I2P — Lurkmore

I2P (*айтупи*, рус. *«Проект Невидимый Интернет»*) — средство, позволяющее ежедневно водить копирастам, спецслужбам и прочим пидорам хуём по губам. Одно лишь упоминание этого чудо-средства заставляет их срать кровавыми кирпичами в количествах, достаточных для постройки новой дурки для РАО, RIAA & MPAA сотоварищи.

Скоро Интернет станет невидимым
Скоро интернет станет невидимым
https://www.youtube.com/watch?v=TL8DYJjtyco
Как я купил дури и попал на дурку

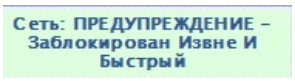
Представляет собой анонимную, самоорганизующуюся, распределённую и опенсорсную децентрализованную сеть. Конечно, за этими красивыми словами скрывается всего лишь связка туннелей, передающих данные через Интернет.

Техническая сторона

Децентрализованность

i2p Windows Tutorial
Как подключиться для слоупоков

Как и подобает любой анонимной сети, I2P децентрализована. В сети нет DNS, вместо них используют так называемые адресные книги, которые, подобно торренту, постоянно автоматически обновляются у всех клиентов от других клиентов. В них идёт сопоставление названия сайта или другого ресурса, известного как «`http://имя_сайта.i2p`», с его фактическим адресом (открытым криптографическим ключом). Вместо IP-адресов во всей сети используются открытые криптографические ключи, не имеющие абсолютно никакой логической связи с реальными компьютерами. Свой открытый криптографический ключ можно даже отослать заказным письмом всем копирастам, не забыв при этом распечатать в цвете немытый хер формата A1 и вложить в конверт, так как даже зная эти ключи, невозможно определить местоположение не только пользователей, но и серверов. ВООБЩЕ. Именно поэтому I2P нельзя отключить, отфильтровать или заблокировать. Она способна работать, даже если в сети останется всего 3,5 анонимуса.



Первое сообщение, которое получает пользователь, запустивший i2p

Толстый троллинг диванных теоретиков и кулхацкеров

Шифрование

Сеть проектировалась с расчетом на то, что каждый компьютер в ней принадлежит копирастам и следит за вами, собирая все пакеты снифферами и прочими примочками, поэтому для противодействия был введен ряд активных мер (например, таких как: Чесночная маршрутизация, многослойное шифрование, односторонние туннели, расхождение шифрованных пакетов по нескольким разным туннелям и так далее). Для дополнительной защиты каждый пакет шифруется по самое нехочу. В каждый пакет дописывается рандомное количество рандомных байт, после чего пакет подвергается сквозному, чесночному, туннельному, а также шифрованию транспортного уровня с использованием over 9000 алгоритмов:

1. 256 бит AES усиленный режим CBC с PKCS#5;
2. 2048 бит Схема Эль-Гамаля;
3. 1024 бит DSA;
4. 2048 бит Алгоритм Диффи — Хеллмана;
5. 256 бит HMAC — алгоритм проверки целостности сообщений;
6. Хэширование SHA256.

Шифрование всего твоего прона с лолями происходит на начальном компьютере, а расшифровка на конечном, и наоборот — всё, что ты качаешь, шифруется на сервере, а расшифровывается у тебя, поэтому всякие кулхацкеры не в состоянии перехватить незашифрованную информацию, как это почти всегда делают в TORe. К тому же даже перехваченный и расшифрованый пакет не несет почти никакой полезной информации, так как хуй поймешь, чей он и кому предназначается. До кучи, входящие и исходящие данные идут по разным туннелям, а данные одного типа дополнительно разделяются по нескольким туннелям. Криптологический пиздец, короче.

Весь трафик идёт по специальным шифрованным туннелям, направление которых через каждые десять минут рандомно меняется. Обычно создаётся несколько односторонних шифрованных туннелей, и пакеты расходятся по ним в произвольном порядке (исходящие через одну группу туннелей, а входящие через другую), направление туннелей же самое разнообразное.

