

THE FARMER'S BOOT CD

Preview Data in Under Twenty Minutes

On January 1, 2006, THE FARMER'S BOOT CD, or FBCD for short, was officially released to the general public. A year in the making, FBCD is the result of my desire to preview data quickly, in a forensically sound manner. I was frustrated in the then currently available programs as I didn't feel any lent themselves to quickly previewing data. It seemed all were designed to acquire and analyze data. So while they could be used to preview data, they weren't all that fast, they were a bit cumbersome, and they offered too much for a quick preview. So I set out to develop a tool which would allow anyone capable of following a few simple steps and some basic computer skills the ability to preview data stored on file systems. In a forensically sound manner, of course.

Behind all of this I had two driving forces for a preview tool. First, within the United States it seemed more and more legalities were coming into play. Scope of investigation, multi-user systems, privacy laws and coming initiatives. Each of these kept me thinking "It's going to be a great idea to perform a quick preview before blindly acquiring any system". Use a tool to preview the data first. If data pertinent to the case is found then switch to acquisition mode. If not, don't spend the time and use the hardware resources necessary to acquire. The second driving force is the sheer size of data found on-site. Acquiring a few hundred gigabytes takes time. If you could spend 20 minutes previewing first, and if this led to the decision not to acquire, then wouldn't the time savings of not acquiring the few hundred gigabytes have value to you?

As I thought of these two forces I became aware of more reasons why a preview tool might prove valuable. One, you could use the tool as a service feeder. What I mean by this is that for a fee you could show the client in a preview mode data pertinent to their interest(s). Many times once the client sees that data they are more eager to commit to the full acquisition and analysis services. A second reason for a preview tool is one more closer to my work. Almost gone are the days that pertinent data resides solely on a single file system. Thumbdrives, external hard drives, network shares, etc., all are potential targets for storing pertinent data in a case. If you could use a tool to quickly preview the target system and identify external storage devices during this preview, then your next action might be to locate those resources and attempt to preview and/or acquire them as well. Because if you leave the site without that data you might find during your full blown analysis you missed potential data. You can identify recently mounted volumes, or file systems, in your preview and I strongly believe you should do this when you are on-site.

Ultimately I decided to develop a tool that would answer all of my questions and provide the user with capability to preview in a forensically sound manner. I knew Linux could be used, but I also knew that most users would prefer to point-and-click within a single program window versus typing in any number of commands and cycling through many different program windows. Linux would be my platform of choice because Linux supports many file system types, partitioning schemas, and hardware devices. A Linux bootable CD would allow me to boot most any x86 system or attach most any device to my system so that I could preview the data and then also acquire if the result of my preview was that the acquisition process should proceed.

THE FARMER'S BOOT CD is a Linux bootable CD that has been designed and optimized for previewing data. Every included application has been configured in such a manner that provides access to all data that may be pertinent to a forensic practitioner. However, this is balanced with another goal of my CD, and that is in making the ISO as small as possible and minimizing

Copyright ©2006 Thomas Rude All Rights Reserved. Reproduction, redistribution or public display, in whole or in part, of this document is prohibited without first receiving express written consent from the copyright holder.

memory consumption. Previewing a computer most typically means dropping the CD into the suspect system and booting it after you've taken steps to make certain the system boots from the CD before any other device. Anytime you preview you are constrained by a few items. One is memory. How much RAM does the system have?

I've configured applications on FBCD so that their memory consumption is as little as possible. Translation – very little caching takes place. When you compare FBCD to other Linux bootable CDs you will find graphics viewers on those CDs do in fact cache the thumbnails of rendered graphics files. The perceived good is that moving between directories gives you instant access to the thumbnails, as they are cached. The negative effect of caching is the consumption of valuable memory. The thumbnails are stored in memory. How many hundreds or thousands of graphics files are found on a typical user's system? They chew up memory like nobody's business! Running out of memory or slowing the system to a crawl is no fun. The included graphics viewer on FBCD does not cache thumbnails in order to conserve memory consumption. It takes a lot longer to reboot a locked system out of memory than it does to render graphics in the current directory you're viewing.

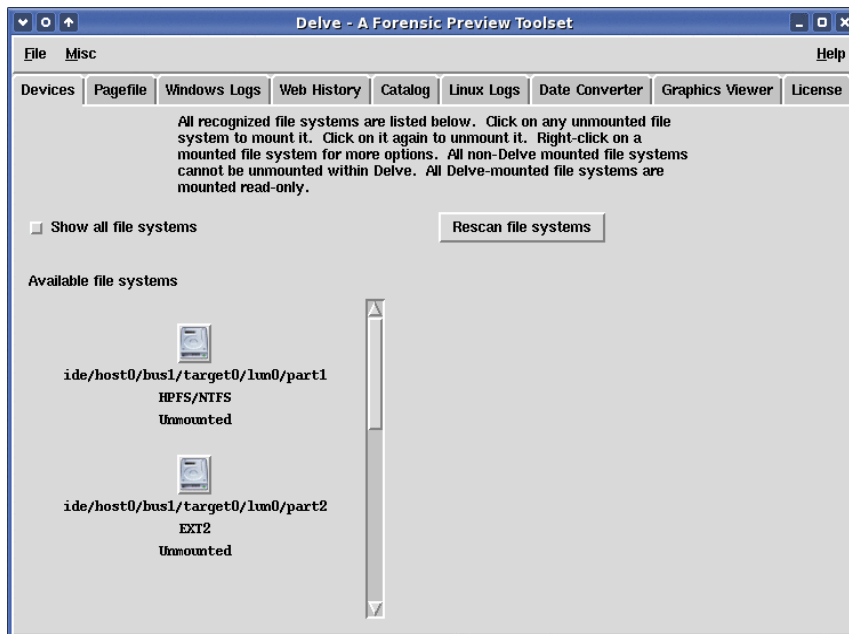
I am often asked what separates THE FARMER'S BOOT CD from other Linux bootable CDs. Many times this is asked because FBCD is a commercial product, not a freebie. Other times people are just curious as to why they should spend the time working with and learning a new CD environment. Time is valuable. What is the return on investment in FBCD?

