

Computer Hacking Forensic Investigator

TM



Module XI

Linux Forensics

Module Objective

This module will familiarize you with the following:

- Use of Linux as a forensic tool.
- Recognizing partitions in Linux.
- Overview of the file system in Linux.
- Linux boot sequence.
- Case study Extracting evidence from a floppy disk using Linux.
- Challenges in disk forensics with Linux.
- Case study Extracting evidence from a hard disk using Linux.
- Popular Linux forensics tools.

Module Flow



Use of Linux as a Forensics Tool

• Why use Linux for forensics?

- Greater Control:
 - Treats every device as a file.
 - Does not need a separate write blocker.
- Flexibility
 - Can be booted from a CD.
 - Can recognize several file systems.
- Power
 - Distributions like THE FARMER'S BOOT CD and Sleuth make Linux a forensic tool in itself.





Recognizing Partitions in Linux

- If a standard IDE disk is being used, it will be referred to as "hdx".
- The "x" is replaced with an "a" if the disk is connected to the primary IDE controller as master and with a "b" if the disk is connected to the primary IDE controller as a slave device.
- Similarly, the IDE disks connected to the secondary IDE controller as master and slave will be referred to as "hdc" and "hdd", respectively.





Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

File System in Linux



File System Description

Directory	Content
/bin	Common programs, shared by the system, the system administrator and the users.
/boot	The startup files and the kernel, vmlinuz. In recent distributions also grub data. Grub is the GRand Unified Boot loader and is an attempt to get rid of the many different boot-loaders we know today.
/dev	Contains references to all the CPU peripheral hardware, which are represented as files with special properties.
/etc	Most important system configuration files are in /etc, this directory contains data similar to those in the Control Panel in Windows
/home	Home directories of the common users.
/initrd	(on some distributions) Information for booting. Do not remove!
/lib	Library files, includes files for all kinds of programs needed by the system and the users.
/lost+found	Every partition has a lost+found in its upper directory. Files that were saved during failures are here.
/misc	For miscellaneous purposes.
/mnt	Standard mount point for external file systems, e.g. a CD-ROM or a digital camera.
/net	Standard mount point for entire remote file systems
/opt	Typically contains extra and third party software.
/proc	A virtual file system containing information about system resources. More information about the meaning of the files in proc is obtained by entering the command man <i>proc</i> in a terminal window. The file <u>proc.txt</u> discusses the virtual file system in detail.
/root	The administrative user's home directory. Mind the difference between /, the root directory and /root, the home directory of the root user.
/sbin	Programs for use by the system and the system administrator.
/tmp	Temporary space for use by the system.
/usr	Programs, libraries, documentation etc. for all user-related programs.
/var	Storage for all variable files and temporary files created by users, such as log files, the mail queue, the print spooler area, space for temporary storage of files downloaded from the Internet, or to keep an image of a CD before burning it.

Mount Command

- Devices like floppies, CDs, hard disk partitions, and other storage devices must be attached to some existing directory on your system before they can be accessed.
- This attaching is called mounting, and the directory where the device is attached is called a mount point.
- After the device is mounted, you can access the files on that device by accessing the directory where the device is attached.
- When you're done and want to remove the floppy or CD or other device, you need to detach, unmount, it before removing it.
- When mounting, you must tell the mount command what is the device or partition you want to mount and what is the mount point. The mount point must be a directory that already exists on your system. For example, to mount your floppy:
 - \$ mount /dev/fd0 /mnt/floppy
- When unmounting, you'll need to tell umount what mounted device to unmount:
 - \$ umount /dev/fd0

Linux Boot Sequence

- The first step in the boot up sequence for Linux is loading the kernel. The kernel image is usually contained in the /boot directory.
- Details of the boot loader can be gained from LILO or GRUB using more /etc/lilo.conf or more /etc/grub.conf.
- The next step is initialization where runlevel and startup scripts are initialized and terminal process controlled.
- The file that controls the initialization is **/etc/inittab** and the file that begins the process is **/sbin/init**.



Linux Forensics

- Linux has a number of simple utilities that make imaging and basic analysis of suspect disks and drives easier. These include:
 - dd Command to copy data from an input file or device to an output file or device.
 - **sfdisk** and **fdisk** Command to determine the disk structure.
 - grep Command to search files for instances of an expression or pattern.
 - The **loop device** Allows you to mount an image without having to rewrite the image to a disk.
 - md5sum and sha1sum Command to create and store an MD5 or SHA hash of a file or list of files (including devices).
 - **file** Command to read file header information in an attempt to ascertain its type, regardless of name or extension.
 - xxd Command line hexdump tool.
 - ghex and khexedit -The Gnome and KDE (X Window interfaces) hex editors.

Case Example

- ⊙Rebecca had filed a lawsuit against Good Company, Inc. for <u>sexual harassment</u> by one of its senior directors, Mr. Peter Samson.
- ⊙She has submitted a floppy as evidence of Mr. Samson's advances.
- ⊙She has also discovered that Mr. Samson used to send her explicit material through floppy disks marked as legitimate work
- ⊙You, a forensic investigator, have been called to investigate the case on behalf of Good Company, Inc.
- •How do you think he should proceed with the evidence?







Step-by-Step Approach to Case

- **1**. Document all processes
 - Begin with creating a directory where all forensic activities can be done.
 - /mkdir evidence
 - It is desirable to create a special mount point for all physical subject disk analysis.
 - mkdir /mnt/investigation
- **2**. Determine the disk structure
 - Create an image of the disk using the simple bit streaming command dd.
 - dd if=/dev/fd0 of=image.suspectdisk
 - Change the read-write permissions of the image to read-only using chmod.
 - Chmod 444 image.suspectdisk



Copyright © by EC-COUNCI All rights reserved. Reproduction is strictly prohibited

- **3**. Mount the restored imaged working copy and analyze the contents:
 - mount -t vfat -o ro,noexec /dev/fd0 /mnt/investigations
 - Another option is to mount a point within the image file using the loop interface rather than mounting the contents to another location.
 - mount -t vfat -o ro, noexec, loop image.suspectdisk /mnt/investigations
- 4. Verify the integrity of the data on the imaged file by checking the file hash:
 - md5sum /evidence/md5.image.suspectfile or
 - shalsum -c /evidence/SHA. image.suspectfile





- 5. Use the **ls** command to view the contents of the disk:
 - **ls -alR** to list all files including hidden files and list the directories recursively.
- 6. Make a list of all files along with access times:
 - ls -laiRtu > /evidence/suspectfiles.list
- 7. Search for likely evidence using:
 - grep. grep -i xxx suspectfiles.list
- 8. List unknown file extensions and changed file appearances:
 - file changedfile
 - Files can be viewed using strings, cat, more or less.



