хачим сотовые телефоны с линухом на борту

крис касперски ака мыщъх, no-email

ворвавшись на мобильные платформы, по прошествии нескольких лет "промышленной" эксплуатации Linux чувствует себя вполне уверенно, успешно конкурируя с Symbian OS/Windows CE, и общая в свою верю все больше и больше производителей сотовых телефонов, число которых стремительно растет. Linux на мобильном это уже не экзотика, а реальность, насчитывая сотни разнообразных моделей, которые любой желающий может хачить, ковыряясь в недрах ядра и наращивая его функционал, что безумно интересно, но, к сожалению, в среде отечественных хакеров практически неизвестно. мыщъх надеется, что своей статьей он сорвет пелену мрака, подтолкнув креативных кодокопателей к исследовательской деятельности

введение

Сотовые телефоны первого поколения представляли "вещь в себе" и не позволяли устанавливать никакого программного обеспечения сверх того, что уже зашито в них производителем. Потом появились Java-мидлеты (игры, органайзеры, etc) но сильно лучше от этого не стало. Тем временем, по своей аппаратной мощности телефоны вплотную приблизились к ПК конца 90х, существенно потеснив наладонники (они же PDA).

Современный сотовый телефон (а точнее, смартфон) представляет собой полноценный компьютер с операционной системой (Symbin OS или Windows CE), поддерживающей развитый набор API-функций и за счет виртуальной Java-машины абстрагирующей программиста от архитектурных особенностей конкретного железа. Так в чем же проблема? Качай SDK и программируй! Хочешь — под Java-машину, хочешь — под "нативный" процессор (благо мобильные оси это позволяют).

Вот только Java-машина тормозит нипадецики, а "нативные" программы страдают хронической непереносимостью, работая на строго определенных моделях, что сужает круг потенциальных пользователей до размеров черной дыры (ну или нейтронной звезды — если это популярная платформа).

Исходных текстов операционной системы нет — как ее хачить? Да и прямого доступа к электронной оснастке телефона она не дает. Короче, сотовые телефоны — это не для хакеров. Но с выходом Motorola A760 ситуация изменилась…

орлята учатся летать

Аппарат Motorola A760, разработанный в 2003 году на базе процессора ARM7, стал первым сотовым телефоном, оснащенной специальной версией Linux'a, адаптированной под мобильные платформы. Собственно говоря, от Linux'a там только сильно урезанное ядро серии 2.4.x/2.6.x, библиотека glibc, драйвера для управления встроенным оборудованием и чисто сотовое программное обеспечение (аудио-кодеки, стек GSM протоколов: RF6003 – fractional-n RF synthesizer, RF2722 – GPRS/EDGE capable receiver, RF3144 – quad-band power amplifier, etc). Ну и, естественно, привычный графический интерфейс с иконками, записными книжками, органайзерами, играми и прочей мишурой.

Внешне (с потребительной точки зрения) телефон ничем не отличается от пестрой армии своих собратьев и большинству пользователей (не сильно продвинутых в техническом плане), откровенно говоря наплевать, какая там ось, главное — это интерфейс. Так в чем же преимущества Linux перед конкурентами?

Во-первых, открытый код, разрабатываемый межпланетным OpenSource сообществом, не только не требует лицензионных отчислений, но и намного более стабилен, поскольку исходные тексты изучает огромное количество людей (только с одного зеркала на SourceForge последнюю версию ядра скачало свыше полутора тысяч человек!).

Во-вторых, известная своими скоромными системными требованиями Linux, отличается быстрой загрузкой и высокой реакционной способностью телефона, который не тормозит, да и к тому же потребляет намного меньше энергии, на что обращают внимание даже блондинки, не говоря уже о продвинутых пользователях.

