Привет! В этом курсе я постараюсь рассказать всю самую основную и ценную информацию по анонимности и безопасности при работе в сети. Данный курс не является призывом к каким-либо плохим действиям. Курс будет free (бесплатным) для всех желающих, потому что не вижу смысла продавать информацию, которая собрана и переделана из различных интернет источников. Данный курс будет построен на основе моего личного опыта, нескольких статей и частично на одном платном курсе по анонимности и безопасности. Зачем слушать несколько часов лекций, сидеть днями и ночами с поисковиком и искать актуальную информацию, когда здесь собрано все в одном месте? Материал будет идти по порядку. Я не расскажу вам ничего такого сверхъестественного, возможно, что кто-то знает все, что здесь написано, а возможно вы новичок и ничего не знаете. В любом случае будет хорошо, если вы ознакомитесь с данным материалом. Все действия и примеры будут проходить на базе Windows 7 и курс предназначен для Windows пользователей. Некоторые элементы и программы нужно будет настраивать и чтобы не захламлять курс информацией по установке и настройке, я буду давать ссылки на материал (все ссылки просмотрены и там только нужная информация без лишней воды).

Содержание:

Часть 1. Настройка ОС Windows для безопасной работы в сети.

Если вы занимаетесь чем-то серьезным в сети и работаете с ОС Windows, то я советую вам пересесть на Linux, но если такого желания нет, то тогда читаем дальше. При работе с Windows используйте только лицензионное ПО и постоянно обновляйте систему с выходом новых обновлений. Обновления можно настроить в Панели Управления (Как их настраивать думаю разберется каждый). Если вы делаете какое-то важное дело в сети, то лучше всего создайте отдельную учетную запись для работы с правами пользователя. Если вы словите вирус, то он не сможет полностью активироваться и прописаться в систему, т.к. большинство вредоносных программ прописывают себя в реестр, а без админских прав этого сделать невозможно. Вы можете работать и с основной учетной записи, но тогда вам нужно быть предельно внимательным к тому, что вы качаете из сети и какие сайты посещаете (дальше будет глава про браузеры). На учетные записи ставьте разные сложные пароли. Пароль должен быть рандомным. Мой совет: если вы и правда занимаетесь чем-то серьезным и опасным, то поставьте VMware Workstation и производите все действия там. Видео по установке виртуальной машины (видео не мое): http://www.youtube.com/watch?v=inuYGUvdnCg

Следующий шаг в настройке - это установка фаервола (Firewall). Устанавливать будем Comodo Internet Security. Скачать фаервол можно по ссылке: http://www.comodo.com/home/internet-security/free-internet-security.php
После скачивания установим. Обязательно включим автоматическое обновление. Инструкции по установке и настройке можно взять по этой ссылке (написано все очень подробно): http://www.comss.ru/page.php?id=1658

Базовую настройку мы выполнили, теперь необходимо перейти к шифрованию данных на ПК и к способам безвозвратного удаления данных.

Часть 2. Шифрование данных на ПК и способы удаления информации безвозвратно.

Для шифрования данных на компьютере будем использовать утилиту True Crypt.

TrueCrypt – это бесплатное, криптографическое программное обеспечение (ПО) с открытым исходным кодом для шифрования данных "на лету" (On-the-fly encryption).

Чтобы не копировать сюда инструкцию по работе с софтом и полный мануал по шифрованию - предлагаю сделать все в точность, как по ссылке: http://wiki.mvtom.ru/index.php/TrueCrypt
Скачать софт можно тут: http://www.truecrypt.org/downloads

Проделайте процедуру шифрования и со своей флешкой.

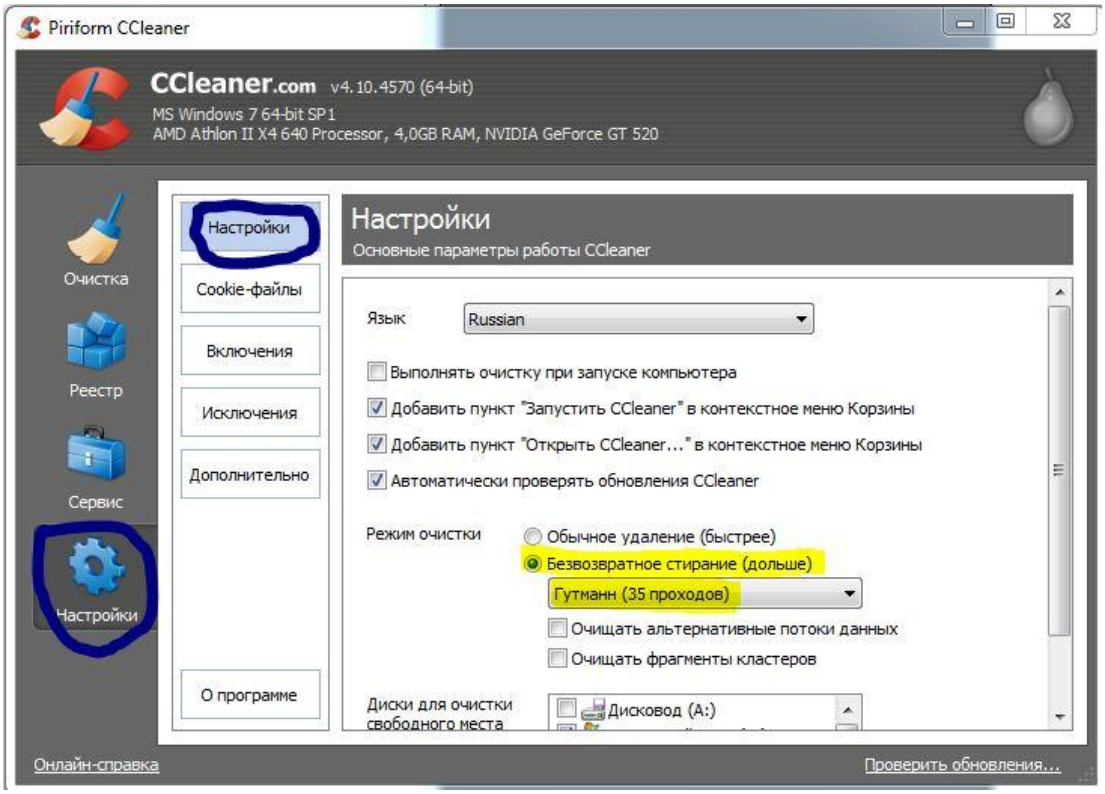
Безвозвратное удаление информации.

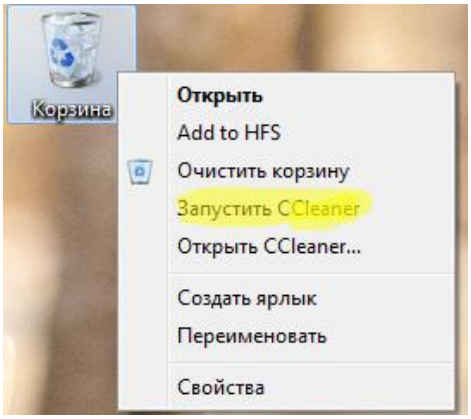
Безвозвратно удалить информацию можно с помощью двух программ: Eraser и CCleaner.

