Waste Networks Setup & FAQ Rev. 4 (03/28/2004)
Waste client current version: 1.4 Alpha 2
Written by: LANman

Waste is an encrypted, decentralized, VPN, peer-to-peer & chat tool.
It allows:
- The secure exchange of all file types.
- Secure group chat capabilities in an IRC 'channels' style.
-Linux & windows compatible

Index:

Highlighted Features
Quick Setup Guide
Configuration & Settings
Waste Config Q & A
Waste Cryptography
Waste History

Disclaimer:

What you do with this setup & FAQ guide is YOUR responsibility and you accept any & all legal issues that may arise by reading this. If you use it for any thing than what it is intended for then that's your problem. Waste is a wonderful tool that can let you transfer personal files to and from work/home safely.

Highlighted Features

An independent decentralized WAN

Waste doesn't depend upon one singular centralized host server/client as it is designed to have multiple waste clients that allow people to connect to them in order to make a strong P2P mesh network. Waste is a dynamic software package that can keep track of new clients; after you trade public keys with some one a new connection will be created between you. Then their IP-address will stay in your connections for a quick reconnection.

It is private

WASTE keeps the private network private by only allowing connections between known users, and by using strong encryption to secure those links.
All of the user connections are visible and you have complete control
over their actions: such as the banning of their connection address so that they may not connect to you. For an added layer of security use a common "network name" and even those that have your IP and public key will not be able to see you.

It is secure

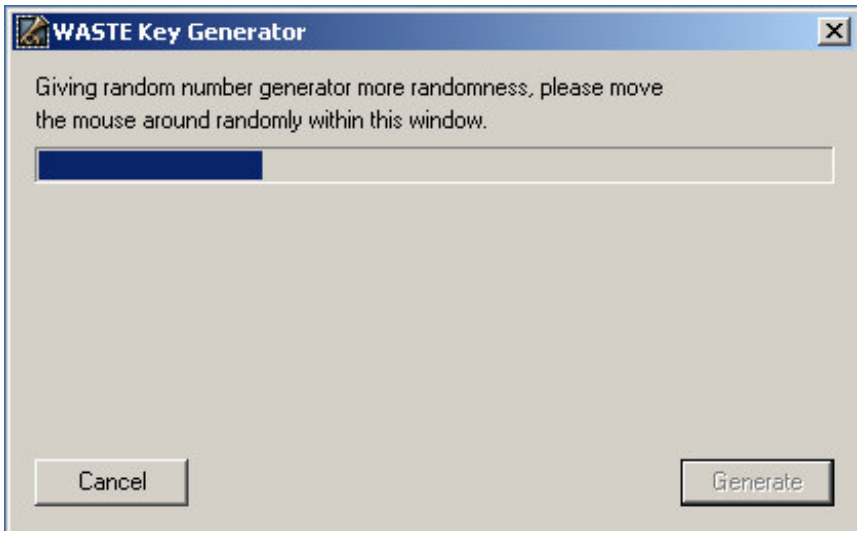
As every user has a private and public key, every user is unique
thus allow for encrypted exchanges: encrypted chat and encrypted transfers.
Before you run off to worry about your encryption key sizes, keep in mind that it's typically easier to break in and recover a private key than it is to crack/factor it. So be sure to keep your keys safe and your systems secure!

It has a tough 1,536bit Key
Some cryptography experts think 1,024-bit keys are too weak for certain kinds of sensitive data like root certificates of an organization's certificate authority or public key infrastructure, for instance. If Moore's Law holds true, it won't be long (perhaps three or four years) before we see 8-GHz Pentium VI machines, increasing the odds of implementing high-speed number crunchers. So we should be quite all right for some time with 1,536bit keys. The only ones you should have anything to worry about would be some form of government agency, the people that have the $$$ and computer power to come even close to cracking such a key. Just don't do anything terrorist like or pirate and they wont give a shit what documents/accounting/video production your sending.

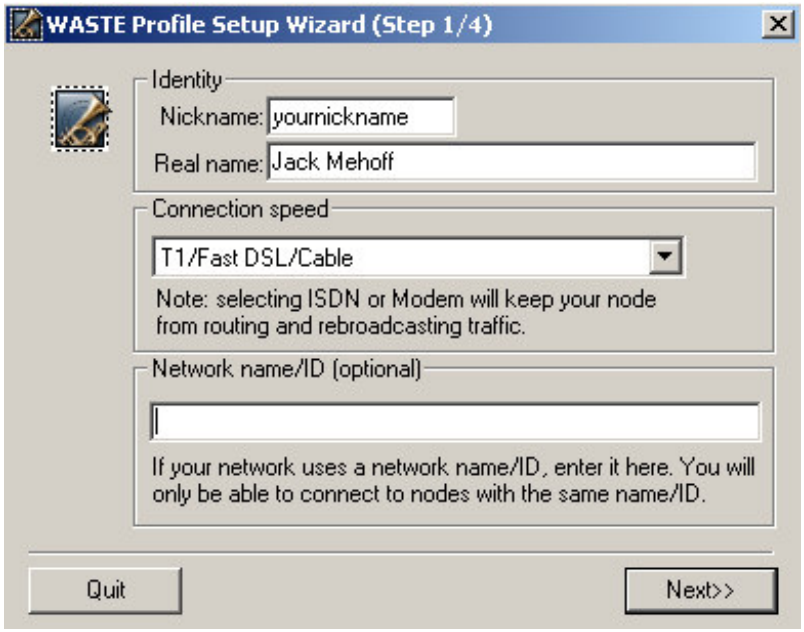
It has basic Chat & Messaging
Instant Messaging – allows users to communicate with other users on a private WASTE network in much the same way as when using AIM/ICQ/etc.
Group chat – allows two or more users to chat on a WASTE network in much the same way as when using AIM/ICQ/IRC/etc.

