

# Linux для судебных экспертов: «подводные камни» монтирования файловых систем

Автор: Суханов Максим

ITDefence.Ru

## Введение

Судебный дистрибутив Linux — дистрибутив Linux, предназначенный для решения широкого спектра задач при проведении судебных компьютерных и компьютерно-технических экспертиз. Как правило, данные дистрибутивы используются для решения следующих задач:

- Предварительное исследование носителей данных (например, для определения установленной операционной системы);
- Создание точных копий исследуемых носителей данных;
- Полное исследование носителей данных, включая, например, поиск файлов по ключевым словам и анализ журналов работы операционной системы.

Кроме того, судебные дистрибутивы Linux могут включать в себя программы для исследования сетевого трафика и копирования энергозависимых данных (например, содержимого оперативной памяти) с работающей системы.

## Требования к судебным дистрибутивам Linux

Для любого судебного дистрибутива Linux можно выделить следующие требования:

- Блокировка любых попыток записи на исследуемые носители данных;
- Возможность успешной загрузки практически на любом аппаратном обеспечении;
- Регулярное исправление ошибок и уязвимостей в используемом программном обеспечении.

Блокировка любых попыток записи на исследуемый носитель данных может быть реализована при соблюдении следующих требований:

1. Загрузочные скрипты и программы не монтируют какие-либо файловые системы без согласия пользователя, активации пространства подкачки (англ. *swap space*) на исследуемых носителях данных не происходит, активации программных RAID на исследуемых носителях данных не происходит;

2. Автоматическое монтирование любых файловых систем отключено.

При этом возможен перевод всех блочных устройств носителей данных в режим «только чтение» на начальном этапе загрузки операционной системы для защиты от некоторых действий пользователя (например, монтирования файловой системы на исследуемом носителе данных в режиме «чтение-запись»).

## Особенности монтирования файловых систем в режиме «только чтение»

Все дистрибутивы Linux предоставляют пользователям возможность монтирования исследуемых файловых систем в режиме «только чтение» (например, с помощью команды

«`mount -o ro /dev/sda1 /mnt/sda1`»). К сожалению, данный режим не гарантирует неизменность данных на исследуемой файловой системе. Например, в случае монтирования поврежденных файловых систем Ext3 будет произведено их восстановление с использованием журнала файловой системы:

```
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.
```

*Пользователи некоторых судебных дистрибутивов Linux могут увидеть сообщение о том, что система только что перезаписала часть данных на исследуемой файловой системе*

При этом происходит обновление даты и времени последней записи данных файловой системы:

#### 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,

*Изменение даты и времени последней записи данных файловой системы  
Ext3 после автоматического восстановления в ходе монтирования*

Аналогичными особенностями обладают процессы монтирования и размонтирования других файловых систем, например, Ext4 (восстановление поврежденной файловой системы при монтировании) и XFS (запись данных при размонтировании).

## **Монтирование файловых систем в гарантированном режиме «только чтение»**

Для монтирования различных типов файловых систем в режиме «только чтение» с гарантией неизменности данных можно использовать несколько подходов:

1. Устройства обратной связи в режиме «только чтение»: включаются использованием при монтировании опций «`ro,loop`» (пример команды: «`mount -o ro,loop /dev/sda1 /mnt/sda1`»);
2. Блочные устройства носителей данных и файловых систем в режиме «только чтение»: перевести блочное устройство в режим «только чтение» можно программой `blockdev`

(пример команды: «*blockdev --setro /dev/sda1*»);

3. Для файловых систем Ext3 и Ext4 можно при монтировании указывать тип файловой системы «*ext2*» и опцию монтирования в режиме «только чтение» — в этом случае восстановления файловой системы не будет. К сожалению, не все файловые системы поддерживают полное отключение записи подобным образом — для файловой системы XFS не существует каких-либо опций для отключения записи данных в процессе размонтирования (однако, запись данных можно заблокировать с помощью описанных выше методов).

Стоит отметить, что монтирование поврежденных файловых систем Ext3 и Ext4 во всех вышеуказанных случаях возможно лишь при использовании альтернативных суперблоков, расположение которых можно узнать с помощью команды «*mke2fs -n*» (пример команды: «*mke2fs -n /dev/sda1*»).

## Особенности автоматического монтирования файловых систем

Автоматическое монтирование файловых систем в Linux возможно в двух ситуациях: в процессе загрузки операционной системы и при подключении нового устройства (например, устройства USB Flash) к работающей системе.

Отсутствие каких-либо записей об исследуемых файловых системах в файле «*/etc/fstab*» не является гарантией того, что в процессе загрузки операционной системы данные файловые системы не будут примонтированы — монтирование файловых систем с последующим изменением данных может произойти в процессе выполнения скриптов *initrd* или в процессе выполнения скриптов обнаружения оборудования.

Автоматическое монтирование файловых систем на подключаемых к работающей системе сменных носителях данных производится специальным программным обеспечением, которое, как правило, отсутствует (или отключено) в судебных дистрибутивах Linux.

