-----BEGIN PGP SIGNED MESSAGE-----

Security and Encryption FAQ - Revision 22.3

by Doctor Who

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Article 12 Universal Declaration of Human Rights

This Faq/Tutorial is offered in good faith and is intended to be an encapsulation of my knowledge and experiences gained over the many years that I have been a computer/Net user. There are many roads to security and privacy on the Net, this is one that I have personally pursued and can recommend from experiences gained. I am not making any claim that it is the best or the only route to privacy and security, just that it works for me.

There are countless reasons why someone may need the reassurance of anonymity. The most obvious is as a protection against an over-bearing Government. Many people reside in countries where human rights are dubious and they need anonymity to raise public awareness and publish these abuses to the world at large. This Faq is to help such people.

Privacy and anonymity are very important principles associated with both freedom of speech and democracy.

"Anonymity is a shield from the tyranny of the majority... It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation - and their ideas from suppression - at the hand of an intolerant society."

Justice Stevens, McIntyre v. Ohio Elections Commission, 1996

Changes since previous revision:

Complete update. I now offer a simpler and (I believe) superior method of obtaining on-site computer security. All recommended security programs now offer open source. I now recommend using VMWare virtual operating systems together with Truecrypt. I have downgraded my preferences for Drivecrypt Plus Pack from enthusiastic recommendation to with caution recommendation. See further down the FAQ for reasons.

I am excluding e-Gold from my recommendations as it is now under the watchful eye of the FBI who are examining all accounts. If you have an e-Gold account, do not under any circumstances use it for any purpose that might cause you embarassment if revealed to the world.

This revision (22.2a) includes several typographical corrections

Part 1 offers an overview approach to achieve security and anonymity.

Part 2 offers practical help with the installation of some of the programs mentioned in Part 1. In some cases this includes detailed setup instructions to help achieve the goal of true computer and Internet privacy and anonymity. I assume a basic understanding of computers, such as the ability to copy and paste and a general knowledge of how to install programs and follow setup instructions.

Part 1 (Questions 1 to 30)

1. How does encryption work?

Essentially the plaintext is combined with a mathematical algorithm (a set of rules for processing data) such that the original text cannot be deduced from the output file, hence the data is now in encrypted form. To enable the process to be secure, a key is combined with this algorithm. The key is protected by a passphrase. Obviously the process must be reversible, but only with the aid of the correct key. Without the key, the process should be extremely difficult. The mathematics of the encryption should be openly available for peer review. At first sight this may appear to compromise the encryption, but this is far from the case. Peer review ensures that there are no "back doors" or crypto weaknesses within the program. Although the algorithm is understood, it is the combination of its use with the passphrase that ensures secrecy.

Thus the passphrase is crucial to the security of the data.

2. I want my Hard Drive and my Email to be secure, how can I achieve this?

You need PGP (Pretty Good Privacy) for your Email and TrueCrypt version 4.3 (or later) for your hard drive encrypted files.

TrueCrypt is an OTF (On-The-Fly) type program. OTF means the encrypted data is only decrypted into RAM (Random Access Memory) and remains at all times encrypted on the drive. Thus a crash close will not leave packets of plaintext on your drive. A very important feature.

PGP is available for all versions of Windows, Linux, Unix, Mac and others. The source code is available for compiling your own version should you wish.

TrueCrypt has now matured into a truly excellent open source encryption program. It does not display any file header info to help a snooper identify the file's purpose. The header is encrypted and shows as random garbage. The program will encrypt both files or a complete drive partition. There are advantages and disadvantages to both options. I

prefer the partition option. Truecrypt does not need the partition to be formatted, nor need it display any drive letter. So it could use a portion of unformatted space at the end of a drive. This space can be any size you wish. I strongly urge you to study the included manual before using it for any critical purpose.

The source code is freely available so it means anyone with the ability can compile the same program. The importance of this cannot be too strongly stressed. It means the possibility of a hidden back-door is reduced to a negligible risk.

A wholly new recommendation included in this latest revision of the FAQ is VMWare Workstation 6. This has nothing whatsoever to do with encryption, but works with Truecrypt to offer total security on your desktop or laptop computer. Workstation 6 can create a virtual bootable operating system. To ensure secrecy, it should be setup to boot from within your hidden TrueCrypt encrypted drive. The method is explained within this Faq, This offers several advantages over my previous recommended method using DriveCrypt Plus Pack. A further advantage of VMWare Workstation 6 is that it is open source, unlike DCPP.

Note 1: PGP, although excellent at ensuring Email privacy, does nothing for anonymity. The difference is crucial.

I will assume that anonymity is also very high on your list of needs and so will concentrate on that issue further down the Faq.

3. What is the difference between PGP and TrueCrypt?

One of the difficulties before asymmetrical key encryption was discovered was how to get the key to the person wanting to send you an encrypted message. In the past trusted couriers were used to get these secret keys to a distant location, maybe an overseas embassy. Nowadays this is unneccessary because of the discovery of what is called public key cryptography. Two different keys are used. One key is secret and the other is made public. The most widespread program of this type for private use is PGP, invented by Phil Zimmerman. In fact it has become the de facto standard on the Net. This program is ideal for Email.

Anybody sending you mail simply encrypts their message to you with your PGP public key. The public key is obviously not secret - in fact it may be spread far and wide so that anybody can find it if they wish to send you encrypted Email. The easiest way to ensure this is by sending it to a public key server. On the other hand, some prefer not to share their key, except within a small closed group. Your choice.

The only way to decrypt this incoming message is with your secret key. It is impossible to decrypt using the same key that was used to encrypt the message, the public key. Thus it is called asymmetrical encryption. PGP is simplicity itself to install and use. It even offers to send your newly generated public key to a key server.

For your normal hard drive encryption, you will need a symmetrical type of encryption program. This means the same key is used for both encryption and decryption. There are many such programs. I strongly

recommend TrueCrypt.