Анонимность

Теперь все аноны, параноики, и лично ты могут спать спокойно: наконец-то создана сеть, где никто никого и никогда не найдёт. Однако, мой маленький друг, даже I2P не гарантирует АБСОЛЮТНОЙ защиты. JavaScript, а ранее ещё и Java, Silverlight и Flash никто не отменял. Для Фуррифокса юзаем QuickJava (иногда приходится вырубать жабу вручную), Java Script Options, FlashBlock и NoScript. Результаты трудов проверяем, например, здесь, здесь и здесь.

Попытки деанонимизации

Ежу понятно, что такое положение дел устраивает далеко не всех. Как же так, преступники планируют теракты, извращенцы смотрят некрозоололи-прон, кулхацкеры ~~сбут гусей~~ воруют деньгу? …Некошегно! Поэтому были произведены попытки деанонимизации. Пруфлинк. Товарищи с forum.i2p быстренько разобрали статейку по полочкам, но отреагировали на удивление спокойно.

> Сама по себе I2P не скомпрометирована, однако при настройке сервера следует затрахнуться, чтобы не спалить себя в будущем, по ссылке (имеется в виду статья) доступны рекомендации, которые снизят вероятность деанонимизации.
>
> Методы деанонимизации
>
> 1. Banner grabs of both eepSites inside of I2P, and against know IPs participating in the Darknet, to reduce the anonymity set of the servers.
> 2. Reverse DNS and who is lookups to find out more information concerning the IPs of the I2P nodes.
> 3. TCP/IP stack OS finger printing.
> 4. Testing I2P virtual host names on the public facing IP of I2P nodes.
> 5. Compare the clock of the remote I2P site, and suspected IP hosts on the public Internet, to our own system's clock. We did this via the HTTP protocols "Date:" header.
> 6. Command injection attacks.
> 7. Web bugs to attempt to de-anonymize eepSite administrators or users. (This turned out more problematic than we originally thought)
>
> С моей точки зрения — побольше бы подобных исследований, **потому что чувство защищённости, которое даёт I2P, потенциально заставляет нас уделять безопасности и анонимности меньше времени**, думая, что I2P всё сделает за нас. Рекомендации, данные в этой статье, в любом случае полезны и помогут сделать сайты ещё анонимнее.

— http://forum.i2p2.de/viewtopic.php?t=5353

Вместе с тем, известен метод определения IP серверов в I2P, который может быть успешно использован при наличии достаточно больших ресурсов у взломщика, — атака пересечением. Существует мнение, что владельцев Silk Road и Freedom Hosting из тора нашли, используя именно эту методику. I2P также подвержен этой атаке, что признают сами разработчики. Более того, решения проблемы в ближайшем будущем не предвидится.

Деанонимизация, как мы видим, вещь не такая уж и нереальная. Кроме того, хитрожопая гэбня давно изобрела прибор, позволяющий значительно повысить шансы на успешное закрытие анонимуса. Один из неизбежных недостатков — это видимые IP адреса. Доказать, что там, на том или ином IP лежит какая-нибудь СР — сложно ровно до тех пор, пока в гости не пришли с проверкой компетентные граждане в штатском. Тем не менее, ввиду наличия этих ваших ~~TrueCrypt~~ VeraCrypt и «Убедительной отрицаемости™», всё не так однозначно, мой дорогой анонимус. Дело в том, что софтина эта была придумана для англичан, находящихся в анальном рабстве Буквы Закона. Оная гласит, что не отдавший сотруднику внутренних органов ключи от сейфов, пароли от компьютеров и деньги из кошелька неминуемо наказывается раскалённой кочергой и попадает автоматически на пять лет ещё более жестокого анального рабства. За сим было придумано создавать скрытые тома (— убедительная отрицаемость пруф). Если хранить на нём всё дорогое сердцу — риск значительно снижается. Хотя, если прикажут…

Реализация клиента на C++

Новая эра I2P — I2Pd (Демон Невидимого Интернета!). Независимым анонимусом была создана новая реализация клиента для доступа к сети I2P на языке программирования C++, как положено с открытым исходным кодом. На смену официального глючного клиента на яве, анонимусам предложили использовать не менее глюченую версию клиента на C++, но зато, у такой реализации есть ряд преимуществ: высокая скорость работы, и низкое потребление оперативной памяти (в 5-20 раз меньше). Однако она не поддерживает расширения, поэтому в ней не будет плюшек вроде встроенных безопасной почты и торрентов (их можно подключить через мосты SAM и BOB).
С появлением I2Pd Browser Bundle, установка стала не сложнее TOR, и вообще не требует от юзера никаких специальных знаний.