Попробуем сначала через CCleaner.

CCleaner - утилита для оптимизации и чистки системы.
Скачать можно тут: http://ccleaner.org.ua/download/

При установке нужно отметить пункт добавления функций очистки к корзине.
Открываем, заходим в настройки, затем еще одна вкладка настроек и там выбираем безвозвратное стирание. Можно поставить 1 проход, но я советую методом Гутмана (35 проходов). Этот софт сам по себе удобен для удаления информации.



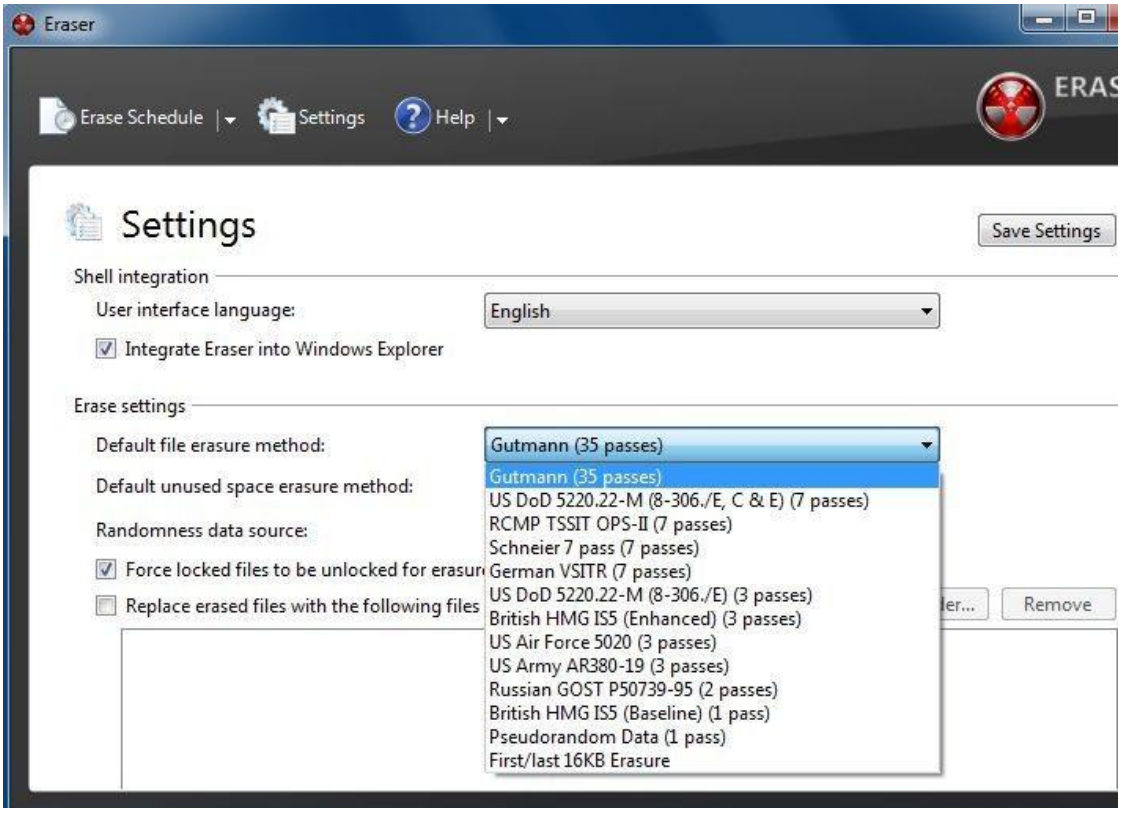


Пробуем удалять информацию через Eraser.

Eraser - бесплатная утилита, позволяющая полностью удалить ненужные данные с жесткого диска ПК без возможности их последующего восстановления. Поддерживается работа под операционными системами Windows 95/98/ME/NT/2000/XP/2003, DOS и частично Windows Vista. Программа использует несколько различных методов затирания данных, способна справляться с зашифрованными файлами и папками, очищает содержимое Корзины. Также Eraser способна удалять информацию из сетевых хранилищ, с дискет , CD-RW, DVD-RAM, DVD-RW и т.д. Поддерживаются файловые системы FAT32 и NTFS.

Скачать софт можно тут: http://softportal.com/get-19219-eraser.html (Источник 2).

Софт может показаться сложным на первый взгляд, кому сложно - используйте первый метод удаления информации. В Eraser тоже ставим метод Гутмана.



Дальше все будет понятно. Информацию по использованию софта можно найти тут: http://www.hack-info.ru/showthread.php?t=46885

Часть 3. Все о паролях. Способы хранения.

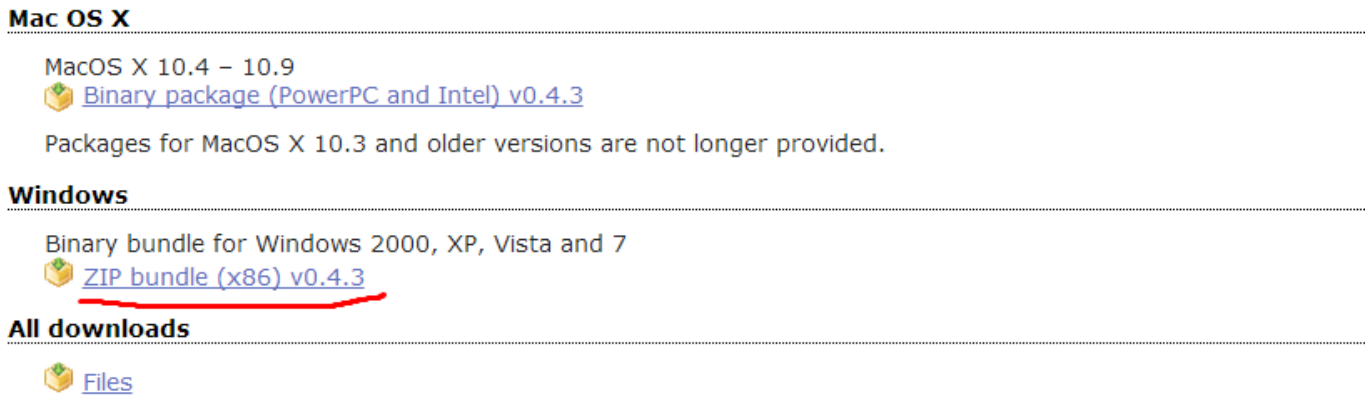
Пароли от каждого сайта должен отличаться между собой. Не нужно ставить в качестве пароля дату своего рождения, свой любимый цвет, фильм, телефон и т.д. и

т.п. - все легко подбирается. Также не используйте пароли типа qwerty, 123456, 12345678,qweasd и любые легкие пароли, которые можно сбрутить за несколько минут. Самый безопасный пароль по мнению экспертов - это пароль состоящий из 16 символов. В основном, при регистрации на сайтах и форумах просят ввести пароль от 6 до 20 символов. 16 символов - самый оптимальный пароль! В пароле используйте буквы верхнего и нижнего регистра, цифры и по возможности символы. Пример безопасного пароля из 16 символов: WPXjVu{pUY{I+AOX. Все пароли лучше записывать. **Сейчас мы поговорим о способах хранения паролей.**

Многие люди хранят пароли в браузерах, чего категорически делать нельзя!!! При первом же попадании трояна (например, того же UFR) - ваши пароли уйдут злоумышленникам. Есть люди, которые хранят пароли в текстовых файлах на компьютере и открывают их через блокнот. Этот вариант тоже не безопасен. Да, есть вариант залить в текстовом файле пароли на флешку, но и этот вариант не безопасен. Как быть тогда? Все очень просто. Мы будем использовать софт KeePassX.