- 9. Search for certain keywords from the entire file list.
 - cat /evidence/ suspectfiles.list | grep blackmailword
 - A systematic approach to searching for keywords would be to create a keywords list. E.g. save it as:
 - /evidence/keywordlist.txt
 - grep the files for the keywords and save it to a file.
 - grep -aibf keywordlist.txt image.suspectdisk > results.txt
 - View the results:
 - cat results.txt
 - To analyze the files at each offset, use the hexdump tool:
 - xxd -s (offset) image.suspectdisk | less



Challenges In Disk Forensics With Linux

- Linux cannot identify the last sector on hard drives with odd number of sectors.
- Most Linux tools are complicated as they are used at the command line.
- Devices can be written to even if they are not mounted.
- Bugs in the open source tools can be used to question the credibility of the tool for forensics use.
- Forensic and Incident Response Environment (F.I.R.E) by William Salusky provides a good tool set.





Jason Smith Case

- Mr. Jason Smith has been accused of hoarding illegal material of questionable moral content on his company network systems.
- You have been called upon to examine the suspect hard disk, and unearth evidence related to the said illegal material.
- How do you think you should proceed in extracting and preserving the evidence?





Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

Step-by-Step Approach to Case

- 1. Note the model information from the hard disk label /manufacturer's Web site, and the size and total number of sectors on the drive.
- 2. Wipe and format a image disk drive using the ext3 file system (> 3x evidence size).
- **3**. Fill the disk with zeros and ensure that the contents match.
 - dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync
- 4. Partition the disk and reboot.
 - fdisk /dev/hda
- **5**. Format with the ext3 file system.
 - mkfs -t ext3 /dev/image.disk



Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

- 6. Prepare the disk for imaging:
 - a. Mount the freshly prepared read-write image disk.
 - a. mount /dev/hda /mnt/image.disk
 - b. Create a directory for all documentation and analysis.
 - a. mkdir /mnt/image.disk/case_no
 - c. Create a sub-directory to hold the evidence image.
 - a. mkdir /mnt/image.disk/case_no/evidence_no
 - d. Document details of the investigation in a text file including investigator's details, case background details, and investigation dates.
 - e. Carry out Document details of the disk media including investigator name and organization, case number, media evidence number, date and time of imaging; make, model, and serial number of computer, IP and system hostname; make, model, and serial number of HD, source of HD and scope of investigation.



- 7. Image the disk.
 - a. Connect both original evidence drive and drive to be imaged to the Imaging System.
 - b. Verify all jumper settings Master / Slave.
 - c. Make sure that the imaging system will boot only from CD by checking the BIOS settings.
 - d. Image the disk using dd.

```
dd if=/dev/hdx of=image.disk conv=noerror,sync
```

```
This will allow dd to try to ignore any errors (conv=noerror) and synchronize the output (sync) with the original.
```

- 8. Check for accuracy by comparing md5sum.
- 9. Mount the disk and extract evidence.
- 10. Images can be carved using dd or the hex dump tool **xxd**.



All rights reserved. Reproduction is strictly prohibited

Popular Linux Forensics Tools

- The Sleuth Kit written by Brian Carrier and maintained at http://www.sleuthkit.org.
- Autopsy HTML front-end for sleuthkit.
- SMART for Linux- by ASR Data, is a commercial data forensics program that runs on Linux.
- THE FARMER'S BOOT CD- by farmerdude, is a bootable CD that is oriented toward fast previewing of data in a forensically sound manner.
- Penguin Sleuth Knoppix based linux distribution with a forensic flavor.





• Forensix

Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

The Sleuth Kit

- The Sleuth Kit is a collection of command line digital investigation tools. The tools run on Linux, OS X, FreeBSD, OpenBSD, and Solaris and can analyze FAT, NTFS, UFS, EXT2FS, and EXT3FS.
- The Autopsy Forensic Browser is an HTMLbased graphical interface for the command line tools in The Sleuth Kit. This makes it much easier and faster to investigate a system.
- mac-robber is a tool that will collect temporal data from mounted file systems. The data can be used to make a timeline of file activity on the system using tools from The Sleuth Kit.



Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

Tools in "The Sleuth Kit"

⊙File System Layer Tools

• fsstat

⊙File Name Layer Tools

- ffind
- fls

⊙Meta Data Layer Tools

- icat
- ifind
- ils
- istat

●<u>Data Unit Layer Tools</u>

- dcat
- dls
- dstat
- dcalc

- jcat
- jls

●<u>Media Management Tools</u>

• mmls

●Image File Tools

- img_stat
- mg_cat

○<u>Disk Tools</u>

- disk_sreset
- disk_stat

Other Tools

- hfind
- mactime
- sorter
- sigfind
 - Copyright © by EC-COUNCI All rights reserved. Reproduction is strictly prohibited

Autopsy

- The Autopsy Forensic Browser is a graphical interface to the command line digital investigation analysis tools in The Sleuth Kit. Together, they can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).
- The Sleuth Kit and Autopsy are both Open Source and run on UNIX platforms. As Autopsy is HTMLbased, you can connect to the Autopsy server from any platform using an HTML browser.
- Autopsy provides a "File Manager"-like interface and shows details about deleted data and file system structures.





The Evidence Analysis Techniques in Autopsy

1. File Listing:

• Analyze the files and directories, including the names of deleted files and files with Unicode-based names.

2. File Content:

• The contents of files can be viewed in raw, hex, or the ASCII strings can be extracted.

3. Hash Databases:

• Lookup unknown files in a hash database to quickly identify it as good or bad.

4. File Type Sorting:

- Sort the files based on their internal signatures to identify files of a known type.
- 5. Timeline of File Activity:
 - Create timelines that contain entries for the Modified, Access, and Change (MAC) times of both allocated and unallocated files.





Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

The Evidence Analysis Techniques in Autopsy (cont'd)

6. Keyword Search:

• Keyword searches of the file system image can be performed using ASCII strings and grep regular expressions.

7. Meta Data Analysis:

• It allows you to view the details of any meta data structure in the file system.

8. Data Unit Analysis:

• It allows you to view the contents of any data unit in a variety of formats including ASCII, hexdump, and strings.

9. Image Details:

• You can view the file system details, including on-disk layout and the time of activity so that it is possible to recover data.







Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

Autopsy – File Listing

L L		RD SEARCH FI	LE TYPE IMAGE	DETAILS META	DATA DATA	UNIT	?	X	
View Directory:	r/r	label.exe	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:45 (EDT)	32016	48	0	182-128-4
	r/r	legacy.inf	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:40 (EDT)	4654	48	0	183-128-4
<u>ok</u>	r/r	lights.exe	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:40 (EDT)	35600	48	0	<u>184-128-4</u>
	r/-	LMREPL.EXE	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0	0	0	Q
The Deleter Prices	r/r	LMREPL.EXE	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:45 (EDT)	86800	48	0	185-128-4
APAND DIRECTORIES	r/r	loadfix.com	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:40 (EDT)	1131	48	0	186-128-4 (realloc)
	r/r	loadfix.com	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:40 (EDT)	1131	48	0	186-128-4
		A	SCII (display - repo	ort) * Strings (displa	y - report) * Export	t* Add N	lote		
	String	Contents Of F	SCII (display - repo File Type: MS V	ort) * Strings (displa Vindows PE 32-bit)	y - report) * Expor Intel 80386 GUI ex	t * <u>Add N</u> ecutable	lote		
	String	Contents Of Fi program cannot	SCII (<u>display</u> - repx File Type: MS V ile: E:\/system3 be run in DOS m	ort) * Strings (displa Vindows PE 32-bit) 2/inetins.exe ode.	y - report) * Expor Intel 80386 GUI ex	t* <u>Add N</u> ecutable	lote		
	String IThis .text .rdat @.data	Contents Of F program cannot a	SCII (display - repx File Type: MS V ile: E:\/system3 be run in DOS m	ort) * Strings (displa Vindows PE 32-bit) 2/inetins.exe ode.	y - report) * Expor Intel 80386 GUI ex	t* <u>Add N</u> ecutable	lote		
	String !This .text .rdat .rsrc @.relo MSVCRT KERNEL USER32 OSUM	Contents Of Fi program cannot a .dll .32.dll .dll	SCII (display - repx File Type: MS V ile: E:\/system3 be run in DOS m	ort) * Strings (displa Vindows PE 32-bit) 2/inetins.exe ode.	y - report) * Expor Intel 80386 GUI ex	t* <u>Add N</u> ecutable	lote		

EC-Council

Autopsy – File Content



Autopsy – Hash Databases

NSRL Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe

Exclude Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

Alert Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

opyrignt © by **دی-Council** All rights reserved. Reproduction is strictly prohibited

Autopsy – File Type Sorting

FILE ANALYSIS	DATA UNIT META DATA IMAGE DETAILS KEYWORD SEARCH FILE TYPE HELP CLOSE
Sort Files by Type	File Type Sortings
	The sorter tool will process an image and organize the files based on their file type. The files are organized into categories that are defined in configuration files. The categories will be saved in the output directory.
	 Sort files into categories by type Do not save data about unknown file types Save a copy of files in category directory (may require lots of disk space)
	 Extension and File Type Validation Exclude files in the NIST NSRL
	 Alert files that are found in the Alert Hash Database Ignore files that are found in the Exclude Hash Database
uncil	All rights reserved. Reproduction is strictly p

Autopsy – Timeline of File Activity

CREATE D	DATA FILE		CREATE TIMELINE	2		View	TIMELINE VIEW NOTES HELP CLOSE ? X	
<u><- May 2002</u> <u>Jul 2002 -></u>								C
				Ju	n	2002	OK	ł
Mon Jun 10 2002 19:33:10	3888	m	-/-rwxrwxrwx	48	0	112-128-4	C:/system32/drivers/NTHANDLE.SYS	C
Thu Jun 13 2002 21:01:34	22299	.ac	-/-rwxrwxrwx	48	0	263-128-4	C:/system32/oemnadem.inf	
Thu Jun 13 2002 21:01:35	20263	.ac	-/-rwxrwxrwx	48	0	270-128-4	C:/system32/oemnadlm.inf	
	39386	c	-/-rwxrwxrwx	48	0	193-128-4	C:/system32/mem.exe	
	56	mac	d/drwxrwxrwx	48	0	49-144-7	C:/system32	
	9488	c	-/-rwxrwxrwx	48	0	191-128-4	C:/system32/lsass.exe	
	9488	c	-/-rwxrwxrwx	48	0	191-128-4	C:/system32/lsass.exe (deleted-realloc)	
	33662	.ac	-/-rwxrwxrwx	48	0	268-128-4	C:/system32/oemnadin.inf	
	86800	c	-/-rwxrwxrwx	48	0	185-128-4	C:/system32/LMREPL.EXE	
	25491	.ac	-/-rwxrwxrwx	48	0	269-128-4	C:/system32/oemnadlb.inf	
	24391	.ac	-/-rwxrwxrwx	48	0	264-128-4	C:/system32/oemnaden.inf	
	22297	.ac	-/-rwxrwxrwx	48	0	266-128-4	C:/system32/oemnadfd.inf	
	85632	c	-/-rwxrwxrwx	48	0	179-128-4	C:/system32/krnl386.exe	
	22296	.ac	-/-rwxrwxrwx	48	0	267-128-4	C:/system32/oemnadim.inf	
	32016	c	-/-rwxrwxrwx	48	0	182-128-4	C:/system32/label.exe	
	35225	.ac	-/-rwxrwxrwx	48	0	265-128-4	C:/system32/oemnadep.inf	\$

EC-Council

Autopsy – Keyword Search

FILE ANALYSIS	DATA UNIT META DATA	IMAGE DETAILS KEYWORD SEARCH	FILE TYPE HE	CLOSE
New Search 2 occurrences of '((jan)l(feb)l(mar)l(ap) were found 126615 (Hex - Ascii) - string begins at 256 butes	ASCII (displa Fragment 126615 Allocated Group: 15 Pointed to by Inode: <u>30184</u> Pointed to by file: /bin/mt	←PREVIOUS NEXT → EXPORT CONTENTS ADD NOTE Ly - report) * Hex (display - report) * Sta File Type: data	rings (<u>display</u> - <u>repor</u> t)
180485 (<u>Hex</u> - <u>Ascii</u>) - string begins at 0 bytes	Hex Contents of Fragment 0 25733a20 57726974 16 20534353 49206d63 32 6661696c 65642e04 48 00000000 00000000 64 25733a20 436f6d76 80 6d6f6465 206e6f74 96 2e0a0000 00000000 112 0000000 00000000 128 25733a20 52652d73 144 68652063 6f6d7077 160 61676520 66616966 176 70726573 73696f66 192 6d707265 7373696f66 192 6d707265 7373696f66 193 6d707265 7373696f66 194 63206174 2053756 194 63206174 2053756 195 60 2449674 2053	126615 (1024 bytes) in images/ 4 696e6720 6d6f6465 %s: Wr: f 64652070 61676520 SCS I i a 00000000 00000000 fail ed 0 00000000 00000000 0 72657373 696f6e20 %s: Con 4 20636861 6e676564 mode no 0 00000000 00000000 0 0000000 00000000 2 65616420 6f662074 %s: Re- 2 65737369 6f6e2070 he c om c 65642e0a 00436f6d age fai e 206f6e2e 0a00436f pres sig f 6e206f66 662e0a00 mpre ss: 0 0000000 00000000 d. 0 0000000 00000000 d. 0 0000000 0000000 d. 0 0000000 0000000 d. 0 0000000 00000000 d. 3 72322f75 73657273 \$Id: // 2 612f7372 632f7379 /mak is 3 302e3562 2f6d742e s/mt -sig e 20417567 20313620 c at Sig	dev_hde8.img it ing mode mo de p age mp ress ion ot cha nged -r ead of t pr essi on p il edCom on onCo io n of f us r2/u sers ar a/sr c/sy t= 0.5b /mt. un Aug 16	
() () () () () () () () () ()	336 206d616b 6973617	2 61406b61 692e6d61 mak is	ar a@ka i.ma	

