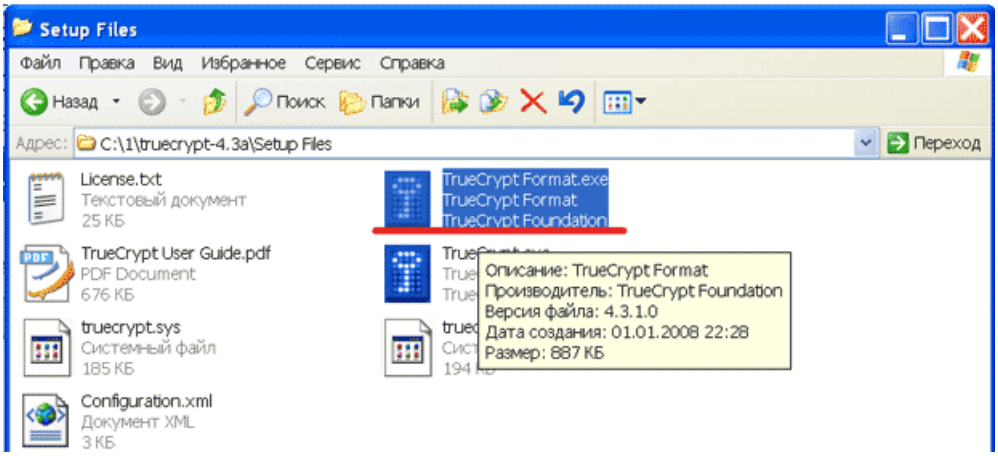
Работа с TrueCrypt

Предисловие. Данное руководство рассчитано даже на самых технически слабодготовленных пользователей. В нём значительное место уделено подробнейшему рассмотрению практических аспектов работы с программой. Но немного теории вначале всё же не повредит.

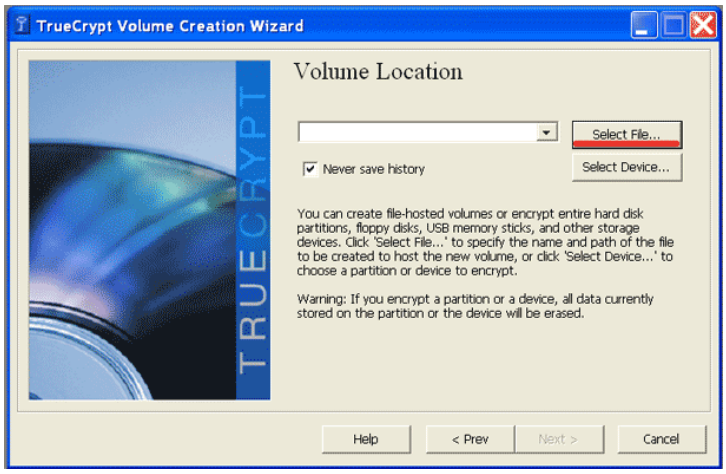
TrueCrypt — это свободное программное обеспечение, используемое для шифрования «на лету». Оно позволяет создавать виртуальный зашифрованный логический диск, хранящийся в виде файла. TrueCrypt также может зашифровать полностью раздел жёсткого диска или иного носителя информации, такой как дискета или USB-флэшка. Всё сохранённое в томе TrueCrypt полностью шифруется, включая имена файлов и каталогов. Примонтированный том TrueCrypt подобен логическому диску и поэтому с ним можно работать как с обычным диском.

Ну а теперь перейдём к делу. Саму программу качаем отсюда: http://www.truecrypt.org/downloads.php . Распаковываем полученной архив. Из него нам нужна только папка «Setup files». Всё остальное не пригодится. Для пытливых умом скажу, что «всё остальное» это обычный инсталятор и применять его нежелательно, дабы лишний раз не следить в системе. TrueCrypt отлично справляется со своими обязанностями и без установки.