KeePassX - это свободное программное обеспечения для хранения паролей, которое распространяется бесплатно на базе лицензии GPL. Софт имеет открытый исходный код. В этом и его отличие.

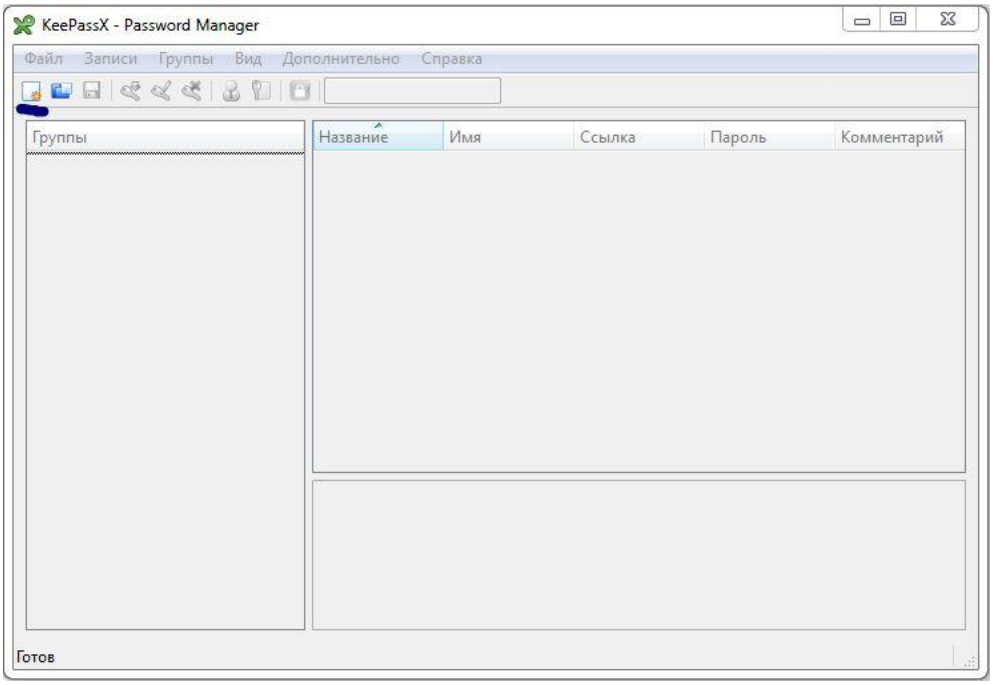
Софт обязательно скачивать с официального сайта! Не качайте софт с торрентов и варезников - в софт может быть вшит троян!
Ссылка для скачивания: http://www.keepassx.org/downloads



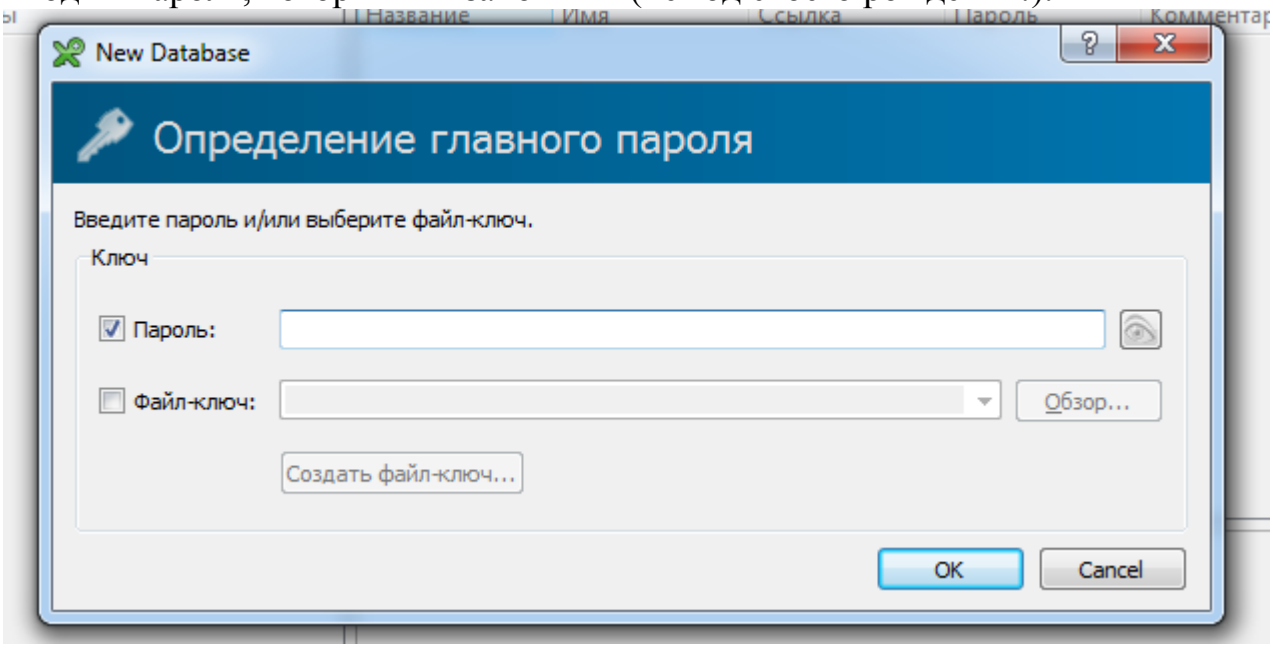
На странице загрузки выбираем архив для Windows. Скачиваем его!

Еще один плюс этого софта - он не требует установке и софт портативный (можно запустить на любом ПК без установки). Софт имеет приятный интерфейс. Распаковываем архив и запускаем. После запуска нам нужно создать базу паролей (когда база создана мы ее будем просто открывать).

Нажимаем новая база:



При создании базы попросит создать пароль или файл-ключ. Файл-ключ надежнее будет, но его можно потерять, поэтому мы остановимся на парольной защите. Вводим пароль, который мы запомним (не год своего рождения!).