Quick Setup Guide

Install & Config:
Follow the installer to get waste installed (its easy just keep clicking next) then run waste from your start menu because it does not make a desktop icon for you.
After launching the waste for the fist time the following will appear:

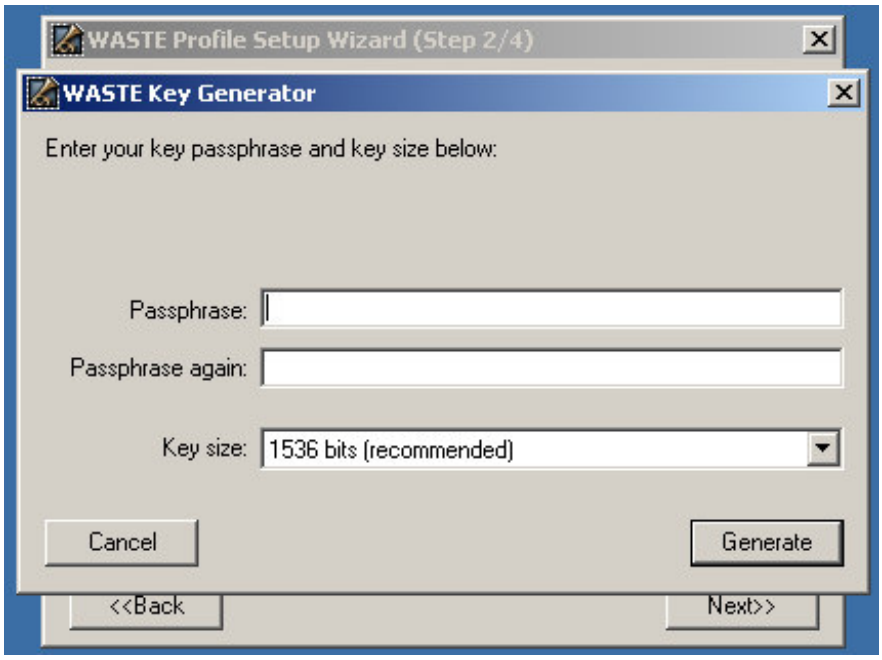


You need to move your mouse all over the box in order to generate the random numbers required by the program to make your key later.

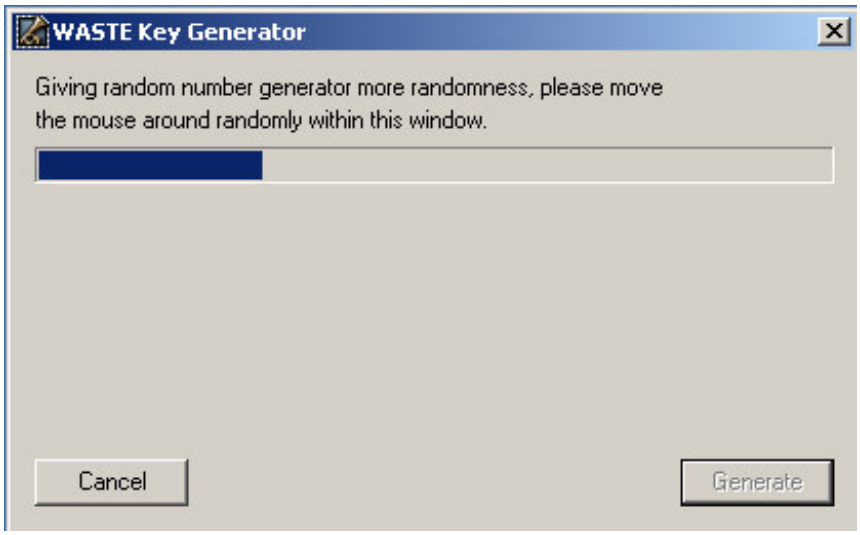


Type in your nickname; use what ever nick you use in chat or your LAN name.
Real name can be what ever.
Set you're connect speed: Set this to what ever your Internet connection best matches.
Network name is blank. (See Q&A at the bottom)
Click next ➔

Click on RUN KEY GENERATOR to generate your public and private keys. The public key needs to be given to some one that is already on a waste network; the private key should remain secret and NOT shared ever.
Click next ➔

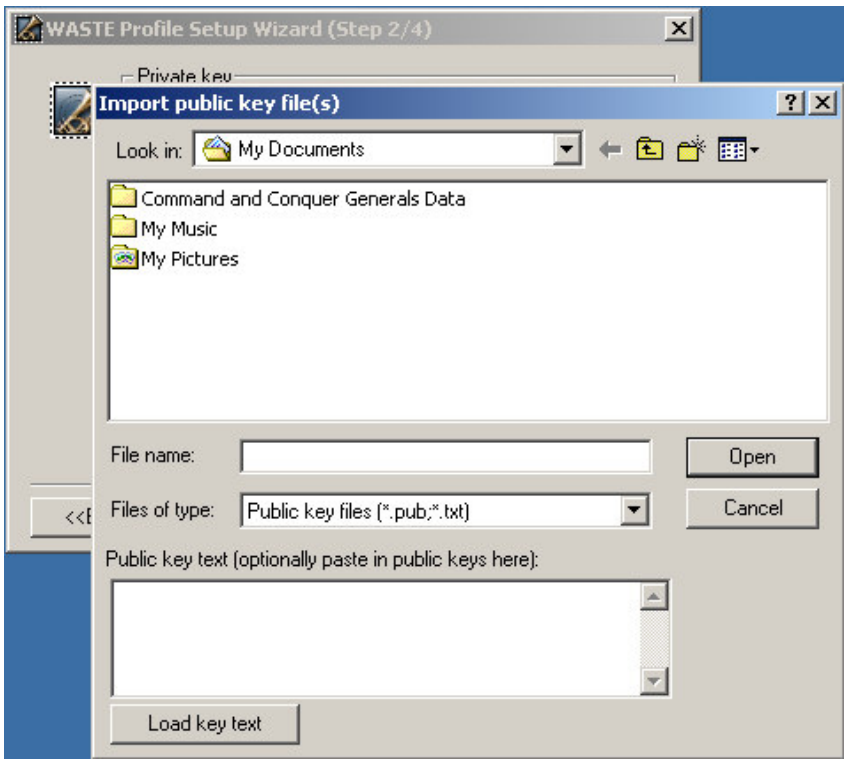


Keys are like passwords don't use the same one twice, and use mixture of letters, numbers, and characters (you will need to enter it to run waste). This “tR3~$8)vQq%” is a good example of what you would want a tough waste password to look like, just make sure it's at least long. I can't stress enough the practice of making your password/key as strong as possible. Keep in mind your data can be decrypted with your password/key because your public/private key pair is generated based on this password. The main weakness that is exploited is small and/or bad keys.
Leave the key the size at its default of: 1536bits (Any larger and file transfers would really suck; any smaller and you increase your chances of being cracked).
Click generate ➔



