

Телекомикс: знаки на стене

История телекоммуникаций столь стремительна, что отследить все взлеты и падения, приход и уход технологий и трендов решительно невозможно. Казалось бы, всего десять лет - тьфу, по сравнению с историческим таймлайном человечества, а поди ж ты! Уже сменилось не одно поколение оборудования, а компьютерно-телекоммуникационный андеграунд изменился неузнаваемо.

Вот, например, давно ли шли холиворы относительно WiMAX? Взлетит, не взлетит? А если "взлетит", то в какую сторону и что делать, если частотного ресурса, в силу его природной ограниченности, на всех не хватит?

Ну, положим, WiMAX не взлетел журавлем, а стал весьма нишевым решением - дорогим и до сих пор неказистым.

А вот кто помнит - что вот это такое держит в руках сей импозантный юноша?



А между тем, это Стив Возняк собственной персоной, от роду ему на этом снимке 17 лет (1967 год), а в руках он держит знаменитую ["синюю коробочку"](#).

В те годы было модно "хакать" телефонную компанию. В единственном числе - потому что была только одна AT&T и эта компания считалась сосредоточием зла и бюрократии, в определенных кругах.

BlueBox теперь хранится в музее под стеклом:



Хотя коробочек разных цветов (не только синего) было сделано немало. Были черные, красные, оранжевые, зеленые, бежевые, пурпурные коробочки. Одна была даже "[вермилионовая](#)". Словарь говорит, что это цвета "киновари" - то есть ярко-красная.

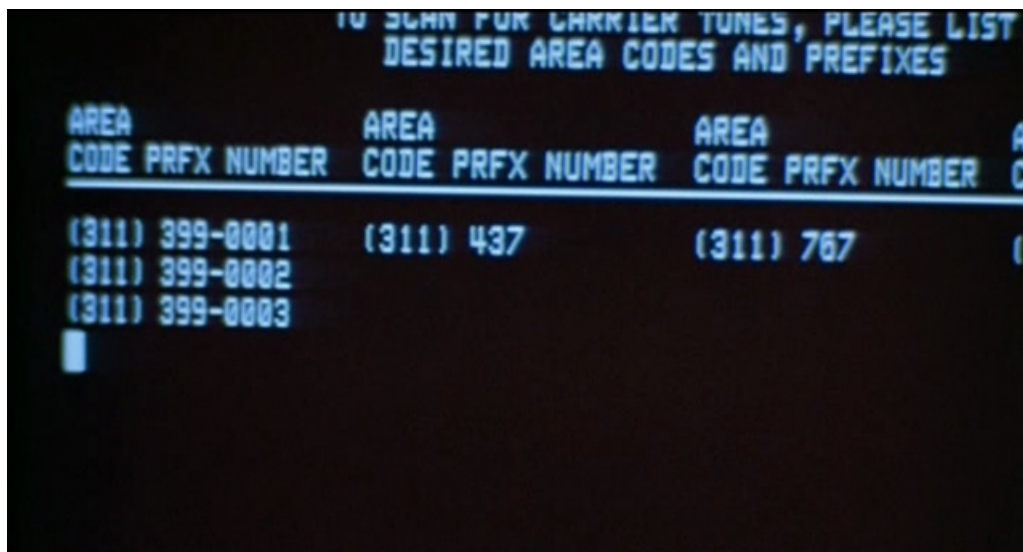
Но время текло, телефонный фрикинг стал не столь интересным, потому что появились новые забавы.

Например, через полвека молодежь занималась уже несанкционированным доступом не к телефонным компаниям, а к только-только появившимся хот-спотам Wi-Fi. Но андеграундный флёр телеком-взломов остался неизменным - уж больно Captain Crunch (в миру - [Джон Дрейпер](#)) оказался прикольным.