EC-Council

Copyright © by <mark>EC-Council</mark>

Autopsy – Meta Data Analysis

File Analysis	DATA UNIT META DATA IMAGE DETAILS KEYWORD SEARCH FILE TYP	E HELP	X
MFT Entry Number: 182-128-4	Alert Database		Î
OK	Details: MFT Entry: 182 Sequence: 1		
ALLOCATION LIST	Allocated UID: 48 DOS Mode: File Size: 32016 Links: 1		
	Name: label.exe \$STANDARD_INFORMATION Times: Created: Thu Jun 13 21:08:40 2002 File Modified: Mon Oct 14 05:38:00 1996		
	MFT Modified: Thu Jun 13 21:08:45 2002 Accessed: Thu Jun 13 21:08:40 2002 \$FILE_NAME Times:		
	Created: Thu Jun 13 21:08:40 2002 File Modified: Thu Jun 13 21:08:40 2002 MFT Modified: Thu Jun 13 21:08:40 2002 Accessed: Thu Jun 13 21:08:40 2002		
	Attributes: Type: \$STANDARD_INFORMATION (<u>16-0</u>) Name: N/A Resident size: 48 Type: \$FILE_NAME (<u>48-2</u>) Name: N/A Resident size: 84 Type: \$SECURITY_DESCRIPTOR (<u>80-3</u>) Name: N/A Resident size: 92		L
	Type: \$DATA (<u>128-4</u>) Name: \$Data Non-Resident size: 32016 <u>77378 77379 77380 77381 77382 77383 77384 77385</u> <u>77386 77387 77388 77389 77390 77391 77392 77393</u> 77394 77395 77395 77396 77397 77398 77399 77400 77401	Convright	

EC-Council

Autopsy – Data Unit Analysis

File Analysis	DATA UNIT META DATA IMAGE DETAILS KEYWORD SEARCH FILE TYPE HELP CLOSE
Cluster Number: 77378	
Number of Clusters:	ASCII (display - report) * Hex (display - report) * Strings (display - report) File Type: MS Windows PE 32-bit Intel 80386 console executable
Address Type: Regular (dd)	Allocated Pointed to by MFT Entry: 182-128-4 Pointed to by file:
Lazarus Addr: 🗖	C:/system32/label.exe
OK	String Contents of Cluster 77378 (512 bytes) in images/ntfs.40.dd
ALLOCATION LIST	<pre>itext .text .text .text .</pre>
	.rsrc
uncil	-د

Autopsy – Image Details

FILE ANALYSIS DA	ATA UNIT META DATA	IMAGE DETAILS	Keyword Search	FILE TYPE	HELP	CLOSE
		~				
Volume ID: 291050747						
Volume Label: NO NAME	0. EAT12					
File System Type (super block	.): FAT12					
META-DATA INFORMATI	ON					
Range: 2 - 45762						
Root Directory: 2						
CONTENT-DATA INFORM	TATION					
Sector Size: 512						
Sector of First Cluster: 33						
Total Sector Range: 0 - 2878						
FAT 0 Range: 1 - 9 FAT 1 Range: 10 - 18						
Data Area Sector Range: 19 - 1	2878					
EAT CONTENTS (in sector)	、 、					
FAT CONTENTS (in sectors)	, 					
$\frac{33-98}{20}$ (66) -> EOF						
$\frac{99-172(74)}{173-266(94)} \rightarrow EOF$						
267-267 (1) -> EOF						
$\frac{268-270(3)}{271-446(176)} > EOF$						
$447-494(48) \rightarrow EOF$						
$\frac{495-506(12)}{507}$ > EOF						
572-572 (1) -> EOF						
573-573 (1) -> EOF						
574-574 (1) -> FOF					Сор	yright © l
					1.	, 0

SMART for Linux

- SMART is a software utility that has been designed and optimized to support data forensic practitioners and Information Security personnel in pursuit of their respective duties and goals.
- It is known as 'The Next Generation Data Forensic Tool'.
- Functions of SMART:
 - "Knock-and-talk" inquiries and investigations.
 - On-site or remote preview of a target system.
 - Post mortem analysis of a dead system.
 - Testing and verification of other forensic programs.
 - Conversion of proprietary "evidence file" formats.
 - Baselining of a system.







Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

Features of SMART for Linux

- SMART lists connected storage devices in the main window list.
- It uses plugins to do much of the work, and the application itself utilizes a highly modular design philosophy.
- It is multi-threaded.
- Its powerful, flexible acquisition options allow you to create pure bit-image copies and quasiproprietary formats that support seekable compression.
- It can acquire and clone a single source to any number of images and devices simultaneously.
- It generates lots of information about hashes.
- It provides the ability to perform real authentication.
- It gives you an easy interface to linux mounts, and GUI environments like KDE and GNOME.
- It enables complex tasks and search result rules to be applied automatically.

file Cases Log Help	Die fas biesetert		Concession of the local division of the loca
Storage Devices	into: /dev/ndi		
Unallocated Data (5.37 MB) /dev/hda (Sector 156,344,580) MAXTOR 4K060H3 (55.917 GB) /dev/hde	Make and Model Serial Number Size	/dev/hde MAXTOR 4K060H3 673131221663 55.917 GB	
Unallocated Data (31.5 KB) /dev/hde (Sector 0)	Bytes Sectors Rus Connection	60,040,544,256 117,266,688 Tortionu Master	
Linux (83) Partition (7.423 GB) /dev/hde1	Dev Major	33	
Extended (f) Partition (48.483 /dev/hde (Sector 15,566,985)	Dev Minor	U Log Ir	nfo Disn
Unallocated Data (31.5 KB) /dev/nde (Sector 15,566,985))		
FAT32 LBA (c) Partition (48 /dev/hde5	.483 GB)	FS: FAT32 (my	stunn)
Unallocated Data (11.67 MB) /dev/hde (Sector 117,242,370)			
DIDE-SCSI		ATT 820	
/dev/scd0	0.115	Bus:0 Channel:0 Id:0 I	Lun:0
USB BR92 BR82		TTUR20	
STORIX AXIS (125.00 MB) /dev/sda		FS: F. Bus:1 Channel:0 Id:0 I	AT16