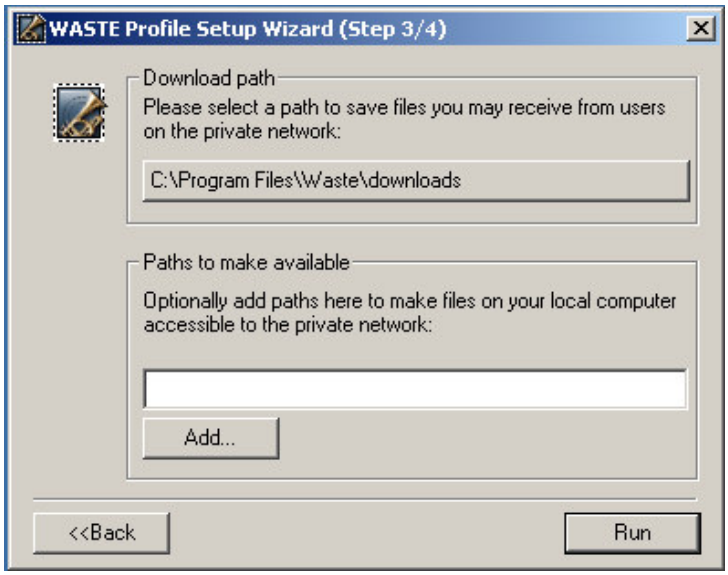
Move the mouse around until Generate is no longer dim.
Click ok ➔

You now have the opportunity to copy your public key into a clipboard so that you can email it or post it on a PM in chat. Connection to a remote machine will be denied unless your key is present & accepted on that machine (See FAQ for keeping your email/logs clean of keys).
Click on “Import public keys” ➔



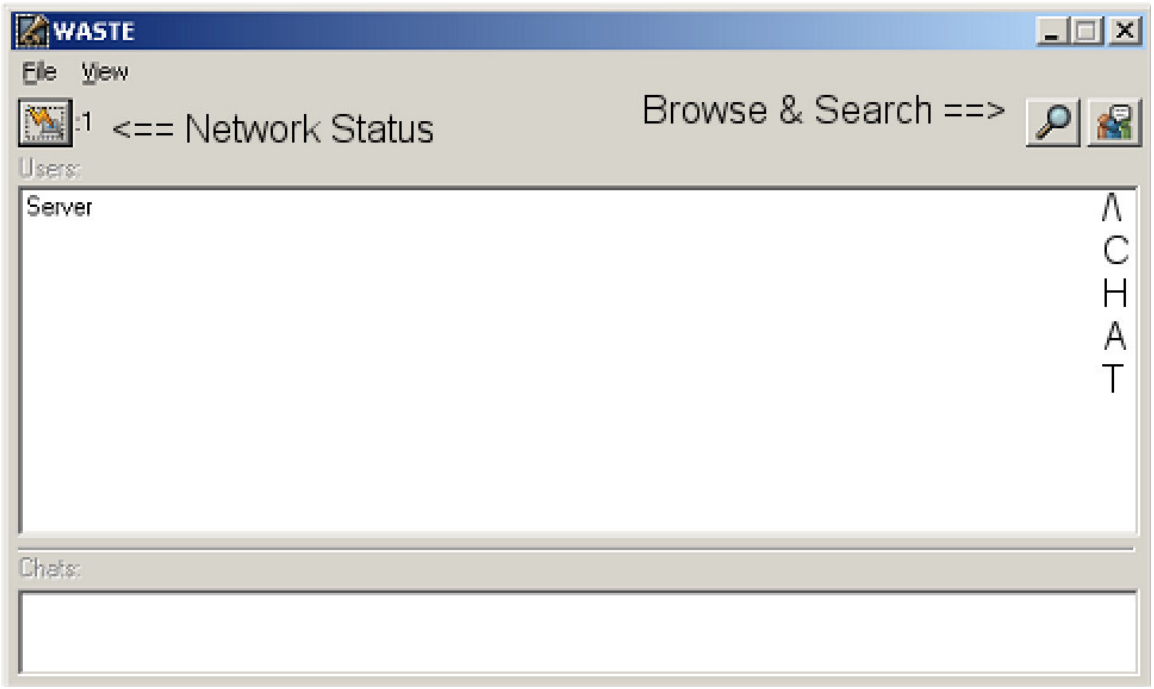
At this point you should have your friend’s public key already, so find the text file with your friend’s public key and open it or you can paste it in the dialog box in the bottom of the screen and click “Load key text”.
Click Ok ➔

Click Next ➔

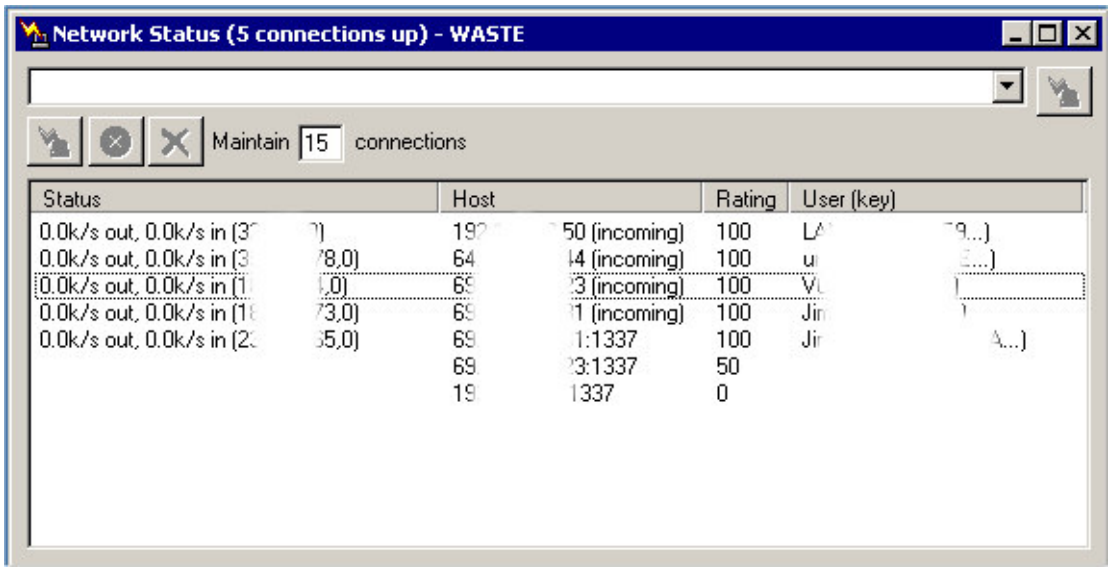


Select a location to be used to store your downloads and define the folders you wish to make accessible to the private network. Note that multiple folders may be added just by continuing to click **ADD** following each entry. Your network should now be configured and you can connect to your client.
That's it for the install, be sure to read over the rest of the FAQ for settings.
Run ➔

The main Waste window:



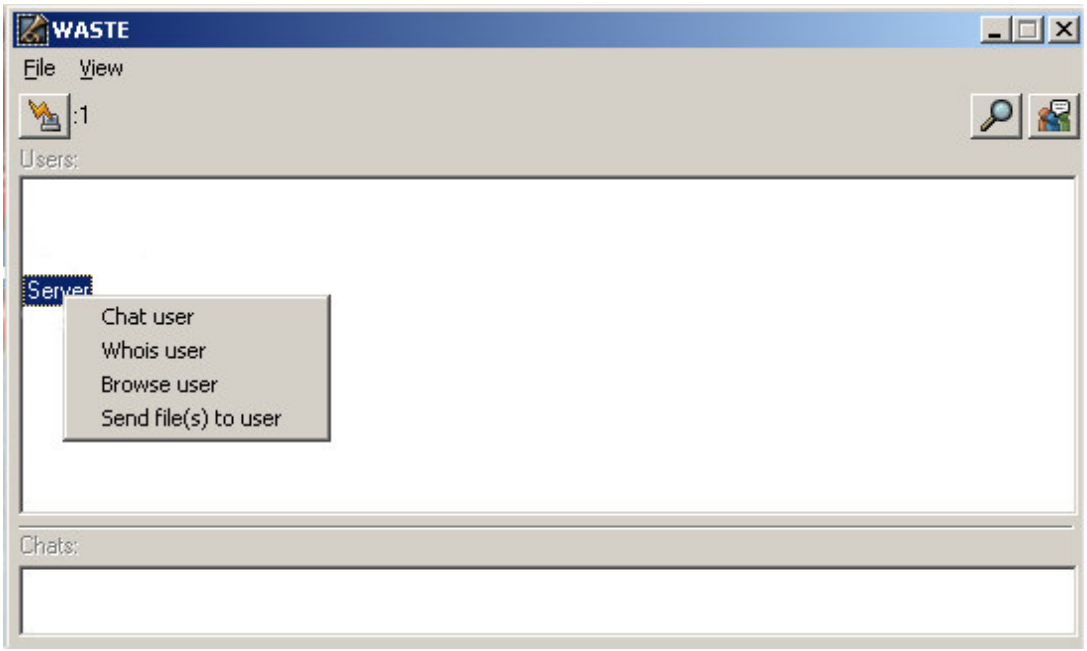
Network Status: makes it possible to view real-time network operations like:
-Connections in progress / Remote connections in progress.
Open browser: The browser allows you to search and browse your friend's shared directories.



Network Status:
In this field, enter the IP-address or the DNS address of the server/client to whom you wish to connect (This will be your friend's IP to start with).

Maintain connections: The number you should maintain will vary, you will want this number to be the average number or people that you want to stay connected to. On larger networks, and depending how many connections you set it to maintain you most likely will not need to maintain a connection to everyone (this will be something that you will have to play with). Keep in mind the more maintained connections you keep up the more of your bandwidth will be used for routing connections.

User connection status is listed here:
- *Status*: Are you connected? Are you sending? (Out) Are you receiving? (In).
- *Host*: IP Address of the current online users.
- *Rating*: The rating tells you how good of a connection you have to this user. A rating of 100 means you are directly connected to them. If it is less than that then you are having connection problems. If they disconnect/loose connection from you it will count down to 0 then stop trying to connect.
- *User (key)*: Username and User Key Signature.



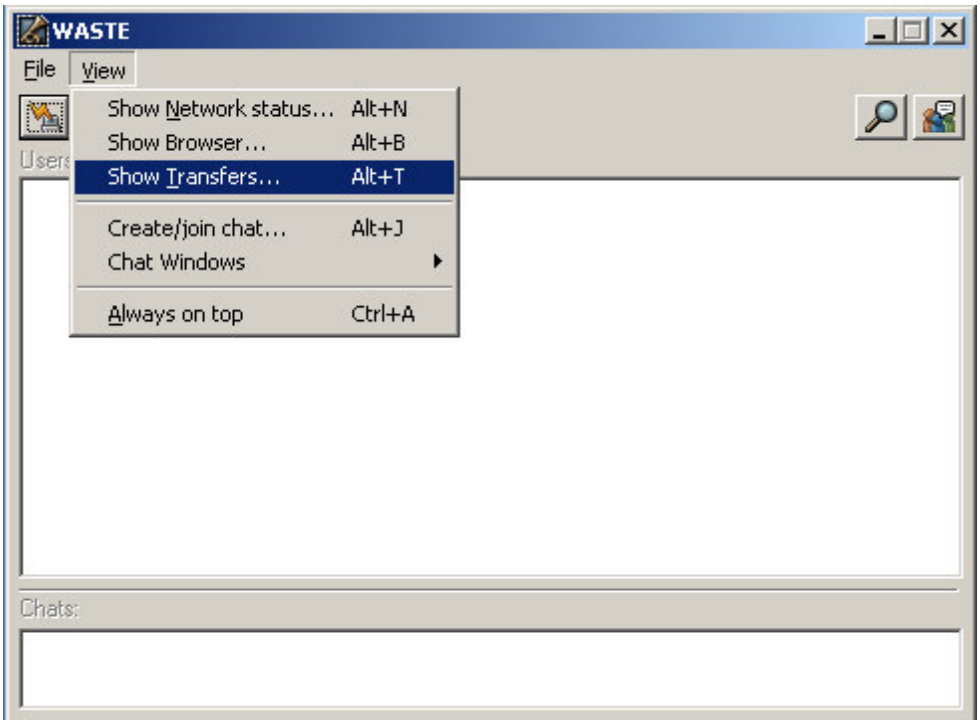
To browse users files, chat privately (IM or PM), do a whois for more info, or send files directly to some one, right click on the person's name in the main menu.