THE FARMER'S BOOT CD is different than most other Linux boot CDs in a number of both visible and invisible to the user ways. First, every application has been configured and tested to benefit the forensic practitioner previewing data. Second, the very stable and fast 2.4 Linux kernel is used and configured for the widest range of support for hardware, protocols, and file systems in the most common of scenarios. Third, device recognition and hotplugging is fast and quite accurate so that the user doesn't spend too much time identifying devices and troubleshooting. Fourth, included is a program that provides a simple and easy-to-use graphical user interface that provides quick and safe access to data during the preview. These are just a few items that set THE FARMER'S BOOT CD apart from other Linux boot CDs.

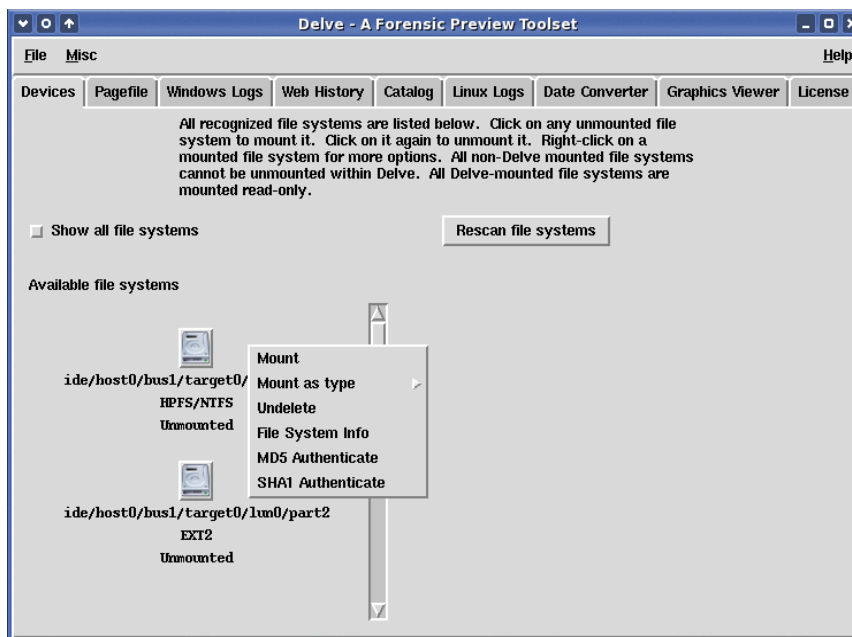
Delve is a preview tool that is found only on THE FARMER'S BOOT CD. A joint venture with a friend and colleague, Delve allows the user to point-and-click until their heart is content during the preview. Because of space constraints the rest of this paper will focus on Delve and how it can be used to quickly preview data in a forensically sound manner. I want to mention that there are many more applications included, though, both graphical in nature and command line, which allow the user to preview, authenticate, and acquire data. Covering every application in detail would take more space than this article permits. Stay tuned for more details and coverage, though!

Working within Delve should be easy and intuitive to the user. It is a tabbed program and you first mount the target file system in the default tab and then move through the other tabs as you like or your case dictates. Delve isn't operating system or file system specific. Some tabs are designed for the Windows operating system environment and they are clearly marked as such. Tabs designed for the Linux operating system environment are clearly marked as such.

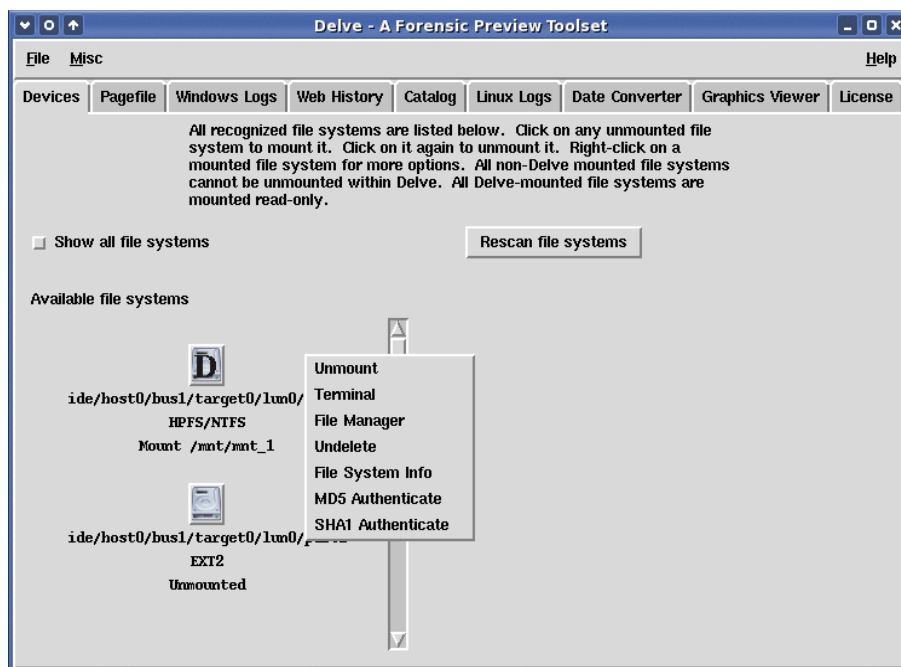
The graphic below shows the DEVICES tab. Within this tab you mount target file system you wish to preview. Every file system mounted within Delve is mounted read only. No matter the file system type, all Delve mounts are read only. This includes both the ext3 and ReiserFS file system types. You will not increment the journal counts for either of these file system types when you mount them within Delve.



