

Home Page

Title Page



Page 1 of 13

Go Back

Full Screen

Close

Quit

Linux as Forensic platform of choice

Jonathan C. Busey

busey@cs.fsu.edu

February 25, 2003

Overview

- advantages
- common tools
- command concatenation
- specialty software

Home Page

Title Page



Page 2 of 13

Go Back

Full Screen

Close

Quit

Advantages of Linux for forensic investigation

- freely available
- runs on nearly every platform
- forensic examination thrives in open source environment
 - easily controlled environment
 - simply made into a bootable cdrom kit
 - security holes widely published (e.g. NTFS partitions)
- over 30 supported filesystem types:

Advantages (II)

- - Extended Filesystems - ext, ext2, ext3
- Reiser Filesystem - reiserfs
- Amiga Fast Filesystem - affs
- High Performance Filesystem - hpfs (OS/2)
- ISO 9660 Filesystem - iso9660
- Minix Filesystem - Minix
- FAT 16 bit - msdos
- Virtual Fat Filesystem - vfat
- Network Filesystem - NFS
- Novell Filesystem - NCPFS (Novell)
- System V Filesystem - sysv (System V Unix variants)
- Uniform Filesystem - ufs (BSD, Solaris, NeXTStep)
- UMSDOS Filesystem - umsdos (Unix filesystem on DOS)
- linuxswap, adfs, autofs, coherent, cramfs, devpts, efs, hfs, jfs, ntfs, proc, qnx4, romfs, smbfs, tmpfs, udf, xenix, xfs, xiafs, loopback and
- RAID, LVM, “distributed filesystems” (exported over network, e.g.Coda, OpenAFS)

Home Page

Title Page



Page 3 of 13

Go Back

Full Screen

Close

Quit

Home Page

Title Page



Page 4 of 13

Go Back

Full Screen

Close

Quit

Standard tools

- `find`
- `strings`
- `stat`
- `dd (fsgrab)`
- `debugfs`
- `md5sum`

Examples—mounted /dev/mem image

```
Eterm 0.9.2
Eterm Font Background Terminal
busey@sait-selinux:/tmp$ sudo dd if=/dev/mem of=/tmp/mem-$(date +%s).img; mkdir
/tmp/memimage ; sudo mount -t proc -o loop,ro /tmp/mem-*.img /tmp/memimage
917504+0 records in
917504+0 records out
469762048 bytes transferred in 20.671625 seconds (22724970 bytes/sec)
busey@sait-selinux:/tmp$ ls /tmp/memimage/
1      2      219    3374   4      6      execdomains  kmsg      partitions  uptime
158    201    222    3624   4022   7      fb           ksyms     pci         version
161    202    248    3668   4090   8      filesystems  loadavg   scsi
166    203    253    3671   4096   94     fs          locks    self
174    204    255    3672   4108   bus     ide        meminfo  slabinfo
178    205    258    3673   4117   cmdline  interrupts  misc     stat
187    206    259    3674   4121   cpuinfo  iomem     modules  swaps
192    207    260    3699   4363   devices  ioports   mounts   sys
194    214    261    3928   4376   dma      irq       mtrr     sysvipc
197    215    3      3938   5      driver   kcore     net      tty
busey@sait-selinux:/tmp$ du -cm /tmp/mem-1046111772.img
448    /tmp/mem-1046111772.img
448    total
busey@sait-selinux:/tmp$ free -m
              total        used         free      shared    buffers     cached
Mem:           438          433             4           0           0          354
-/+ buffers/cache:           78          359
Swap:          980             2          977
busey@sait-selinux:/tmp$
```