По поводу этой реализации уже давно бушуют холивары в разных уголках даркнета! Главнейший из которых — подозрение в причастности к разработке I2Pd российских спецслужб. На это косвенно указывают баннеры проправительственных ресурсов, заботливо размещённые на главной странице роутера. Плюс к тому, разработчики I2Pd создали собственную криптовалюту GOSTCoin, в которой используются чекистские криптосредства ГОСТ Р 34.10-2012.
В то же время, никаких закладок и бэкдоров в исходном коде I2Pd обнаружено не было (правда, их никто и не искал).

Копирасты и I2P

Хоть про сеть знает не так много народу, но она всё же успела засветиться в СМИ:

> **Интернет идет в темную зону**
>
> **Киберпреступники начали создавать параллельный виртуальный мир**
>
> Пока правоохранительные органы совместно с юристами ломают головы над тем, как законодательно наладить эффективный контроль за привычным Интернетом, киберпреступники всех мастей создают свои новые виртуальные сети.
>
> Параллельный Интернет — это уже реальность.
>
> Такие мнения высказывали участники прошедшего в Москве «круглого стола» «Международное право и Интернет». В нем приняли участие юристы-международники из Дипакадемии МИДа, Института актуальных международных проблем, Центра международного права и безопасности Координационного центра Домена. RU и Домена. РФ. Они говорили о том, что отношения в сфере Интернета объективно требуют решения многих вопросов на межгосударственном уровне. В виртуальном пространстве с каждым днем все больше становится реальных преступлений. Здесь и мошенничество с банковскими карточками, и грабежи, и вымогательство, даже настоящие убийства. Например, отключить дистанционно, находясь порой за тысячи километров, дыхательный аппарат больному в клинике способен редкий киллер. Понятно, что такие люди ищут любые возможности быть незамеченными. И находят их.
>
> Причем киберпреступники зачастую пользуются плодами вполне законопослушных программистов и даже спецслужб. Дело в том, что сейчас возможности ухода из традиционного Интернета ищут и на государственном уровне многие страны, ведь сегодня привычная нам Мировая паутина устроена таким образом, что она глобально подконтрольна США, а это нравится далеко не всем. Например, большая часть российского интернет-трафика коммуникативно проходит через Норвегию, страну НАТО. Понятно, что в случае любого конфликта зону «ru» нам просто отключат, и тогда, как говорил известный актер, «кина не будет». Подобная картина уже была в 2008 году, когда оказалось, что российские войска в Цхинвале либо прослушивались неприятелем, либо вообще были лишены связи. Кроме того, в период этого конфликта Грузия полностью заблокировала доступ к зоне «ru» не только для своих граждан, но и для имеющей через неё доступ соседней Армении.
>
> Поэтому появление новых независимых доменных зон, как, например, кириллическая зона «ру», — это наш государственный ответ на стратегические киберугрозы. Пока особой активности киберхакеров в ней не наблюдается. Причин несколько. Она еще невелика, а потому менее интересна, чем, например, доменная зона «com», в ней пока меньше банков, онлайн-платежей. К тому же зона «ру» отслеживается отечественными правоохранительными органами. **Незаконопослушные программисты ищут другие удобные для себя варианты. Они начали создавать свои виртуальные миры. Например, как вам нравится „I2P — «Проект Невидимый Интернет»“? А ведь он уже работает, и не только он.**
>
> По мнению интернет-эксперта Сергея Шипилова, в подобных сетях злоумышленники могут обмениваться информацией, не опасаясь посторонних глаз и ушей. Даже если киберполиции станет известно о распространении в данной сети, скажем, детской порнографии, вычислить адрес отправителя и получателя будет крайне сложно. Это в привычном нам Интернете любой шаг пользователя оставляет след. В иных виртуальных мирах контролировать заходы по адресам, кто в какую дверь стучался, пока крайне затруднительно.
>
> Помочь найти преступников могут только совместные усилия всего международного сообщества. Для этого надо заключать договоры и создавать единые правила игры по одним законам в виртуальном пространстве.
>
> В этом году в Москве при поддержке Минкомсвязи России состоялся первый российский форум по управлению Интернетом. Нынешний «круглый стол» стал логическим продолжением форума.

