

# Введение в Linux для специалистов в области компьютерной безопасности и судебных экспертов



Ernest Baca

[ebaca@linux-forensics.com](mailto:ebaca@linux-forensics.com)

[www.linux-forensics.com](http://www.linux-forensics.com)

# Этапы развития Linux

- n В 1991 аппаратных средств персональных компьютеров хватало только на функционирование ОС DOS. Другой альтернативы не было, т.к. цены на Macintosh Apple были астрономические.
- n Другим миром операционных систем компьютеров был мир Unix. Unix был более дорог и, поэтому, был не доступен пользователям персональных компьютеров. Исходный текст Unix, когда-то переданный Bell Labs университетам, держался в тайне.
- n Решение, которое маячило на горизонте - MINIX. Эту ОС самостоятельно написал Эндрю С. Тейннбаум (Andrew S. Tanenbaum) - голландский профессор, который хотел продемонстрировать студентам работу операционной системы. Она была разработана для процессоров Intel 808.

# Этапы развития Linux(продолжение)

- n MINIX не была лучшей операционной системой, но ее несомненным преимуществом был открытый исходный текст.
- n В 1991 Лайнус Бенедикт Торвальдс (Linus Benedict Torvalds) был студентом 2 курса Университета Информатики в Хельсинки. Торвальдс любил эксплуатировать компьютеры на грани их возможностей. ОС , которая отвечала бы его требованиям, у него не было. MINIX был хорош, но, тем не менее, это была операционная система для студентов, разработанная как инструмент обучения.
- n В то же самое время, программисты во всем мире были очень вдохновлены проектом GNU Ричарда Столлмана (Richard Stallman). Это движение стартовало в 1983 и обеспечивало бесплатное качественное программное обеспечение (GNU – это понятие, который фактически означает 'GNU - не UNIX').



# Этапы развития Linux(продолжение)

- n 25 августа 1991 Лайнусом Торвальдсом было послано историческое сообщение в MINIX конференции.
- n Лайнус не верил в, что Linux способна произвести большие изменения в компьютерном мире.
- n Linux версии 0.01 была выпущена к середине сентября 1991 и помещена в сети Internet. Энтузиасты скачали эту версию, внесли в нее свои изменения и отправили их Лайнусу. Linux 0.02 вышла 5-го октября.
- n Это было началом нового поколения операционных систем.

# Зачем изучать Linux экспертам?

- n Linux - одна из наиболее быстро развивающихся операционных систем. Экспертам все чаще приходится сталкиваться с Linux системами.
- n В сети Internet работает большое количество Linux систем. Изучение основ Linux поможет экспертам эффективнее расследовать киберпреступления.
- n Хакеры, в своем большинстве, не используют Windows системы. Изучение основ Linux поможет специалистам эффективнее опрашивать свидетелей и допрашивать подозреваемых.
- n Изучение Linux поможет эксперту при реконструкции места преступления, совершенного с участием Linux-системы.

# Типичные представления о Linux

- n Linux сложна в изучении!
- n Linux – только для компьютерных гуру!
- n Linux сложна при установке!
- n Если Вы знаете Linux, Вы - КОМПЬЮТЕРНЫЙ БОГ!
- n Linux – плохой предмет для исследования.
- n Linux управляется только из командной строки и, поэтому, трудна!
- n Вы должны знать все команды Linux.



# ОСНОВЫ Linux

- n Версии Linux – это версия ядра
- n Linux - системы распространяются как дистрибутивы.
- n Дистрибутив - совокупность программного обеспечения, которое выполняется на ядре Linux.
- n Различные дистрибутивы работают по - разному (например, файловая структура может быть различной)
- n Все дистрибутивы доступны для загрузки из сети Internet.
- n Исходный текст ядра доступен для всех дистрибутивов Linux.