Examples-strings

Home Page

Title Page



Page 6 of 13

Go Back

Full Screen

Close

Quit

```
Eterm 0,9,2
Eterm Font Background Terminal
busey@sait-selinux:~$ strings funnyfile | head
%PDF-1.2
7 0 obj
/Type/Encoding
/Differences[33/exclam/quotedblright/numbersign/dollar/percent/ampersand/quoteri
ght/parenleft/parenright/asterisk/plus/comma/hyphen/period/slash/zero/one/two/th
ree/four/five/six/seven/eight/nine/colon/semicolon/exclamdown/equal/questiondown
/question/at/A/B/C/D/E/F/G/H/I/J/K/L/M/N/O/P/Q/R/S/T/U/V/W/X/Y/Z/bracketleft/quo
tedblleft/bracketright/circumflex/dotaccent/quoteleft/a/b/c/d/e/f/g/h/i/j/k/l/m/
n/o/p/q/r/s/t/u/v/w/x/y/z/endash/emdash/hungarumlaut/tilde/dieresis/Gamma/Delta/
Theta/Lambda/Xi/Pi/Sigma/Upsilon/Phi/Psi/Omega/ff/fi/fl/ffi/ffl/dotlessi/dotless
j/grave/acute/caron/breve/macron/ring/cedilla/germandbls/ae/oe/oslash/AE/OE/Osla
sh/suppress/Gamma/Delta/Theta/Lambda/Xi/Pi/Sigma/Upsilon/Phi/Psi
173/Omega/ff/fi/fl/ffi/ffl/dotlessi/dotlessj/grave/acute/caron/breve/macron/ring
/cedilla/germandbls/ae/oe/oslash/AE/OE/Oslish/suppress/dieresis
255/dieresis]
endobj
10 0 obj
/Encoding 7 0 R
/Type/Font
busey@sait-selinux:~$ strings -fa -t x caseman1 | head
caseman1:      0 GIF89a
caseman1:      1e ;TH-
caseman1:      33 |rkN
caseman1:      94 E7#/&
caseman1:     102 vVQ@
caseman1:     20a N?@.
caseman1:     222 NQ;:76
caseman1:     264 =3iV
caseman1:     278 #)|3Z
caseman1:     285 _`aG
busey@sait-selinux:~$
```

Home Page

Title Page



Page 7 of 13

Go Back

Full Screen

Close

Quit

concatenating commands: **ls**, **stat**, and **find**

```
Eterm 0.9.2
Eterm Font Background Terminal
busey@sait-selinux:~$ find /usr/bin -name $suspiciousfile -exec stat -c Name:" "%n"
"ATime:" "%x" Inode #"%i {} \;
Name: /usr/bin/wipe ATime: 2003-02-24 14:01:19.000000000 -0500 Inode #902644
busey@sait-selinux:~$ find $suspiciouslocs -atime -3 -exec ls -lt {} \;
total 676
-rw-r--r-- 1 busey busey 61163 Feb 24 11:50 alec.jpg
-rw-r--r-- 1 busey busey 29871 Feb 24 11:49 vita.pdf
-rw-r--r-- 1 busey busey 222282 Feb 24 11:49 IDS.pdf
-rw-r--r-- 1 busey busey 370578 Feb 24 11:49 SecOvrVw.pdf
-rw-r--r-- 1 busey busey 222282 Feb 24 11:49 YasinsacDossier/IDS.pdf
-rw-r--r-- 1 busey busey 370578 Feb 24 11:49 YasinsacDossier/SecOvrVw.pdf
-rw-r--r-- 1 busey busey 61163 Feb 24 11:50 YasinsacDossier/alec.jpg
-rw-r--r-- 1 busey busey 29871 Feb 24 11:49 YasinsacDossier/vita.pdf
busey@sait-selinux:~$
```

Home Page

Title Page



Page 8 of 13

Go Back

Full Screen

Close

Quit

Specialty software

TASK • Linux

- Mac OS X
- Open & FreeBSD
- Solaris

Autopsy

chkrootkit <http://www.chkrootkit.org/>

TCT The Coroner's Toolkit

Home Page

Title Page



Page 9 of 13

Go Back

Full Screen

Close

Quit

Autopsy screenshot

Case: sotm15
Host: host1

CASE GALLERY HOST GALLERY HOST MANAGER

mount		name	
/	<input checked="" type="radio"/>	images/dev_hde8.img	details
/boot/	<input type="radio"/> (<input type="radio"/> unalloc)	images/dev_hde1.img	details
/usr/	<input type="radio"/>	images/dev_hde5.img	details
/var/	<input type="radio"/>	images/dev_hde7.img	details

OK ADD IMAGE CLOSE HOST

HELP

VIEW NOTES FILE ACTIVITY TIME LINES IMAGE INTEGRITY

HASH DATABASES

Home Page

Title Page

◀ ▶

◀ ▶

Page 10 of 13

Go Back

Full Screen

Close

Quit

Autopsy screenshot

The screenshot displays the Autopsy forensic tool interface. At the top, there are several tabs: FILE ANALYSIS (active), DATA UNIT, META DATA, IMAGE DETAILS, KEYWORD SEARCH, FILE TYPE, HELP, and CLOSE. Below the tabs is a search icon. The main area is divided into two panes. The left pane contains a tree view with 'ALL DELETED FILES' and 'EXPAND DIRECTORIES' buttons. The right pane shows a table of file analysis results.

