

Linux for computer forensic investigators: «pitfalls» of mounting file systems

Author: Suhanov Maxim

ITDefence.Ru

Introduction

Forensic Linux distribution is a customized Linux distribution that is commonly used to complete different tasks during computer forensics investigations. These distributions are often used to complete the following tasks:

- Quick preview of various data storage devices (for example, to determine installed operating system);
- Creating «bit-to-bit» copies of data storage devices;
- Conducting full analysis of data storage devices.

Some forensic Linux distributions may include network forensics tools and tools for acquiring volatile data from a running system.

Requirements for forensic Linux distributions

Every forensic Linux distribution should satisfy the following requirements:

- Do not allow any writes to evidentiary media without user's permission;
- Boot on most common hardware configurations;
- Use only up to date software and fix all security problems as soon as possible.

Blocking any writes to evidentiary media can be achieved by following these steps:

1. Boot scripts and programs do not mount any file systems, do not activate the swap space and do not activate software RAID arrays on evidentiary media without user's permission;
2. Automounting for all file system types on connected removable devices is disabled.

It is also possible to set all block devices to read-only mode during the boot process to protect evidence from incorrect user actions.

«Pitfalls» of mounting file systems in read-only mode

All Linux distributions allow users to mount a file systems in read-only mode (for example, using the following command: «`mount -o ro /dev/sda1 /mnt/sda1`»). However, mounting file systems in such a way does not guarantee that file system's data will never be altered by the operating system. For example, mounting a damaged Ext3 file system with only «-o ro» option will result in data modification during the recovery process:

```
EXT3-fs: INFO: recovery required on readonly filesystem.
EXT3-fs: write access will be enabled during recovery.
kjournald starting. Commit interval 5 seconds
EXT3-fs: recovery complete.
EXT3-fs: mounted filesystem with ordered data mode.
```

Some forensic Linux distributions may show user a message saying that some data on evidentiary media has been overwritten

In this case some file system metadata gets updated after recovery:

FILE SYSTEM INFORMATION

File System Type: Ext3
Volume Name:
Volume ID: 5962a06aa4c895b5104749a687ccb9e0

Last Written at: Mon Sep 7 17:41:01 2009

Last Checked at: Fri Sep 4 18:39:00 2009

Last Mounted at: Mon Sep 7 17:41:01 2009

Unmounted properly

Last mounted on:

Source OS: Linux

Dynamic Structure

Compat Features: Journal, Ext Attributes, Resize

Inode, Dir Index

InCompat Features: Filetype, **Needs Recovery**,

Read Only Compat Features: Sparse Super, Has

Large Files,

FILE SYSTEM INFORMATION

File System Type: Ext3
Volume Name:
Volume ID: 5962a06aa4c895b5104749a687ccb9e0

Last Written at: Mon Sep 7 18:02:57 2009

Last Checked at: Fri Sep 4 18:39:00 2009

Last Mounted at: Mon Sep 7 17:41:01 2009

Unmounted properly

Last mounted on:

Source OS: Linux

Dynamic Structure

Compat Features: Journal, Ext Attributes, Resize

Inode, Dir Index

InCompat Features: Filetype,

Read Only Compat Features: Sparse Super, Has

Large Files,

Metadata changes after damaged Ext3 file system recovery

Mounting other file systems (for example, Ext4, ReiserFS and XFS) with only «-o ro» option may result in data writes too.

Mounting file systems in a forensically sound manner

To mount various file system types in a forensically sound manner the following methods can be used:

1. Loopback devices in read-only mode: can be switched on using «*ro,loop*» mount options (for example: «*mount -o ro,loop /dev/sda1 /mnt/sda1*»);
2. Block devices for disks and partitions in read-only mode: you can switch any block device to read-only mode by using blockdev tool (for example: «*blockdev --setro /dev/sda1*»);
3. You can disable all journal recovery actions for Ext3 and Ext4 file systems by using «*ext2*» file system type during the mount. Unfortunately, not all file systems support such kind of write protection — for example, there are no working write protection mount options for XFS (however, this was fixed in very recent kernel versions).