Right-clicking on an unmounted file system will present a number of options as shown in the graphic below. Of particular interest to many users are the “Undelete” and “File System Info” options.



To mount a file system of interest simply click on it with your mouse. Delve mounted file systems will appear with a bold **D** across them and their mount point will appear beneath them. Additionally, there will be a change in the right-click options available when a file system is mounted. These are shown below.

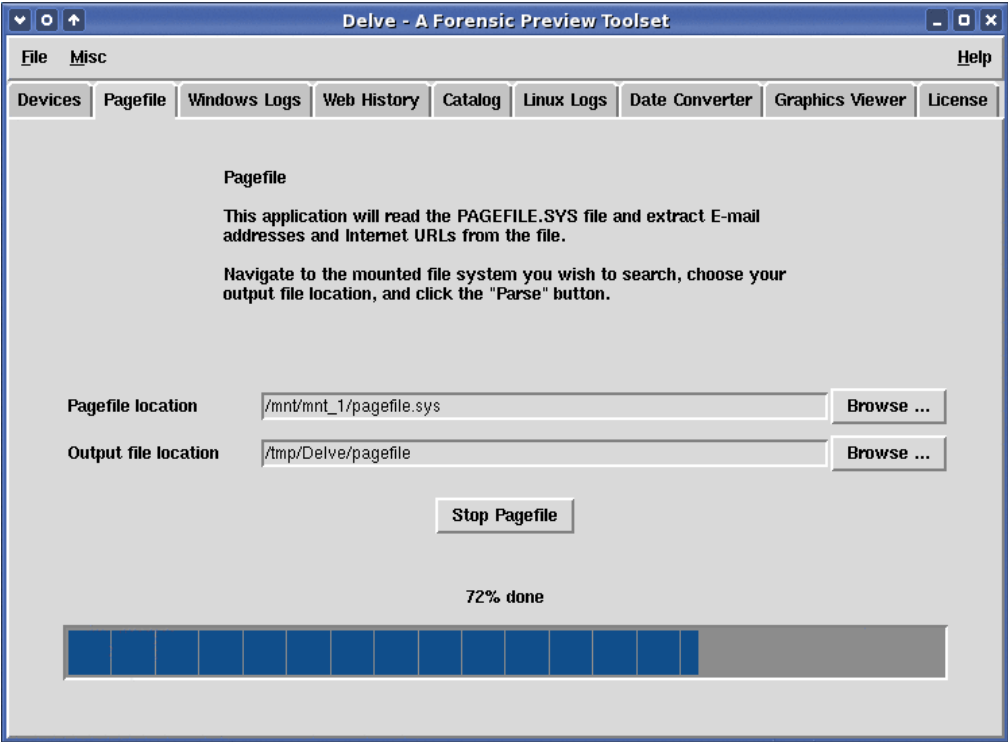


Popular right-click options for Delve mounted file systems are “Terminal” and “File Manager”. You can open a terminal to that mount point and then run your scripts or commands as you like with the safety that the file system is mounted read only. Separately, you can open the file manager against that mount point also with the comfort of knowing your actions are against a read only file system. The file manager has been heavily customized so that you can point and click your way through the suspect file system using a familiar looking file manager, all the while double-clicking on files of interest to view their content. Yes, even without such space hogs as Open Office you can double click on documents, spreadsheets, and presentations to view their content. Care has been taken to make certain that the most common file types can be viewed by double-clicking on them.

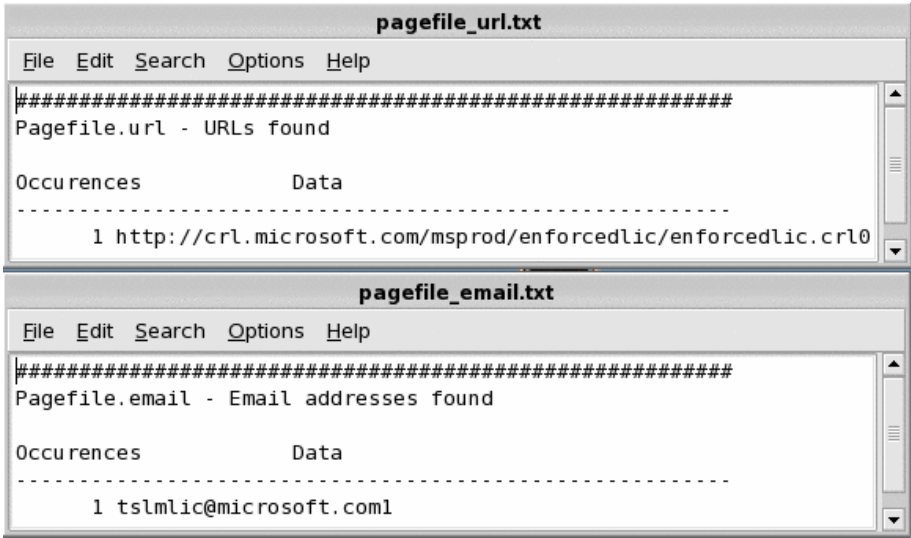
It really is this simple to mount file systems read only within Delve – a click of the mouse. To unmount simply click the Delve mounted file system again. Note that you cannot unmount file systems that were mounted outside of Delve.

Once you have your suspect file system mounted you can navigate through the other tabs to preview data of interest.