EC-Council

hibited ignts reserved. Reproduction is strictly p





Acquire: /dev/sda1	×
Configure Image 1 Device 1	
Using 100.0%- 30.97 MB at 0	Data Filters: None
FATIS (6) Partition (30.97 MB) /dev/sda1	FS: FAT16 (thumb)
What operations would you like to perform?	
Acquire to 💌 1 🛋 image file(s). Hash Protocols: 🔲 SHA1 🔽 MD5 🔲 CRC32	
Cione to 💌 1 🛋 storage device(s).	
	Cancel Okay

Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

SMART					X		
File Cases Log Help							
Storage Devices	Case: Austin	523					
	ESR92	R82 브라 니 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이	TTT R20		*		
Manual Manua Manual Manual Manua Manual Manual Manu	drive (30.97 MB) Firmage D Image D	523/Thumb drive.image.00	FS: FAT16 (thumb) 11	R0: /SMART/mnt/7-0			
	Filesystem 👂	Unmount					
	Copy Authenticate ↓ View Data Search Import Image	Browse Terminal Here Copy Mount Point SMART ▷			4 4		

Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

SMART	and the second		X
File Cases Log He Storage Devices O IDE/ATA MAXTOR 6 /dev/hda Unalloca /dev/hda	Configure Unallocated Include what classes of unal here will remain in effect unti rescanned, or you reconfigu Pure Unallocated Deleted Files	 located data? (Your choice I SMART is closed, devices are re unallocated). ☑ Active File Slack ☑ Deleted File Slack ☑ Deleted File Slack ☑ Okay	Primary Master
Linux (83 /dev/hda	3) Partition (2.007 GB) 2	FS: EXT	3 (blueshift) RW: /
Linuv /83	B) Partition (2.007 GB)	ES: EVT3 (RH7 2)	Rur Imnt/sandhov

and 100.0% 21.487 GB d0 Data Filter: No HPFS/NTFS (7) Partition (21.487 GB) /dev/hda1 Studied: NTFS ght-click to add search terms. Image: Studied: NTFS ave This Term + Auto-Export. (Click to Enable) Image: Studied: NTFS tatch Regex mythology Image: Image: Studied: NTFS ave This Term + Auto-Export. (Click to Enable) Image: Image: Studied: NTFS tatch Regex (xd0/xcfx11/xe0/xa1/xb1) Image: Image: Image: Image: Studied: NTFS Pre-Select 0 B ♦ (Data leading up to the match offset.) oot Select 1 Image:	Searching /dev/hda1		×						
ght-click to add search terms. ave This Term + Auto-Export: (Click to Enable) 1atch Regex mythology ave This Term + Auto-Export: (Click to Enable) 1atch Regex \vd0\vcfw11\ve0\va1\vb1 1atch Regex \vd0\vcfw11\ve0\va1\vb1 Pre-Select 0 B ♦ (Data leading up to the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) ave This Term + Auto-Export: (Click to Enable) Ignore Case Pre-Select 0 B ♦ (Data leading up to the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) oot Select 1 MD ♦ (Data starting from the match offset.) oot Select 1 Ignore Case ind Regex: \v25v25EOF\v20d Ignore Case ind Regex: \v25v25EOF\v20d Ignore Ca	HPFS/NTFS (7) Partition (2 /dev/hda1	1.487 GB)	Data Filter: Nons Studied: NTFS						
ave This Tem + Auto-Export: (Click to Enable) Image:	Right-click to add search terms.								
Match Regex mythology Ignore Case ave This Term + Auto-Export. (Click to Enable) Image: Vertice Comparison of Section (Click to Enable) Match Regex Vertice Case Pre-Select 0 B (Data leading up to the match offset.) oot Select 1 MD (Data starting from the match offset.) ave This Term + Auto-Export: (Click to Enable) Imatching bytes.) ave This Term + Auto-Export: (Click to Enable) Imatching bytes.) ave This Term + Auto-Export: (Click to Enable) Imatching bytes.) ave This Term + Auto-Export: (Click to Enable) Imatching bytes.) ave This Term + Auto-Export: (Click to Enable) Imatching bytes.) ave This Term + Auto-Export: (Click to Enable) Imatching bytes.) ave This Term + Auto-Export: (Click to Enable) Imatching bytes.) attraction of the match offset. Imatching bytes.) attract Regex: Imatching bytes.) Imat	Save This Tem I Auto-Export: (Click	k to Enable)	X						
ave This Tem + Auto-Export: (Click to Enable) Image: Vxd0/xcfx11/xe0/xa1/xb1 Aatch Regex Vxd0/xcfx11/xe0/xa1/xb1 Image: Ignore Case Pre-Select 0 B (Data leading up to the match offset.) ost Select 1 MD (Data starting from the match offset.) ave This Tem + Auto-Export: (Click to Enable) Image: Vx25PDF Image: Ignore Case and Regex: Vx25Vx25EOF/x0d Ignore Case	Match Regex mythology		🔽 Ignore Case ≚						
Match Regex \xd0\xcfx11\xe0\xa1\xb1 Ignore Case Pre-Select 0 B (Data leading up to the match offset.) oot Select 1 MD (Data starting from the match offset.) ave This Term I Auto-Export: (Click to Enable) Imatch offset.) tart Regex: \x25PDF Imatch offset.) ind Regex: \x25\x25EOF\x0d Ignore Case	Save This Term + Auto-Export: (Clici	k to Enable)	X						
Pre-Select 0 B ♦ (Data leading up to the match offset.) oot Select 1 MD ♦ (Data starting from the match offset. '0' selects all matching bytes.) ave This Tem I Auto-Export: (Click to Enable) × tart Regex: ×25PDF ✓ Ignore Case ind Regex: ×25i×25EOF×0d ✓ Ignore Case	Match Regex Vxd0/xcfx11/xe0/xa1/xb1								
oot Select MD (Data starting from the match offset. '0' selects all matching bytes.) ave This Tem + Auto-Export: (Click to Enable) x tart Regex: [x25PDF I gnore Case ind Regex: [x25]x25EOF[x0d	Pre-Select 0 B ♦	(Data leading up to the match offset.)							
ave This Tem + Auto-Export: (Click to Enable) tart Regex: \v25PDF Ignore Case Ind Regex: \v25\v25EOF\v0d Ignore Case Ind Regex: \v25\v25EOF\v0d Ignore Case	Post Select 1 MD 🔶	Data starting from the match offset. "O' selects a	all matching bytes.)						
tart Regex: W25PDF	Save This Term I Auto-Export: (Clici	= k.to Enable)	X						
End Regex: ₩25₩25EOF₩0d Ignore Case	Start Regex: Vx25PDF		🔽 Ignore Case						
	End Regex: \x25\x25EOF\x0d		Ignore Case						
nd match must be within 1 MB ⇔ of Start match, or select failback range ⇔	End match must be within 1	MB 🔶 of Start match, or select fallback	range 👄						
allback Range: 500 KB 🔶 (A value of 0 will select all bytes matching the 'start' regex.)	Fallback Range: 500 KB	♦ (A value of 0 will select all bytes matching the select all	he 'start' regex.)						
			4						
			Cancel Search						
Cancel Search									