The zone 'Chats:' provides you with a list of the *visible* channels

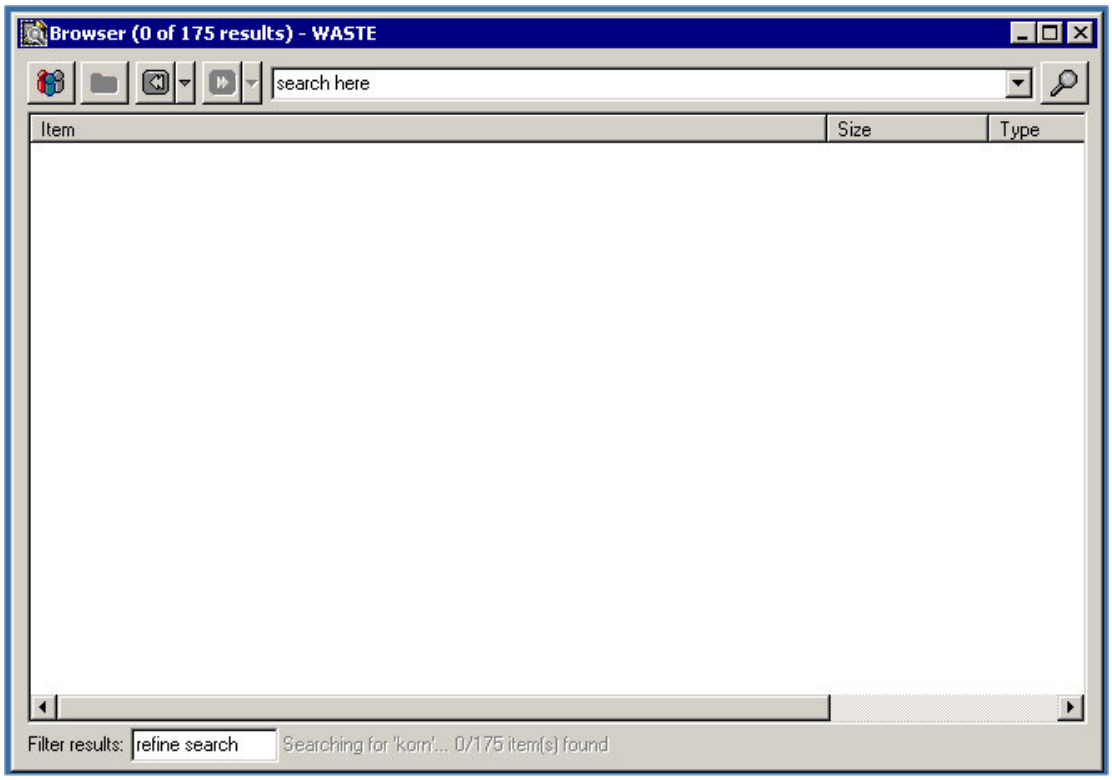
If you wish to join an *invisible* channel, you must know it's exact name

A *visible* channel will appear in the following form: #wanparty double click on it to join.

An *invisible* channel will need to be typed in manually from the chat button: &hidden

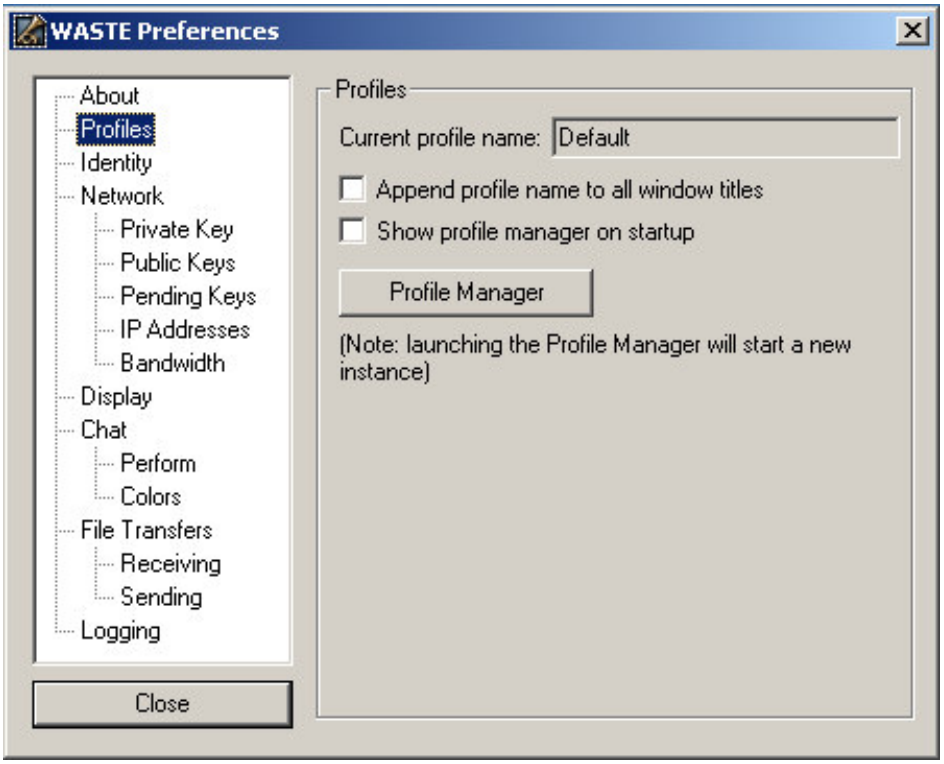


To manage your uploads and downloads open your Transfers window.



Complete a global network search from your browser.
Enter your search parameters in the top dialog box and press enter.
The results will be posted directly below.
To refine your search be a little more, type in the filter results box after you have done a search.

Waste configuration & settings



About: Program information & version number.

Profiles: If you aren't the only person using the program on your system.
(Tip-don't share waste with some one else that is on your computer)

Identity: The name everyone will see in waste, you can set this to what ever you like but don't leave it blank.

Network:

- ***Connection speed*:** This is where you set your connection speed, set this based on your Internet connection.
- ***Route traffic*:** If you don't have port 1337 open or you have no way of allowing connections in then uncheck this or you could cause problems when other clients try to download files or connect to people.
- ***Listen on port*:** Leave this at 1337 unless everyone on your network has decided on a different port.
- ***Advertise port on private network*:** With is important if you want others to connect to you, waste will broadcast the fact that you can accept connections. This feature is the key to waste and its ability form strong redundant mesh P2P network.

Network Submenu:

- ***Private Key*:** If you ever need to regenerate a new set of private and public key pair this is where you do it. It also gives you easy access to your public key so you can copy it and send it to others.
- ***Public Keys*:** This is where all your authorized keys are kept, if you decide that you don't like someone that is on your network you can remove them here. Make sure that everyone else is set the same or it will do you no good.
- ***Pending Keys*:** If you wish not to auto authorize new clients then their keys which have been broadcasted to you and need your approval. ***After you have your waste network setup between friends everyone should uncheck "auto accept broadcasted public keys" so that if some one you don't know joins the network you have to accept them first.***
- ***IP-addresses*:** If you can open port 1337 and accept incoming connections then you need to type in your static IP-address or your DNS address so that waste will broadcast your real IP-address and not the fake IP that your system has. To have even more control over who can or cannot connect to you check "Use access control list" then you can block or authorize IP-address that you see fit.
- ***Bandwidth*:** You will want to manage the amount of bandwidth is used. Inbound for download speed, and outbound for uploads. This is one feature that I go in and change on a regular basis, at night full speed and during the day 1/3 speed. For some this will be very important because some ISP don't like it when you download/upload more than 6 GB of data.
  - Limit incoming in kb/sec (I.E. downloads – 768k DSL – 60k to 70K max
  - Limit outgoing in kb/sec (I.E. uploads – 384 DSL – 30k to 40k max
  Be sure that these settings are not to high because it will consume your internet connection very easily.
- ***Connection saturation*:** If you enable this it will be constantly blasting misc. crap data when ever your not downloading or uploading files (but it will eat up your entire internet connection and that of who you connect to). So DON'T check the boxes for connection saturation!