— Тимофей Борисов, «Российская газета» — Федеральный выпуск № 5373 (294) от 28 декабря 2010 года

I2P и интернеты

Из I2P можно невозбранно выходить в обычную сеть и, более того, использовать почту, торренты, IRC, а для параноиков — HTTPS и SSL вкупе, однако есть пара нюансов. Для выхода в интернеты в I2P используется несколько общих шлюзов, преимущественно в Дойчланде. Поэтому со скоростью в направлении I2P ↔ интернет немного туго (в реале до 5 Мбит/с). К тому же некоторые шлюзы находятся в черных списках, и поэтому не все ресурсы через них можно посмотреть. Cookies работают только при сёрфинге I2P → интернет. При попытке доступа интернет → I2P (например, через шлюз) печенюшки режутся напрочь, так что авторизация на сайтах не проходит. Радикально решает проблемы надстройка Orchid, которая подключается к TOR, после чего из I2P становятся доступны и луковые сайты, и луковые же outproxy во внешние интернеты.

Практика использования показывает, что для создания правильных ресурсов самые продвинутые аноны создают сайты .i2p, запуская шлюзы на VPS хостерах, которые находятся не в этой стране.

Вебмастеринг в I2P

Поскольку скорость и стабильность коннекта в сети I2P оставляет желать лучшего, эта сеть идеально подходит школовебдезигнерам, застрявшим во времена FrontPage 2002. В то время как новомодные веб-движки, требующие постоянного конекта и передач гигабайт данных, глючат и тормозят, чистый HTML прекрасно сочится сквозь динамично меняющиеся туннели (или тоннели, х.з.).

pgpru.com о сабже

> I2P — это двойник сети Tor, но его авторы часто применяют "противоположные" методы для решения тех же инженерных задач. Например, вместо транспортного протокола TCP используется UDP, вместо роутинга в интернет — внутренняя закрытая сеть (хотя возможно и то и это), вместо "луковичной" маршрутизации — "чесночная", а цепочки называются туннелями. Есть аналоги скрытых сервисов Tor. Туннели разделены на два пути, проходящие через разные наборы узлов (по замыслу авторов это усиливает анонимность, но однозначного мнения исследователей на этот счёт нет — возможны аргументы в пользу обоих мнений). Каждый узел I2P является в принудительном порядке и клиентом и сервером. Ради лучшей анонимности пользователи могут выбирать более длинные цепочки и более высокие задержки трафика, но доказательства того, что это не упрощает профилирование трафика пользователей, не предоставлено. Сеть I2P также нестойка к глобальному наблюдателю. Интересно, что сами разработчики I2P предпочитают оставаться анонимными, что имеет, по крайней мере, такой недостаток: хотя исходный код проекта и открыт, сам проект (его теоретическая проработка) получит заведомо меньше внимания со стороны научного сообщества.
>
> — *https://www.pgpru.com/faq/anonimnostjobschievoprosy#h37444-4*