EC-Council

Copyrignt © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

Penguin Sleuth

- The Penguin Sleuth Kit is a bootable Linux distribution based on KNOPPIX.
- It is the collection of some very useful tools, including The Coroner's Toolkit (TCT), Autopsy, and The Sleuth Kit, as well as penetration testing and virus scanning tools.
- It offers a GUI environment, as well as the good, old-fashioned command line environment fitting the novice user to the experienced user.



Tools Included in Penguin Sleuth Kit

- **Sleuth Kit** Command Line Forensic Tools
- Autopsy Part of Sleuth Kit
- Foremost Command line data carving tool
- **Glimpse** Command line data indexing and searching tool
- Wipe Command line utility to securely wipe hard drives and files
- Etherape Visual network monitor
- Fenris Multipurpose tracer
- **Honeyd** Command line honypot program
- Snort Command line network intrusion tool
- **Dsniff** Command Line network auditing and penetration testing tools
- John The Ripper Command Line Password Cracking tool
- Nikto Webserver scanner

Tools Included in Penguin Sleuth Kit (cont'd)

- Nbtscan Command-line tool that scans for open NETBIOS nameservers
- **Xprobe** Command line remote operating system fingerprinting tool
- Ngrep Command line Network grep Function
- Nemesis Command Line network packet injector
- Fragroute Command line network intrusion testing tool
- **Fping** Command line multiple host ping utility
- **TCPtraceroute** Command line traceroute TCP packages
- **TCPReplay** Command line utility that replays a TCP dump
- **Nessus** Graphical Security Scanner
- Ethereal Graphical Network analyzer
- **Netcat** Command line tool to read and write over network
- **TCPdump** Command line tool that dumps network traffic

Tools Included in Penguin Sleuth Kit (cont'd)

- **Hping2** Command line packet assembler / analyzer
- **Ettercap** Command line sniffer / interceptor / logger for Ethernet networks
- **Openssh** Secure remote connection utility
- **Kismet** Graphical wireless network sniffer
- AirSnort Graphical wireless network intrusion tool
- **GPG** Encryption utility
- **OpenSSL** Secure remote connection utility
- **Lsof** Command line utility that lists all open files
- **Hunt** Command line TCP / IP exploit scanner
- Stunnel SSL connection package
- ARPwatch Command line Ethernet monitor
- **Dig** Command line tool for querying domain name servers
- Chkrootkit Looks for signs of root kit

Forensix

• The goal of the Forensix ("4N6") Project is to allow a system to be monitored so that, in the event of a security compromise, it is easy to track the compromise back to its source and recover from it.

Source: http://forensix.sourceforge.net/

• Forensix performs a complete kernel event audit on the target system and streams the high-definition audit trail to a backend database that has been optimized for reconstruction queries.

• Functions:

- Accurately replaying any and all system compromises.
- Determining what specific data (such as credit card numbers) has been accessed on the system as a result of a compromise.
- Automatically determining what modifications have been made to a system by an illicit user.
- Selectively "undo"-ing illicit system modifications.

Maresware

- Linux Forensics provides tools for investigating computer records while running the LINUX operating system on Intel processors.
- Maresware is useful to all types of investigators, including law enforcement, intelligence agency, private investigator, and corporate internal investigators.
- This software enables discovery of evidence for use in criminal or civil legal proceedings.
- http://www.dmares.com/maresware/linux_forensics.htm



Major Programs Present in Maresware

- Bates_no:
 - A unique program for adding identifying numbers to filenames in edocuments.
- Catalog:
 - Catalogs every file on a Linux file system and identifies headers.
- Hash:
 - Performs MD5 (CRC, or SHA) hash of every file on a drive.
- Hashcmp:
 - Compares outputs of successive hash runs.
- Md5:
 - Calculates MD5 hash of a file.
- Strsrch:
 - Searches files for text strings.
- \odot U_to_A:
 - Converts *ix text to DOS text.

Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

Captain Nemo

- Widely used by law enforcement personnel, forensic investigators, and network administrators. Captain Nemo enables you to access any Linux drive from your Windows computer, without requiring a network setup.
- Just connect the Linux drive to your machine, and Captain Nemo will let you mount your Linux partitions in Windows.
- You can read, search, and view all your Linux files and copy them to your Windows drive.
- Supports ext2fs and ext3fs

Captain Nemo - The Win95/98 File Edit Help	3/NT-Novell-Ntfs-Linux Multi	Platform File I	Manager			<u>_ ×</u>
🐕 🐏 🖺 🍈 🖹 🗁 💆 🂖	📴 🤐 🚉 🗈 🕐 🔍	. 로 <mark>メ</mark>				
All Directories	C:*.*					Ē.
⊞ 4 3½ Floppy (A:)	Name	Size	Туре	Date	Attr	
	Documents and Settings		File Folder	1/18/2007 1:43:14 AM	_d	
Engen (B.) Engen Hala Stend (E.)	fcf5c7e42ad4374c3600		File Folder	1/19/2007 11:00:56	_d	
	iplayData		File Folder	1/17/2007 10:54:24	_d	
			File Folder	1/18/2007 3:13:36 PM	_dhr	
	Program Files		File Folder	1/24/2007 8:31:14 PM	_dr_	
	RECYCLER		File Folder	1/18/2007 7:41:28 AM	_d_sh	
	System Volume Information		File Folder	1/18/2007 3:11:50 PM	_d_sh	
			File Folder	1/24/2007 8:31:32 PM	_d	
			File Folder	1/18/2007 1:39:18 AM	_d	
	AUTUEXEC.BAT	UKB	Windows B	1/18/2007 1:38:44 AM	a	
		1 KB	Configuratio	1/18/2007 3:02:38 PM	ashr_	
			System file	1/18/2007 1:38:44 AM	a	
			System file	1/10/2007 1:30:44 AM	a_snr_	
			System file	1/16/2007 1:36:44 AM	a_shr_	
		48 NB 200 KB	Application	1/18/2007 2:58:50 PM	a_shr_	
		230 ND	System nie Custaas fila	171072007 2:00:00 FM	a_snr_	
		1,010,013 ND 720 MD	System nie Filo	1/22/2007 4.20.40 FM	a_sn_	
		720 ND 4 MD	rile 1 Eilo	1/22/2007 4.44.30 FM	a	
	⊡ (1p0.1	4 ND	1 File 2 File	172272007 4:44:36 FM	a	
	I III (1ро.2	4 ND 700 KD	2 File 2 File	172272007 4:44:36 FM	a	
		720 NB	3 File	172272007 4:44:36 PM	a	
	J	teres of the t				