Затем жмем ОК и вводим ключ повторно. Теперь мы можем работать с паролями своими. Добавляем все самое необходимое и ценной и сохраняем базу (обязательно!). "Файл - Сохранить базу паролей как..." Вводим название базы и сохраняем ее в надежное место и затем записываем на флешку! База всего занимает несколько килобайт и надежно зашифрована методом AES. Открыть базу паролей можно на любом компьютере, где установлен софт KeePassX (запишите лучше на флешку его).
При открытии базы запросит пароль базы, вводим пароль и работаем с базой паролей.

Часть 4. Выход в интернет, выбор браузера и его настройка.

Мы уже разобрали много вещей (от настройки системы - до защиты файлов). Теперь настал момент выхода в сеть, выбора браузера и его настройки.

На рисунке ниже представлены основные браузеры, про которые мы немного поговорим:

Яндекс Браузер, Браузер от Майла и прочие с хромовидной иконкой работают на базе движка Google Chrome. Я ничего не имею против хрома и остальных браузеров, но они нам для работы не подойдут. IE, Opera, Chrome - подвержены проникновению эксплоитов, а значит ваш ПК может быть заражен опасным трояном. Браузер Mozilla Firefox подходит для работы больше всего. Он самый популярный и надежный браузер типа опенсоурс. Качаем браузер только с официального сайта! С браузером мы определились, теперь необходимо поставить необходимый плагины и выключить слежку.

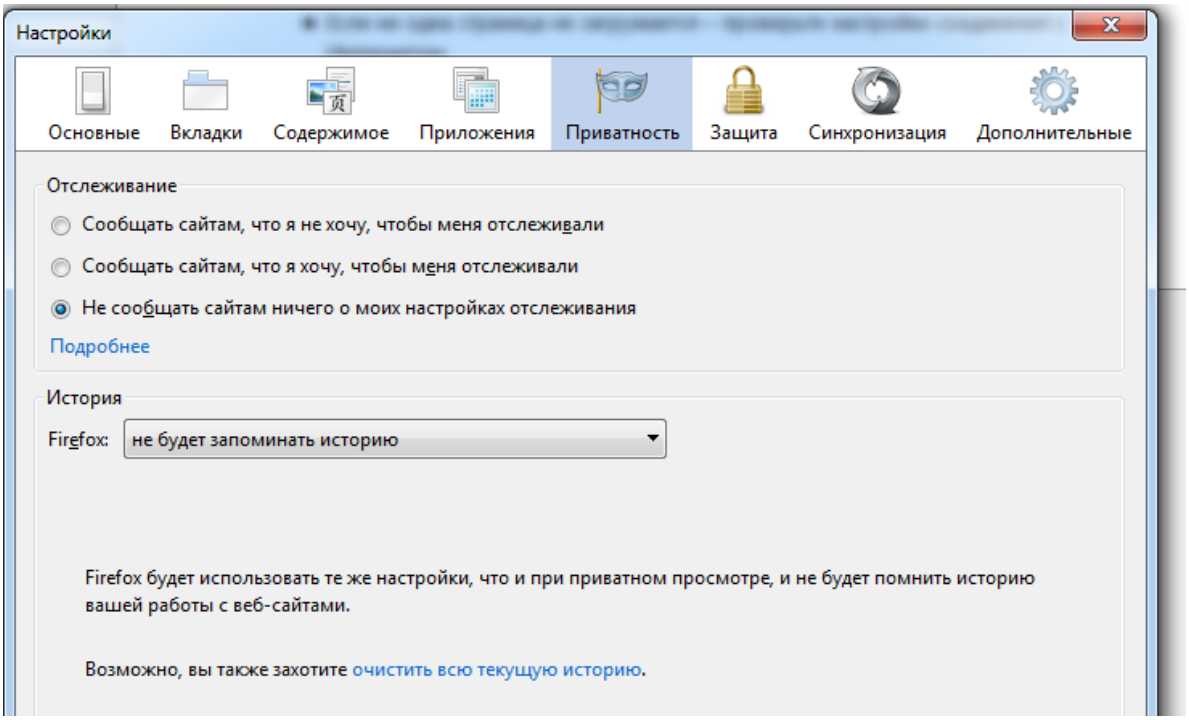
Для начала работы нам нужно обязательно установить несколько плагинов.

NoScript - плагин, который позволяет блокировать весь Flash и потенциально опасные объекты на сайтах.

WOT (Нет, это не World Of Tanks) - это дополнение, которое будет информировать нас о надежности и безопасности сайта. Плагин может показать, что сайт опасен - тогда посещать его не рекомендуется.

AdBlock Plus - плагин для блокировки назойливой рекламы и всплывающих окон на сайтах.

Теперь отключаем слежение, куки, пароли и историю:



Ставим все, как на скрине.

Во вкладке "Защита" убираем галочку "Запоминать пароли сайтов".

Желательно иметь портативную версию браузера и хранить его на защищенной флешки. Как защитить флешку можно узнать выше, описывалось это.

Теперь давайте поговорим о браузере TOR

Если вам нужно срочно где-то зарегистрироваться и вы не хотите светить свой IP, а портативного браузера настроенного нет под рукой - на помощь придет TOR. Он также подойдет для любых целей, но если нужно сделать очень важное дело, то лучше использовать полноценный настроенный ПК или дедик (о которых поговорим позже). Не слушайте вы эти слухи о торе - это все слухи. На практике не было случаев, когда кого-то ловили через тор.

Скачать браузер можно с официального сайта: https://www.torproject.org/download/download-easy.html.en

При скачивании выберите русский язык. После скачивания распакуйте архив. В архиве будет портативный браузер лисы. Как работать с тором знают многие, там все просто, по этому описывать не буду. Айпи меняется каждые несколько минут.

Часть 5. Безопасная почта, одноразовые заметки и передача файлов.

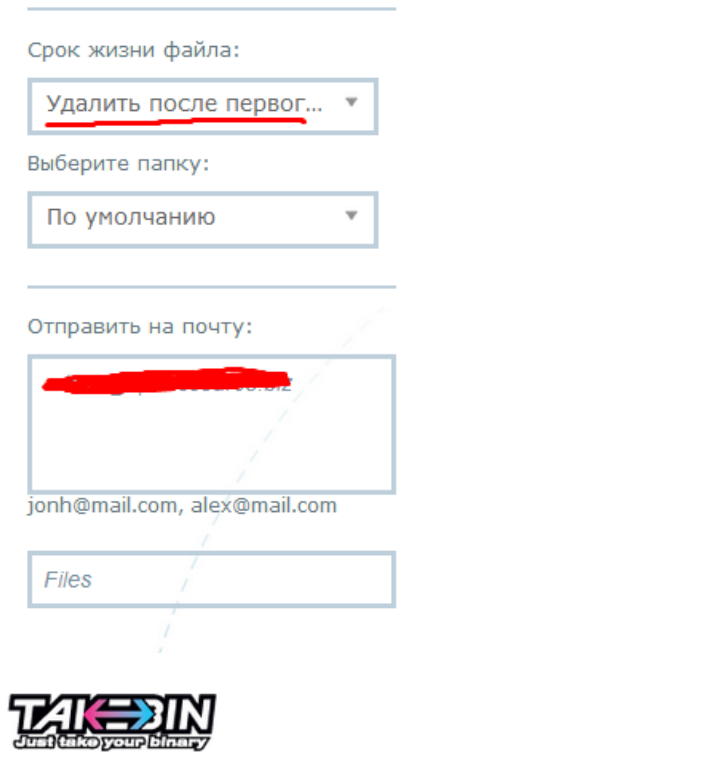
Куда же мы без E-mail в интернете? Почта нужна всем. Для белых целей регистрируем почту на gmail.com. Включаем двойную аутентификацию. Получаем доступ по паролю + смс. Такую почту взломать невозмжно.