Итак, переходим в папку «Setup files» и запускаем «TrueCrypt Format.exe», который и поможет нам создать зашифрованный контейнер:

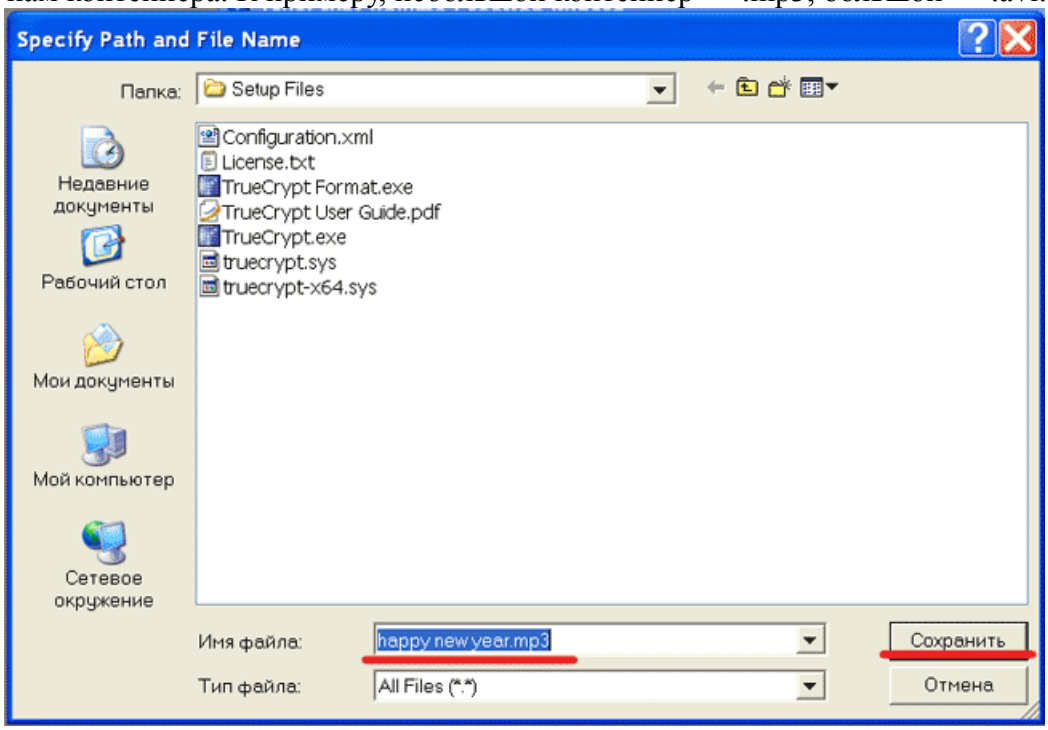


В открывшемся окне мастера выбираем «Select File...» (можно и «Select Device», если надо зашифровать целый диск, к примеру флэшку или даже hdd):



И подключаем свою фантазию для выбора имени и типа файла, исходя из размера

нужного нам контейнера. К примеру, небольшой контейнер – *.mp3, большой – *.avi:

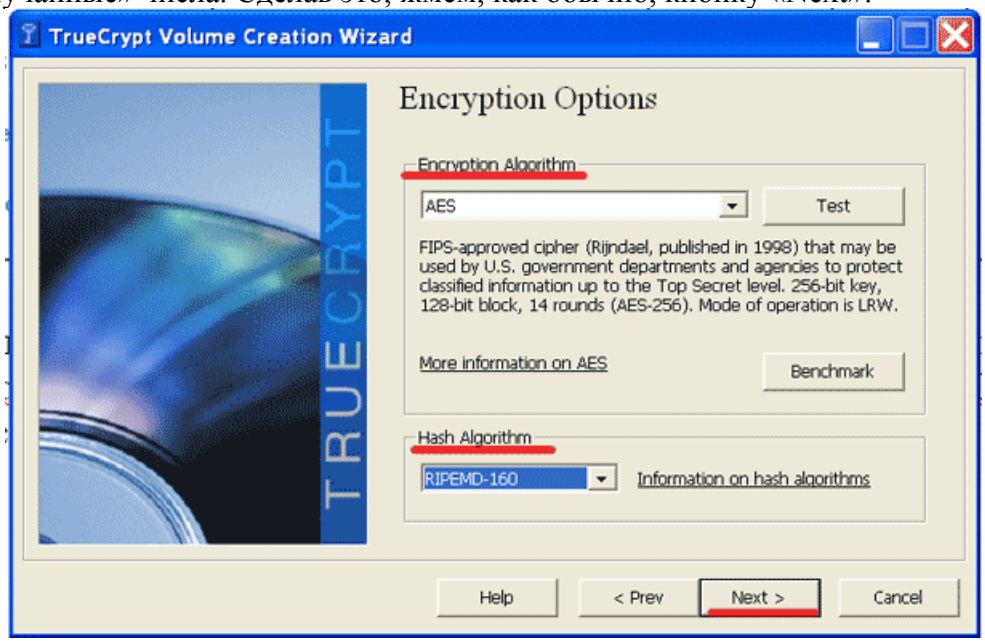


Жмём «Сохранить» и, вернувшись в окно мастера, жмём на кнопку «Next». Тут мы видим возможность выбора алгоритма шифрования (encryption algorithm). Вот краткая таблица их сравнения:

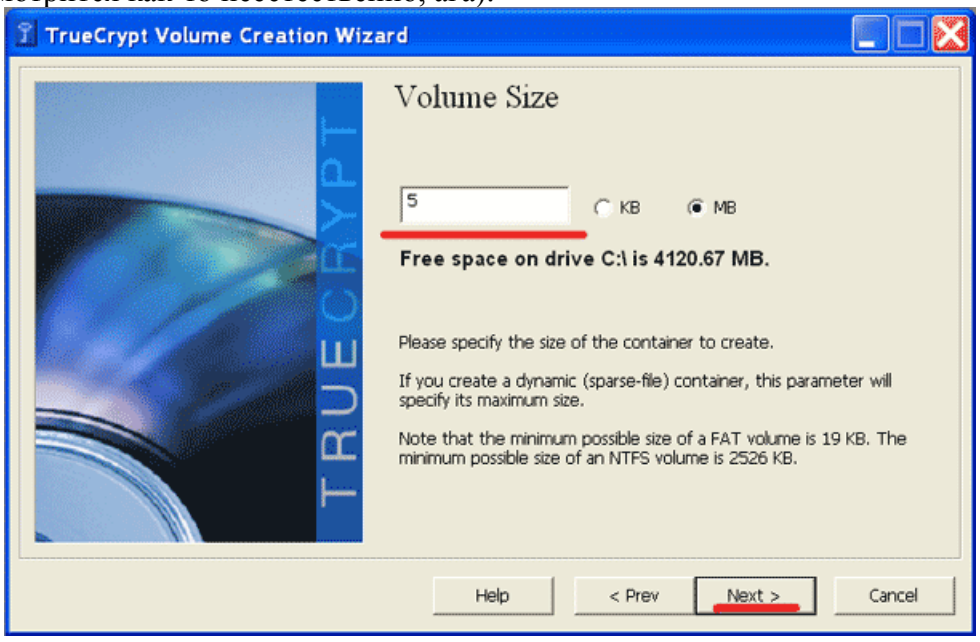
Algorithm	Designer(s)	Key Size (Bits)	Block Size (Bits)	Mode of Operation
AES	J. Daemen, V. Rijmen	256	128	LRW
Serpent	R. Anderson, E. Biham, L. Knudsen	256	128	LRW
Twofish	B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson	256	128	LRW
AES-Twofish		256; 256	128	LRW
AES-Twofish-Serpent		256; 256; 256	128	LRW
Serpent-AES		256; 256	128	LRW
Serpent-Twofish-AES		256; 256; 256	128	LRW
Twofish-Serpent		256; 256	128	LRW

Более подробно про них вы сможете узнать, пройдя по ссылкам в конце документа.