TrueCrypt uses the passphrase to encrypt a randomly created key. It stores an encrypted copy of the key within the headers of the encrypted device. It is the plaintext of the key that is used to encrypt (and decrypt) the contents of the disk or container on an as needed basis into RAM memory.

With PGP a public key is chosen to encrypt the message. PGP will then generate a one time session key which it uses to encrypt the message. This session key is then itself encrypted with the public key of the intended recipient of the message. This encrypted copy of the session key is then wrapped in the headers and sent along with the encrypted copy of the message to the recipient. Only the recipient has the private key which can decrypt this session key. If there are multiple recipients, then this session key is encrypted to the public key of each recipient in turn. All these different encrypted versions of the session key are then wrapped in the headers of the message. Each recipient can decrypt his version of the session key, which will then be able to decrypt the message. PGP also has a keystore. The keystore is protected by the passphrase.

The sender of a PGP message may choose to sign a message. The message may or may not be encrypted. PGP will then encrypt the hash of the message contents using the senders private key. His public key can then be used by the recipient to check that this hash of the message is identical to the original, thus proving it was made using the sender's private key. Only one private key, the sender's, can encrypt the hash such that it will check out correctly with the sender's public key. If even a white space between two words is closed up in a message, the signature will show as bad. This offers a very secure method of checking both the accuracy and the authenticiity of a message.

Truecrypt and many other symmetrical encryption programs store the key within the headers of the partition or container. One question often asked by newbies is whether the passphrase is also stored somewhere within the encrypted file. No. The passphrase is passed through a hash. It is the hash output that is stored within the headers of the encrypted container. The program will compare this hash with the hash it produces from your passphrase that you type in to mount (open) the container. If they are identical, the program will use your passphrase to decrypt the key that the program generated to encrypt the disk or container. It is this key that will then be used to decrypt the disk or container on the fly. Truecrypt explains this in detail within the users manual that is downloaded with the program. I strongly urge you to read and digest.

Hashing is a one way action only; it is impossible to derive the key from the hash output. The hashing process is simply a way of checking that the correct passphrase has been input. If the program was somehow altered to force it to use an incorrect passphrase, the output would be garbage. There is no shortcut or fix, without the correct passphrase the output will be junk.

4. I have Windows, am I safe?

Windows is a closed source operating system which is a law to itself.

Each new update that is released by Microsoft seems to need further updates to fix the security holes discovered in the previous releases. It has been an ongoing process over many years with no end in sight. These weaknesses can manifest themselves as security holes when on the Net. A further problem with this operating system is its seeming determination to write to your hard disk all sorts of information that may be hidden from your view in all sorts of places that could be found by a forensic examination of your computer.

Thus we have a two fold problem. Firstly, the problem of Windows having the potential of security holes that might be exploited by snoops and hackers using the Net and a different security problem of writing all sorts of information to sometimes hidden folders that might not be obvious from a cursory check by you, but easily found by a forensic examination.

If you wish to protect yourself from these potential weaknesses you need to have an effective firewall, an effective anti-virus and an anti-spyware program. That will hopefully help to minimize the threats from outside. That is only the start. You also need to replace your Windows Internet Explorer browser and your Outlook or Outlook Express Email client for something a lot more secure. I like FireFox and Quicksilver. Even these need support by using specialist programs.

Even with Firefox or any other Web browser it is imperative that you disable Java and Javascript. More about the reasons why later in the Faq.

In some countries, even this might not be enough. Such countries can force you to hand over your passphrases to these encrypted drives by threatening imprisonment. As more and more judicial systems seem to be leaning ever closer to this sort of injustice (injustice because the culprit is being forced to self-incriminate himself which is in direct violation of Article 5 of the Bill of Rights; the right to refuse to be a witness against oneself), so it is more and more important for the individual to protect himself.

Because of these encroachments on our liberty I propose in this Faq a method of plausible deniability. This means you can justify every one of the files and folders that are on your computer. More than that you must be able to justify every single program, naturally including TrueCrypt and VMWare.

In the past I have strongly recommended Drivecrypt Plus Pack (DCPP). However to use this program, or any of the encryption programs from Securstar, it is necessary to enable both cookies and Javascript. I can live with cookies as they can be removed immediately after use, but I will not tolerate Javascript. These both need to be enabled to register the program before it can be used after its trial period has expired. This together with it being closed source have caused me to change my suggested solution to desktop and laptop security.

5. So what do you recommend now?

I recommend using VMWare Workstation 6 together with Truecrypt. VMWare is expensive, around 200 US dollars. But so is DCPP. I believe VMWare

is far superior when used in conjunction with TrueCrypt. It is also open source. It is far easier to justify having on your computer, yet will hide your activities, provided it is setup as suggested in this Faq. I find it far easier to use in conjunction with my usual desktop programs.

It is a program for software development engineers and IT professionals. It creates a virtual desktop which can be either Windows, Linux or even Solaris. It will appear very daunting at first, but if you follow the suggested steps, it will become relatively straight forward and even obvious after a couple of experimental uses. Importantly, everything is done in RAM and within your encrypted TrueCrypt drive. Despite Windows saving snippets of your activities, it matters not a jot, because everything it writes is within your encrypted drive. A very elegant solution to the problem of how to keep control of Windows.

6. How does this system work?

A detailed setup procedure follows later in the Faq, but briefly:

VMWare Workstation 6 will allow you to create a new bootable Windows (or Linux or Solaris) operating system, after having already booted into Windows or Linux in the usual way. It is necessary to open your Truecrypt container or partition from within Windows first, but that is the limit of your liability. Meaning that you then start VMWare Workstation 6 and choose to boot into your virtual Windows from within your now opened Truecrypt drive. There is always the slight risk of a Trojan or Tempest attack. To minimize this risk, you must choose a good firewall and anti-spyware program. I recommend Zonealarm for this.

The VMWare program installation can and should be within your usual desktop. This might sound alarming, but it is not a problem. What is important is that your VMWare virtual machine must be installed within your secret TrueCrypt drive.