В-третьих, системные вызовы Linux'a давно стандартизированы и под него написано огромное количество программного обеспечения, перенос которого на новые мобильные

платформы осуществляется простой перекомпиляцией (ну, пускай не без адоптации, но это совсем не тоже самое, что полное переписывание кода с нуля). Что касается хакеров, теперь можно зарядить телефон боевой амуницией и грабить Bluetooth-трафик, создавать ICMP-тоннели для бесплатной связи по GPRS и… делать много других интересных вещей.

В-четвертых, код ядра легко модифицировать по своему усмотрению, наращивая функциональность телефона или разблокируя функции, заблокированные производителем по тем или иным соображением. Допустим, в телефоне на аппаратном уровне реализован режим turbo-зарядки батарей, но как следует не отлажен и потому отложен до лучших времен. Или же производитель не хочет, чтобы модели начального уровня конкурировали со своими старшими собратьями…

В-пятых, в сотовых телефонах (вот ужас!) нет BIOS и заботу по инициализации оборудования берет на себя ядро, выставляющее тактовые частоты процессора, тайминги оперативной памяти, режимы работы дисплее. Ну а какой русский не любит быстрой езды, тьфу, разгона процессоров?! Да-да!!! Теперь процессоры сотовых телефонов тоже можно разгонять! Зачем?! Ну вот, допустим, видео при просмотре слегка тормозит, но стоит чуть-чуть повысить тактовую частоту как тормоза исчезнут. Ну разве не прелесть?!

В-шестых, в Linux нет (и не будет) ни DRM, ни прочей дряни, загрязняющей информационное пространство и отравляющее пользователем жизнь. Открытый код не позволяет защищать цифровой контент, поскольку ничего не стоит отломать защиту, перекомпилировать ядро, залить его в телефон и наслаждаться своей любимой музыкой или клипами.

стандартизация мобильной версии Linux'a

Скачать исходные тексты ядра Motorola A760 можно как с официального сайта (https://opensource.motorola.com/sf/sfmain/do/home), так и с Кузни (http://sourceforge.net/project/showfiles.php?group_id=116309). Официальный сайт, естественно, предпочтительнее и вряд ли даже стоит объяснять почему.

