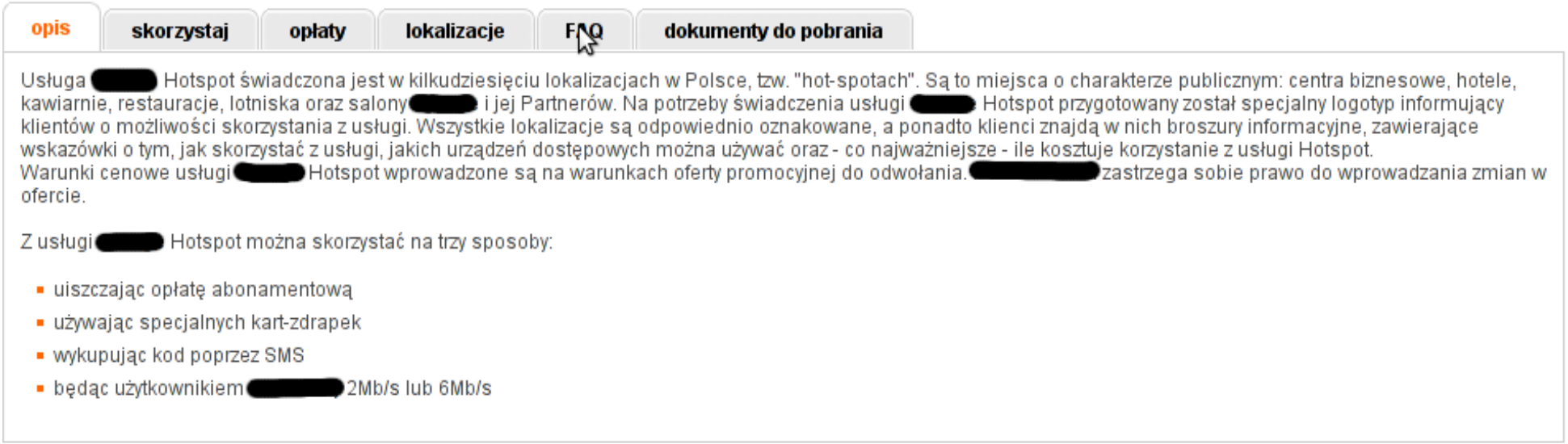
Jak zdobyć internet?

Czyli co nieco o tunelowaniu.

Często mamy do czynienia z sytuacją w której nasz dostęp do sieci jest mocno ograniczony. Przykładowo, chcemy skorzystać z HOT-SPOTa w jakimś hotelu, ale jedyne co ukazuje się naszym oczom to okienko logowania i wielki przycisk „Zapłać”.



Jeden z bardziej popularnych płatnych HOT-SPOTów.

Lub... użyć tunelowania.

