in mind, and should work fine with computers running one of those operating systems.

Using Nigilant32 we can explore the file system and possibly locate hidden files or folders, recently deleted content, or extract files for offline analysis without risk of contamination.

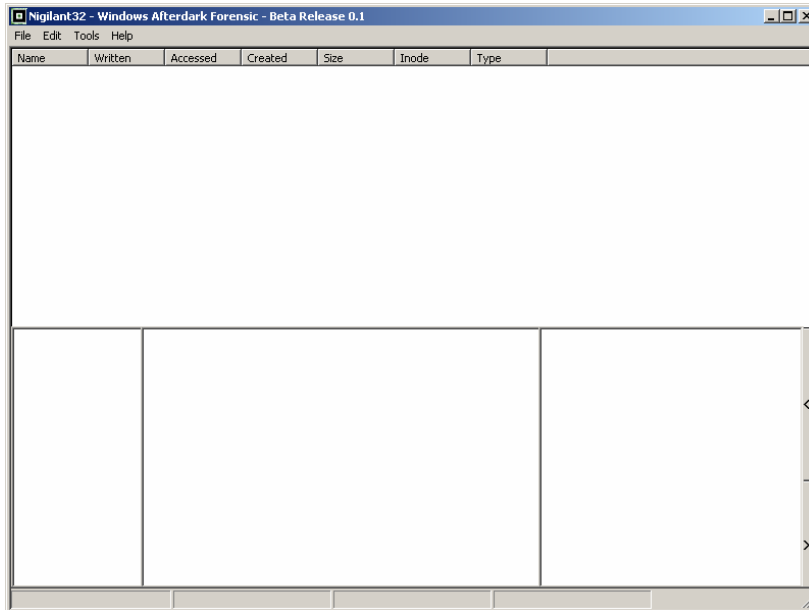
Let's look at an example.



The Nigilant32 main console

This article is the second in a series of publications developed to assist the first responder in understanding the many uses of Nigilant32 <n-eye-jill-ant32> in an incident response capacity. In this article we cover using Nigilant32's filesystem analysis engine to review the hard drive in a safe manner.

Nigilant32 was developed by Agile Risk Management LLC, the most recent and update to date version can always be found at www.agilem.net.

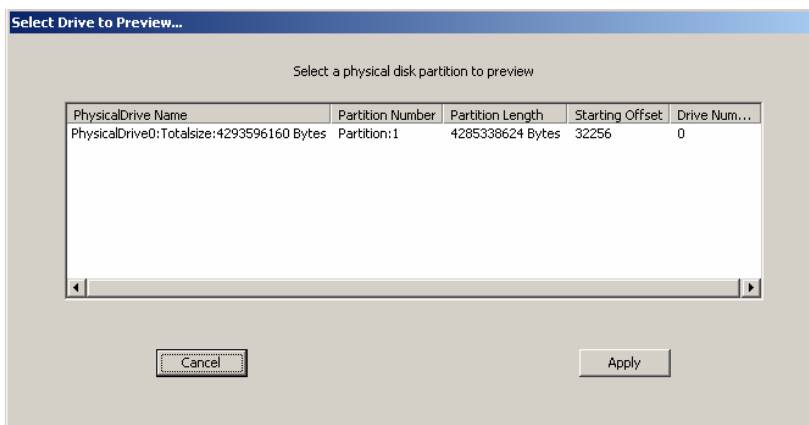


In order to review the active filesystem, let's look at the File Menu.



The Preview Disk... option uses code from the Sleuthkit project to explore the active filesystem. This was done to remove any potential modifications or disruptions the native Win32 API could create.

Let's review the output of the Preview Disk... command.



The Sleuthkit Project is maintained and actively developed by Brian Carrier. For more information on Sleuthkit visit www.sleuthkit.org.






The first step is to select the partition you wish to review, currently Nigilant32 can review NTFS and FAT32/16 partitions.