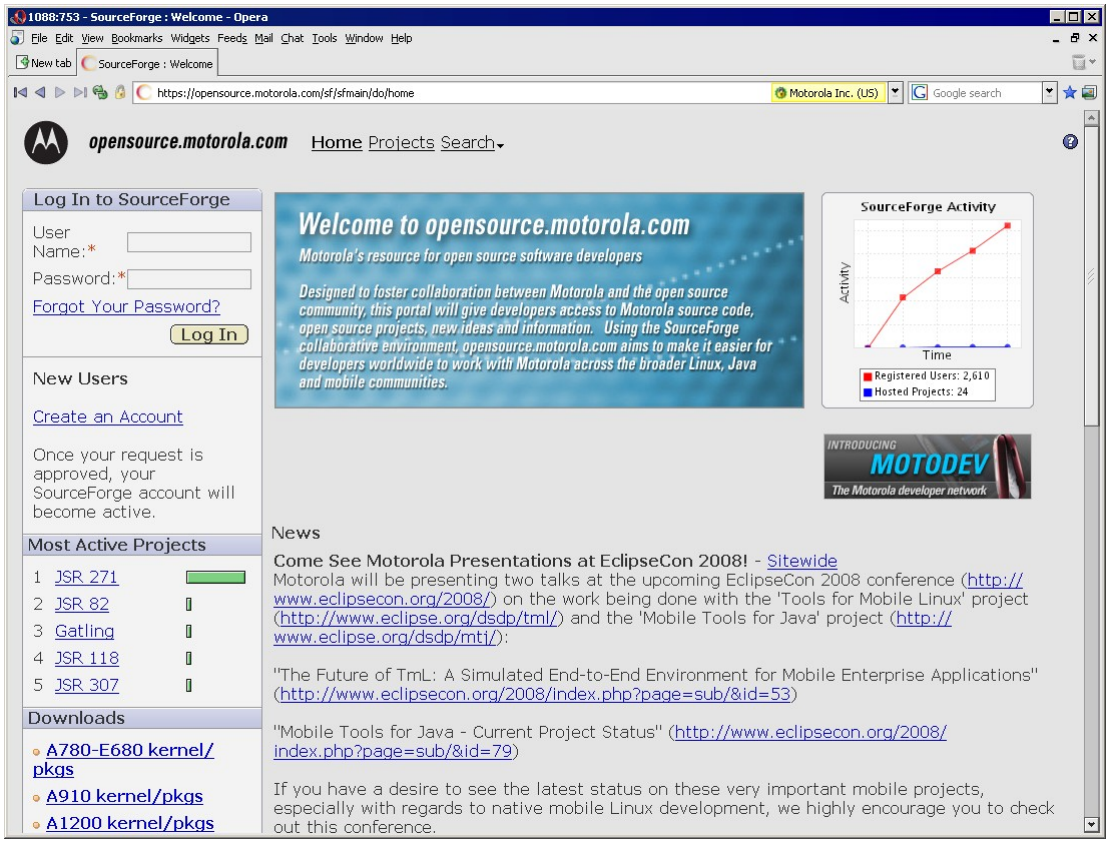

Рисунок 1 компания Motorola раздает исходные тексты Linux-ядра, используемого ее в своих телефонах, всем желающим

Но ядро — это еще не все, далеко не все. Помимо него требуются драйвера и куча других моделей, часть из которых специфичны для каждой модели, а часть — системнонезависимы. То есть они станут системнонезависимыми, когда будет выработан единый стандарт, которому станут следовать как производители железа, так и разработчики софта.

Рисунок 2 Motorola Rokr E6 — сотовый телефон с Linux'ом на борту

Проект OpenEZX (http://openezx.org/) в ходе которого было создано программное обеспечение для телефонов Motorola A728, A760, A768, A780, A910, A1200, E680, E680i, E680g, E690, Rokr E2, Rokr E6, Rizr Z6, Razr 2 и i876. На сервере компании (http://wiki.openezx.org/Main_Page) выложено описание аппаратной части, исходные тексты ядра и остальных компонентов, распространяющихся по лицензии GPL, бинарные сборки (для самых ленивых), загрузчик, позволяющий заливать перекомпилированное ядро в телефон и управлять параметрами загрузки, а так же инструментарий для разработки своих собственных программ, созданный на основе кросс-среды от Дэна Кегела (Dan Kegel) — http://wiki.openezx.org/Crosscompile.

Как нетрудно заметить, проект OpenEZX, несмотря на свою открытость, замыкается на продукции компании Motorola и не находит применения за ее границами.