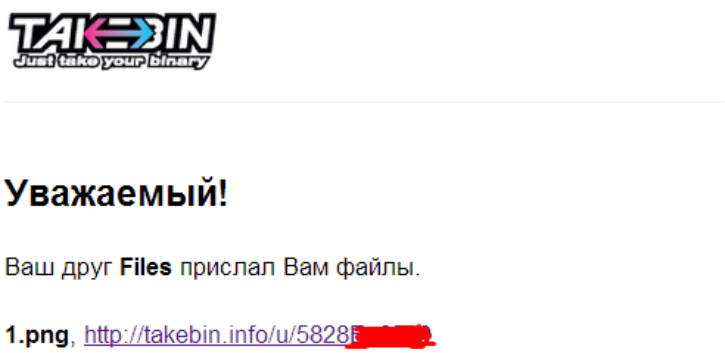
Для серых и черных дел можно использовать временную почту. Сервисов полно, самый популярный - это http://10minutemail.com/10MinuteMail/index.html

Бывает, что нам надо передать информацию другому человеку, если информация важная или секретная, то воспользуемся сервисом одноразовых заметок https://privnote.com Как оно работает? Вы создаете заметку. на выходе получаете ссылку, отправляете ее собеседнику и после открытия заметки - она удаляется. Очень удобно.

Для передачи файлов можно воспользоваться файлообменниками. Мы советуем: http://takebin.com и http://sendspace.com

У takebin.com присутствует возможность отправки файлов на почту, а точнее отправка ссылок на скачивание. Для анонимной передачи файлов мы зальем файл с параметрами:





Можно поставить хранение файла 1 час, по истечению часа файл удалится.

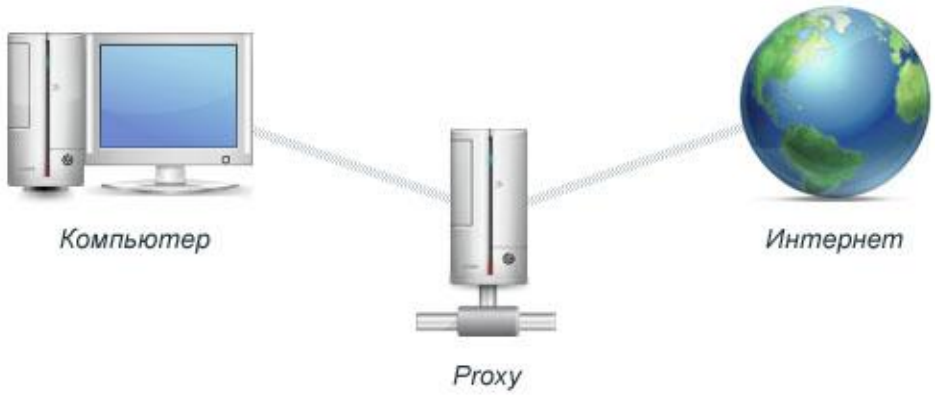
На почту придет потом письмо-уведомление, что вам отправили файл. В сендспейсе есть похожая функция. Сендспейс используйте для передачи серой информации, а тайкебин для белой :)

Часть 6. Анонимайзеры, Proxy, Socks5 и работа с ними.

Анонимайзер - средство для скрытия IP адреса. Допустим у вас на работе заблокирован доступ к социальным сетям, мы открываем анонмайзер и через его входим в социальную сеть. Другими словами - меняем айпи для конкретного сайта.

Самый известный анономайзер - это http://cameleo.ru/ Больше анонимайзеров можно найти тут http://2ip.ru/anonim/. Также 2ip.ru служит источником проверки IP адреса компьютера и анонимайзера.

Proxy - удаленный компьютер, который, при подключении к нему вашей машины, становится посредником для выхода абонента в интернет. Прокси передает все запросы программ абонента в сеть, и, получив ответ, отправляет его обратно абоненту. Примерная схема работы:



Еще больше информации о Proxy вы можете узнать на сайте: http://2ip.ru/article/proxy/

Где взять proxy?

Proxy можно взять на раздаче или купить. Для серьезной работы я советую потратить несколько долларов и купить прокси, т.к. они намного качественней тех проксей, которые в раздачах. Но если у вас нету денег или жалко тратить, то вы можете воспользоваться одним из сервисов по раздаче (на самом деле их масса): http://fineproxy.org (там раздают прокси, там же можно и купить!) и http://hideme.ru (там в разделе прокси есть раздача и также можно купить, но мне не нравится качество проксей у этого сервиса).

У проксей есть несколько ступеней анонимности:

Нет (прокси не анонимна и будет показывать всю основную информацию о вас)

Низкая (анонимности почти нет - основная информация будет показана, в том числе ваш айпи в статусе "скрывается за прокси сервером".)

Средняя (информация о вас почти показываться не будет, только будет написано, что айпи скрывается за прокси сервером)