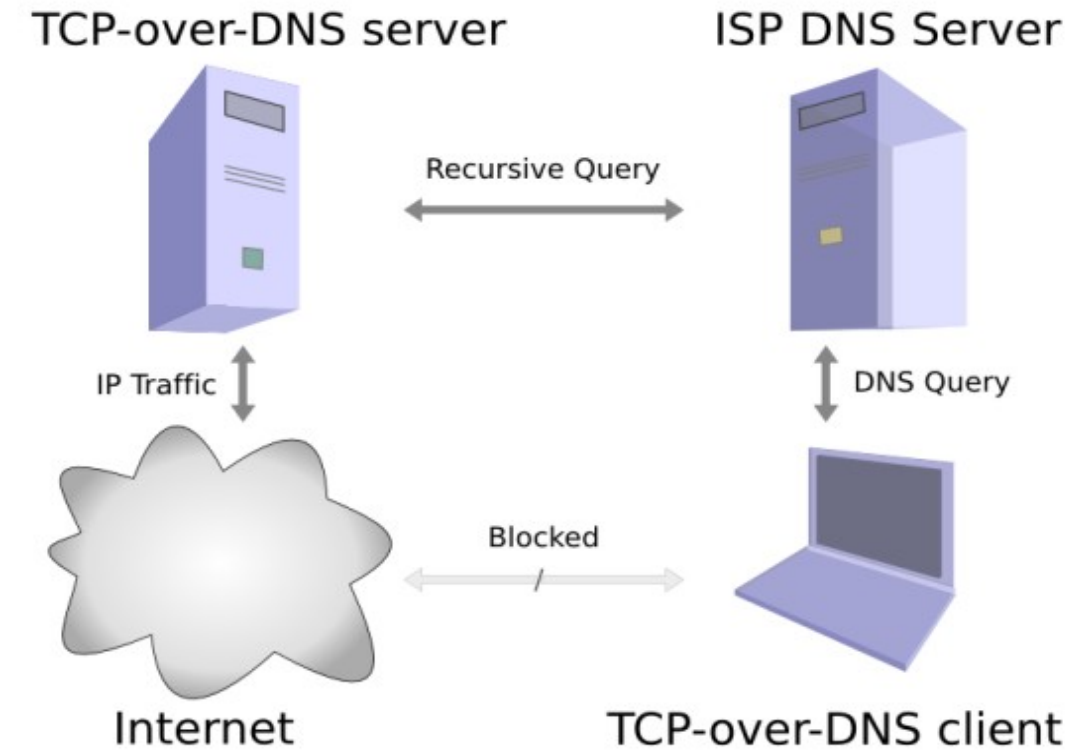
IP over DNS

Czyli tunelowanie ruchu TCP/IP poprzez zapytania DNS. Wymaga to zastosowania serwera DNS, który będzie „rozumiał” naszą komunikację i umożliwiał przesyłanie pakietów.

Prędkość takiego połączenia zależy od wielu czynników. Od użytych pól zapytania DNS, prędkości wykonywania zapytań, użytego klienta/serwera, limitów zapytań, … Można przyjąć, że średnio połączenie zestawione jest z prędkością ok. 128kb/s.

W większości wystarcza to do sprawdzania poczty, przeglądania stron, połączenia ssh itp.

Przyjemne HOWTO można znaleźć na stronie http://analogbit.com/tcp-over-dns_howto.


TCP-over-DNS server
ISP DNS Server
Recursive Query
IP Traffic
DNS Query
Blocked
Internet
TCP-over-DNS client

TCP over DNS

Przykładowe aplikacje:

nstx (http://thomer.com/howtos/nstx.html) – używa interfejsów tun/tap do tunelowania ruchu. Wymagane wsparcie w jądrze.

dns2tcp (http://www.hsc.fr/ressources/outils/dns2tcp/) - enkapsulacja na poziomie tcp, program działa w całości w userlandzie, nie potrzebuje uprawnień administracyjnych.

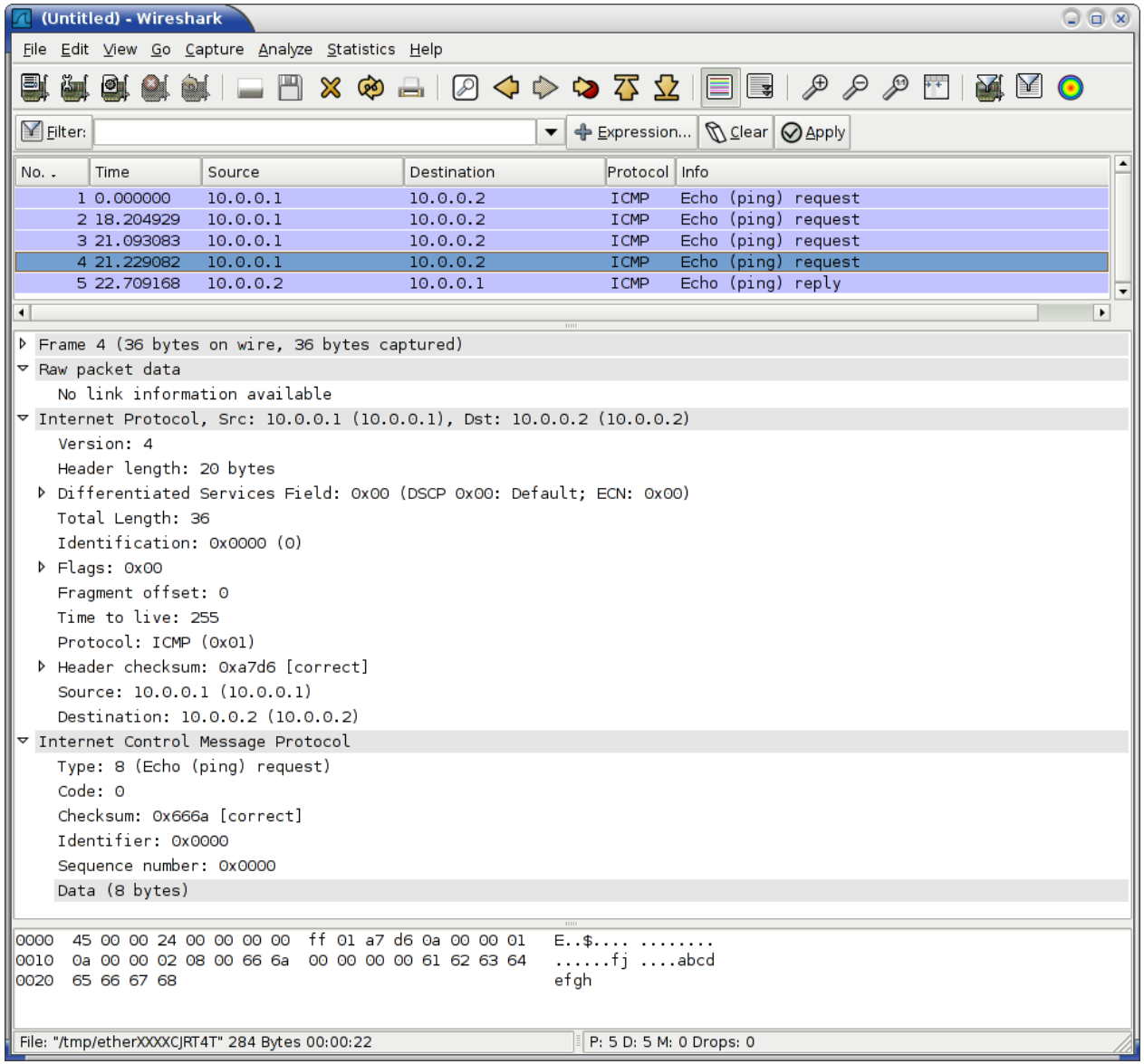
AnalogBit tcp-over-dns (http://analogbit.com/software/tcp-over-dns) – podobny do NSTX, tylko działa – cytat ze strony domowej ;) Co dla nas ważne: działa pod Windowsem. Napisany w Javie.