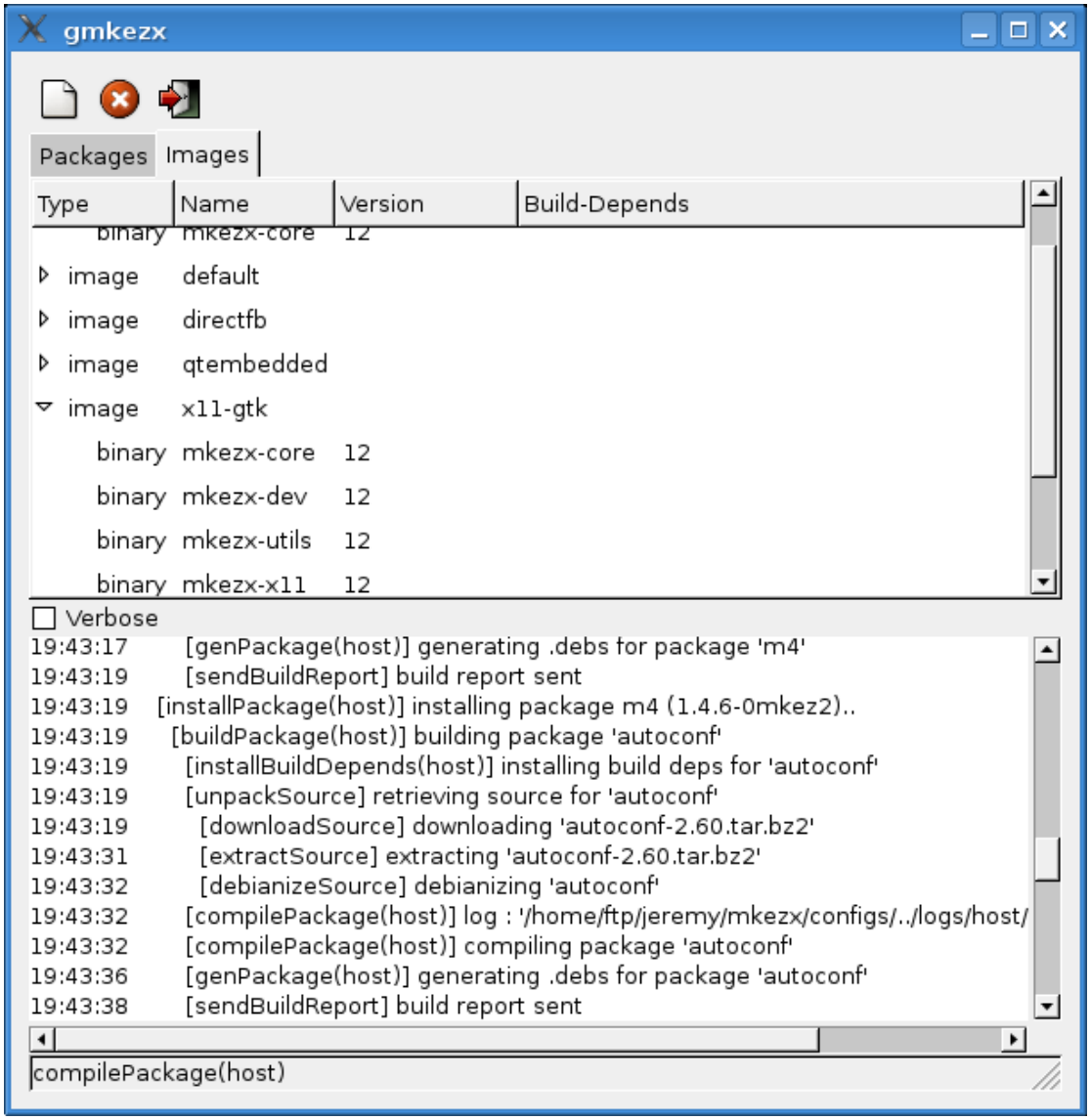

Рисунок 3 среда разработки приложений для телефонов, основанных на OpenEZX

Проект OpenMoko (http://www.openmoko.org), впервые реализованный на платформе FIC Neo1973, оказался более удачным и в настоящее время используется на Motorola E680i/ A780 OM2007.2/ A1200E OpenMoko 2007.2, Treo 650, Palm TX, а так же некоторых других аппаратах, список которых постоянно расширяется.

Рисунок 4 сотовый телефон FIC Neo1973 с мобильной версий Linux'а, основанной на проекте OpenMoko

На главной страницы проекта http://projects.openmoko.org/ выложено не только ядро, но и большое количество исходных текстов различных мобильных приложений (например, GPRS locator) и утилит для разработчиков, самой полезной из которых был и остается универсальный загрузчик U-boot loader (http://wiki.openmoko.org/wiki/U-boot), разработанный невероятно креативным программистом Гарольдом Вельтом (Harald Welte) у которого есть свой собственный блок с огромным количеством технической информации http://laforge.gnumonks.org/weblog/index.html, где, в частности, можно найти инструкцию по разблокированию заблокированных аппаратных возможностей.