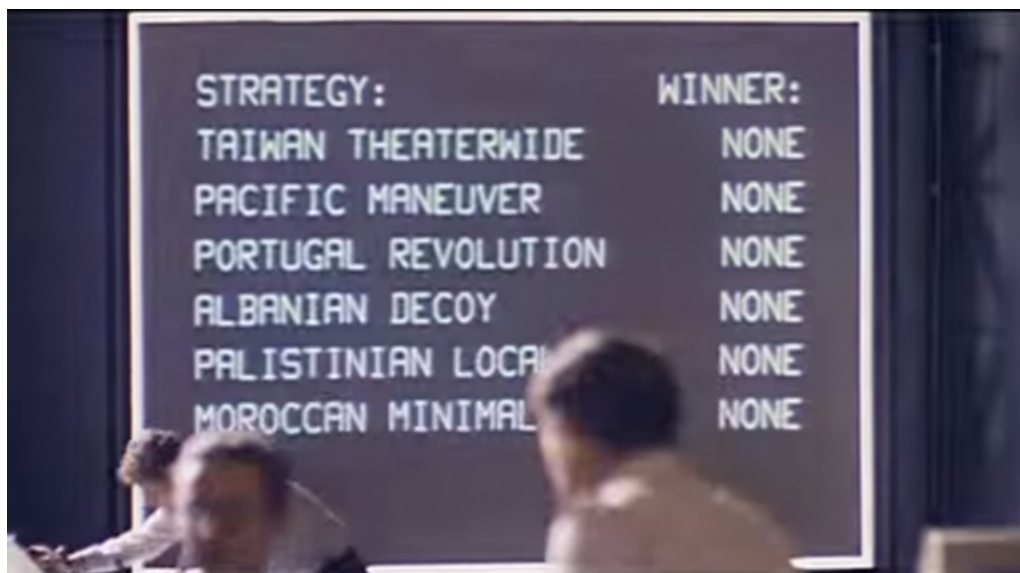
Процесс поиска и последующего взлома Wi-Fi хот-спотов был скопирован с другого хакерского андеграундного метода, связанного с поиском модемов в сети - [wardialing](#)'а. Суть которого сводилась к простому перебору телефонных номеров в заданном префиксе или диапазоне с целью найти на нем модем. Делалось это с помощью специальных программ, некоторые из которых были довольно изощренные.

Хот-споты же приходилось искать на улице, ибо радиоканалы "светят" через стены и при некоторой сноровке можно поймать "волну" просто пройдя мимо здания с работающим Wi-Fi роутером.

Стоит упомянуть, что народную популярность Wardialing приобрел после фильма "[Военные игры](#)", где этот метод был показан в полный рост на широкую публику:



И клюквы, свойственной синематографу восьмидесятых, в фильме тоже предостаточно:



"Португальская революция" и "Албанская ловушка" - очень красиво звучит.

Но когда появился Wi-Fi, новое поколение хакерствующей молодежи переключился на эту технологию. Целью было просто попасть в Интернет "на халяву" - в начале 2000-х доступ в сеть был достаточно дорог, использовались повременные или помегабайтные тарифы. Поднимите руку те, кто хоть раз в те времена не "попадал на бабки", по причине того, что виндовс внезапно решила обновиться, и скачала полгигабайта каких-то файлов? :)

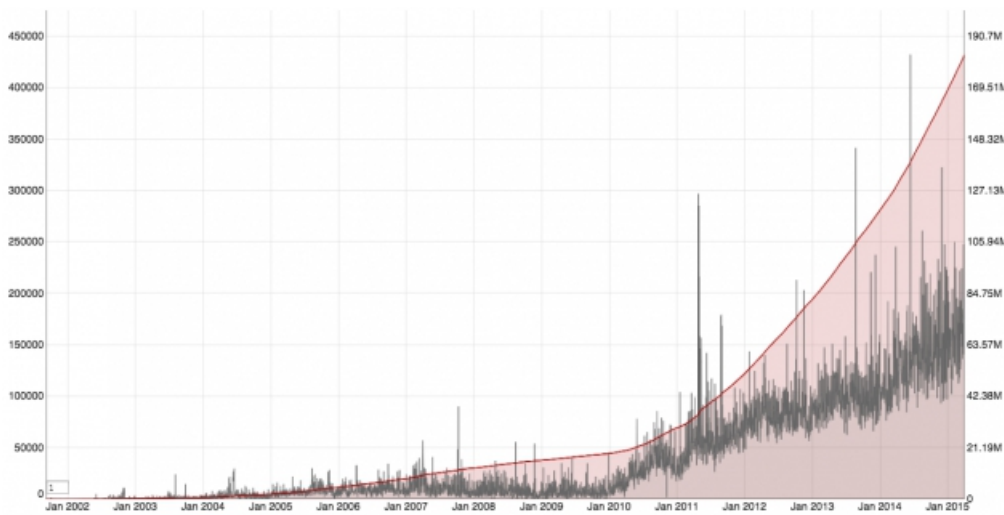
Но не только воровство трафика, заставляло "цифровых пиратов" выходить на улицу. На самом деле, это просто очень интересный процесс - найти, взломать, получить доступ к неким ресурсам.