It should be noted that mounting damaged Ext3 and Ext4 file systems using these ways is only possible by utilizing alternate superblocks. You can get alternate superblocks locations by using «*mke2fs -n*» command (for example: «*mke2fs -n /dev/sda1*»).

«Pitfalls» of automounting file systems

Automounting of file systems in Linux may occur in following situations: during the boot process and after connecting removable device (for example, USB Flash drive) to a running system.

Removing all entries for file systems on evidentiary media from «*/etc/fstab*» does not guarantee that they will never be mounted during the boot — file systems can be mounted (and modified) during execution of *initrd* scripts or during execution of hardware detection scripts.

Automounting of file systems on removable data storage devices is controlled by special software programs that are properly configured (or disabled) on most forensic Linux distributions.

Testing popular forensic Linux Live CD distributions

I have tested several major forensic Linux Live CD distributions for various mounting issues.

<u>Distribution</u>	<u>Base distribution</u>	<u>Version</u>	<u>Web site</u>
Helix3	Ubuntu	2009R1	http://www.e-fense.com/helix3-download.php
Helix3 (old version)	Knoppix	1.9	(not available)
Helix3 Pro	Ubuntu	2009R2	http://www.e-fense.com/helix3pro.php
SMART Linux (Slackware)	Slackware	2009-04-18	http://asrdata2.com/
SMART Linux (Ubuntu)	Ubuntu	2009-08-18	http://asrdata2.com/
FCCU GNU/Linux Forensic Boot CD	Debian Live	12.1	http://www.lnx4n6.be/
DEFT Linux	Xubuntu	4.2	http://deftlinux.net/
grml	Debian	2009.05	http://grml.org/
SPADA	Knoppix	4	http://www.spada-cd.info/
BackTrack	Ubuntu	4 Pre Release	http://www.remote-exploit.org/backtrack.html
LinEn Boot CD	Knoppix	6.14	http://www.guidancesoftware.com/
CAINE Live CD	Ubuntu	0.5	http://www.caine-live.net/
RIPLinux	Slackware	9.3	http://www.tux.org/pub/people/kent-robotti/looplinux/rip/

Information about tested forensic Linux Live CD distributions

Test results:

- All tested distributions do not automount file systems on connected USB Flash devices;
- Some distributions automatically mount (using only «-o ro» option) file systems on evidentiary media during the boot process: SPADA mounts file systems during execution of hardware detection scripts, other automounting distributions alter the data on evidentiary media during execution of *initrd* scripts.

<u>Distribution</u>	<u>Does the distribution mount file systems during the boot?</u>	<u>What methods does the distribution offer for forensically sound mounts?</u>
Helix3	Yes	Various mount options are used to try to disable the journal on journaling file systems
Helix3 (old version)	No	
Helix3 Pro	Yes	
SMART Linux (Slackware)	No	«ro,loop» mount options (via SMART interface)
SMART Linux (Ubuntu)	Yes	
FCCU GNU/Linux Forensic Boot CD	Yes	— (the distribution does not offer any methods to mount file systems in a forensically sound manner)
DEFT Linux	Yes	
grml (forensic mode)	Yes, but all block devices are set to read-only mode (no data modification)	
SPADA	Yes	
BackTrack (forensics mode)	Yes	
LinEn Boot CD	No	
CAINE Live CD	Yes	
RIPLinux	No	—

Test results

Testing automatic swap space activation

The following distributions were tested for automatic swap space activation during the boot (only distributions that passed previous test): Helix3 (old version), SMART Linux (Slackware), grml, LinEn Boot CD and RIPLinux.

None of these distributions activate the swap space on evidentiary media during the boot process.

Conclusions

I have found that some forensic Linux Live CD distributions do mount and recover several file system types during the boot process. However, I didn't test Linux RAID and LVM activation issues, so it is recommended to use distributions that do not activate software RAID arrays and LVM without users' permission (e.g. grml).