Загрузчик не только для обновления ядра, но и заливки "нативных" Linux-приложений самостоятельной разработки. Сами же приложения создаются при помощи инструментария, предоставленного поставщиками мобильных версий Linux (впрочем, при желании можно обойтись и штатным компилятором GCC, поскольку Linux он и в Африке Linux).

Рисунок 5 универсальный загрузчик U-boot loader в действии

телефоны с Linux'ом "левой" сборки

Стандарты — это, конечно, замечательно, но некоторые производители предпочитают использовать свои собственные, ни с чем не совместимые, решения, что вызвано не столько снобизмом, сколько сыростью и неразвитостью существующих стандартов. Естественно, хачить такие телефоны очень сложно и от их приобретения лучше воздержаться.

В первую очередь хотелось бы обратить внимание на компанию ImCoSys (http://www.imcosys.com/), выпускающую мобильные устройства на базе Linux, но зажимающую исходные тексты, чем вероломно нарушающую лицензию GPL, отправляя все претензии от сообщества Open Source прямиком в /dev/nul. Даже если оставить юридические разборки в стороне, пользы от Linux'а без исходных текстов — никакой. И хачить его невозможно.

Аппараты Grundig Dreamphone G500i/B700/U900 так же основаны на Linux, но исходных текстов что-то не наблюдается. Ну как их прикажете хачить?!

Аппараты ROAD GmbH: S101, S101K, L101 (http://www.road-gmbh.de/) работают под управлением самостоятельно адоптированной версии Linux с ядром версии 2.6, но ни исходных текстов, ни инструментов для разработки программ, ни какой бы то ни было документации на сайте компании нет.

Аппараты Neuf Twin Tact E28/E2831/GW1/GW3 используют Linux под эгидой своего собственного проекта OpenTwin (http://www.opentwin.org/) с открытыми исходными текстами, документацией и средами разработки, однако, поддержки остальных производителей он не получил. Motorola оказалась единственной компаний, выпустившей модель телефона на основе OpenTwin – A910i и эта модель оказалась одна. Других не последовало. Во всяком случае пока.

Поэтому, приобретая телефон с Linux'ом, необходимо заблаговременно убедиться, что производитель придерживается лицензии GPL и не скрывает исходные коды от потребителей. В принципе, исходные тексты ядра не так уж и важны. Если ядро не слишком сильно покоцано и номера системных вызовов не изменены (а обычно все так и есть), то разработка собственных приложений не станет большой проблемой, однако, прежде чем написать "hello, world!" придется выполнить объемный ресерч, дизассемблировав ядро и разобравшись с архитектурой конкретной мобильной платформы, а так же сконструировать свой собственный загрузчик. Настоящие хакеры не бояться трудностей, ибо трудности нас только закаляют, ну а дизассемблер — это вообще основной инструмент Windows-хакеров, которые весьма плодотворно исследуют недра операционной системы. Отсутствие исходных текстов их не останавливает. Однако, начинать лучше всего с хорошо изученных аппаратов с открытыми исходными текстами и вменяемой документацией, собравших вокруг себя целое сообщество хакеров, к которым всегда можно обратиться за помощью, если что-то непонятно или не клеится. Как, вероятно, уже успел заметить читатель, наиболее перспективной в этом плане является линейка телефонов Motorola (и это не реклама!).

>>> врезка поставщики мобильных версий Linux'а

Некоторые производители телефонов самостоятельно адоптируют ядро Linux'а (обычно зажимая при этом исходные тексты и не предоставляя никакой поддержки для создателей независимого ПО), но большинство компаний предпочитает использовать мобильные версии Linux'а от сторонних разработчиков, экономя свое собственные силы и время.

Основных поставщиков Linux'а на мобильный рынок всего два. Корейская фирма Mizi Research Incorporated (http://www.mizi.com/) главным потребителем продукции которой является корпорация Samsung Electronics, уже выпустившая телефоны Samsung SCH-i839/SCH-i858/SCH-i819/SCH-i519, вполне пригодные для хака и прочих издевательств.