Once a virtual machine has been created, it is then used to install a fresh copy of your chosen operating system. This might be Windows or Linux or even Solaris. This new operating system will automatically be installed and run from wherever you installed the virtual machine. In this case, within a TrueCrypt container. After it is mounted, this container which might be a file or even a whole partition, will appear as a new drive with its own designated drive letter to Windows. After booting into your TrueCrypt virtual machine, you will see in "My Computer" a similarly designated drive C. This is not your original boot drive C. It is a virtual drive that exists within your TrueCrypt virtual machine only. This virtual drive has no contact with your orignal bootable drive C whatsoever. This cannot be stressed too strongly.

To help with plausible deniability, you should have another virtual machine (you can have as many as you wish) which should be your honeypot version. This should be installed within its default location on your desktop within "My Documents".

Whereas your truly secret virtual machine must be installed within a TrueCrypt container.

You only need to create the virtual machine once. Likewise, you only need to install your Windows (or whatever) operating system once. This is because you can import a once created virtual drive to any other drive as many times as you wish. You can change several parameters at this time, including the size of the virtual drive you have already created. All your programs that are recommended further down the Faq, will be installed only into your truly secret virtual operating system.

Once setup, you will then use it exactly as you would your usual desktop. This means you boot into your Windows/Linux desktop, then you open your TrueCrypt drive, then start VMWare, open your Virtual Machine by navigating to it in your TrueCrypt drive, then starting it by clicking on "Power on this virtual machine". You shut down by reversing this procedure.

Note 1: It is possible to tell VMWare to look outside its own specially created virtual drive, to read other drives contents. Meaning it could write to these other drives. I would only do that if you are sure you know what you are doing. No harm is done by keeping all your data within the VMWare virtual drive. I strongly urge you to do this unless or until you are a true expert in its use.

Note 2: It is important to tell VMWare not to share its memory with its host (the host is your usual desktop or laptop operating system).

Full details on all this later in the Faq.

7. Could I boot off a CD or DVD?

Yes. Using BartPE (do a search on the Web if you wish to find out more). I found it very slow. Too slow for my purposes. The VMWare documentation talks of creating an ISO file from your virtual machine and presumably burning to CD or to an USB stick and then using it to boot. However, this CD/DVD or USB stick will not be encrypted and is therefore a possible subject for forensic examination in the case of a search. In any case it will be very slow in use, as is the BartPE.

8. How difficult is it to break into TrueCrypt or PGP?

Very difficult, in fact for all practical purposes, it is considered impossible. In most cases, the weakest link will be your passphrase, or being compromised by a hardware key-logger through not having good security on your desktop. From time to time non-expert net users make speculative suggestions that the American intelligence agencies have already cracked these programs. FUD - Fear, Unease, Despair. Probably put out by these self same agencies to try and detract you from using these programs. Cryptanalysts are certain that these modern programs with large key sizes of around 256 bits are impossible to crack into with todays technology, or even whatever is on the horizon. Even with the future of quantum computers, which should be able to factor very large primes very quickly, this may well affect PGP but not TrueCrypt.

The likely weakest link will be your passphrase.

Your passphrase should be long. Every extra character you enter makes a dictionary search for the right phrase twice as long. Each time a bit is added it doubles the number crunching time to crack into the program.

Each keyboard character roughly equates to 8 bits, and is represented on the drive as two hexadecimal characters. This suggests a 20 character passphrase is roughly equal strength to the encryption. In practice, probably not. A keyboard has around 96 different combinations of key strokes, thus multiplying this number by itself 20 times is a hugely large combination, ensuring a high probability of defeat at guessing a passphrase. But few people can remember a truly random 20 character passphrase. So most people use a less than random one. This means it should be longer to help compensate for this lack of entropy.

9. What about simple file by file encryption?

I recommend either PGP Tools which comes free with PGP or Kremlin. Of course this is not necessary for files within your encrypted drive. But is essential to clear files off your computer that are outside your encrypted drive. Fortunately, if you follow my suggested method, there should be no traces of any of the activities you perform within your TrueCrypt virtual machine. As already explained, VMWare cannot see your usual C drive, or indeed any other of your drives unless you tell it to do so.

PGP Tools is a long winded process just to encrypt a single file, as it asks you to first choose a key before entering the passphrase. Kremlin is quicker because it allows you to right click on the file to be encrypted, a password box opens and that is it. It also similarly allows you to wipe any file by right clicking. This can also be done by PGP. Another recommended program to erase individual files is Eraser.

10. Can I encrypt files on a floppy or USB stick?

Yes, use TrueCrypt or PGP Tools or Kremlin.

11. Does using both VMWare Workstation 6 and encryption slow things up?

Using VMWare Workstation 6 will on occasion slow things up quite considerably. Far more than does the use of encryption alone. However, if the right choices are made when installing, this is not such a major factor. But it is a price that needs to be paid for maximum security of your desktop data. Naturally, the faster your computer, the less noticeable this will be.

12. Do I need a PGP passphrase if I store my keyrings within my encrypted drive?

Definitely. Just because you have encrypted your drive does not relieve you of the necessity of protecting yourself whilst online.

13. I use Mac, OS2, Linux, (fill in your choice), what about me?

No problem with Linux or Solaris. Just install the correct version of VMWare and Truecrypt for your choice of operating system.

14. How can I ensure I do not leave traces of unwanted plaintext files on my system?

If you follow this FAQ, the only evidence that will be found is that you have both VMWarer Workstation 6 and Truecrypt, among all your other desktop programs. More details further on about ensuring good plausible deniability with the use of Truecrypt. If you are paranoid about temp files, I suggest using Windows Washer.

Note: Windows Washer will not remove evidence of the use of TrueCrypt. Thus my strong recommendation that you create a honeypot version to justify its presence on your computer.

15. What programs can I install into this new bootable operating system?

All your usual programs that you need to use your computer normally, plus the more specialised ones to help you achieve anonymity. See further down the Faq. With VMWare, you are literally opening a new window (pun intended) into your online activities. A very secret window, with virtually no connection with your usual Windows system.