Copyright © by <mark>EC-Council</mark> All rights reserved. Reproduction is strictly prohibited

THE FARMER'S BOOT CD

- THE FARMER'S BOOT CD allows you to examine hard disks directly from Linux,
- Boots most any x86 system and mounts file systems in a forensically sound manner.
- Preview data using a single, unified graphical user interface (GUI).
- Acquire media after you've previewed the data and found it pertinent to your investigation.
- <u>http://www.forensicbootcd.com</u>







Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited

			Delve - A	Forensic	Preview To	oolset		_				
<u>File Mis</u>	iC								<u>H</u> elp			
Devices	Pagefile	Windows Logs	Web History	Catalog	Linux Logs	Date Converter	Graphics Viewer	License				
All file sys on it agair change de Delve-mo the RESC hold onto FILE SYS	stems cum n to unmou pending up unted file s AN FILE S' that devic TEMS butt	ently recognized nt it. Right-click oon the mount st systems are mou YSTEMS button t e information, inc on.	by the Linux ke on any mounte atus. All non-D nted read-only o view file sys luding partition	ernel are s ed or unmo elve moun . If you ao tems on ti s and file :	hown below. Junted file sy ted file syste Id a device to hat device. I systems, unt	Click on any unm stem to view avail ems cannot be unm) your system wai lote that if you rer il you force it to re	ounted file system able options. Note nounted within Delv t a few moments a nove a device the l scan by also clicking	to mount it that option e. All nd then clic Linux kerne ng the RES	t. Click ns will ck on el may CAN			
🗌 Show	r all file sy	stems			Rescan	n file systems						
Available	e file syste	ms										
	sda2	.e.		Copyriq	ght @2007	/ farmerdude	All rights rese	rved.				
	Unmounte	ed		For inc	lusion in E	C-Council CHF	i course only.			☐ Show all file s	systems	
	sda3									Available file sys	tems	
	EXT3	,								5	Mount	1
	nount /]	sdaž HPFS/N	Mount as type Undelete Files	*
										Unmoun	File System Info MD5 Authentication	
											SHA1 Authentication	

Copyright © by <mark>EC-Council</mark> All rights reserved. Reproduction is strictly prohibited

		Delve - A l	orensic	Preview T	oolset				
<u>File M</u> isc								<u>H</u> elp	
Devices Pagefile	Windows Logs	Web History	Catalog	Linux Logs	Date Converter	Graphics Viewer	License		
Pagefile This applicatio Navigate to th	n will read the "p e mounted file sy	agefile.sys" file stem you wish	and extra to search	uct E-mail add I, choose you	lresses and Intern r output file locati	et URLs from the t on, and click the P	īle. ARSE butti	on.	
Pagefile lo	cation //m	nt/sda2/pagefile.	sys			Broy	vse		
Output file	e location //tm	p/Delve/pagefilo)			Brov	vse		
			Sto	p Pagefile					
			68	3% done	(page	ile_url.ixt 0 :
						<u>File Edit S</u> earch ####################################	<u>O</u> ptions <u> </u> ######## - URLs	<u>H</u> elp ######## found	*****
Copyright @20	007 farmerdi	ude All righ	ts rese	rved. For	inclusion in E	Occurrences		Data	Offsets
						3 w 2 ht 2 w 1 w 1 ht	w.googl tp://ww w.googl w.l.goo tp://dl	e.com 10 w.google e.com/to gle.com .google	0789736,10970736,10997476 e.com/search?q= 12365972,14105608 ools/swg2/update?auv=1&r=4&up=30&p 10979616 .com/swg/0.0.0.0/wontdownload 1100
Council							All	rights re	Copyright © by <mark>EC-Counc</mark> eserved. Reproduction is strictly prohibite

	Delve - A Forensic Preview Toolset		
<u>F</u> ile <u>M</u> isc		<u>H</u> elp	
Devices Pagefile Windows	Logs Web History Catalog Linux Logs Date Conve	erter Graphics Viewer License	
Windows Logs			
This application will scan the them in the results pop-up wi	targeted file system for key Windows log files. You can ndow.	then view files of interest by clicking on	
Navigate to the mounted file :	system you wish to search, choose your output file loca	tion, and click the PARSE button.	
Copyright @2007_farm	erdude All rights reserved. For inclusion	in EC-Council CHFI course only.	
		·····,	
Search location	/mnt/sda2/	Browse	
Output file location	/ /tmp/Delve	Browse	
	1		
			🗖 FileDisplay 🗙
	Stop		/tmp/Delve/SysEvent.Evt.txt
			/tmp/Delve/SecEvent.Evt.txt
2/39600: /mnt/sda2//WINDOWS/	/system32/config/systemprofile/Local Settings/Temporary Inte	ernet Files	/tmp/Delve/info2_results.txt
			Close
		A11	Copyright © by EC-Counc
-Council		All rights res	erved. Reproduction is strictly prohibite