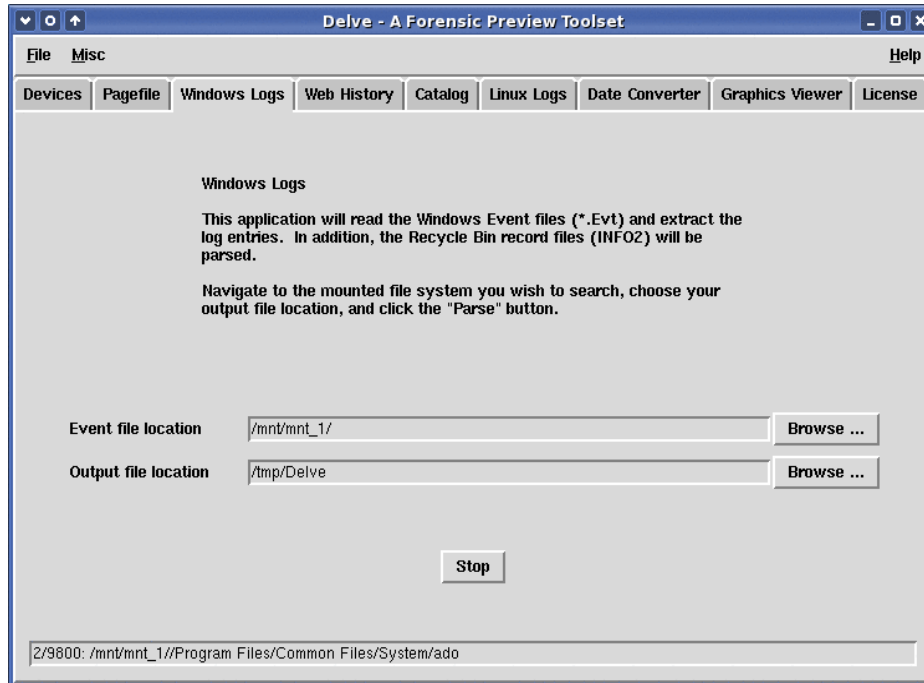
The PAGEFILE tab is shown below. This is a Windows operating system specific tab, in that the system file, "pagefile.sys", is parsed for both E-mail addresses and universal resource locators (URLs). This is a very fast way to read through this system file that is typically a heavily used cache by many programs (such as web browsers).



When the parse process completes two files will open such as those shown below. The number of occurrences for the data will be listed followed by the actual data. You can then further parse through these entries if you know the specifics for which you are searching for.



The WINDOWS LOGS tab provides access to all "INFO2" files (Recycle Bin database files) and the Windows event logs (Application, Security, and System). You navigate to your Delve mount point for the suspect Windows file system and then launch the process. Upon completion each of the event log files and the INFO2 records will be displayed as shown below.



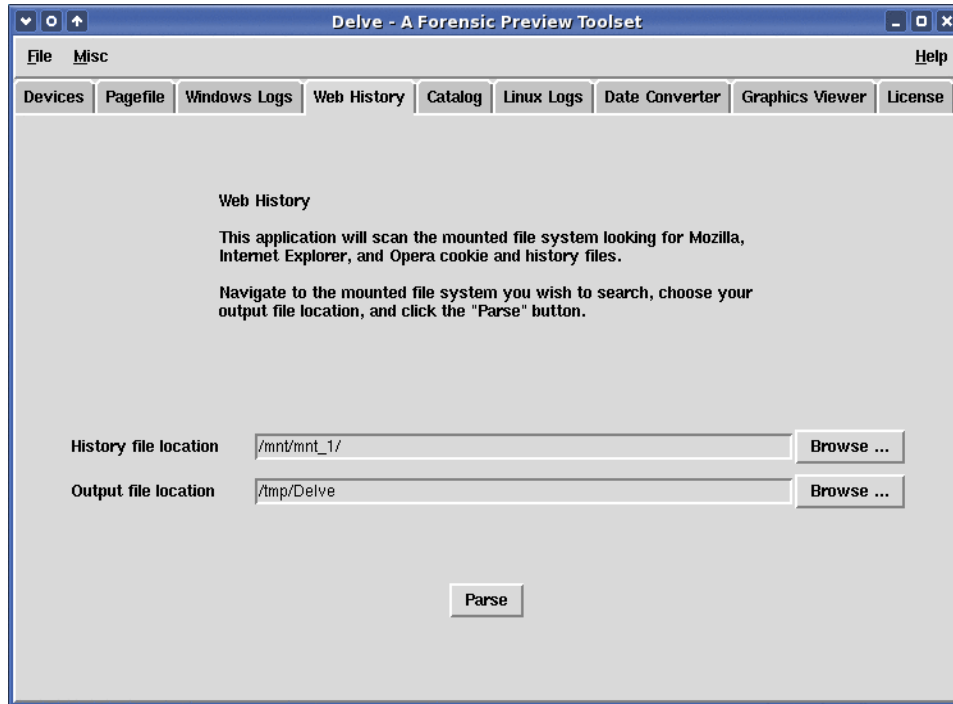
SecEvent.Evt.txt									
Type	Date	Time	Source	Category	Event	User	Computer	Strings	
Success Audit	1/31/2006			4:33:37 PM	Security		System Event	517 SYSTEM WASP-QCYJS	

SysEvent.Evt.txt									
Type	Date	Time	Source	Category	Event	User	Computer	Strings	
Information	4/26/2006	12:55:45 AM			Service Control Manager	(0)	7036	N/A WASP-QCYJS	
Information	4/26/2006	12:55:44 AM			Service Control Manager	(0)	7036	N/A WASP-QCYJS	
Information	4/26/2006	12:55:24 AM			RemoteAccess	(0)	20159	N/A WASP-QCYJSEPZR1 Ea	
Information	4/26/2006	12:02:30 AM			RemoteAccess	(0)	20158	N/A WASP-QCYJSEPZR1 fa	