16. How do I "cover my tracks" online?

Never surf naked. Always, always use a proxy. The easiest method is to use Tor. Tor is now bundled together with Vidalia and Privoxy. it is simple to install and use. Vidalia is the control panel for Tor. However, you can achieve the same by right clicking on the Tor icon on the Taskbar.

17. Earlier on you mentioned plausible deniability, what is it?

Plausible deniability is the ability to offer irrefutable justification for every single file, folder, container, partition and drive that might contain encrypted data.

All the files for your new (secret) Windows (or Linux) operating system are held within your Truecrypt drive. This might be within a hidden Truecrypt partition, recommended of course.

You will create an initial VMWare Windows (or Linux) operating system that is openly visible for inspection as justification for its presence on your computer.

VMWare is very useful because VMWare Workstation 6 allows you to take a snapshot which will allow you to backtrack if you have installed a rogue program or you catch a virus. Alternatively, you could try installing a different operating system. If your usual desktop OS is Windows, try installing a copy of Linux. It need not be successful. The fact you can show a plausible reason is all that is necessary.

You should also create a TrueCrypt container into which you will put some private or moderately embarassing files as justification for the TrueCrypt container. Again, this is justification for its presence on your system.

But you will also create a second truly secret Truecrypt partition or container into which you will install another virtual machine. It is this version that will contain all your truly secret data.

Note: It is not essential or even necessary to install the VMWare program itself within your TrueCrypt container. Naturally, the more paranoid may choose to do so, but from my tests there was no benefit whatsoever, but there was a slow down because of the extra overhead of the encryption.

18. What if encryption is illegal in my country?

VMWare should not be an issue as it is not an encryption program. But to help, TrueCrypt offers what it refers to as Travellers mode. Full details within the users manual. It will have to be run off a floppy or a USB stick and you will still need to hide the media effectively in the case of a search. I am sorry I cannot help you here. It must be down to your own initiative.

19. Are there any other precautions I should take?

Make copies of all your PGP keys, a text file of all your secret account numbers and passwords and the other details for your secret bank accounts, full details of your Virtual Debit Card account, copies of INI files for critical programs, your anonymous Email account details plus anything else that is so critical your life would be inconvenienced if it were lost. All these details should now be stored in a folder called "Safe" on your encrypted drive. A copy of this folder should be stored on an encrypted CD, preferably within the hidden part of a TrueCrypt container and stored off-site.

If you are going to rely on any variation of the ploys suggested here, then you should keep this Faq within your hidden encrypted drive.

You will need to take further precautions whilst you are online against threats from hackers and snoops.

20. What are these threats?

They are known as Tempest and Trojan attacks.

21. What is a Tempest attack?

Tempest is an acronym for Transient ElectroMagnetic Pulse Emanation Surveillance. This is the science of monitoring at a distance electronic signals carried on wires or displayed on a monitor. Although of only slight significance to the average user, it is of enormous importance to serious cryptography snoopers. To minimize a tempest attack you should screen all the cables between your computer and your accessories, particularly your monitor. The modern flat screen (non CRT) monitor offers a considerable reduction in radiated emissions and is recommended.

22. What is a Trojan?

A trojan (from the Greek Trojan Horse), is a background program that monitors your key-strokes and then either copies them to a secret folder for later recovery or sends them to a server when you next go online. Sometimes referred to as spyware. This may be done without your knowledge. Such a trojan may be secretly physically placed on your computer or picked up on your travels on the Net. Perhaps sent by someone hacking into your computer whilst you are online, or whilst visiting a Website.

23. How do I do avoid these threats?

First of all you must have a truly effective firewall. It is not sufficient for a firewall to simply monitor downloaded data, but to also monitor all attempts by programs within your computer that may try and send data out. I suggest installing Zonealarm. This firewall very cleverly makes an encrypted hash of each program to ensure that a re-named or modified version of a previously acceptable program cannot squeeze through and "phone home". Zonealarm version 7 also incorporates both anti-virus and anti-spyware checking, making it an excellent choice. To save money, there is a freebie version of ZoneAlarm. If you choose this version, I recommend then also using the freebie version of Kaspersky anti-virus. This is because the freebie ZoneAlarm is purely a firewall.

That is but the start. You also need a Web browser that does not leak information, plus a method of passing data across your ISP's servers strongly encrypted to prevent prying eyes from watching all that you do on the Net.

24. I use the Net for Web browsing, Usenet and Email, am I safe?

Whilst you are online anyone could be monitoring your connection. They do not need access to your computer to do this. They need only have access to your ISP. To minimize these risks you must encrypt the data passing across your ISP's servers.

My suggestion is to use a combination of several programs. Each is easily set up (see Part 2). Between them you will be secure and anonymous. The best news, all these programs are free and open source!

25. Which programs do you recommend?

You need four main programs besides the news client such as Agent (my favorite) and the Web browser such as FireFox (again my favorite) and the Email client such as Quicksilver, (yes, another favorite).

Quicksilver will ensure that only text is displayed; all HTML is banished. This is important because it prevents you being caught by Email marketeers and perhaps snoops and hackers that use linked graphic files as a means of tracking "live" Email addresses.

You can still receive HTML and attachments with Quicksilver, it just protects you by putting them into a separate folder where you can view them at your leisure when offline.

Other programs are: Stunnel, Freecap, Privoxy and Tor. All are free and all are open source.

They are all very easy to use and really can be setup by a newbie if you follow the setup instructions I offer in Part 2. They are totally transparent to the user. Once setup there is no maintenance or searching for proxies, etc. It is all done in the background with no further input required from you.

26. Tell me more about these programs?

Stunnel encrypts the data between you and your news server and is very simple to use.

Freecap is also easy to setup and acts as the bridge between Stunnel and Tor.

