Tor (lub I2p)

- Umożliwia dostęp do Internetu, należy jednak zachować ostrożność.
- Umożliwia dostęp do anonimowych serwerów sieciowych oraz innych usług (tzw. hidden services).
- Umożliwia hostowanie anonimowych serwerów sieciowych - należy się nimi wtedy opiekować jak każdym innym własnym serwerem. Są tak samo narażone na ataki DoS. Zaletą jest możliwość tworzenia zaawansowanych serwisów (takich jak w Internecie) w sieci Tor.
- Niektóre kraje podejmują próby jego blokowania, z różnym stopniem powodzenia. Istnieje możliwość zbierania informacji na temat ukrytych TORowych połączeń i blokowania ich przy odpowiednim wysiłku.
- Stanowi rozwiązanie zdecydowanie dojrzalsze niż Freenet (więcej użytkowników, stron, developerów).

Freenet

- Umożliwia dostęp **wyłącznie** do treści wysłanych do Freenet, z uwzględnieniem statycznych stron, poczty Email, wymiany plików, forów, blogów etc. Wszystkie te treści uploadowane są anonimowo (lub pseudoanonimowo, po stworzeniu tożsamości na Freenecie)
- Treści hostowane są w sposób rozproszony - każdy użytkownik jest zarówno hostem i nie jest świadom jakie treści są przechowywane na jego komputerze. Wszystkie treści sę rozproszone na wielu węzłach.
- Zapewnia, iż popularne treści będą zawsze dostępne.
- Starszy niż Tor, aczkolwiek o charakterze bardziej eksperymentalnym- przez to mniej dojrzały.

W trybie darknet

- Łączy się tylko do węzłów sieci, które użytkownik dodał do ‘znajomych’.
- Wolny ale bezpieczny.
- Niezmiernie trudny do zablokowania, parametr ten można dodatkowo poprawić przy zastosowaniu wtyczek transportowych. Obecnie Freenet funkcjonuje poprzez UDP over IP, w planach natomiast jest o wiele więcej protokołów, niektórych z nich ukrywających komunikację Freenetową jako coś innego. Przykłady:
    - voice over IP,
    - strumieniowanie przez RTP/RTSP (konkretnie udawanie aplikacji RealPlayer)
    - HTTP
    - bunnycams - protokół steganograficzny czyli kodujący treści w obrazach.
    - VPN
- Zapewnia dobry poziom anonimowości, a przy zastosowaniu tuneli PISCES - http://arxiv.org/abs/1208.6326.
- Jest stuprocentowo zdecentralizowany.

W trybie opennet

- Łączy się do każdego węzła jaki napotka, bez względu na status znajomości.
- Jest łatwy do zablokowania.
- Zapewnia ograniczoną anonimowość.
- Nie jest do końca scentralizowany.