ile hlipp		Uala	
ile <u>M</u> isc			
evices Pagefile Windows	Logs Web History	Catalog Linux Logs Date Converter Graphics Viewer License	
Web History			
This application will scan th	ne targeted file syste	em looking for Mozilla, Internet Explorer, and Opera cookie and history files.	
Navigate to the mounted fil	le system you wish	to search, choose your output file location, and click the PARSE button.	
opyright @2007 farme	rdude All right	s reserved. For inclusion in EC-Council CHFI course only.	
History file location	/mnt/sda2/	Browse	
Output file location	/tmp/Delve	Browse	
		all_cke.txt	
		Image: Search Options Help COOKIE KEY COOKIE KEY	E FILENAME
		all_cke.bxt File Edit Search Options Help COOKIE KEY COOKIE VALUE DOMAIN PATH COOKIE SET DATE COOKIE EXPIRE PREF ID=eee74e01e1152f24:TM=1148641237:LM=1148641237:S=aIfuB0EXPWg0eR7	E FILENAME
		all_cke.txt Ele Edit Search Options Help COOKIE KEY COOKIE VALUE DPREF ID=eee74e01e1152f24:TM=1148641237:LM=1148641237:S=aIfuB0FXPWgQeR7_ UID (DP21PA72) P582, 4083, 9E64, 0C98ADA74A5E1, updateservice, service	E FILENAME google.c
		Image: Search Options Help COOKIE KEY COOKIE VALUE DOMAIN PATH COOKIE SET DATE COOKIE EXPIRE PREF ID=eee74e01e1152f24:TM=1148641237:LM=1148641237:S=aIfuB0FXPWgQeR7_ UID {DB21BA72-B582-49B3-8E6A-0C8BADA7AA5E} updateservice.sonic.com/	FILENAME google.c 2007-01-
		Image: Search	FILENAME google.c 2007-01-
		Image: Construct of the search options Help COOKIE KEY COOKIE VALUE DOMAIN PATH COOKIE SET DATE COOKIE EXPIRE PREF ID=eee74e01e1152f24:TM=1148641237:LM=1148641237:S=aIfuB0FXPWgQeR7_ UID {DB21BA72-B582-49B3-8E6A-0C8BADA7AA5E} updateservice.sonic.com/ Image: Construct of the search options Help Image: Construct options Help	FILENAME google.c 2007-01-
		all_cke.txt File Edit Search Options Help COOKIE KEY COOKIE VALUE DOMAIN PATH COOKIE SET DATE COOKIE EXPIRE PREF ID=eee74e01e1152f24:TM=1148641237:LM=1148641237:S=aIfuB0FXPWgQeR7_ UID {DB21BA72-B582-49B3-8E6A-0C8BADA7AA5E} updateservice.sonic.com/ Image: Search Options Help Image: Search Options Help URL MODIFIED TIME ACCESS TIME TYPE DIRECTORY HTTP HEADERS FILE	FILENAME google.c 2007-01-
		Image: Search Options Help COOKIE KEY COOKIE VALUE DOMAIN PATH COOKIE SET DATE COOKIE EXPIRE PREF ID=eee74e01e1152f24:TM=1148641237:LM=1148641237:S=aIfuB0FXPWgQeR7_ UID {DB21BA72-B582-49B3-8E6A-0C8BADA7AA5E} updateservice.sonic.com/ Image: Comparison of the part of the pa	FILENAME google.c 2007-01- ENAME Z URL
		Image: Search Options Help COOKIE KEY COOKIE VALUE DOMAIN PATH COOKIE SET DATE COOKIE EXPIRE PREF ID=eee74e01e1152f24:TM=1148641237:LM=1148641237:S=aIfuB0FXPWgQeR7_ UID {DB21BA72-B582-49B3-8E6A-0C8BADA7AA5E} updateservice.sonic.com/ Image: Construction of the point of	FILENAME google.c 2007-01- ENAME Z URL Z URL

	Deive - A I	Forensic	Preview Te	oolset					
<u>File M</u> isc							Help		
Devices Pagefile Windows	Logs Web History	Catalog	Linux Logs	Date Converter	Graphics Viewer	License			
Catalog This application will scan the t Extensions groups, or click on After selecting the file types o and click the SEARCH button.	argeted file system lo the ADVANCED buttor f interest navigate to	oking for t 1 for more the mount	the file types granular cap ted file syste	you select. You r abilities. m you wish to sea	nay select from th rch, choose your o	e top level utput file l	File ocation,		
Copyright @2007 farme	rdude All rights	reserve	ed. For in	clusion in EC-	Council CHFI c	ourse o	nly.	DialogRoy	
Search location	/mnt							Dialogoox	
Output file location	/tmp/Delve/catalog	_results.txt			Documents: Executables:	bat	■ pdf _ p	ps _ ppt _ rtf _ sxc _ sxi . tat i dll i exe i lib i pl i	」sxw 」txt 」xls sh
File Extensions:	□ Documents	⊒ Ex Ad	ecutables	🔟 Graphi	c Graphics: Video: Other (space si Start Date (mm	⊔ bmp ⊔ asf eparated) n/dd/yyyy)	gif jj; avi _ m pst	beg jpg png tiff xpm ov mpeg mpg wmv 	i dentify files by header
			Search		End Date (mm	n/dd/yyyy)	02/20/2007		
						ОК	Ī	Can	cel
					·C	atalogDi	splay		×
		/Docume /Docume	ents and Setti ents and Setti	Filename ngs/kosmo/My Doc ngs/kosmo/My Doc	uments/My Pictures uments/My Pictures	/img001.jpq /img002.jpq	Size 1252604 1303024165	Modified Date Tue Jan 2 15:19:00 2007 GMT? Tue Jan 2 15:53:13 2007 GMT?	Accessed Date Mon Jan 29 19:03:36 20 Mon Jan 29 19:03:36 20
C-Council							All rights	Copyright reserved. Reproduction is	© by <mark>EC-Council</mark> strictly prohibited

		Delve - A l	Forensic	Preview T	oolset				
<u>File M</u> isc								<u>H</u> elp	
Devices Pagefile W	indows Logs	Web History	Catalog	Linux Logs	Date Converter	Graphics Viewe	er License		
Linux Logs This application will so on them in the results Navigate to the mount Copyright @2007	can the targets pop-up windo ted file systen farmerdud	ed file system w. n you wish to s e All rights	ooking for earch, chi reserv	[,] key Linux lo oose your ou ed. For ir	og files. You can ti Itput file location, a nclusion in EC·	hen view files of Ind click the SEA •Council CHFI	interest by o RCH button. COULSE C	clicking only.	
Search locatio Output file loc	on /	p/Delve/linuxlog	ıs_results.t	xt		Br	owse	-	FileDisplay
				Stop				//etc/ii //etc/p //home //home //root/ //var/i //var/i	nit.d/cron bam.d/cron e/farmerdude/.bash_history e/farmerdude/Downloads/root/.bash_history /.bash_history log/cups/access_log log/cups/error_log
19/152700: //usr/src/lin	ux-headers-2.6	i.17-11-generic/	include/co	nfig/jffs2				//var/l //var/l //var/l //var/l	log/installer/syslog log/messages log/syslog log/wtmp
									Close
C-Council								All right	Copyright © by <mark>EC-Co</mark> t is reserved. Reproduction is strictly prohi

Summary

- Linux imparts greater control, flexibility, and power as a forensics tool.
- Linux has a number of simple utilities that make imaging and basic analysis of suspect disks and drives easier.
- Linux cannot identify the last sector on hard drives with odd number of sectors.
- There are several popular Linux tool kits that provide GUI as well for convenience.



"Cinderella got married and lived happily ever after until she got back from her honeymoon and stepped on the scales."



"How can anyone say we're not a green company? We've been dumping green stuff in the river for years!"

> Copyright © by **EC-Council** All rights reserved. Reproduction is strictly prohibited