Факты

- Сеть очень похожа на torrent по своей структуре (см. хотя бы обмен адресными книгами).
- Хинт: для быстрого включения/выключения любого прокси (Tor/I2P/...) в Огнелисе есть Quick Proxy;
- Хинт 2: для автоматического переключения — FoxyProxy;
- Хинт 3: для безопасного переключения предлагается использовать специальную сборку лисы Tor Browser Bundle. Либо можно настроить браузер на использование прокси из файла: %корневая_директория_I2P%/scripts/i2pProxy.pac. Вообще, сами авторы категорически не рекомендуют использовать автоматическое переключение прокси и вообще пользоваться и I2P и открытой сетью через один и тот же профиль в браузере, во избежание деанонимизации.
- DNS в пределах сети I2P не глобальна. Есть популярный регистратор stats.i2p, но его правилами запрещается регистрация «плохих» ресурсов, а при регистрации форумов и т. п. ресурсов, наполняемых пользователями, требуется включать эти правила в условия использования самого ресурса. Можно использовать другой регистратор, например, inr.i2p, как это делает Hiddenchan, но дистрибутив I2P по дефолту не настроен забирать домены с этого регистратора. Можно жить на длинном b32 адресе. Можно вообще без регистраторов, использовать домен, а, чтобы этот домен можно было отрезолвить, добавлять i2paddresshelper в ссылки. Наиболее эффективное решение — использование Emercoin Blockchain, такой домен невозможно отозвать или спиздить.
- Осознавая значимость I2P, пятнадцатирублёвые регулярно вандалят русскоязычный сегмент сети и даже открывают там свои ресурсы.

Сервисы I2P

- I2P-Bote — анонимный

Объективное сравнение самых популярных анонимных сетей

децентрализованный распределённый аналог почты. С обычной почтой несовместим. Встраивается как плагин в I2P.
- I2P-Mail — обычная почта, только в I2P, к тому же со шлюзом в обычные интернеты. Для работы с ней можно использовать любой почтовый клиент, инфы по настройке полно.
- I2P-Messenger — анонимный децентрализованный IM. Да-да, асечка, только насквозь анонимная. Звук получения сообщения, как обычно, невозбранно спизжен из той самой аськи. См. TorChat.
- I2P-IRC . Как настроить, написано даже на главной странице I2P-роутера.
- I2P-Jabber. В свете наличия I2P-Messenger нужен разве что как лишняя альтернатива.
- I2P Speedtest — как бы speedtest.net, тока в I2P. Фэйл, так как показывает только скорость через текущую цепочку туннелей, а они меняются раз в десять минут.
- Rapidshare.I2P по аналогии. Файлообменник.
- Анонимный вариант Gnutella. Чем-то напоминает DC, с чатом и поиском, только без хабов и IP-адресов.
- I2P tahoe-lafs — распределённая сетевая крипто-фс, только запущенная в I2P. Если такая хрень будет установлена на каждом домашнем роутере или файлопомойке по дефолту, попахивает вином. Сайт tahoe-lafs; в I2P.
- iMule — аналог eMule для I2P. Пиринговая файлообменная сеть поверх пиринговой криптосети, мечта параноика.
- Радио Анонимус. Нахера он нужен в I2P, не знают даже сами создатели радио: вещания через I2P пока нет и хз, будет ли. Вот адрес.
- PrivacyBox — зеркало privacybox.de в I2P. Вещь полезная, однозначно.

Ресурсы I2P

Пруфпик Hiddenchan'а (2012 год)

- Главная страница проекта в сети I2P.
- Русская I2P-Вики. Если бы не унылость и, как следствие, непопулярность, стала бы новой бордой для очередного политосрача (см. новый логотип).
- Русская анонимная торговая площадка для купли/продажи полу/не/легальных веществ оплата Bitcoin/BTC, личные сообщения с PGP. Имеет кучу зеркал nvspc.ru, nvspc.biz, nvspc.com, nvspc.net в обычном инете. Qiwi-Bitcoin обменник.
- Первый сносно работающий поисковик.
- Hiddenchan — русский имиджборд на просторах анонимной сети. На данный момент закрыт — админу надоело. Архив хидденчана.
- Флибуста — ещё одна.
- Postman — торрент-трекер.
- DifTracker — ещё один.
- Русский торрент-трекер, иногда даже работает.
- Зеркало ноунеймклуба, торрент трекера.
- Список сайтов в сети I2P.
- Freezone.i2p — социальная сеть по типу хабра (но не по качеству).
- id3nt.i2p — местный сервис микроблоггинга.
- open4you.i2p — бесплатный хостинг в I2P.
- Hiddenbooru — своя бура с лолями и проч.
- Баш — Скрытобашорг.
- Hiddengate — портал, посвящённый i2p и анонимности чуть более, чем полностью. Имеется вики, форум и имиджборда.
- Onelon — анонимная социальная сеть. Удобнее, чем имиджборды, безопаснее, чем социальные сети.
- traditio.i2p — Торадицийо же (зеркало)!
- 102chan.i2p — одна из немногих относительно живых русскоязычных борд. Создана и поддерживается ООО «Главсеть»