Tor is a connection-based low-latency (meaning fast) anonymous communication system that protects TCP (Transmission Control Protocol) streams for Usenet, web browsing, instant messaging (IM), internet relay chat (IRC), Secure Shell (SSH), etc.

In basic language Tor is a socks server that accepts and encrypts data from any program that is "socksified", meaning set up to communicate with it.

Tor is a new program and is still in Beta development mode. But it is still a fully functioning Socks proxying system that offers the promise of great anonymity and privacy. It is free and open source. It is

supported by the Electronic Freedom Foundation, a web based charity dedicated to freedom of speech online.

Tor will build automatically and transparently to the client (you) an anonymous and encrypted route across the Net. It uses multiple layers of encryption, each node only knowing the previous and next node, so with several nodes your data becomes anonymized. The principle is like an onion with many layers of encryption and anonymity. Thus it is called onion routing.

Remember, the data is encrypted both by Tor which uses TLS (Transport Layer Security) and by Stunnel which uses SSL (Secure Socket Layer) as it leaves your desktop through your ISP and on into the Tor network. Where it exists the Tor network it continues onwards as SSL encrypted data on its way to the news server or wherever.

For Web browsing we need Privoxy. This again acts as a bridge between your browser and Tor.

A web proxy is a service, based on a software such as Privoxy, that clients (i.e. browsers) can use instead of connecting directly to the web servers on the Internet. The clients then ask the proxy to fetch the objects they need (web pages, images, movies etc) on their behalf, and when the proxy has done so, it hands the results back to the client.

There are many reasons to use web proxies, such as firewalling (security), caching (efficiency) and others, and there are just as many different proxies to accommodate those needs.

Privoxy is a proxy that is solely focused on privacy protection and junk elimination. Sitting between your browser and the Internet, it is in a perfect position to filter outbound personal information that your browser is leaking, as well as inbound junk. It uses a variety of techniques to do this, all of which are under your control via the various configuration files and options. This need not be a concern as the latest Vidalia bundle now includes Privoxy with Tor and does all the setup for you transparently.

Privoxy will bridge the connection between your browser and Tor the Socks proxy host. It will minimize pop up ads, etc. But its main advantage is it will help prevent information leakage from your desktop to any third party trying to sniff your data. Used in conjunction with Tor it ensures all your Web browsing is totally anonymous.

There is no need to close Privoxy if you wish to use your news client or whatever. These programs are totally transparent to you once they are running. The latest version of Tor is supplied with the Vidalia bundle that automatically installs and sets up Privoxy for you. Vidalia also has a neat looking control panel that allows you to choose several options when using Tor. All very easy and obvious.

27. Is the data encrypted after it leaves the remote server and Tor?

Yes, providing you are using Stunnel. The only precaution you must take to ensure both privacy and anonymity, is to use Stunnel in combination with FreeCap, which ensures it routes all data over the

Tor network.

It is possible to use Stunnel alone, but not recommended. Choosing to do so, would bypass Tor.

28. How do I subscribe anonymously to a news provider?

You can send cash, a postal order or use a prepaid Debit Card.

There are now several news servers offering SSL (Stunnel) encrypted connections through port 563. Thus I strongly advocate you choose one of these. It costs no more to enjoy this extra level of security, so why accept anything less?

There are also remailers that accept an SSL encrypted connection, which significantly improves your Email security.

I no longer recommend e-Gold. In its place I suggest Pecunix or perhaps Ebullion. Pecunix (like e-Gold) is not intended to be anonymous, unless you take steps to ensure it is. Ensure you sign up using your choice of discrete details With anonymous access from different IP addresses using Tor. I recommend opening a second Pecunix account and transfering funds from the first into the second on an as needed basis. Any spending of your Pecunix gold should then only be done from the second account. This doubles the difficulty for anyone trying to do a backtrace. Obviously the accounts should not share any information. Meaning different Email addresses and other details, particullarly the passphrases.

29. How do I create a secure/anonymous Email account with Quicksilver?

I recommend opening a simple POP3 account with one of the many sites offering a free Email service. Provided you only ever access them via Quicksilver and Tor, you should be safe.

One example of this is Hotpop. There are many others. Take a look here:

http://www.emailaddresses.com/email_pop.htm

All these are only soft anonymous, but they can all be hardened by using Quicksilver and ensuring it routes only through Tor. You could use Hotpop as your Email incoming POP3 account and send or post through Tor and the Mixmaster remailer network.

Both Hotmail and Hushmail (and the latest version of Yahoo) insist on you having both Java and Javascript enabled before they allow you to open an account. This is unacceptable to me. I would never recommend using any Email service with such a requirement. Explanations follow in Part 2.

30. Can you briefly summarise all the above?

You need a VMWare virtual machine to run Windows (or Linux) from its

default location in "My Documents" as your honeypot.

You need TrueCrypt into which you should store personal data that may be revealed under duress. This is your honeypot secret data. You should also have a hidden TrueCrypt drive from which your VMWare virtual machine is run. This is your truly secret encrypted drive.

You need PGP and Quicksilver for your Email. These recommended programs should help you achieve a very high level of plausible deniability and privacy.

You will need other programs to ensure you are anonymous whilst online.

You need to be anonymous online for both browsing and whilst subscribing to any Web services. For this you need at least one, but preferably two Pecunix accounts and a pre-paid Debit Card. You must only access your email POP3 accounts using Quicksilver in conjunction with Tor.

Part 2

31. How do I achieve maximum plausible deniability?

Firstly, install VMWare Workstation 6 onto your computer. You should think of this program as a picture frame. The framework holds the Windows (or Linux) operating system which is your secret operating system to achieve total online and desktop secrecy.

One slight problem you will likely encounter is with Windows. It will probably tell you to validate your installation. Whether this happens will depend on what the differences are between your existing installation and the new virtual one.

Before proceeding further in VMWare turn off memory swapping. It is on by default. In VMWare, Go to Edit > Preferences > Memory and check "disable all swapping".