Display:

- How waste windows are displayed with misc. settings that will vary from person to person.

Chat:

- All chat options with misc. settings that will vary from person to person.
- ***Perform*:** this is good for thing like running chat commands like "/join #wanparty" so each time you run waste you join chat room wanparty.
- ***Colors:*** More IRC Standard options for those of you that use wastes chat feature.

File Transfers:

- Be sure to have "Allow my nickname to be associated with file transfers" so people will know who is downloading from you and not cut you off.
- *Important!!!* *Check the box that's says bring up direct connections for transfers.* If you don't do this there will be tons of unneeded data transfer through the people that accept incoming connections. This option can add security to waste by confusing someone that may be monitoring your downloads by having your data go all over before it reaches you or the person downloading from you.

File Transfer Submenu:

- ***Receiving*:**

Download folder: You can set your download folder anywhere you like, just make sure its not the same folder that ANY other P2P client is using or would default to. You don't want misc. Kazaa people getting their hands on your partial downloads; it could be a major security risk.
***Allow others to send me files*:** Its up to you if you want others sending you files but I would leave it enabled because some one you know may wish to send you a file that is not shared. You can always check prompt before accepting to set this feature to manual. (For unknown files & downloads be sure to always have antiviral software running)
***Limit downloads*:** Try to limit your downloads to around 4 because you don't want to pull to many files at the same time you will never get them.
Use paths: This can be handy if you are downloading files in a folder that you wish to keep the directory structure after its downloaded. You will have to adjust this accordingly.

- ***Sending*:**

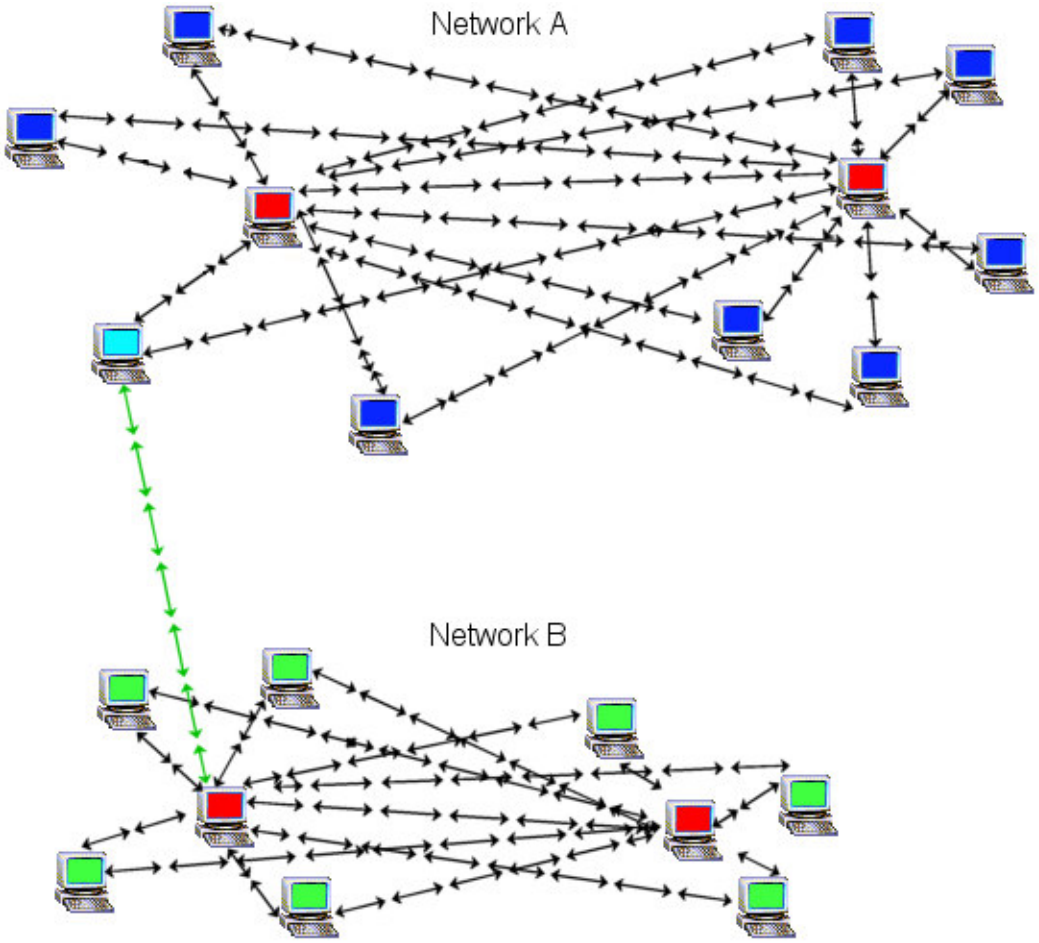
***File limit*:** Limit the number of file requests (default is fine).
***Index files, allow searching and browsing*:** Make sure these are checked this is an important one! I mean come on if your not going to share files then what are you doing here?
***Directories to scan*:** This should be obvious, add the list of folders you wish to share out. Keep in mind that if you share out a drive (I.E. C:\) you also share out everything on that drive.
***Rescans & cache file list*:** The option to rescan your directories every X amount of seconds may be use full to you only if new files are added before you have a chance to close and reopen waste to update file lists. You can set this one as you like, but keep it around 240+ minutes (or 4 hours) because if it is to high you will have your hard drives running constantly to re-index little or no file changes at all.
If you don't have waste set to rescan your files at X amount of time then this option must be enabled or you will never have an updated file list. Make sure "cache file list…" is enabled to help speed up waste when you open it, or it will have to completely re-index all your files each time.

Logging:

- So you can log your chat sessions.