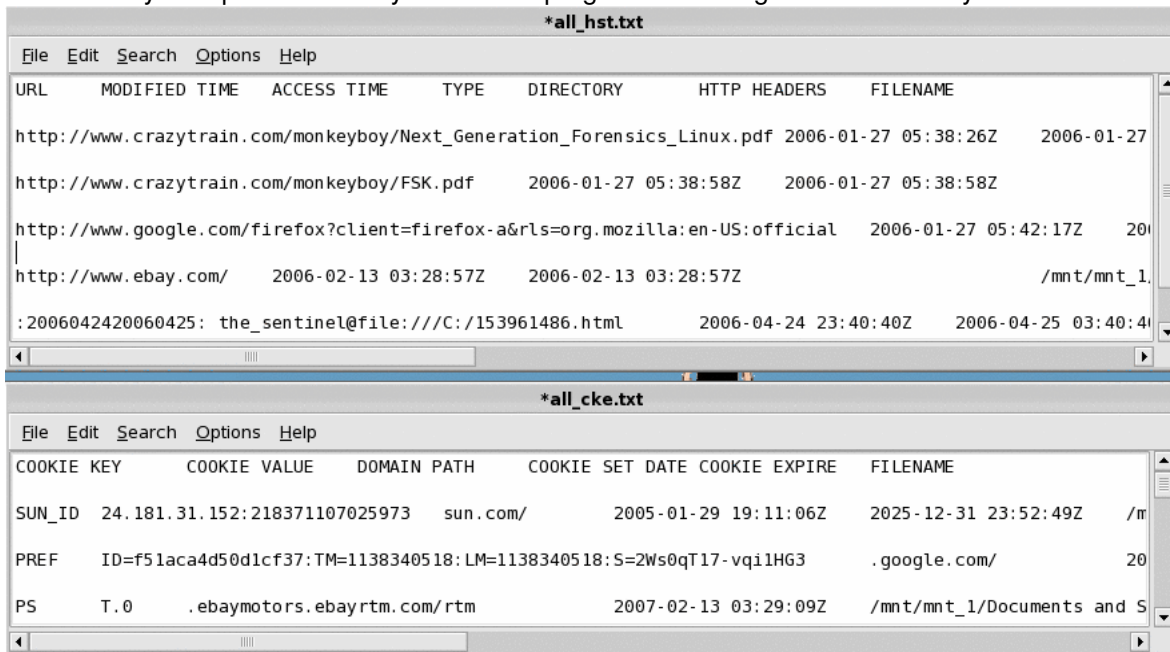
AppEvent.Evt.txt									
Type	Date	Time	Source	Category	Event	User	Computer	Strings	
Information	1/27/2006	5:37:22 AM			MsiInstaller	(0)	11728	Product: WebFldrs XP -- Co	
Error	12/7/2005	3:35:00 PM			WLTRY SVC	(0)	2	SYSTEM WASP-QCYJSEPZR1 SetService	
Information	11/16/2005	10:12:45 PM			LoadPerf	(0)	1001	N/A WASP-QCYJSEPZR1 Wm	
Information	11/16/2005	10:12:45 PM			LoadPerf	(0)	1000	N/A WASP-QCYJSEPZR1 Wm	

info2_results.txt									
INDEX	DELETED TIME	DRIVE NUMBER	PATH	SIZE					
1	04/25/2006 10:53:01	2	C:\Testing\Graphs\firefly.jpg	8192					

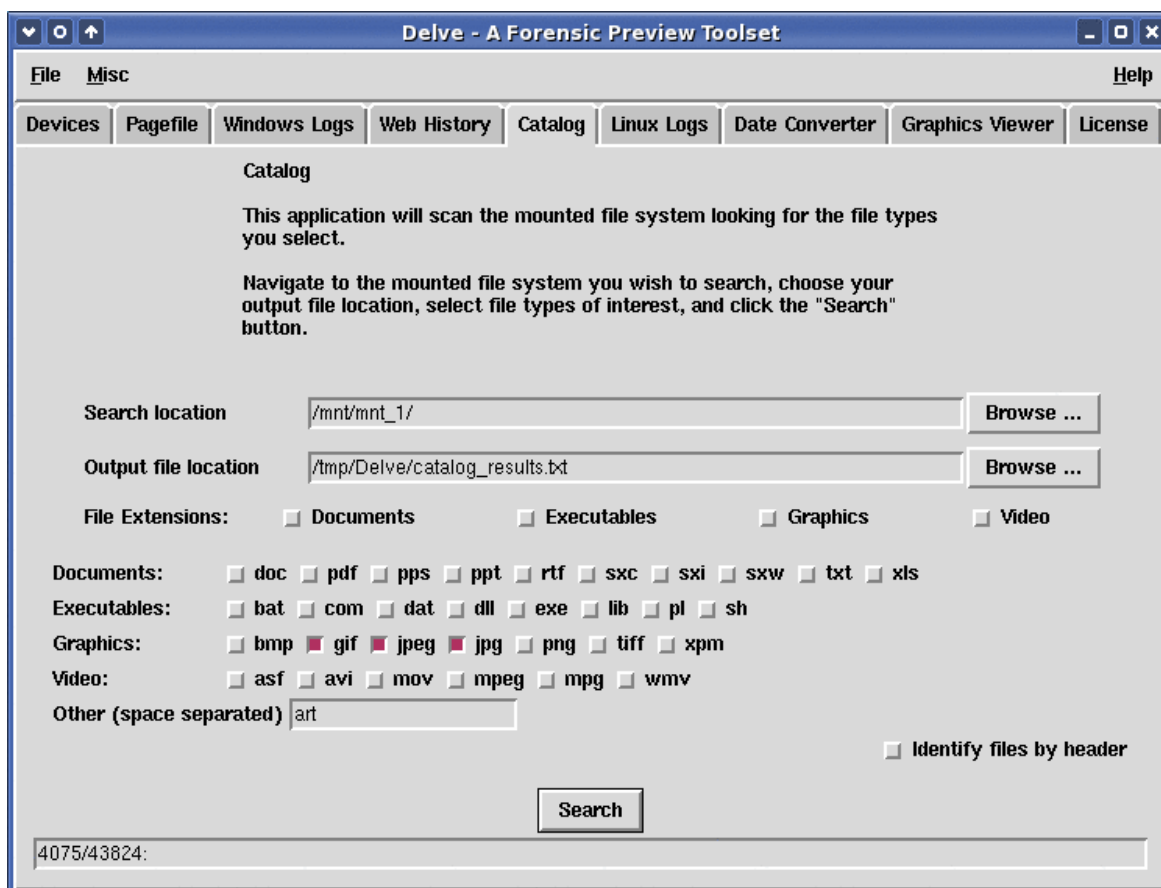
The WEB HISTORY tab provides a way to quickly preview both the cookies and histories for Internet Explorer, Opera, and Mozilla web browsers. This is operating system neutral. You can start from the top level Delve mount point for the suspect file system, or alternatively, you can drill down to a specific user's home directory on the suspect file system, to preview the web history.