At the opening screen of VMWare Workstation 6, click on "New Virtual Machine". Follow the wizard step by step. For your first attempt just accept the initial screen defaults. On the Network screen choose "Use network address translation (NAT)" This can be changed later if necessary.

In the following screen choose "Allocate all disk space now". This will considerably speed up the program's operation. Of course, it is referring to the virtual disk that you are going to create, not your usual drive C disk.

Your first install can and should be openly visible. Do this by allowing it to install a virtual machine within its default location in "My Documents". This will become your honeypot version. It is the justification for having this program on your computer.

After creating the virtual machine, you are ready to install a bootable

operating system. You will need your Windows (or Linux) installation CD. VMWare will take care of all the little details of how to ensure there is no conflict with your usual Windows system. When you have inserted your Windows or Linux installation CD, on the tool bar click on "Power on this virtual machine".

You should then see the initial black screen within the program window, with the usual MS Windows (or Linux) startup messages of examining your computer, copying files, etc. Just leave it to install in the usual way.

In my case I found only my external USB connected DVD writer was seen by VMWare for installation of the windows operating system. My built-in CD writer seemed invisible. So if your installation cannot start, check if it is because it cannot see your CD or DVD. Once this is sorted, all else chould be plain sailing.

This is the longest bit: installing the operating system. When it has completed, you should click on VM > Install VMWare Tools. These will allow you to have much improved screen resolution. In fact it allows superb screen quality, as good as your usual desktop.

You should now check your Internet connection. If you are using an ADSL modem connected to an ethernet port, it will be seen by VMWare by default. If you are using an USB connected modem, there may be more hassle before it is seen. To check, just click on Windows Update. If it connects to the MS Website, all is well.

When you are happy with things, take a snapshot. Just click on the icon on the tool bar. This is simply a precaution in case something goes wrong with the installation of your future programs. You can revert back to this state at any time by clicking on Manage Snapshots. Easy.

After you have installed all your programs, I suggest taking another snapshot. You now have a safety net if anything goes wrong in the future. Naturally, you can take as many snapshots as you please, disk space is the limiting factor here. VMWare is an excellent vehicle within which to test out magazine cover CD/DVD's or downloaded software prior to normal installation on your desktop. You can at any time revert back to a previous snapshot without worrying whether it has messed up the computer.

Remember it is a virtual drive. Your new system when created, cannot see or even know of the existence of your usual drive C. Thus it cannot write to it, except to the VMWare virtual machine files within "My Documents". In fact, unless you tell it, it cannot see any of your other computer components, apart from your mouse your keyboard and your monitor. All else is a closed book. You must tell it which USB components you wish it to see and use. For example, you may choose to use an external DVD writer or an external hard drive. To communicate with anything else, on the Toolbar click on VM > removable devices > USB devices > click to enable any from the drop down list. When you enable anything, expect your desktop to tell you it is now safe to disconnect the device. This is VMWare doing its thing by taking complete control of the component away from your desktop.

Having created a successful bootable operating system which is openly visible, you now need to import it into your TrueCrypt hidden container. After importing it, you will then refine things by further installation of

all the critical programs you need to ensure privacy online.

Click on File > Import, and follow the import wizard. It really is very easy. You can make changes to various things, such as the size of the virtual machine's hard drive, RAM, or network connections, if necessary. For your first attempts, I suggest just accepting the existing settings.

With practice you will realize that you should ideally allow a maximum virtual disk size around half of the TrueCrypt drive size. Snapshots take up gigabytes of space and it is surprising how quickly you can fill what was originally a huge Truecrypt drive. Of course there is no need to keep all the snapshots. You may decide to keep only the first and the latest.

You will find that with Windows you will normally need to validate your new installation at some point. I would not bother unless essential to log on, until you have finished experimenting. You may decide to scrap that install and try again and again and. . . ! There is a very steep learning curve with VMWare. Trust me, it is well worth it. I know, I nearly threw it away several times before I truly mastered it.

You must also defragment this virtual drive C. Do this exactly as you would with a normal hard drive. In fact you need to do it thrice over. Once from within the up and running virtual machine by going to "My Computer" and right clicking on the C drive and choosing Tools and defrag and then after shutting down VMWare displays a summary view of this virtual machine. This shows among other parameters, the size of the hard drive. By left clicking on the hard drive you choose utilities and defrag. Finally, after closing this virtual machine, from within your usual desktop you can defrag your TrueCrypt drive by right clicking on its drive letter in "My Computer" and choosing Properties > Tools > defrag.

Nothing you do within your virtual Windows operating system should appear in your usual Windows registry. However, the VMWare virtual machine itself contains a Windows registry and swap file. Unless this virtual machine is within a TrueCrypt container, data held within it will also appear in plaintext on your real Drive C hard drive. Thus it is imperative that your secret virtual machine be installed within a secret TrueCrypt drive.

A few other important points. If you live in a country where there is the possibility of being raided without any warning, you must have some means of switching off your computer instantly. Better to lose some data than your life. Also, ensure you have disabled the hibernation feature within your normal desktop. I am aware this all sounds very melodramatic, but some who will be reading this Faq live in very repressive regimes where human rights are non-existent.

32. This sounds like a lot of work, is it worth it?

It is most definitely a lot of work. Whether or not it is worthwhile is down to the individual and how much he desires true anonymity. If privacy is important to you, then nothing is too much bother.

33. Can you summarize all the above?

The aim is to be able to justify the possession and usage of both VMWare and Truecrypt.

VMWare should be openly installed and visible using its initial default choice of location in "My Documents". This is your honeypot VMWare installation.

TrueCrypt can be justified by using it to store copies of all your private data, letters, family photos, etc. This is your honeypot TrueCrypt container and is the justification for TrueCrypt.

Your hidden Truecrypt container will probably be far larger and hold your truly secret VMWare virtual machine. Into this installation will be made all the programs you need for online security and anonymity. It might also hold all data that is precious and very private. Data that you do not wish revealed to the rest of the world.

The above is a bare bones method.