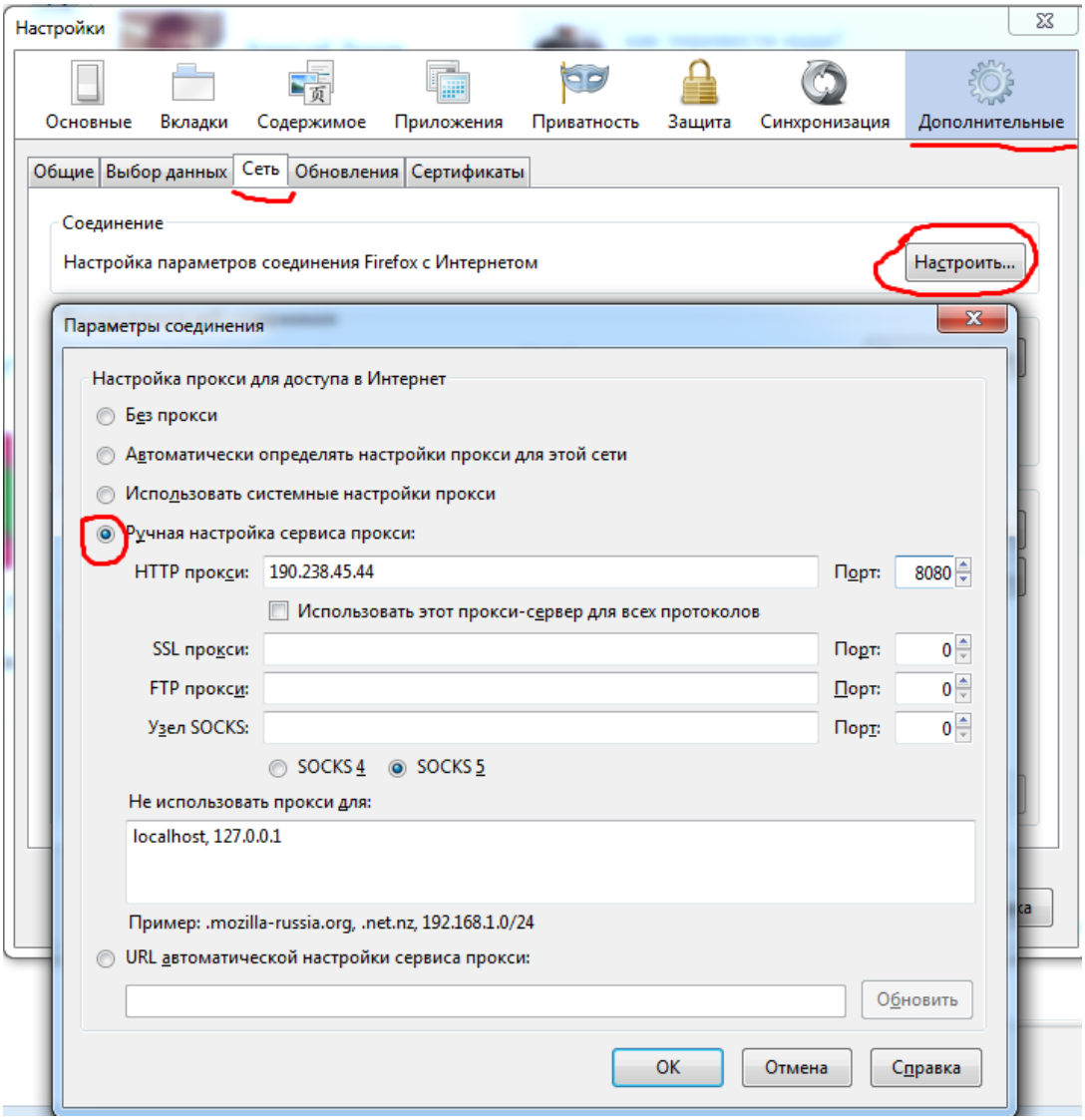
Высокая (информации о вас не будет и в айпи адресе будет айпи прокси).

Программ для работы с прокси много, всю информацию о программах можно найти на сайте: http://www.freeproxy.ru/ru/programs/index.htm

Рассмотрим способ работы с прокси через браузер Mozilla Firefox.

Допустим у нас есть прокси 190.238.45.44:8080 (8080 - это порт, они у каждой прокси бывают разные).

Открываем настройки браузера и дальше делаем также как на скрине. По аналогии настраиваются соксы5.



SOKS5 настраивается таким же образом, только вместо http прокси вписываем в графу соксов айпи и порт.

Сокс - это по сути тоже самое, что и прокси. Это узел сети другого компьютера.

Найти соксы можно на том же hideme. Сайты, которые продают соксы: http://5socks.net/ (регистрация ручная) и vip72.com (все происходит автоматически).

Часть 7. Дедики и работа с ними. Схема работы через дедики.

Дедик - сбрученные компьютеры разных стран, которые предназначены для работы. Суть работы с дедиком заключается в удобстве. Не нужно покупать прокси и соксы, а достаточно подключиться к дедику и работать. Другими словами мы получаем доступ к настроенной машине. Постоянно работать через дедик не особо удобно, так как маленькая скорость, но зато безопасно. Через связку впн + дедик выйти на человека сложно, но можно. Дедиками в основном пользуются кардеры (не будем вдаваться в подробности).

Дедики также можно взять на раздаче и купить. Брать на раздаче не советаю - они уже отжили свое или будут очень сильно тормозить и 100% вы будете не один хозяин. Советую дедик купить. Необходимо написать продавцу, указать страну и характеристики. Дедики не дорогие, от 3 долларов. Информации по работе с дедиками полно. Людей, которые продают тоже.

Подключиться к дедику можно через: Пуск - Стандартные - Подключение к удаленному рабочему столу. Заходить советую уже с включенным впном (про впн будем говорить далее). Также в конце данного курса будет ждать бонус схема!

Часть 8. VPN и все про VPN.

VPN - это замена соксам и прокси. Пустив трафик через впн сервер вы будете чувствовать себя в безопасности, так как весь трафик идет сначала на сервер впн, а затем к провайдеру. Провайдер уже не видит ваших логов.

Впн сервисов в наше время очень-очень много. При выборе один лучше другого, но давайте рассмотрим так ли это? Самый оптимальный вариант - это собственный впн сервис. Для этого нужно купить вдс/впс подальше от России и поднять там собственный впн. Статей по поднятию очень много, но кому лень этим заниматься, те могут просто зайти на http://inferno.name , выбрать тариф самый дешевый (15 долларов за 3 месяца) и написать при оформлении заказа, чтобы поставили впн и отключили логи! Но если и этим лень заниматься, то тогда можно купить доступ у впн сервиса.

Я хочу вам сказать, что ведут логи все. Если сам сервис логов не ведет, то трафик могут снифать в ДЦ. Поэтому я отобрал для вас самый надежный впн сервис,

который не ведет логов на сервере и предоставляет отличные связки. Для работы я советую использовать Дабл впн + сокс/тор, а лучше через впн подключиться на дедик и там делать всю свою работу. Вся информация по подключению впн и настройке на ПК представлена на сайте сервиса. Ссылка на сервис: http://vpnlux.com . Вы можете использовать любой сервис, но то, что мы советуем - самый надежный.

Есть впн сервисы, которые подписывают трафик, а есть которые не подписывают. Те впн, которые подписывают трафик ведут логи, Это не утверждение, это догадки.

С форума "Античат" я нашел небольшой список сервисов, которые подписывают трафик и которые нет.

Подписывают трафик:

DoubleVPN.com

tsunamivpn.com

5VPN.net

kebrum.com

VPN-Service.us

spicevpn.com

opp-corp.com

vipvpn.com

proxpn.com

cyberghostvpn.com

torvpn.com

hide-my-ip.com

COMODO TrustConnect

usaip.eu

hideme.ru

buyswitchvpn.com

Не передают лишней информации о себе (не подписывают трафик):

VIP72.ORG

hotspotshield.com

secsys.net

vpntunnel.se

securitykiss.com

privatetunnel.com

packetix.net

free-vpn.org

vpn.insorg.org

anonimitynetwork.com

openvpn.ru

lysator.liu.se

webmastervpn.com

Если сервис трафик не подписывает - это не значит, что он не ведет логи! Логи может вести сам ДЦ. Для обычной работы в сети (общаться на форумах и сайтах хватит обычного впн (например, впнлюкс)).