Two files will open when the process completes, and these are shown below. These are tab-delimited files so it's easy to import them into your favorite program for sorting and further analysis.

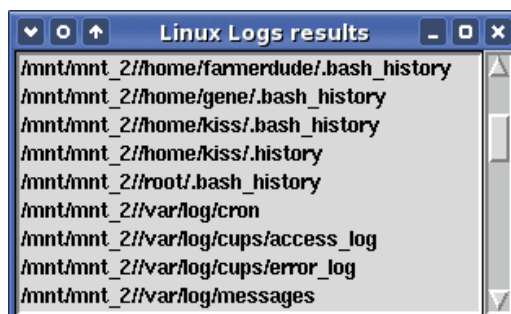
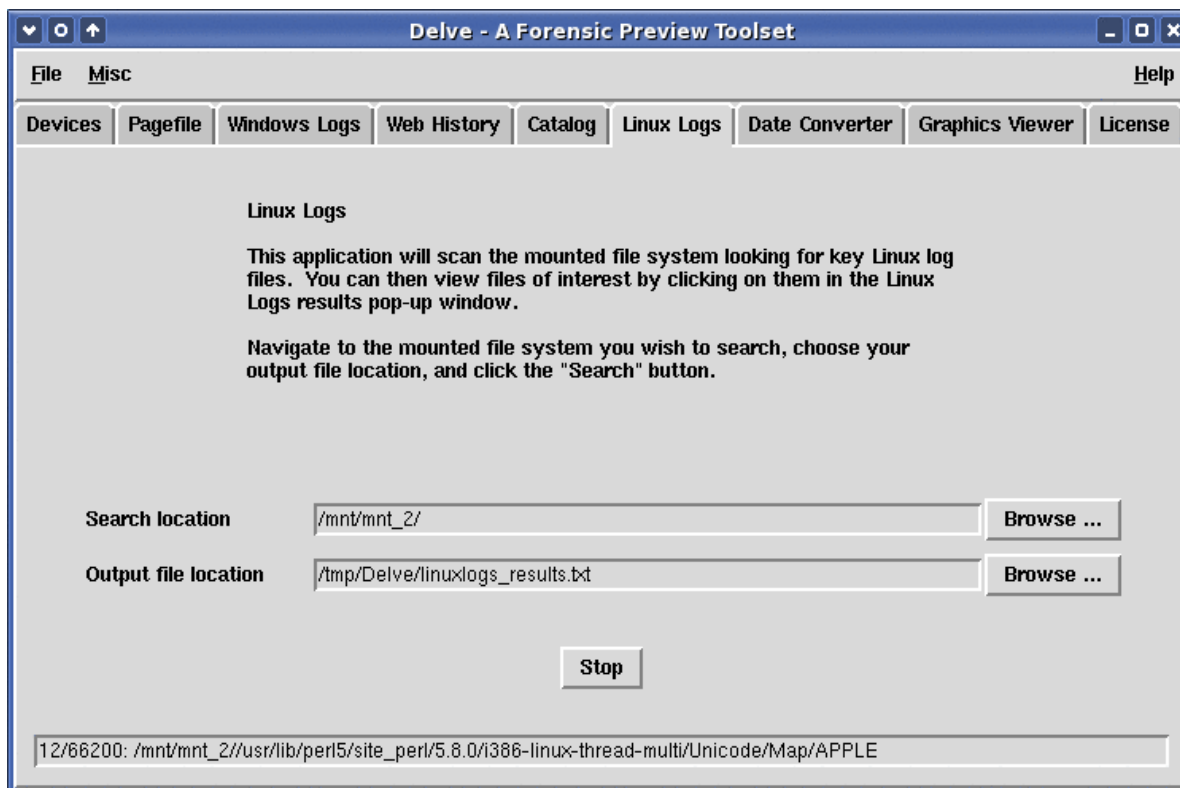


The CATALOG tab provides the capability to quickly identify file types of interest and catalog them, using their fully-qualified path filename. You can select from a top level group, individual extensions, or input your own extensions. An option allows you to identify files by header instead of extension if this suits your case. Simply navigate to your Delve mount point, select the file types of interest, and then kick off the process. When the process completes the results will be shown in the output file. The example below shows “gif”, “jpeg”, “jpg”, and “art” file types selected.