## Тестирование распространенных судебных дистрибутивов Linux

Для тестирования были выбраны следующие распространенные судебные дистрибутивы Linux:

<u>Название дистрибутива</u>	<u>На основе дистрибутива</u>	<u>Версия</u>	<u>Сайт</u>
Helix3	Ubuntu	2009R1	<a href="http://www.e-fense.com/helix3-download.php">http://www.e-fense.com/helix3-download.php</a>
Helix3 (устаревшая версия)	Knoppix	1.9	(отсутствует на сайте производителя)
Helix3 Pro	Ubuntu	2009R2	<a href="http://www.e-fense.com/helix3pro.php">http://www.e-fense.com/helix3pro.php</a>
SMART Linux (Slackware)	Slackware	2009-04-18	<a href="http://asrdata2.com/">http://asrdata2.com/</a>
SMART Linux (Ubuntu)	Ubuntu	2009-08-18	<a href="http://asrdata2.com/">http://asrdata2.com/</a>

FCCU GNU/Linux Forensic Boot CD	Debian Live	12.1	<a href="http://www.lnx4n6.be/">http://www.lnx4n6.be/</a>
DEFT Linux	Xubuntu	4.2	<a href="http://deftlinux.net/">http://deftlinux.net/</a>
grml	Debian	2009.05	<a href="http://grml.org/">http://grml.org/</a>
SPADA	Knoppix	4	<a href="http://www.spada-cd.info/">http://www.spada-cd.info/</a>
BackTrack	Ubuntu	4 Pre Release	<a href="http://www.remote-exploit.org/backtrack.html">http://www.remote-exploit.org/backtrack.html</a>
LinEn Boot CD	Knoppix	6.14	<a href="http://www.guidancesoftware.com/">http://www.guidancesoftware.com/</a>
CAINE Live CD	Ubuntu	0.5	<a href="http://www.caine-live.net/">http://www.caine-live.net/</a>
RIPLinux	Slackware	9.3	<a href="http://www.tux.org/pub/people/kent-robotti/looplinux/rip/">http://www.tux.org/pub/people/kent-robotti/looplinux/rip/</a>

Таблица 1. Некоторые распространенные судебные дистрибутивы Linux

Результаты тестирования вышеуказанных судебных дистрибутивов Linux:

- Ни один дистрибутив не монтирует файловые системы на подключаемых носителях USB Flash автоматически;
- Некоторые дистрибутивы автоматически монтируют файловые системы на исследуемых носителях данных в процессе загрузки операционной системы: в связи с этим, возможно автоматическое восстановление некоторых поврежденных файловых систем (например, Ext3). Дистрибутивы, монтирующие файловые системы автоматически в процессе загрузки (за исключением SPADA), производят монтирование в процессе выполнения скриптов *initrd*; SPADA монтирует файловые системы в процессе автоматического поиска подключенного оборудования.

<u>Название дистрибутива</u>	<u>Автоматическое монтирование ФС на подключенных НЖМД в процессе загрузки</u>	<u>Способ монтирования ФС с обеспечением неизменности данных</u>
Helix3	Да	Монтирование с опциями отключения журнала ФС
Helix3 (устаревшая версия)	Нет	
Helix3 Pro	Да	
SMART Linux (Slackware)	Нет	Опции «ro,loop» (через интерфейс SMART)
SMART Linux (Ubuntu)	Да	

FCCU GNU/Linux Forensic Boot CD	Да	—  (ФС монтируются пользователем через командную строку)
DEFT Linux	Да	
grml (режим <i>forensic</i> )	Да, но записи каких-либо данных не происходит (программная блокировка записи)	
SPADA	Да	
BackTrack (режим <i>forensics</i> )	Да	
LinEn Boot CD	Нет	Монтирование с опциями отключения журнала ФС
CAINE Live CD	Да	
RIPLinux	Нет	—

Таблица 2. Результаты тестирования судебных дистрибутивов Linux на предмет автоматического монтирования ФС в процессе загрузки

## Тестирование автоматической активации пространства подкачки

Тестирование автоматической активации пространства подкачки проводилось для следующих дистрибутивов: Helix3 (устаревшая версия), SMART Linux (Slackware), grml, LinEn Boot CD и RIPLinux.

В процессе тестирования вышеуказанных дистрибутивов Linux автоматической активации пространства подкачки не происходило.

## Выводы

В ходе тестирования было обнаружено, что не все судебные дистрибутивы Linux обеспечивают неизменность данных на исследуемых носителях. Установлено, что неизменность данных в процессе загрузки и при подключении сменных носителей USB Flash обеспечивают следующие судебные дистрибутивы: Helix3 1.9 (устаревшая версия; не поддерживается), SMART Linux на основе Slackware (коммерческий дистрибутив; доступна бесплатная демо-версия), grml (дистрибутив, поддерживаемый сообществом), LinEn Boot CD (коммерческий дистрибутив, доступный пользователям EnCase) и RIPLinux (дистрибутив, предназначенный для восстановления данных).

На данный момент не проводилось исследование проблемы автоматического монтирования в режиме «чтение-запись» некоторых устройств (например, карт флеш-памяти) в последних версиях дистрибутива Helix3 (включая версию Pro), не проводилось исследование методов обеспечения неизменности данных при работе с программными RAID (Linux RAID) и файловыми системами на томах LVM. В связи с этим автор рекомендует использовать судебные дистрибутивы Linux, не активирующие программные RAID и тома LVM без согласия пользователя, например, grml.