There are many variations on the above scenario. If you can think of a superior way of doing things, excellent! The more variant your ideas, the better your plausible deniability will be.

34. What if I have chosen to create a hidden TrueCrypt drive?

In this case it is preferable that no further data are added to your honeypot drive at the risk of destroying altogether your hidden drive. Fortunately, TrueCrypt will allow you to add data provided you choose this option when mounting the drive. See the manual for this procedure. My experiments suggest you use this option with care and a lot of common sense. If you attempt to add too much data, you will get write behind cache failed messages and loss of data.

Another small hint: If you ever wish to delete very large quantities of data from your secret TrueCrypt container, you might be tempted to simply format it using Windows. Indeed, Windows will oblige and do it. But be prepared for similar write behind cache failed error messages. Either delete unwanted files or use TrueCrypt to re-format the drive.

35. Any more hints about this system?

Experiment. I suspect that your first attempts will be written off and further attempts be made before you are truly happy with all apsects of your system. Remember, that it is likely that windows will demand you validate these installs. Sometimes, a copy can be made without re-validating. Some enterprising soul may realize they can import their complete drive C and use it as their virtual machine. True. But that install will likely contain MSIE and perhaps outlook, plus some personal details such as credit card usage, etc. Bad news. Also, Windows will know what you have done and perceive it as an illegal copy and may prevent you from logging on until you have re-validated the copy. What you are doing is perfectly acceptable to MS, provided it is on the

original machine on which the original copy of Windows was installed.

Microsoft themselves offer a free download of a virtual machine. But as with most MS products, it offers only the basics. It also assumes a child-like trust in Microsoft.

36. What programs do I need and where do I get them?

There are five other programs besides VMWare and TrueCrypt that I recommend for security and anonymity:

PGP, Stunnel, FreeCap, Privoxy and Tor.

And three others recommended for Email, Usenet and Web browsing: Quicksilver, Agent and FireFox.

In all cases where there is a choice of download, ensure you download the version that is compliant with your operating system, e.g. Windows XP or whatever.

Get them here:

VMWare Workstation 6: http://www.vmware.com/products/ws/

PGP: http://www.panta-rhei.dyndns.org/downloads/PGP/pgp658ckt08.zip

TrueCrypt: http://www.truecrypt.org/

Tor comes bundled wth Vidalia and Privoxy. Get them here:

http://tor.eff.org/index.html.en

Stunnel is used for NNTP secure connections to your news provider.

Stunnel: http://www.stunnel.org/download/binaries.html

Stunnel requires the executable file plus 2 others.

stunnel-4.05.exe
stunnel-4.05.exe.asc (digital signature file optional but recommended)

OpenSSL Libraries (required files). These are put in the same folder as Stunnel:

libssl32.dll
libeay32.dll

libssl32.dll.asc (optional)
libeay32.dll.asc (optional)

FreeCap: http://www.freecap.ru/eng/?p=index

Privoxy: http://www.privoxy.org/ (no longer needed as a separate program because it is now included with the Tor bundle.)

Not essential, but strongly recommended:

Agent: http://www.forteinc.com/main/homepage.php

FireFox: http://www.mozilla.org/products/firefox/

Quicksilver: http://www.quicksilvermail.net/

Note: There are later versions of PGP. Ignore them. They are closed source.

37. Where do I put these files?

All instructions below assume you are installing into your secret VMWare virtual machine with TrueCrypt.

Create a new folder called Proxy. This can be within Program Files or in the root of the virtual drive. Open Proxy and create the following sub-folders: FreeCap, Stunnel. Install by copying all of the downloaded files of each of these programs into their respective folders. Ensure the library files for Stunnel are in the same sub-folder.

Each program can then have shortcuts made and placed on your virtual desktop.

38. How do I configure Tor?

The latest version of Tor is now offered with the Vidalia bundle which includes Privoxy and a Windows install. Ensure you download the latest release. An earlier release suffered from a fatal security flaw.

It is probably best to accept the default installation folders. Vidalia will present you with a control panel to help you configure Tor and to control its usage.

Note: I recommend checking back regularly for the latest version of Tor as it seems to be changing very frequently. I also recommend you take the bother of reading at least the basics of how Tor works.

39. How do I configure Privoxy?

Nothing to do. It is already pre-installed within the Vidalia bundle.

40. How do I configure Stunnel?

Stunnel is required for an NNTPS, meaning a secure connection to Usenet.

Copy and paste all of the following in Notepad and save it in the

Stunnel folder, name the file stunnel.conf:

```
#Stunnel client configuration file
#
client = yes
options = ALL
RNDbytes = 2048
RNDfile = Random.bin
RNDoverwrite = yes

#[Meganetnews_NNTPS]
#accept = 119
#connect = news.meganetnews.com:563
#delay = no

[nntps]
accept = 119
connect = news.aioe.org:563
delay = no

#[Putty_nntps]
#accept = 119
#connect = news1.meganetnews.com:563
#delay = no

#[nntps]
#accept = 119
#connect = secure.news.easynews.com:563
#delay = no

#[nntps]
#accept = 119
#connect =  news.x-privat.org:563
#delay = no

#[Octanews_NNTPS]
#accept = 119
#connect = snews.octanews.com:563
#delay = no

#[putty_nntps]
#accept = 119
#connect = 127.0.0.1:563
#delay = no

# End of config file
```

Remove the # from the beginning of any bunch of lines you wish to make active. The above is setup to optionally allow (When the # is removed) routing through several news providers using a secure SSL connection.

Note the lines:

```
#[putty_nntps]
#accept = 119
```

```
#connect = 127.0.0.1:563
#delay = no
```

This is an option to route your Usenet connection through a SSH (Secure Shell) host server using Putty.

This option is strongly recommended for Usenet posting when used together with Tor for maximum anonymity and security. These Secure Shell servers are offered on a subscription service. I suggest doing a Google search or try Cotse. I have had no experience with Cotse, but some speak highly of them.