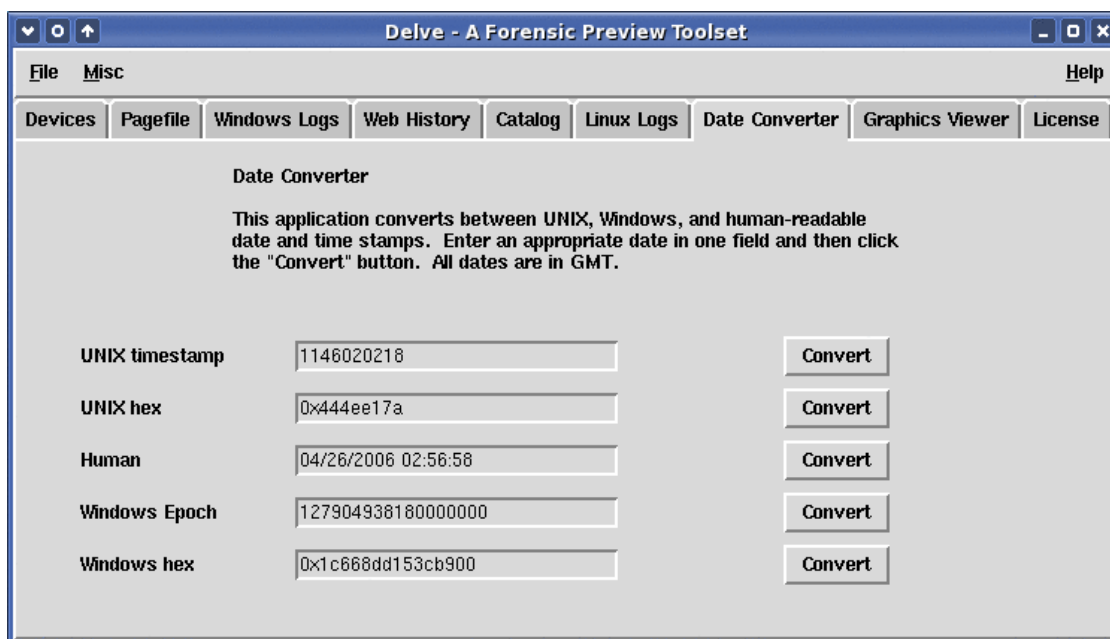


Note the “4075/43824:” in the graphic above near the bottom left. When the catalog process completes this shows the number of found items against the number of items searched. We can interpret these numbers in this example as 4075 file types of interest found out of 43824 files searched.

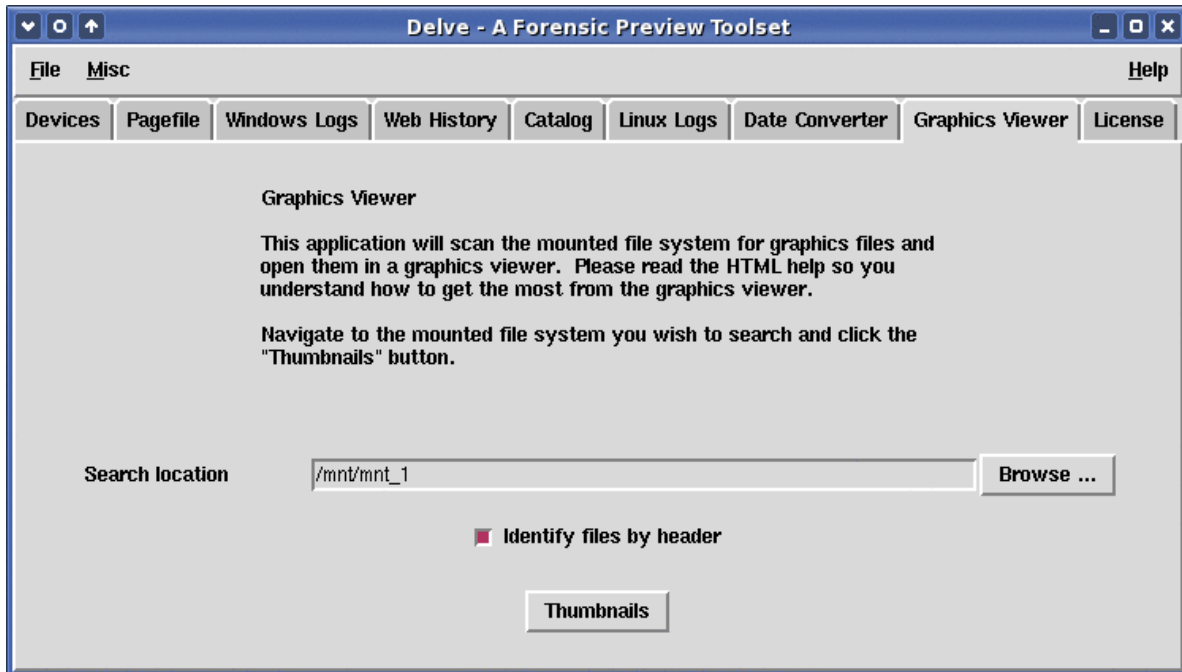
The LINUX LOGS tab is a Linux operating system specific tab. Within this tab you can quickly identify common logs of interest on a Linux system and view their contents. Once again, navigate to the Delve mount point for your Linux file system and either accept or change the output file location, then launch the process. When the file system has been searched a pop up window will open showing the found files of interest. Simply click on each file of interest in this pop up window to view its contents.