Provided the partition can be accessed and read by Nigilant32, the following filesystem information is presented:

Name	Written	Accessed	Created	Size	Inode	Type
\$AttrDef	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	2560	4	0
\$BadClus	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	4285337600	8	0
\$Bitmap	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	130784	6	0
\$Boot	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	8192	7	0
\$Extend	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	344	11	1
\$LogFile	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	23527424	2	0
\$MFT	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	13292544	0	0
\$MFTMirr	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	4096	1	0
\$Secure	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	286376	9	0
\$UpCase	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	131072	10	0
\$Volume	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	Fri Jan 20 04:15:19 2006	0	3	0
	Fri Jan 20 13:10:38 2006	Fri Mar 10 16:19:46 2006	Fri Jan 20 13:10:38 2006	4152	5	1
arcdrr.exe	Thu Jun 19 15:05:04 2003	Fri Jan 20 09:50:17 2006	Fri Jan 20 09:50:17 2006	150528	2919	0
arcsetup.exe	Thu Jun 19 15:05:04 2003	Fri Jan 20 09:50:17 2006	Fri Jan 20 09:50:17 2006	163840	2920	0
AUTOEXEC.BAT	Fri Jan 20 09:32:14 2006	Fri Jan 20 09:32:14 2006	Fri Jan 20 09:32:56 2006	0	7015	0

Nigilant32's filesystem navigation console provides information about each item, including Name, Last Write Date/Time, Last Accessed Date/Time, Last Create Date/Time, Size, Inode, and Type (Folder/File).

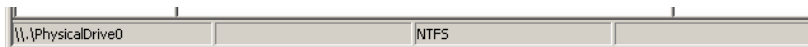
In addition, the icons next to each indicate its state. Use the following legend to understand the item's meaning:

-  Allocated (Active) File
-  Un-Allocated (Deleted) Folder
-  Allocated Folder
-  Un-Allocated (Deleted) File
-  Unavailable Unallocated File or Folder

Selecting an unavailable unallocated file or folder will display the \$MFT table on an NTFS filesystem.

Next you will notice In our example we reviewed an NTFS partition, therefore you will see the NTFS metadata files (\$Secure, \$MFT, etc).

Also you will note in the status bar at the bottom of the window we provide the drive currently being reviewed (“\\.\PhysicalDrive0”) as well as the filesystem format (“NTFS”).

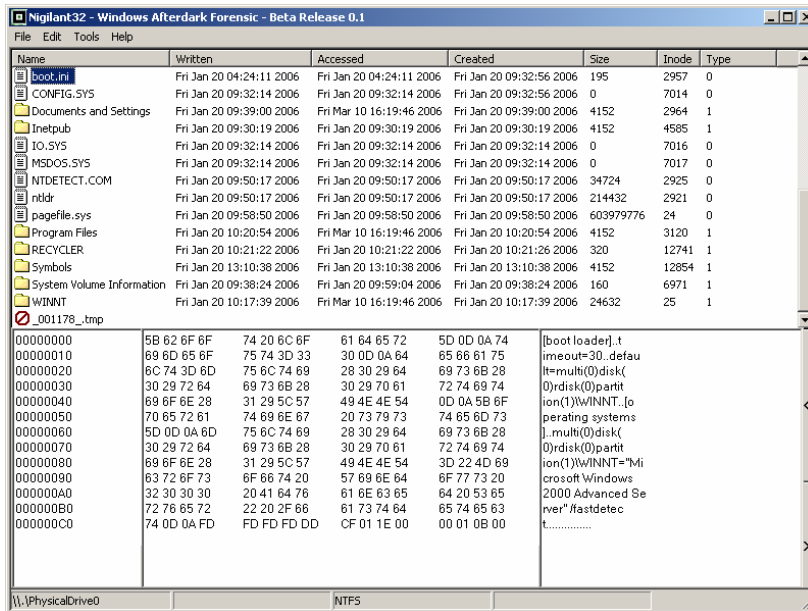


Double clicking on a folder will display the contents of the folder, double clicking on a file will populate the file contents display panels below.