# Дистрибутивы Linux

- n Redhat - наиболее популярный среди масштабных систем
- n Debian – множество дистрибутивов основаны на нем
- n Mandrake - очень популярный дистрибутив
- n Suse – дистрибутив с богатым программным обеспечением.
- n Slackware - наиболее популярный среди хакеров. Отличается недружелюбным интерфейсом
- n Gentoo – дистрибутив, постепенно заменяющий Slackware
- n Многие, многие другие!



# Экспертиза



Linux - систем

# Первые этапы экспертного исследования

- n Создание образа носителя
- n Аутентификация образа
- n Анализ данных
- n Представление результатов исследования в удобном виде

# Чем Linux удобен для экспертов?

Linux имеет встроенные средства создания образа носителя, его аутентификации, поиска по нему, и даже средство гарантированного удаления данных!



# Выгоды от Linux как инструмента эксперта

- n Все, включая аппаратные средства, представляется как файловая система
- n Поддержка большого числа файловых систем (многие из которых не поддерживаются windows)
- n Возможность подключения отдельных файлов
- n Возможность анализировать систему с минимальным воздействием (нет необходимости в специальных аппаратных средствах или программном обеспечении, блокирующих носитель информации от записи)
- n Возможность перенаправлять стандартный вывод (группа команд в одной строке)
- n Возможность анализа исходного кода большинства утилит
- n Возможность создавать самозагружаемые носители
- n Linux бесплатна, как и ее исходный текст
- n Инструментальные средства бесплатные или дешевые

# Основные вопросы!

- n В Вашем программном обеспечении есть ошибки?
- n Что на самом деле делает ваше программное обеспечение, когда Вы с ним работаете?
- n Можете ли Вы проверить результаты своей деятельности?

# Инструментальные средства Linux

- n TASK & Autopsy - инструмент, используемый при восстановлении данных, а также применяемый для экспертизы данных [www.atstake.com](http://www.atstake.com)
- n Foremost - инструмент извлечения данных. [Foremost.sourceforge.net](http://Foremost.sourceforge.net)
- n Corners Toolkit - инструмент для восстановления данных [www.porcupine.org/forensics/tct.html](http://www.porcupine.org/forensics/tct.html)
- n Maresware – программные средства для компьютерного эксперта. [www.dmares.com](http://www.dmares.com)
- n SMART Forensic Software – базовая система, имеющая графический интерфейс пользователя, используемая для сбора, поиска, расчета контрольных сумм и экспертизы данных, находящихся на носителе информации, а так же составления отчетов. [www.asrdata.com](http://www.asrdata.com)
- n Glimpse – инструмент индексации и поиска данных. [www.glimpse.cs.arizona.edu](http://www.glimpse.cs.arizona.edu)



# Самозагружаемые дистрибутивы Linux

- n Bootable Business Card – образ загрузочного компакт-диска с Linux. [www.lnx-bbc.org](http://www.lnx-bbc.org)
- n PLAC – переносимая версия Linux [sourceforge.net/projects/plac](http://sourceforge.net/projects/plac)
- n F.I.R.E - другой самозагружаемый компакт-диск Linux. [Fire.dmzs.com](http://Fire.dmzs.com)
- n Knoppix – базовый графический интерфейс пользователя Linux для самозагружаемых компакт-диск. [www.knoppix.de](http://www.knoppix.de)

# Полезные Ссылки Linux

- n <http://Ohiohtcia.org/linuxintro-1.8.1.pdf> - Введение в Linux для экспертов.
- n <http://www.crazytrain.com/> - Сайт, посвященный экспертам, занимающихся производством КТЭ
- n <http://www.linux.org/> - Хороший ресурс Linux для изучения
- n <http://www.linux-directory.com/> - Другой хороший Linux ресурс
- n <http://www.linux-forensics.com/> - Мой сайт, посвященный использованию Linux как инструмента для эксперта (в настоящее время на реконструкции).

# СПАСИБО ЗА ВНИМАНИЕ!

Перевод: Фомичев Александр Николаевич

Корректоры: Михайлов Игорь Юрьевич

Капинус Ольга Валерьевна