Подписки для i2p

- http://biw5iauxm7cjkakqygod3tq4w6ic4zzz5mtd4c7xdvvz54fyhnwa.b32.i2p/uncensored_hosts.txt
- http://bl.i2p/hosts2.txt

- http://cipherspace.i2p/addressbook.txt
- http://dream.i2p/hosts.txt
- http://hosts.i2p/
- http://hosts.i2p/hosts.cgi?filter=all
- http://i2host.i2p/cgi-bin/i2hostetag
- http://i2p-projekt.i2p/hosts.txt
- http://inr.i2p/export/alive-hosts.txt
- http://joajgazyztfssty4w2on5oaqksz6tqoxbduy553y34mf4byv6gpq.b32.i2p/export/alive-hosts.txt
- http://rus.i2p/hosts.txt
- http://stats.i2p/cgi-bin/newhosts.txt
- http://tino.i2p/hosts.txt
- http://trevorreznik.i2p/hosts.txt
- http://www.i2p2.i2p/hosts.txt

Обычные ссылки

- Главная страница проекта в обычном интернете
- Официальная инструкция по настройке

Интернет

Интернеты 127.0.0.1 ADSL Bitcoin CMS DDoS Frequently asked questions GPON I2P Internet White Knight IPv6 IRC MediaGet Miranda NO CARRIER QIP Ru@razlogoff.org SEO Skype Tor TOS Via WAP Ёбаное ВТ Админ Акадо Американские интернеты Анонимус Аська Бан Бесплатный хостинг картинок Блог Блогосфера Бот Ботнет Браузерка Бугагашечки Бурление говн Вап-чаты Веб 1.0 Веб 2.0 Вики Виртуал Вордфильтр Голосование ногами Гостевуха Диалап Дом.ру Домашняя страница Дорвей Единый реестр запрещённых сайтов Жаббер Заповеди интернета Заработок в интернете Идентификация пользователей в интернете Известные интернет-флешмобы Имиджборд Инвайт Интернет-магазин Интернет-сервисы Искра Кик Кириллические домены Кликбейт Коммент Комьюнити Лесенка Лог Локалка Макхост Мем Микроблог Мобильный интернет Модератор Некропост Ник Оптимизатор Ответы Офлайн Оффтопик Письма счастья Подкаст Поисковая бомба Покровитель интернетов Пост Правила интернетов Предыдущий оратор Премодерация Пруфлинк Рерайтинг Ростелеком Сабж Сетевые онанисты Симпафка Синдром вахтёра Ситилайн Скайнет Скриншот Смайл Социальная сеть

Имиджборды

Wakaba 1chan 2-ch.ru 2ch 2ch.hk 2channel 410chan 4chan A Altogether Anonymous Directory Apachan B Bo Boku no Pico Brchan Brofist Bump Butthurt Combo breaker Cool story bro Creepy threads D Drawhore Duckroll Facepalm Fg Fl Forever Alone Futaba GIF GTFO Gununu I see what you did there I2P In before Int Internet Hate Machine It's Raping Time! ITT Ja Low Orbit Ion Cannon Moar Mu Not Your Personal Army O RLY? OBEY Oh noes Oh, exploitable! Olanet Overchan Paper Child Pepe the Frog Pic related Polandball Prepare your anus Project Chanology Project Chanology/B России Project N.I.G.R.A. PS3 has no games R Rage Comics Rarjpeg Rf RGHost Rick Roll S Sage The Xynta There are no girls on the Internet Tr Uchan UWBFTP Vg Wh Wishmaster X, X everywhere YOBA ZOMG TEH REI Øchan Анимешник Анонимус Анонимус доставляет Бамплимит Банхаммер Бесплатный хостинг картинок Битард Битардск Богиня Быдло-кун Вайп Валюты имиджборд Вин Во все поля Война имиджборд Все ебанулись Гайдзин ёнкома Гельминтарий Гет Двач