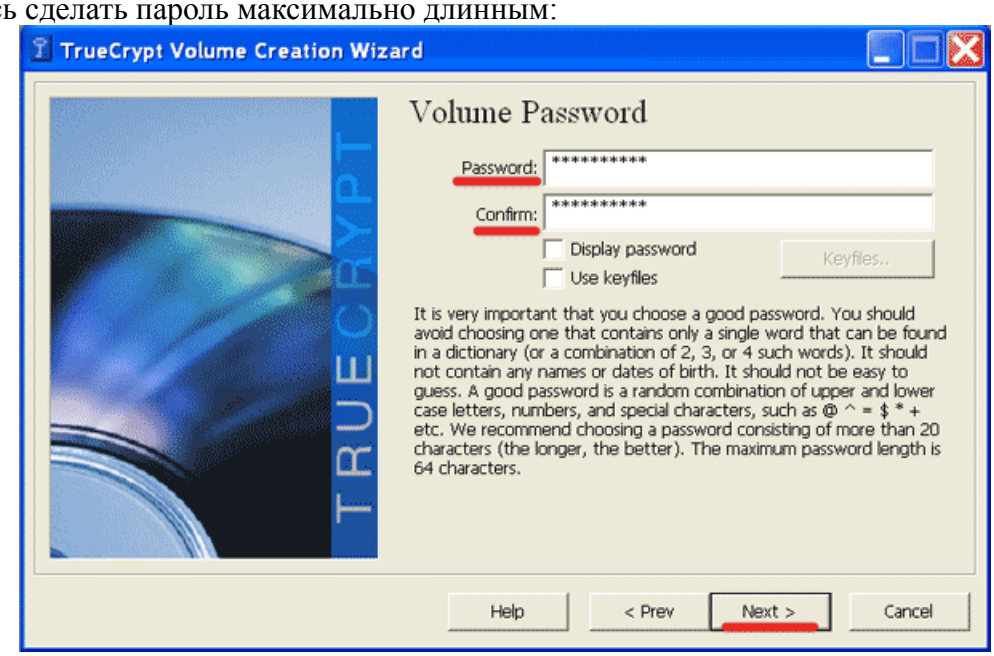
Выбрав encryption algorithm, выбираем hash algorithm, по-которому TrueCrypt будет мутить «случайные» числа. Сделав это, жмём, как обычно, кнопку «Next»:



И попадаем на этап выбора размера контейнера. Тут всё просто: задаём нужный нам размер и давим «Next», не забывая при этом про указанный раннее тип файла (mp3 на 700 мегабайт смотрится как-то неестественно, ага):



Следующее окно посвящено выбору пароля от контейнера. К данному этапу следует отнестись максимально ответственно. Не используйте пароль, который вы применяете или применяли где-то ещё. Не используйте какую-либо осмысленную фразу или слово. Используйте только произвольную комбинацию цифр и букв разного регистра (для незнающих, что такое регистр: «а» и «А»), а также различных символов (! ,№ ,% , (...). Старайтесь сделать пароль максимально длинным:

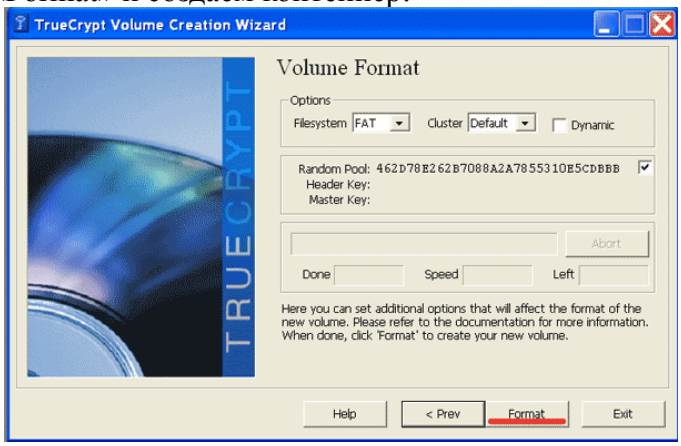


Для дополнительной защиты вы также можете использовать ключевые файлы (Keyfiles), однако это опасно тем, что вы лишитесь навсегда доступа к своему зашифрованному контейнеру и всей информации на нём, если потеряете или измените хотя бы один ключевой файл.

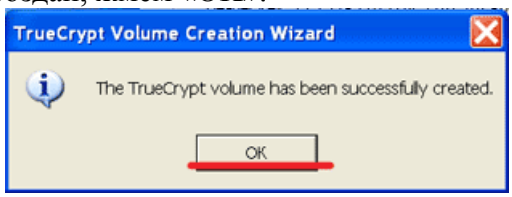
Установив пароль мы попадаем в последнее окошко мастера. Здесь можно сделать ваш контейнер динамическим, то есть увеличивающим или уменьшающим свой размер в зависимости от объёма файлов, хранящихся в нём. Сделать это можно, поставив галочку возле соответствующей надписи «Dynamic».