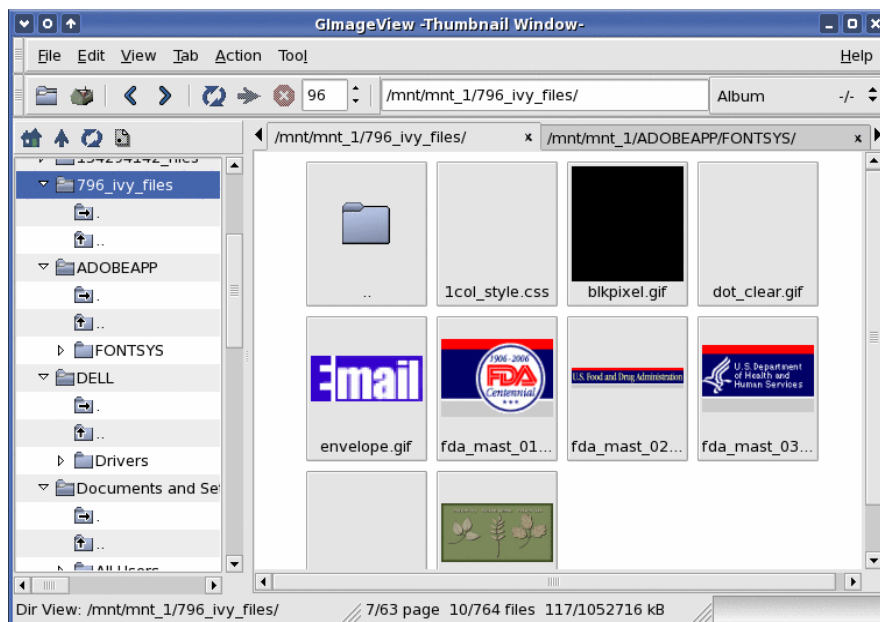
The DATE CONVERTER tab provides the capability to punch in one timestamp and convert it to the other four timestamps. One example where this comes in handy is pulling a timestamp embedded as metadata within a document and entering it in this tab to convert it from the Windows hexadecimal format to the human readable format.



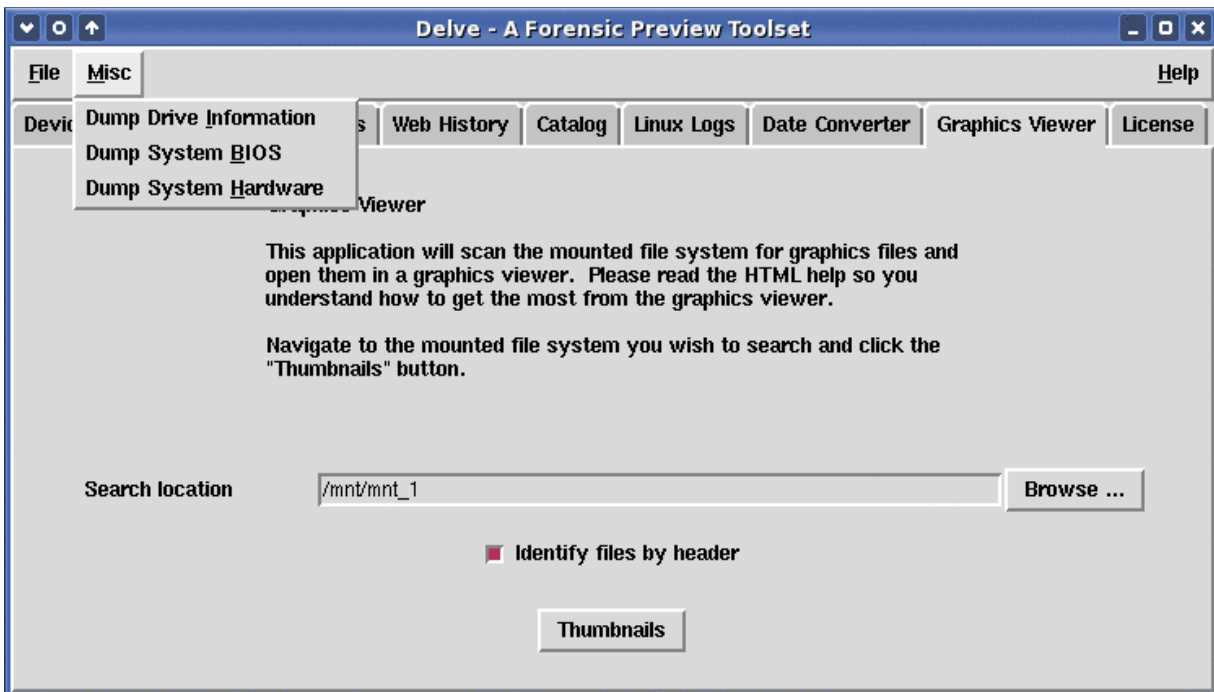
The GRAPHICS VIEWER tab provides quick access to all graphics files on the target system in the form of thumbnails. Simply navigate to your Delve mount point of interest and launch the process. The option to identify graphics by header and not by their extension is available as well.



The graphics viewer will open as soon as the process is launched. You will be able to see thumbnails in real time as they are identified and rendered. You can stop this process at any time. Within the graphics viewer you will always know where you are on the file system as the fully qualified path is visible and you can move up or down directories as you see fit.



The MISC program menu option is shown below. Dumping drive information to a file results in the device node, partition schema, and drive information for all recognized drives being written to this file. Make, model, manufacturer, size, serial number, etc. will be obtained and listed in the output file. Dumping the system BIOS tables results in a file containing the symbios tables information. You will find serial numbers, dates, universally unique identification numbers, etc., all within this file. Dumping system hardware results in the creation of three files, each of which details the hardware attached to the system in various levels of detail. What's great about all three of these options is that you get a great catalog of the suspect system that will be unique to that system. If you're not seizing the entire system this is a great process to complete. When opposing counsel questions if you acquired the correct system from a room containing 20 like systems you can pull out these files which contain those UUIDs and serial numbers which are unique as proof of the correct suspect system.



That's it, in a nutshell, for now. Delve is but one program on THE FARMER'S BOOT CD that may assist you in previewing data on suspect systems in a forensically sound manner. If you have any questions or comments please contact me at info@forensicbootcd.com