Permissions	File Name	Created	Modified	Accessed	Size	Blocks
r/r	lights.exe	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	35600	48
✓ 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
r/r	LMREPL.EXE	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:45 (GMT)	86800	48
✓ r/r	loadfix.com	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	1131	48
r/r	loadfix.com	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	1131	48
✓ r/r	locale.nls	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	145290	48
r/r	locale.nls	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	145290	48

Below the table, there are buttons for 'ASCII (display - report)', 'Strings (display - report)', 'Export', and 'Add Note'. The file type is identified as 'MS-DOS executable (EXE), OS/2 or MS Windows'. The bottom pane shows the 'String Contents Of File: C:/system32/krn1386.exe' with the following text:

```
<Net
KERNSTUB: Error during boot
KERNEL
GPV
/Microsoft Windows Kernel Interface Version 3.10
ROMBIOS
GLOBALUNLOCK
WOWCLOSECOMFORT
GLOBALDOSALLOC
GETPRIVATEPROFILEINT
```

Home Page

Title Page

Navigation arrows

Navigation arrows

Page 11 of 13

Go Back

Full Screen

Close

Quit

Autopsy screenshot

FILE ANALYSIS DATA UNIT META DATA IMAGE DETAILS KEYWORD SEARCH FILE TYPE HELP CLOSE

New Search

2 occurrences of '((jan)|(feb)|(mar)|(ap... were found

126615 (Hex - Ascii)
- string begins at 256 bytes
180485 (Hex - Ascii)
- string begins at 0 bytes

Fragment 126615
Allocated
Group: 15
Pointed to by Inode: [30184](#)
Pointed to by file:
/bin/mt

ASCII (display - report) * Hex (display - report) * Strings (display - report)
File Type: data

Hex Contents of Fragment 126615 (1024 bytes) in images/dev_hde8.img

0	25733a20	57726974	696e6720	6d6f6465	%s: Writing mode
16	20534353	49206d6f	64652070	61676520	SCS I mode page
32	6661696c	65642e0a	00000000	00000000	failed..
48	00000000	00000000	00000000	00000000
64	25733a20	436f6d70	72657373	696f6e20	%s: Compression
80	6d6f6465	206e6f74	20636861	6e676564	mode not changed
96	2e0a0000	00000000	00000000	00000000
112	00000000	00000000	00000000	00000000
128	25733a20	52652d72	65616420	6f662074	%s: Re-read of t
144	68652063	6f6d7072	65737369	6f6e2070	he compression p
160	61676520	6661696c	65642e0a	00436f6d	age failed..Com
176	70726573	73696f6e	206f6e2e	0a00436f	pression on..Co
192	6d707265	7373696f	6e206f66	662e0a00	mpression of...
208	00000000	00000000	00000000	00000000
224	00000000	64ba0408	00000000	00000000 d... ..
240	00000000	00000000	00000000	00000000
256	2449643a	202f7573	72322f75	73657273	\$Id: /usr2/u sers
272	2f6d616b	69736172	612f7372	632f7379	/mak isar a/sr c/sy
288	732f6d74	2d73742d	302e3562	2f6d742e	s/mt -st- 0.5b /mt.
304	63206174	2053756e	20417567	20313620	c at Sun Aug 16
320	30393a35	313a3137	20313939	38206279	09:5 1:17 199 8 by
336	206d616b	69736172	61406b61	692e6d61	mak isar a#ka i.ma

Home Page

Title Page



Page 12 of 13

Go Back

Full Screen

Close

Quit

Autopsy screenshot

The screenshot shows the Autopsy software interface. At the top, there are menu items: CREATE DATA FILE, CREATE TIMELINE, VIEW TIMELINE, VIEW NOTES, HELP, and CLOSE. Below the menu is a navigation bar with a search icon and a date range selector showing "< May 2002 Jul 2002 >". A dropdown menu is open for "Jun" 2002, with an "OK" button. The main area displays a list of files and folders with their timestamps, sizes, permissions, and paths.

Timestamp	Size	Permissions	Attributes	Path
Mon Jun 10 2002 19:33:10	3888	m..	-/rwxrwxrwx 48 0 112-128-4	C:/system32/drivers/NTHANDLE.SYS
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/kml386.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/oemnadepl.inf

Home Page

Title Page



Page 13 of 13

Go Back

Full Screen

Close

Quit

Links to forensics with Linux

- <http://www.atstake.com>
- <http://www.linux-sec.net/Tracking>
- <http://cert.uni-stuttgart.de/forensics>
- <http://www.cerias.purdue.edu/homes/carrier/forensics>