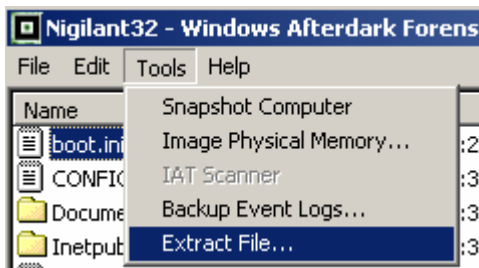
Each display panel provides different information from the selected file. The first panel shows the hexadecimal offset for each line in the file. The second panel shows the contents of the file in hexadecimal format. The third and final panel shows the contents of the file in ASCII format.

All three panels are linked to the scroll bar directly next to the third panel, use that scroll bar to navigate the contents.

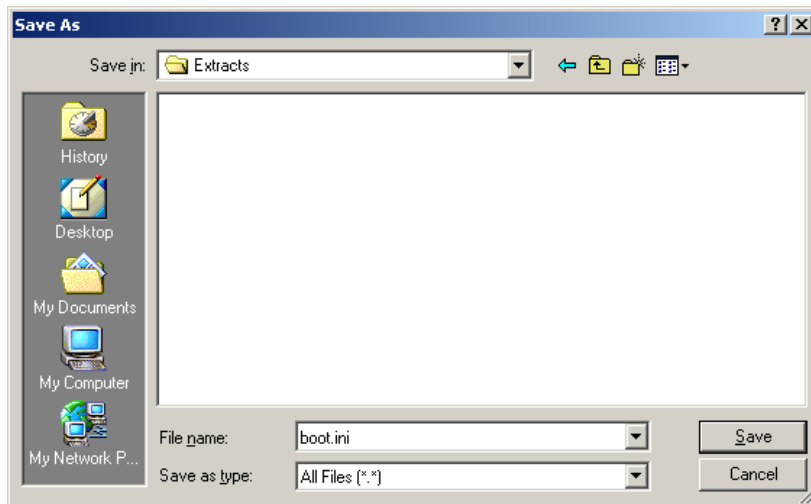
In addition, the display panel contents have been limited so as not to consume additional memory. Therefore in order to navigate beyond 512k in a given file you must use the Page Up < and Page Down > buttons to the right of the scroll bar.



Once a file of interest has been selected, it can be easily extracted to an external disk using the Tools-> Extract File... option.



The extract file option will allow you to select the location and name of the file being extracted.



Always remember to extract file content to a disk other than the disk being reviewed, such as a portable USB drive or network share.

Matthew Shannon has over seven years of professional experience in private industry, including KPMG LLP, ExxonMobil, and United Technologies. Mr. Shannon has successfully led multiple information security assessment engagements, including successful penetration of multi-million dollar financial institutions, both international and domestic. In addition, Mr. Shannon has been the lead investigator on numerous computer forensics engagements, including intellectual property theft and employment law. Mr. Shannon is also a well received speaker and author. He has instructed the United States Secret Service on specific digital forensics techniques and was a well received speaker at the DEFCON 11 annual Information Security conference in Las Vegas Nevada. Additionally, Mr. Shannon has been published in the International Journal of Digital Evidence for his work on incorporating statistical inference into digital forensics investigations as well as multiple bar journal articles and online digital forensics publications.

Mr. Shannon graduated cum laude from The University of Florida in Decision and Information Sciences (BSBA) in 1999. He is a member in good standing of ISSA, in addition, Matthew holds numerous professional information technology certifications, and is the developer of Nigilant32, Agile Risk Management LLC's Incident Response Tool.

Matthew M. Shannon CIFI,
CISSP
Principal
Agile Risk Management LLC
mshannon@agilem.net