А как быть максимально анонимным - вы узнаете в конце курса.

Часть 9. Методы безопасного общения в сети.

Всем мы знаем, что icq,skype,vk давно под контролем органов и все просматривают и слушают. Для безопасного общения существует jabber.

Jabber - протокол мгновенного общения.

Сейчас уже почти все селлеры имеют жаббер. Но жаббер также может вести логи (это касается публичных серверов). Я не советую использовать для общения jabber.ru - он ведет и хранит логи с 2006 года. Самый безопасный жаббер - это свой. Поднять свой жаббер не сложно. Достаточно купить впс и установить необходимые пакеты. Но поднимать жаббер на впс я не советую - у впс могут снифать трафик. Для жаббера самое оптимальное - это самый дешевый выделенный сервер, который куплен официально. Но если такой возможности нет можно воспользоваться следующими жаббер серверами (проверенные, логов нет): xnteam.ru (от команды форума xaker.name) и exploit.im (от форума exploit.in). У Takebin скоро будет тоже свой защищенный жаббер сервер, дело времени!

Для общения через jabber я рекомендую клиент PSI+ + OTR. Я не буду тут расписывать как установить, всю информацию по установке и настройке клиента и отр можно почитать тут: http://forum.beznal.cc/topic/1528-zhabber-psi-otr/ и http://forum.psi-plus.com/viewtopic.php?f=7&t=43

К безналу не имею никакого отношения!

По себе знаю, что с 64 разрядной системой могут быть проблемы в установке, но у меня все получилось.

Если вы заняты серьезным делом - то окончательно забудьте про icq и skype! Не передавайте всю личную информацию через их (пароли, адреса, телефоны и прочее).

Общение ведите строго через Jabber + OTR. Альтернатива OTR - это PGP.

Еще Jabber клиенты, которые поддерживают OTR и PGP:

1. Miranda

2. Pidgin

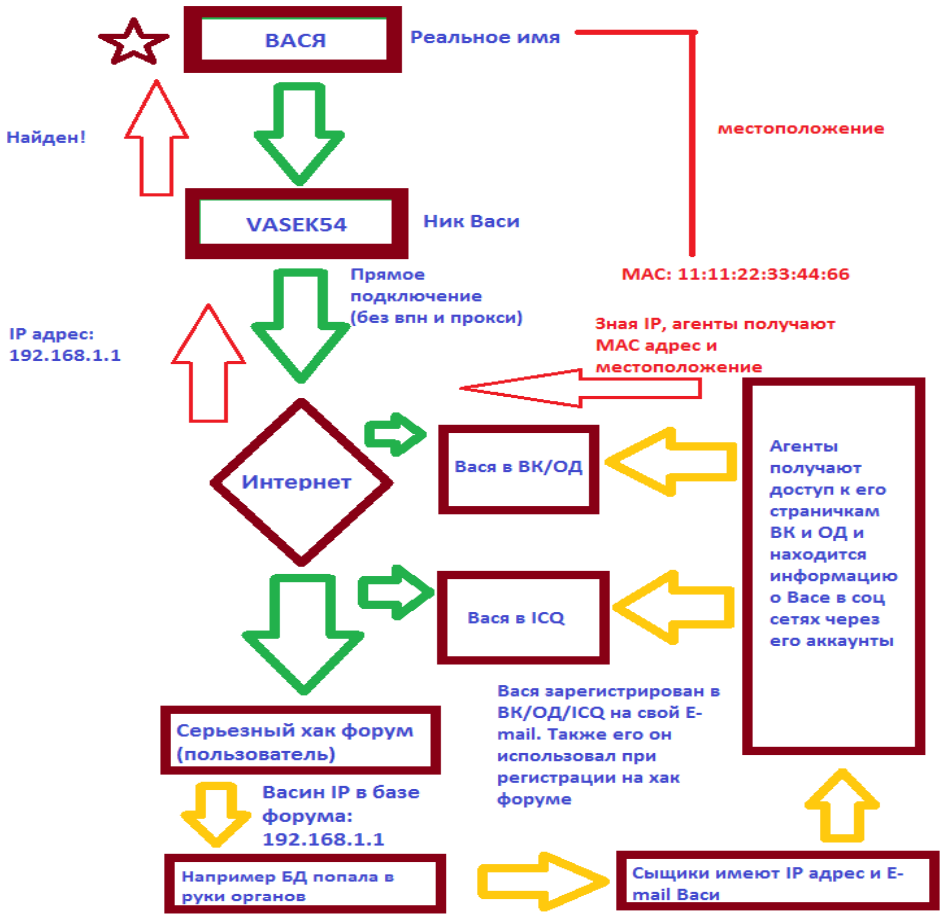
3. QIP (не поддерживает ни один метод шифрования, просто переписка).

Часть 10. Бонусная статья "Как остаться максимально анонимным + примеры"

Данная статья была уже на openssource.biz, но многие пользователи ее не видели, поэтому я посчитал, что она будет идеальным дополнением к этому курсу!

Чтобы остаться анонимным, человек не должен оставлять следы о своей реальной личности в сети. Чтобы это понять, я сделал небольшую схему:

*** — на схемах будет указан IP адрес, как реальный 192.168.1.1 — это не IP роутера — это IP для примера в статьи. Вместо 192.168.1.1 — находится ваш ип. Также все ип у впнов, которые на схемах будут другие — это пример.**



Пояснение к вышеуказанной схеме:

Есть человек по имени Вася, он имеет ник: vasek54. Вася захотел присоединиться к форуму черной тематики (будь то хак, то форум по отмыву, не суть). У Васи был 1 E-mail адрес, на котором были привязаны профили его ВК и Одноклассников. Этот E-mail он оставил при регистрации на черном форуме. Например у органов есть база данного форума или же за форумом следят и имеют доступ (неудачный немного пример), они смотрят информацию о пользователе vasek54 и имеют что-то следующее:

Ник: vasek54
IP: 198.168.1.1
E-mail: vasek54azaza@gmail.com

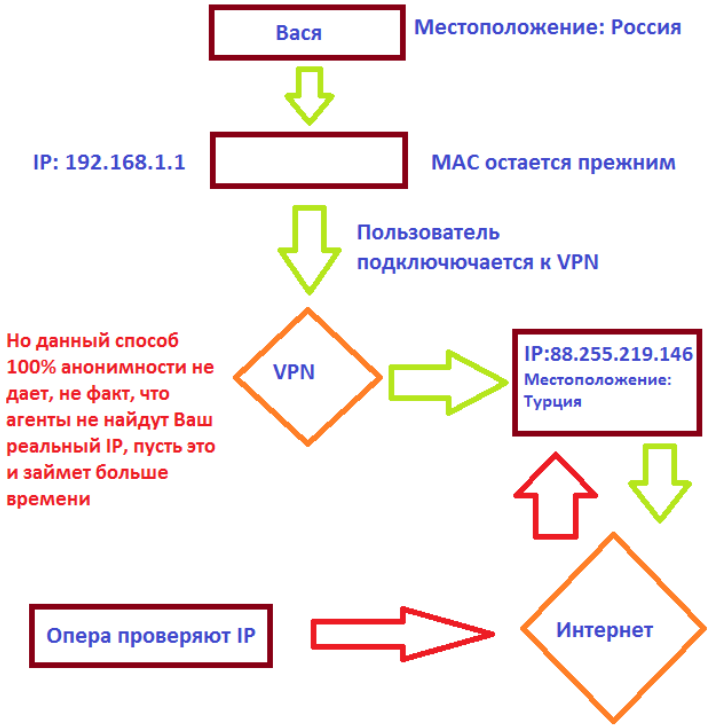
Теперь, когда у полицаев есть данные (ip,e-mail), Васю пытаются разыскать через интернет. А по сколько e-mail привязан например к ВК, а на страничке Васи его реальные данные, фотки, телефоны и т.д., то можно считать, что Вася «принят». За ним устанавливают слежку.

PS. Страничку Вконтакте найти можно через E-mail, ввести его в графу «Забыли пароль» и, если страница привязана на этот e-mail, то она будет показана.

Также можно узнать E-mail через скайп. Как это делается можно почитать тут.

Теперь давайте разберем ошибки пользователя.

Если бы пользователь защитился через:Vpn, прокси или SSH тунель, то схема выглядела бы примерно таким образом:



Пояснение: Вася имеет IP 192.168.1.1, он подключается к VPN и весь трафик начинает передаваться через VPN сервис. Если бы Вася зарегистрировался на форуме через VPN, то агенты получили бы не его IP, а IP его VPN сервиса, что усложнило бы поиск Васи. Но данный способ не гарантирует анонимность на все 100%, т.к. возможно получить реальный IP, зная IP Vpn'а, но это не под силу обычному пользователю.

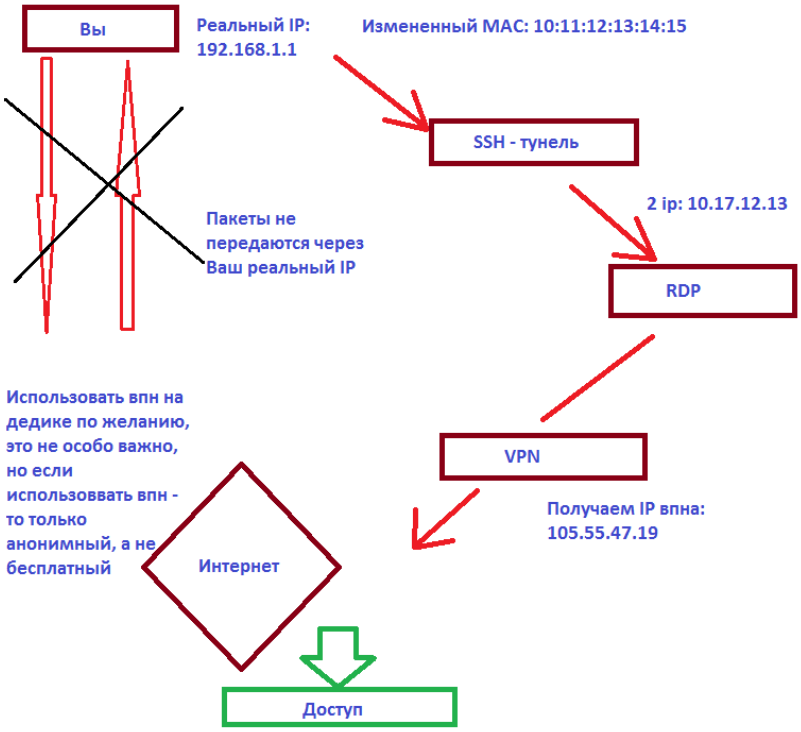
Используйте фейк данные!

На нашем примере мы видим, что Вася использовал один E-mail везде (вк,од, форумы). Если вы где-нибудь регистрируетесь, то заведите еще один E-mail и не создавайте на его никакие соц.сети! Также если вы занимаетесь чем-то серьезным, то не стоит в соц.сетях выкладывать личную информацию, ведь насколько известно, из ВК фото не удаляются, переписка тоже. По всем важным вопросам переговоры ведите через Jabber + OTR, но никак не через Вконтакте и ICQ.

Смена MAC адреса.
Слежка может идти и через MAC адрес. Как изменить MAC адрес, можно узнать через google, забив запрос: **Mac Address Spoofing**

Но как же быть, если необходимо что-то провернуть?

Если необходимо что-то провернуть, то лучше использовать для этого RDP (удаленный рабочий стол, или же другими словами — дедик).Дедик использовать нужно для того, если же вы хотите сделать что-то не хорошее. Продавцов дедиков полно, ищите. Также советую почитать мануалы «Как чистить логи на дедике» и т.д. Здесь это я описывать не буду.



Пояснение: При входе в сеть допустим мы имеем IP: 192.168.1.1 и уже изменили MAC адрес. Подключаемся и пускаем весь трафик через SSH тунель (как это делать я описывать не буду, мануалов много, как и селлеров, которые продают SSH тунели). После того, как мы пустили весь трафик через ssh тунель, мы подключаемся к дедику. По желанию вы можете на дедике пустить трафик через впн. Дальше делайте, что хотели. После окончания работы на дедике потрите логи.

Часть 11. Заключение и выводы

Давайте подведем итоги:

- Не нужно работать под учетной записью администратора!
- Прокси и соксы не такие уж и анонимные.
- Все ведут логи!
- При работе используйте дедик (а лучше связку, как на схеме последней)
- Не общайтесь в icq и скайпе по работе и не передавайте личную информацию
- Общение ведите только через jabber+otr!

И так, вы прочитали мой курс по анонимности и безопасности при работе в сети. Мы разобрали все методы анонимности при работе, разобрали несколько программ. Здесь была написана все самая нужная и необходимая информация, которая будет актуальна всегла! Вы могли заметить, что я нигде не указала реферальные ссылки, мы ценим своих читателей.

Спасибо всем тем, кто дочитал курс до конца, если у вас возникнут вопросы - мы будем рады вам помочь, отписывайтесь в комментариях на openssource.biz и вам обязательно помогут!

Самую полезную и актуальную информацию по работе в сети можно найти на этих форумах: http://forum.antichat.ru ; http://xaker.name ; http://exploit.in

Полезную халяву и рабочие способы можно взять тут: http://openssource.biz

Безопасная передача файлов: http://takebin.com

Всем спасибо за внимание!

С Уважением,

команда проекта openssource.