Waste Config Q & A

"How do new clients connect to my waste network?"
In order for someone to join your network they first need to be given your public key and the IP-address or DNS of any waste client that is setup to allow incoming connections. *The more nodes that accept connections, the stronger the mesh will be and the less load that will be put on the network. This network is designed to be in a mesh topology, not a star a topology.*



- The red computer is a client (effectively a server) that has port 1337 open and other waste clients have connected to its IP-address directly or through a DNS address (I.E. mydnsaddress.dtdns.net). You are part of network A.
- Now the blue computers are waste clients that have not opened port 1337 or cannot open any incoming ports. In some cases you may have an Internet connection that does not allow incoming connections, such as an Internet connection that has N.A.T. running at the ISP level. If this is the case the only way around it is to get a static IP and that can cost lots of $$$.

- The light blue computer is part of your existing network but is the first to expand the network. This is the guy you need watch out for, if he is currently part of your network then joins up with another client they could merge with your network. Now there is nothing wrong with adding more waste clients to your network, but you may not trust the rest of their clients. To keep this from happening have everyone that is a part of your network go to: Preferences: Network: Pending Keys: and uncheck auto accept. Keep in mind to check this window for new clients you will have to manually authorize.

"How do you browse files?"
File browsing – allows users to browse a virtual directory structure for each user on the network. Each user can specify a list of directories to make available to other users on the network. You can browse individual users by right clicking on some ones name listed in the main window and select browse.

"How do I search?"
You can search from any chat window with "/search movieclip.avi", or you may search from the Browser Window (Alt-B). The top section that shows the Path you are browsed to is also a search window.

"How do you chat?"
This feature is primarily accessed through the main WASTE window. You can click on the create/join chat button and create a new room or type in a know room name. If some one already has a chat room created it will show at the bottom of the screen. To PM some one just right click on their name and click chat user. Also to join the same chat room each time you open waste type in "/join #wanparty" in the Chat: Perform: window.

"Why do I only have one connection and/or people can't connect to me?"
Waste is meant to distribute network connections; after your client makes a connection to anyone that is part of the network waste then broadcasts your IP-address out to everyone that is currently connected. This function of waste works great, but with DSL routers performing N.A.T. you end up having a fake IP-address on the system running waste. Then your client connects to a waste network and your fake IP-address is broadcasted to everyone that is part of the network and then no one can connect to you because the wrong IP-address is being sent out. This is also the reason that if you check your network connections there are a lot of IP-address that you keep trying to connect to but can't.

"Well then how do I setup waste so it will allow people to connect to me?"
In order for waste to work it needs to have as many people with port 1337 open and their "real" IP-address broadcasted out as possible so if one of the hosts are offline then the entire network will not go down. As of version 1.3C of waste it has no way of telling if the IP-address of the system that waste is on is your real IP-address, but there is a way around this. You need a service that updates your IP-address to a DNS server; that way your personal DNS address (I.E. mydns.dtdns.net) will point to your current IP-address (The IP that your ISP gives you I.E. 66.143.98.23).

“Port 1337 huh?”
Yep that’s that standard TCP/IP port that waste talks on. To open it you need you go into your router or firewall software and do a port forward (port 1337 to 1337 with both UDP and TCP enabled for that port) to your fake internal IP-address. The IP-address you set your port forward to needs to be a static IP-address, because the IP-address you have now may not be the one you have tomorrow with DHCP. Now I am not saying you should not run DHCP you just need to manually set an IP to the system that is running waste. Depending on what OS you are running the way to see what network settings your DHCP server has given you can differ. After getting your settings (I.E. IP block 192.168.0.***), subnet mask, default gateway, and your DNS servers) you can pick an IP-address that’s much higher up than what you have now (like if your using .3 or .5 or even .100s) like IP-address .200 should be safe for most. You can really use any address you want just make sure your DHCP server is not going to give it out (for most people you will never use more than 10 IP-addresses).

“Ok how do I setup a DNS service now?”
First you need to sign-up for a dynamic DNS service to forward your IP-address to a DNS server. Then you need to find a DNS updating client that will work with your DNS service. The web site you get your service from will have a list of clients with various features; you may need to try a few clients in to find the one that works for you. IF your running Windows NT, 2000 or XP try to get a version that runs the DNS updating client as a service so it can run in the background. You need to leave the service running all the time so it can update your IP-address as it needs to, don’t worry it uses very little system resources and very little bandwidth.

“Where can I find such a service?”
Well just about anywhere on the Internet, a google search for an IP poster, dynamic DNS, or DNS hosting will get you some kind of service that will do the job. Here are a few options for that you can try:
http://www.ddns.net/services/page/free/dynamic/dns
This is a good fee service but the web site has adds.
http://www.dtdns.com/
This is my preferred service, it lets you update your IP every 10 min. but it costs a one-time fee of $5.
http://www.dyndns.org/account/create.html
This is another good free service but they only let you update your IP-address every few hours.

“Now I am ready to share files, connect to others, and have others connect to me what now?”
Ok in your waste client go under: File: Preferences: Network: IP-address: check the force incoming IP to:
Type in your DNS address (I.E. mydns.dtdns.net) then waste will send out your real IP-address and not your fake one, now after you connect to someone are they connect to you your real IP will now be broadcasted out and everyone on the network will be able to connect to you. The great part about waste is after you have connected to someone or if someone broadcasted their IP to you it keeps that address in waste connections and allows you to quickly reconnect with them in the future.

“Can I or the network be hacked into?”
It is important to remember: All encrypted messages can be cracked through brute force cracking! This can take quite some time, depending on the key length (**upward of 900 years with some**). Other attacks use known weaknesses in an algorithm that can be very complicated and confusing to comprehend. Weak keys are the number one cause of these systems getting compromised. The size of the key determines the amount of time it will take. They capture the message and then begin guessing as to what the key could be. The guessing is done by some kind of brute force program and the guesses are every possible key that the key could be. They figure out the algorithm used, what the key length is, and then go at it.

“Ok I goofed and gave out my key to some one I don’t trust and I think that myself and the others that are part of my network could be in danger, what now?”
Chances are you are being paranoid, the RIAA or the movie moguls are after the 4+ million file sharing people on open P2P networks not you and your (at most 50) friends. What you will need to do is go into Preferences: Private key: and then generate a new pair of private and public keys WITH A NEW PASSWORD. Having a new key (and a long one) is very important; make sure it is not like the old one. You will also have to have every one else do this as well and then re-exchange your public keys.

“What network name/ID should I use? Or should I even use it?”
A network name can be useful for example, your waste network could grow way to large and go past the intended limit or you have accidentally merged with another waste network and you wish to split up your networks. After you have chosen a network ID anyone that does not have it set the exact way (case sensitive) you do will not be able to join your network or even see you (even if they have your IP-address AND you have shared keys). Your waste client and every one else’s will simply ignore them. You can set a network name/ID at the time of install or later under preferences.