Адоптированная версия Linux'а носит гордое название PRISM (хвост его знает, что оно обозначает, но звучит гордо), распространяясь по лицензии GPL. Вместе с исходными текстами ядра с FTP сервера компании можно свободно (и бесплатно!) скачать SDK и эмулятор. Ну, эмулятор vs. живой телефон — это дело вкуса, а вот SDK это очень даже хорошо!

Заходим на http://www.mizi.com/index.php/developers# и качаем. Документация лежит на http://www.mizi.com/docs/products/Prizm3_whitepaper_EN.pdf, а по соседству с ней и спецификации — http://www.mizi.com/index.php/prizm-specifications.

SDK включает в себя кросс-компилятор, заголовочные файлы и IDE, внешне похожую на популярную графическую среду разработки Eclipse 3.0, но в отличии от последней, работающей не только в Linux, но и под Windows. Поддерживаются следующие языки программирования: Си, Си++ и Питон.

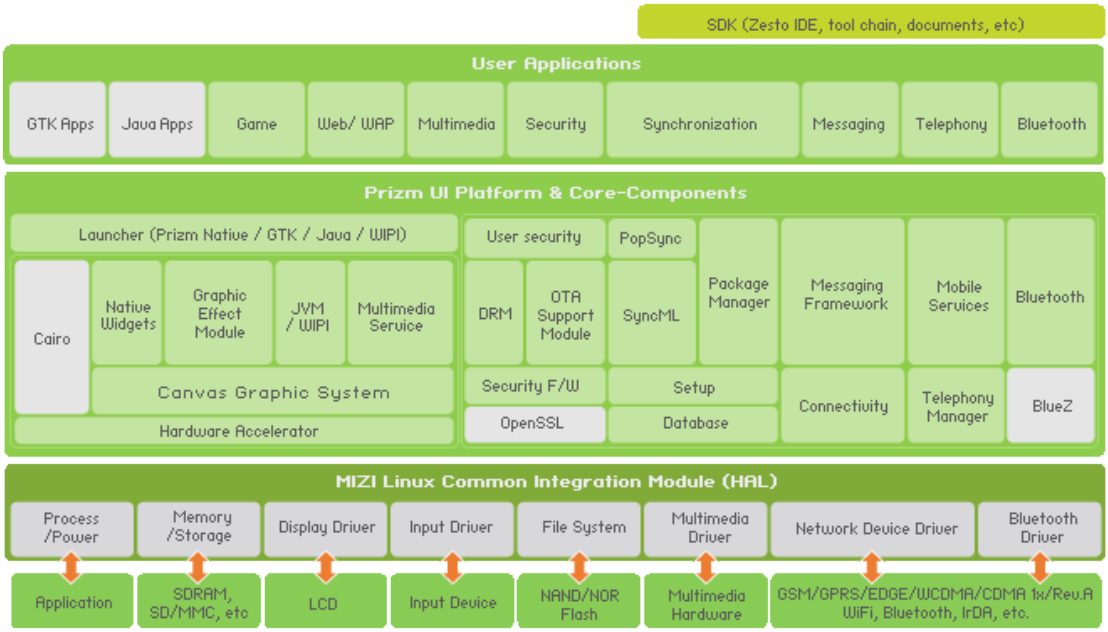

Рисунок 6 архитектура PRISM Linux от компании Mizi Research Incorporated

MontaVista Software (http://www.mvista.com/) — другой крупный поставщик Linux, завоевавший доверие таких фирм как NEC, Panasonic и Motorola. Собственно говоря, MontaVista Linux базируется на проекте Motorola EZX, что вызывает некоторую путаницу, внося сумятицу в ряды программистов и вызывая огромное недовольство самой Motorol'ы, но такова уж природа GPL-лицензии. Motorola выпустила открытое ядро, а MontaVista Software выхватила его у нее из рук и стала предлагать другим компаниям на своих условиях, впрочем, отвечающим требованиям GPL.