Некоторые увлекающиеся персонажи тратили приличные деньги на соответствующее оборудование и софт:



В комплект обязательно входил заряженный ноутбук с соответствующим софтом, GPS-трекер для определения координат найденного спота и хорошая внешняя антенна для сами знаете чего.

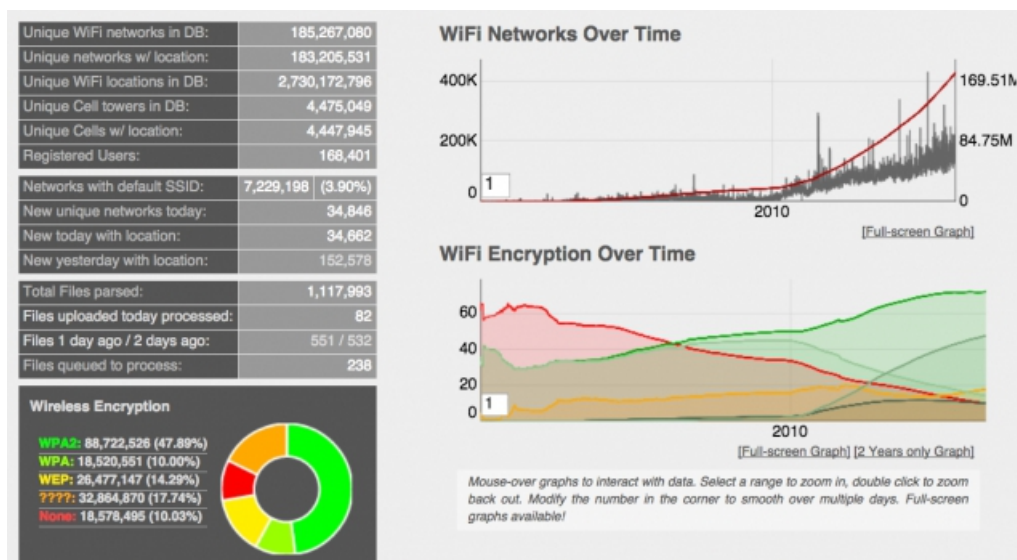
Со временем, появились и специализированные девайсы - все ж школа Капитана Кранча:



Серым считается хот-споты "ежедневно он-лайн", а красным - total.

[Сайт называется wigle.net](http://wigle.net)

Там довольно много интересных данных, кстати:



Видно, что более половины действующих хот-спотов на сегодня используют шифрование [WPA/WPA2](#), которое появилось только в 2006 году. До этого момента использовался алгоритм [WEP](#), который взламывается за несколько минут, чем и вовсе пользовались воришки. График справа снизу показывает, как одна технология защиты сети вытесняется другими, более совершенными - видно, что WEP до сих пор используется некоторыми недалёковидными владельцами.

На сайте Wigle.net есть и специальная база данных, где можно поискать и собственный хот-спот. Я свой домашний не нашел. Очевидно, это связано с тем, что до моей деревни ни один хацкер со сканером (сейчас это просто [программка под андроид](#), исходный код которой [лежит на GitHub](#)) не добрался.

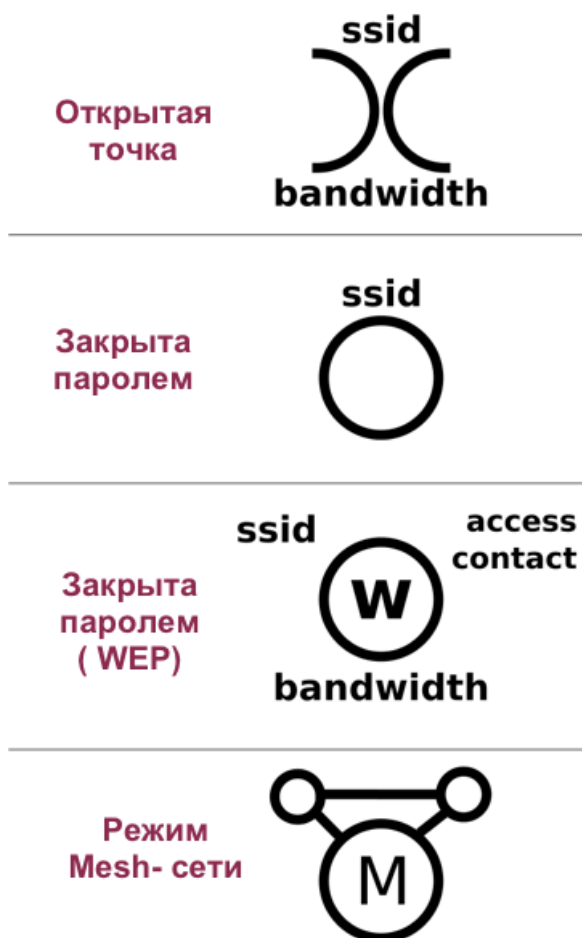
Вот так выглядит карта нашей деревни с точки зрения Wigle:



Или более сложные:



Обозначения знаков были следующие:



Это явление называется [warchalking](#), где первая половинка от wardriving, а вторая, "chalking" - означает "рисовать мелом".

"Открытая точка" - все понятно. Пароля нет - пользуйтесь. Иногда пишут еще SSID и максимальную скорость, которая эта точка дает. Ну, чтоб люди не тратили лишнее время. Если точка доступа очень медленная - писали просто "SLOW"

"Закрытая точка" - это с установленным паролем, но с каким-нибудь простым паролем. Или по-умолчанию. Сам пароль обычно не писали - чтоб хозяин волноваться не начал.

"Закрыта паролем" с буквой W означает спот, который использует устаревшее шифрование WEP. Чтоб зайти в такую сеть нужен специальный софт, который, впрочем, у человека, понимающего о чем этот символ, должен быть.

Последний символ означает, что точка может работать в режиме [mesh-сети](#).

Вот более сложные символы с описанием. Я не стал переводить - и так все понятно.

let's warchalk..!		Proposed New Signs	
KEY	SYMBOL		
OPEN NODE	ssid  bandwidth	 Unrestricted access	 AP with MAC filtering
CLOSED NODE	ssid 	 Open access with restrictions	 Pay for access AP
WEP NODE	ssid access contact  bandwidth	 AP with WEP	 AP with multiple access controls (not for public use)
blackbeltjones.com/warchalking		 AP with closed ESSID	 Honeypot

Поясню лишь последний - [Honeypot](#).

Раз речь идет о "войне", у тех, кто нападает могут появиться и враги - те, кто защищает. Логично, что лучший способ защиты - словить тех, кто безобразничает. А как словить того, кто целенаправленно ищет и взламывает хот-споты? Конечно, дать ему хот-спот! Но, во-первых, такой, чтобы никто из "нормальных людей" им пользоваться не начал, а, во-вторых, никаких действительно важных вещей в приманке не содержалось.

Далее проще - как только на Honeypot'е появляется пользователь, администратору поступает сигнал "ура! нас атакуют!". Все действия безобразника, разумеется, логируются. Остается только выйти во двор и посмотреть, кто это здесь такой умный с ноутбуком, а доказательная база может основываться, например, на типе браузера в логах.

Вардрайверы научились со временем выявлять такие хот-споты и помечать спец-символами. Глаз - один из них.

Еще немного нагугленных символов:





Из последних веяний:



"Глаз" с характерными радиоволнами означает, что ведется мониторинг Wi-Fi устройств. В данном месте установлен Wi-Fi датчик, который собирает сведения о всех mac-адресах устройств в поле видимости. Затем эти данные используются для аналитики и в маркетинговых целях. Ничего страшного в этом мониторинге нет - сведения же обезличены полностью, - но находятся параноики, которым это не нравится. Им можно посоветовать только выключать на своих гаджетах Wi-Fi в тот момент, когда перестаете им пользоваться.

В конце телекомикса хочу дать коллегам один небольшой совет. Дело в том, что вот такие значки Wi-Fi:



которые так полюбились народу, в пространственном дизайне использоваться не могут. Этот логотип имеют право использовать только и исключительно члены [Wi-Fi Alliance](#) - некоммерческой организации, которая занимается развитием стандарта и сертификацией устройств.

Знак "инь-янь Wi-Fi" предназначен для нанесения на устройства, которые прошли проверку в Wi-Fi Альянсе и признаны ~~хорошими~~ совместимыми с другими устройствами, а за неправомерное использование значка можно и загребеть в суд ([ст. 14.10 КоАП РФ](#)). Прецеденты уже случались.

Для обозначения хот-спота же, существует специальный официальный символ:

[\[Телекомикс: знаки на стене\]](#)

Это символ можно невозбранно [скачать с официального сайта Альянса](#) в нескольких вариантах и цветовых решениях. Доступны "сорцы" в кривых. Вся правовая информация - там же.