“I can’t open my firewall up or I can’t run a DNS service, can I still partake in the waste network?”
Due to the way this network works, you do not HAVE to. Also keep in mind that if there are to many people on you network with out port 1337 with some way to connect to them it will create a weak network, and if your only connection goes down- you all do. People can download files from you via your existing outbound connections to other servers. Every waste network requires a least ONE node that allows access to port 1337 and a way to get their updated IP-address.

“Should I save my password when I open waste?”
The only problem with a long password/key is that it hard to remember, the paranoid part me says “No! Don’t save your password” but you will have to use your best judgment for saving passwords (I.E. a family computer, public computer, your company’s computer, or if you share your computer). REMEMBER the weakest link is always the person that is careless about his/her security.

WASTE cryptography

Since WASTE requires a small trusted network to function efficiently, it benefits greatly from cryptography. Using public-key encryption for session key negotiation and user authentication allows both the prevention of unknown users from joining the network as well link data security to prevent unknown users from "sniffing" network traffic.

WASTE also provides for an additional "network name or ID" that can be used to secure a network against people who do not have the name or ID. This can be useful if you wish to easily prevent multiple networks from merging, or change it to easily remove access of user(s) without having to make everybody ban those user(s) public keys.

WASTE uses a (hopefully) cryptographically secure random number generator based on the implementation in the RSA reference code. The code uses a 32 byte state, with 16 bytes of counter and 16 bytes of system entropy constantly mixed in, and produces random values by using MD5.

WASTE connections use RSA (with 1024 bit or greater public key sizes) for exchange of 56 byte Blowfish session keys, and 8 byte PCBC initialization vectors.

The link connection negotiation, where A is connecting to B, goes something like this:

1. A sends B 16 random bytes (randA), or blowFish(SHA(netname),randA) if a network name is used.

2. A sends B blowFish(randA, 20 byte SHA-1 of public key + 4 pad bytes).

3. B decrypts to get the SHA-1 of A's public key.

4. If B does not know the public key hash sent to it, B disconnects.

5. B sends A 16 random bytes (randB), or blowFish(SHA(netname),randB) if a network name is used.

6. B sends A blowFish(randB,20 byte SHA-1 of public key + 4 pad bytes).

7. A decrypts to get the SHA-1 of B's public key.

8. If A does not know the public key hash sent to it, A disconnects.

9. A looks up B's public key hash in A's local database to find B's public key (pubkey_B).

10. A generates sKeyA, which is 64 random bytes.

11. If a network name is used, A encrypts the first 56 bytes of sKeyA using the SHA-1 of the network name, to produce EsKeyA. Otherwise, EsKeyA is equal to sKeyA.

12. A sends B: RSA(pubkey_B,EsKeyA + randB) (+ = concatenated).

13. B looks up A's public key hash in B's local database to find A's public key (pubkey_A).

14. B generates sKeyB, which is 64 random bytes.

15. If a network name is used, B encrypts the first 56 bytes of sKeyB using the SHA-1 of the network name, to produce EsKeyB. Otherwise, EsKeyB is equal to sKeyB.

16. B sends A: RSA(pubKey_A, EsKeyB + randA), (+ = concatenated).

17. A decrypts using A's private key, and verifies that the last 16 bytes are equal to randA.

18. B decrypts using B's private key, and verifies that the last 16 bytes are equal to randB

19. If a network name is used, A decrypts the first 56 bytes of sKeyB using the SHA-1 of the network name.

20. If a network name is used, B decrypts the first 56 bytes of sKeyA using the SHA-1 of the network name.

21. Both A and B check to make sure that the first 56 bytes of sKeyA does not equal the first 56 bytes of sKeyB. If they do (which is statistically unrealistic and would lead one to believe it is an attack), they disconnect.

22. Both A and B check to make sure the final 8 bytes of sKeyA differs from the final 8 bytes of sKeyB. If they are equal, disconnect.

23. A uses the first 56 bytes of sKeyA XOR sKeyB to initialize Blowfish for send and receive. A uses the final 8 bytes of sKeyA as the PCBC IV for send, and the final 8 bytes of sKeyB as the PCBC IV for receive.

24. B uses the first 56 bytes of sKeyA XOR sKeyB to intialize Blowfish for send and receive. B uses the final 8 bytes of sKeyB as the PCBC IV for send, and the final 8 bytes of sKeyA as the PCBC IV for receive.

25. All further communications in both directions are encrypted using the initialized Blowfish keys and PCBC IVs.

26. A sends B the constant 16 byte signature ("MUGWHUMPJISMSYN2")

27. B decrypts verifies the signature

28. B sends A the constant 16 byte signature ("MUGWHUMPJISMSYN2")

29. A decrypts and verifies the signature

30. Message communication begins (each message uses a MD5 to detect tampering – if detected, connection is dropped).

Waste history

The quiet launch of Waste was the work of Nullsoft's principal developer, Justin Frankel, a soft-spoken 20-something known for his tech savvy and his streak of rebelliousness.

He released his latest project, WASTE, onto the Nullsoft site on May 28, 2003; and it quickly became big news. The software gets its name from Thomas Pynchon's The Crying of Lot 49, an is an acronym for "We Await Silent Trystero's Empire." W.A.S.T.E. is an underground postal system in the novel. Frankel's WASTE got mentioned on Slashdot and on Daypop and a lot of people managed to download it before it was taken offline.

Waste had been used internally to share files between AOL's San Francisco office, where Nullsoft is based, and its Dulles, Va., headquarters, according to Ian Rogers, a former founding member of Nullsoft.

Nullsoft has had its conflicts with AOL in the past, such as in 2000 when Frankel developed a music file-swapping technology called Gnutella. AOL quickly pulled it off the Web fearing legal ramifications, but not before developers downloaded it and began creating services based on its software code.

At this point waste is under an open source license at *sourceforge.net* and is free to the general public.

My sources for this FAQ:
http://www.irmi.com/
http://news.com.com/
http://protox.biz/
http://webspiffy.com/
http://waste.globaldisarray.org/
http://www.google.com/
http://www.zeropaid.com/
& The WASTE.doc v1.0 from who ever created it.

This guide is dedicated to all the people who have contributed any kind of advancement or betterment of waste.

Any comments/ideas/mistakes/things I left out; please don't hesitate to post them at wastes source forge site: http://sourceforge.net/projects/waste/.