Другими словами, в нашем распоряжении имеется и исходные тексты ядра, и документация, и SDK, и даже Application Developer Kit, включающий в себя DevRocket 5 IDE, представляющую собой набор утилит для создания, сборки и отладки мобильных приложений. В отличии от Mizi SDK, DevRocket 5 IDE основан на настоящей Eclipse, а ее утилиты представляют ни что иное как плагины. То есть, Linux-программисты будут чувствовать себя в своей тарелке, а вот Windows-разработчикам придется забывать, что такое Visual Studio и учиться по новому.

Документация и Developer Kit находится по следующим адресам соответственно www.mvista.com/product_datasheets.php и www.mvista.com/product_detail_tools.php.

заключение

Linux уже давно вышел из детского возраста, превратившись из игрушечной системы в мощное оружие хакерского пролетариата, атакующее рынок проприетарного софта и оккупировавшего все доступные ниши: от встраиваемых устройств до суперкомпьютеров. Открытая модель разработки таит в себе огромные возможности, о которых закрытому коду нечего и мечтать!

Купив сотовый телефон с мобильной версией Linux'a, придерживающегося лицензии GPL, мы получаем в свое распоряжение аппарат, с которым можно хачить по полной программе в свое удовольствие. К мобильным версиям Linux'a, нарушающим лицензию GPL (то есть основанным на закрытых исходных текстах) сказанное не относится и они ничуть не лучше Windows CE и даже хуже ее, поскольку Windows CE – известный зверь, а кустарно адоптированная Linux без документации и SDK – это просто тихий ужас и ночной кошмар программистов, пытающихся ее раскурить.

>>> врезка полезные ссылки

- Linux Distributions and Kernels for Mobile SmartPhones:
  - основной портал для хакеров, интересующихся мобильными устройствами с Linux'ом на борту: http://tuxmobil.org/mobile_phone_linux_distributions.html;
- Linux and Mobile (Cellular, Smart) Phones:

- список мобильных устройств, основанных на Linux, с указанием типа системы и поставщика мобильной версии: http://tuxmobil.org/phones_linux.html;

- A760 includes the GPL'd sources of Motorolas A760 Linux smartphone:
  - исходные коды Linux-ядра, используемого в сотовом телефоне Motorolas A760: http://sourceforge.net/project/showfiles.php?group_id=116309;
- OpenSource.motorola.com:
  - официальный портал компании Motorola с исходными текстами всех Linux-ядер, которые только используются в выпускаемых ею сотовых телефонных: https://opensource.motorola.com/sf/sfmain/do/home;
- Eight Great Linux Smartphones:
  - технические характеристики восьми лучших сотовых телефонов в Linux'ом (на английском языке): http://blog.wired.com/gadgets/2007/03/eight_great_lin.html;
- Blob — a StrongARM boot loader:
  - исходные тексты мобильного загрузчика Linux'a для ARM-платформ: http://sourceforge.net/projects/blob/;
- Bootloader:
  - описание универсального мобильного загрузчика, поддерживающего большое количество платформ: http://wiki.openmoko.org/wiki/U-boot;
- Harald Welte's blog:
  - блог разработчика Bootloader'a с кучей полезной технической информации: http://laforge.gnumonks.org/weblog/index.html;
- Das U-Boot: The Universal Boot Loader:
  - интересная статья об Bootloader'е (на английском языке): http://linuxdevices.com/articles/AT5085702347.html;
- Bootloader source code:
  - исходные коды Bootloader'a: svn.openmoko.org/trunk/src/target/u-boot/patches/;
- Bootloader binary:
  - готовые бинарные сборки Bootloader'a: http://buildhost.openmoko.org/snapshots/;