IP over ICMP

Jest to tunelowanie TCP/IP w pakietech ICMP ping. Używamy wtedy kiedy możemy coś zapingować, ale inny ruch sieciowy nie jest możliwy.

Wykorzystujemy fakt, że w pakietach ICMP musi „coś” być. Zwykle są to ciągi liczb, zera lub inne losowo wybrane dane. W naszym przypadku wsadzamy tam pakiety.

Uzywająć IP over ICMP można wyciągnąć ok. 150 kb/s up, 50 kb/s down (za pomocą PingTunnel).



Pakiet ICMP w Wireshark-u. Widać tu dane w środku pakietu PING request.

Przykładowe aplikacje:

ICMPTX (http://thomer.com/icmptx/) - używa tun/tap, wymagane wsparcie w jądrze.

Hans (http://code.gerade.org/hans/) - bazowany na ICMPTX, używa tun/tap, działa na Mac OS X, iPhone/iPod touch, *BSD

PingTunnel (http://www.cs.uit.no/~daniels/PingTunnel/) - wspiera Windowsa (potrzebne mingw, winpcap), posiada nawet autentykację w razie gdyby ktoś chciał wykorzystać nasz tunel ;)

Opisane powyżej metody są dosyć skomplikowane...

Opisane powyżej metody są dosyć skomplikowane...
...bo najprościej jest użyć serwera OpenVPN działającego na porcie 53.

Korzystając z okazji, że operatorzy chcą by ich usługa działała wszystkim użytkownikom wykorzystujemy otwarty port 53 udp.

(Zawsze znajdzie się ktoś, kto ma wpisany na stałe adres DNS inny niż przydziela dhcp)

Dzięki OpenVPN mamy bardzo szybkie, szyfrowane połączenie z autentykacją i autoryzacją użytkowników. Jednym słowem zwykły VPN.

Legalność. „Co nie jest zabronione jest dozwolone”.

Metody obrony. Bo tam gdzie jest atak, są i metody zapobiegawcze.

Jeżeli chcemy uchronić nasz HOT-SPOT przed tunelowaniem powinniśmy:

- Zabronić dostępu do sieci z wyjątkiem strony logowania do HOT-SPOTa oraz dostępem do serwerów DNS (port 53, udp).
- Przekierować ruch na port 53 na nasze serwery DNS. Pozwoli to na dowolną konfigurację DNS po stronie klienta, a jednocześnie zabroni komunikacji z usługą tunelowania działającą na innym serwerze.
- Na każde zapytanie DNS klienta nieautoryzowanego odpowiadać naszymi adresami. Można to osiągnąć np. za pomocą widoków w serwerze BIND.