Однако данная опция не рекомендуется, так как она снижает производительность контейнера и самое главное, его безопасность.

Жмём кнопку «Format» и создаём контейнер:

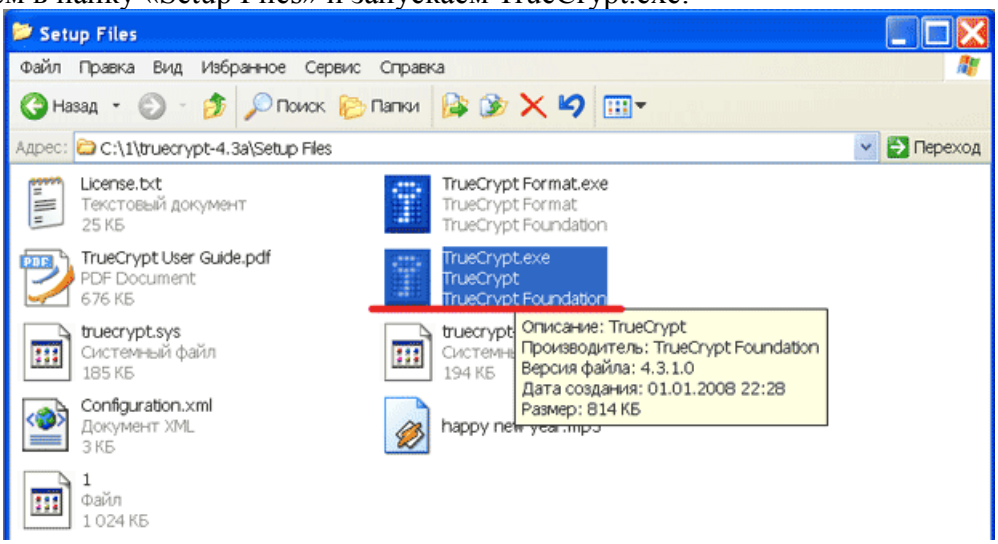


Контейнер успешно создан, жмём «OK»:

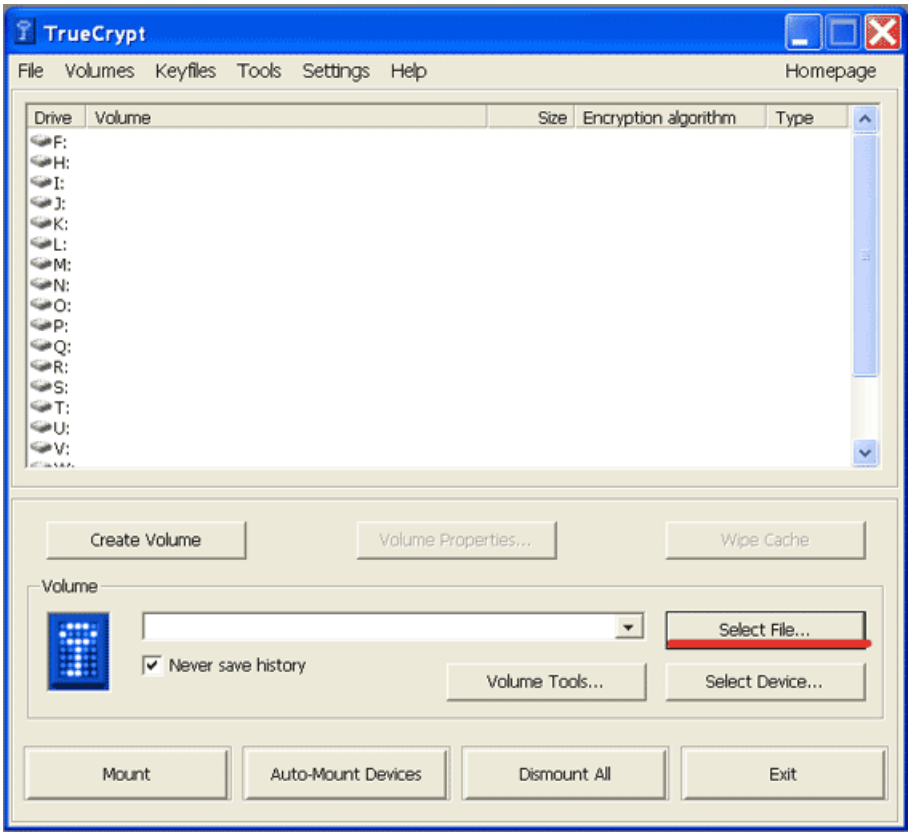


После чего видим окно дальнейшего выбора: создать ещё один контейнер или выйти. Пока нам хватит и одного, посему выбираем «Exit»:

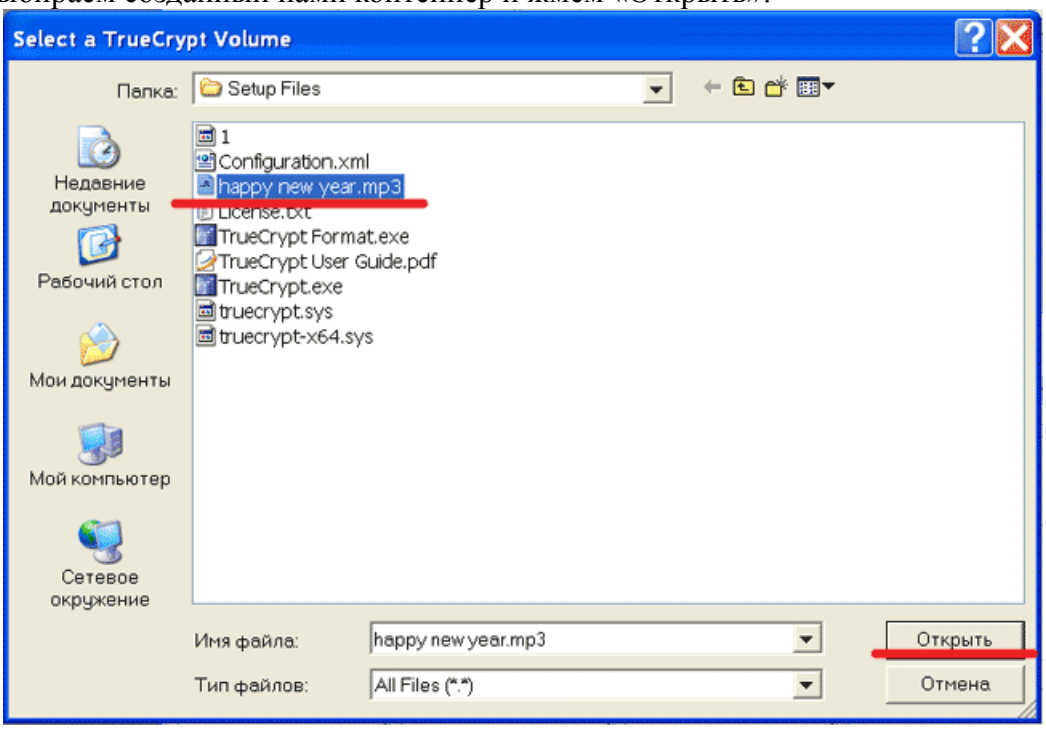
Идём в папку «Setup Files» и запускаем TrueCrypt.exe:



В открывшемся окне кликаем по «Select File...»:

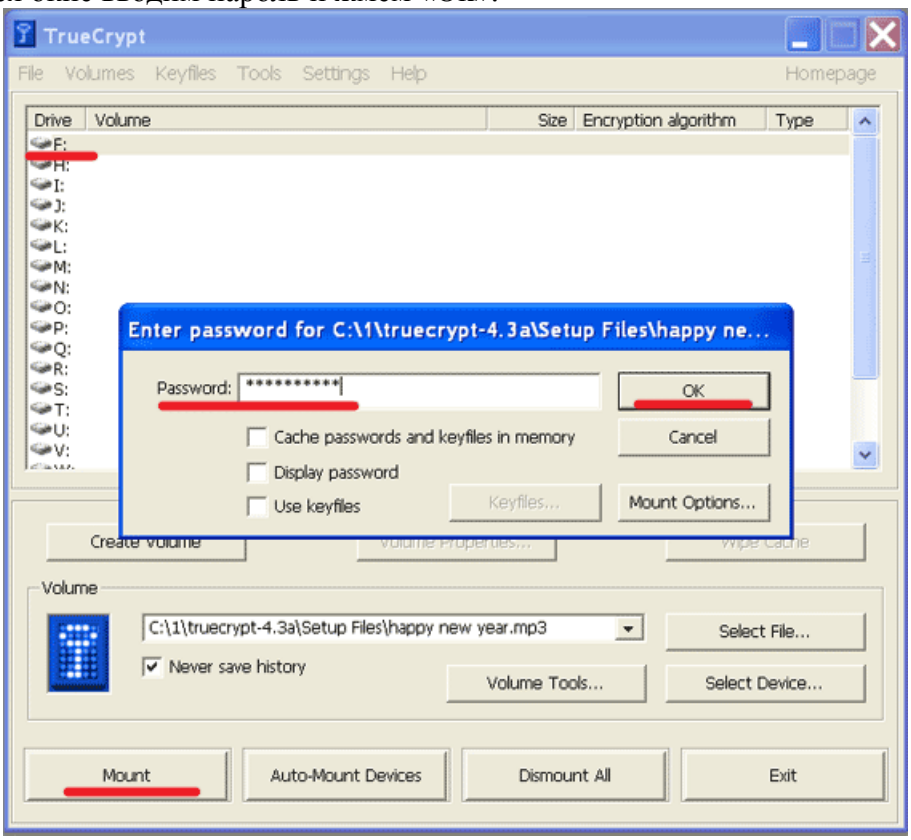


Выбираем созданный нами контейнер и жмём «Открыть»:

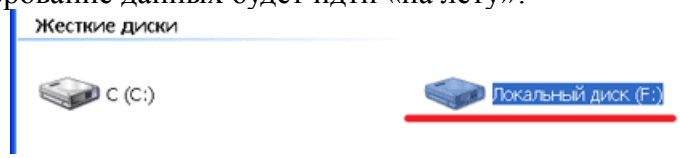


В главном окне выбираем букву для монтируемого контейнера, жмём кнопку «Mount»,

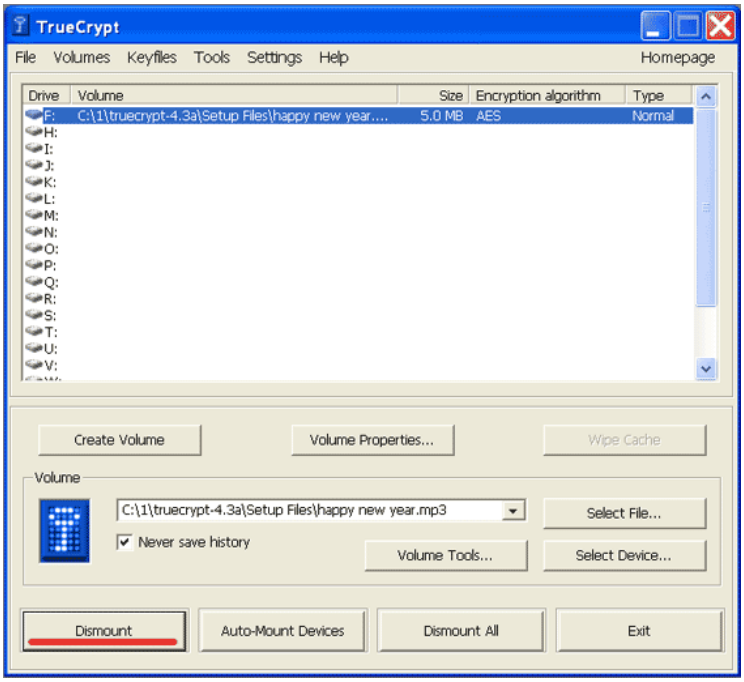
в открывшемся окне вводим пароль и жмём «Ok»:



Вуаля, у нас в системе появился новый диск. С ним можно работать, как и с обычным жёстким диском, шифрование данных будет идти «на лету»:



Отсоединить от системы его можно, нажав в главном окне TrueCrypt кнопку «Dismount»:



Полезные ссылки по TrueCrypt:
http://ru.wikipedia.org/wiki/TrueCrypt
http://www.truecrypt.org/
https://www.pgpru.com/

2008 г.