Software

12309 1C 3DS MAX 8-bit Ache666 Alt+F4 Android BonziBuddy BrainFuck BSOD C++ Chaos Constructions Cookies Copyright Ctrl+Alt+Del Denuvo DOS DRM Embrace, extend and extinguish FL Studio Flash FreeBSD GIMP GNU Emacs Google Google Earth I2P Internet Explorer Java Lolifox LovinGOD Low Orbit Ion Cannon Me MediaGet MenuetOS Microsoft Miranda Movie Maker MS Paint Open source Opera PowerPoint PunkBuster QIP Quit ReactOS Rm -rf SAP SecuROM Sheep.exe Skype StarForce Steam T9 Tor Vi Windows Windows 7 Windows Phone 7 Windows Phone 8 Windows Vista Wine Winlogon.exe Wishmaster Word ^H ^W Автоответчик Антивирус Ассемблер Баг Билл Гейтс и Стив Джобс Блокнот Бот Ботнет Браузер Варез Винлок Вирусная сцена Генерал Фейлор Глюк Гуй Даунгрейд Демосцена Джоэл Спольски Донат Защита от дурака Звонилка Интернеты Кевин Митник Китайские пингвины Костыль Красноглазики Леннарт Поттеринг Линуксоид Линус Торвальдс Лог Ман Машинный перевод Мегапиксель

Just Another Fucking Acronym

14/88 1C 265 A.C.A.B. ADSL AFAIK AFK AISB AJAX Aka All your base are belong to us AMV ASAP ASL ASMR ASUS EEE BAT BBS BDSM BOFH BRB BSOD BTW CMS Command & Conquer Copyright Counter-Strike CYA DC DDoS Delicious flat chest Direct Connect DIY DJ Doki Doki Literature Club! DOS DRM EFG Etc Five Nights at Freddy's Frequently asked questions FTL FTN FTW FUBAR GIF GIMP GNAA GPON Grammar nazi Grand Theft Auto GTFO Happy Tree Friends HBO How It Should Have Ended I see what you did there I2P IANAL IDDQD IIRC IMHO In before Internet Explorer IRC IRL ITT JB (ЛОР) JFGI Kerbal Space Program KFC KISS Let's get ready to rumble! LFS Livejournal.com LMAO LMD LOL Low Orbit Ion Cannon M4 MacOS Microsoft MILF MMORPG MSX MTV N.B. NASCAR NEDM NES NoNaMe Not Your Personal Army NRB NSFW O RLY? OK OMG OS/2 P. S. P2P Panty and Stocking with Garterbelt

Пиратство

1C Copyright Denuvo Direct Connect DRM EDonkey2000 GamerSuper I2P Infostore Metallica Microsoft Neogame Nintendo NoNaMe One Piece P2P Rapidshare RGHost Rutracker.org SecuROM SOPA StarForce Steam The Pirate Bay Акелла Варез Горбушка Денис Попов Дискета Диски с приколами Единый реестр запрещённых сайтов Зайцев.нет Компьютерные пираты Копираст Копирсрач Крякер инета Кулхацкер Либрусек Линукс Литрес Морские пираты Никита Михалков Нойзбункер Пиратские игры девяностых Радиопираты Распечатать лицензию на Линукс Российское авторское общество Русефекации Русский щит Сомалийские пираты Таблэтка ТНТ Файлообменник Фаргус Хакер Экранка Яблочник

w:I2P en.w:I2P (anonymity network) wr:I2P