The file stunnel.conf does not exist until you create it. Stunnel cannot work without its presence. You will just get some server error. This might happen if you or Windows names it incorrectly.

You may need to get Explorer to show extensions to known file types, otherwise Windows may save the file as stunnel.conf.txt. If you are not sure, go to Tools > Folder Options > View > uncheck "Hide extensions to known file types". Click on Ok.

41. How do I configure FreeCap?

Go > File > Settings > Proxy Settings > Default Proxy.
Type 127.0.0.1 into the server window and 9050 into Port. Click OK.
Under Protocol ensure SOCKS v5 is checked.

With the program back at the opening screen, drag and drop the Stunnel shortcuts into the FreeCap window. You will immediately see the Stunnel icons position themselves along the top of the screen. As each is loaded, re-name it to easily distinguish it from the others. Do this by right-clicking on an icon and selecting Modify. Change the name on the top line to something self-descriptive, such as Easynews or Putty or whatever.

You have now socksified Stunnel. That is all it takes. Whenever you run Stunnel you must start it by clicking on one of the icons from within FreeCap, which obviously means first starting Freecap. Stunnel secures the programs and by socksifying it with Freecap, ensures all data is routed over the Tor network. Just minimize Freecap after starting Stunnel. To close Stunnel, right click on its icon on the taskbar and select Exit. Always close Stunnel prior to closing Freecap. This ensures that no data jumps across, bypassing Tor.

Note: Some may experience problems with FreeCap. If you do, an excellent, free for non-commercial use alternative, (but not open source) is SocksCap. It is here:

http://www.socks.permeo.com/Download/SocksCapDownload/index.asp

42. How do I configure my Browser?

To ensure your browser chooses to route through Tor you must now go to

its Proxy settings Window. With FireFox this is > Tools > Options > Connection Settings.

Input 127.0.0.1 into each line except Socks Host. Leave that line completely clear. Input 8118 into the Port window for each line, but again leave the Socks Host line clear. Privoxy listens for connections on port 8118 by default. This is telling Privoxy to pass on its connections to Tor which is listening on Port 9050 by default.

Click on > Tools > Options > Web Features and uncheck "Enable Java" and "Enable Javascript". This is very important to ensure no remote site can take control of your desktop and invade your privacy. I would also disable "allow Web Sites to install software"

Another absolute no-no is Adobe Macromedia Flash player. I also strongly urge you not to use either Windows Media Player or Real Player. Both are notorious for phoning home with usage data.

You will find some Web sites will not now work correctly. This is the penalty of ensuring you do not give away your private details to any snooper who may be trying to sniff them.

The latest versions of Firefox now offer many add-on freebies, including one that allows instant on/off control of Tor, showing its status bottom right of the Firefox window. I only use it for my usual Drive C. My secret TrueCrypt version of Firefox is permanently setup to use Tor. This saves me any embarassing mistakes. Most importantly, do not install any search add-ons, such as Google or Yahoo. They have a nasty habit of phoning home directly, meaning bypassing Tor.

Another tweak, in Control Panel > System > Advanced > Error Reporting > click on "Disable error reporting". As a further precaution I would do the same within both your usual desktop and your virtual machine.

Sometimes when Windows wants to send an error report it includes large sections of your hard drive. Sometimes this will contain file names that you might prefer not to be sent to MS. This ensures no error messages should ever be sent. Of course, ZoneAlarm should alert you anyway. But what is wrong with a belt and a pair of braces?

43. How do I configure my news client?

You must now configure your news client by inputting 127.0.0.1 into the window which asks for your news server name. If you have never used a proxy prior to this, go to the screen displaying "News Server". In Agent 1.91 this will be Options > User and System Profile > User. Enter 127.0.0.1 for the server name. Click OK. The port is set in the Agent.ini file to 119, do not change that. Stunnel has already been configured to listen on port 119 anyway and to forward through port 563. Yes, you can change this port, but only do so if you know what you are about.

Note: Stunnel can only be used with a news provider that offers a secure (NNTPS) connection (by default on port 563). For other news providers Stunnel is useless. For these less secure sites I suggest socksifying Agent, by dragging and dropping the Agent shortcut into

FreeCap. Not nearly as secure, as your data will not be encrypted after it leaves the Tor network on its way to the News provider. It costs no more to subscribe to a secure news provider than it does to one that does not offer an encrypted connection. So why choose anything less?

Each of these four programs, Stunnel, FreeCap, Privoxy and Tor accepts connections from either your Web browser, into Privoxy and on to Tor, or from your News client into Stunnel, socksified by FreeCap and again on to Tor. Many programs can be socksified, not just those mentioned. The procedure is exactly the same, just drag and drop the shortcut of the program to be socksified into Freecap.

44. How do I test these are all working?

Let's check the Web first.

Start Privoxy (which by default normally starts with Windows).

Open your browser and input: http://p.p/

You should see the Privoxy main page with the following:

"This is Privoxy 3.0.3 on localhost (127.0.0.1), port 8118, enabled."

If you see that, be assured you have accessd via Privoxy.

If you see "p.p. could not be found, please check the name and try again." You are definitely not accessing via Privoxy.

Go back through the above and check everything very carefully.

Note: This is an internal test, not via the Web. It just proves that Privoxy was invoked to display that page from its own folder, which you will see displayed if you click on "View and change the current configuration"

You will then see a clear display of all the configuration settings.

Do not change anything unless you have a backup file and know what you are doing.

Let's assume your Web browser is functioning as it should and you see the p.p. page displaying the confirmatory message.

You should now test your news reader client.

45. How do I test my news connection is anonymous?

Open FreeCap and click on the Stunnel icon in the FreeCap Window.

Without opening Tor at this stage, start your news client. As a small precaution ensure you are in an appropriate newsgroup and attempt to download its headers. You should see connecting to 127.0.0.1 displayed on the lower taskbar in Agent or wherever in the version you

are using, followed by error reported by Winsock driver. Good. This proves Stunnel was attempting to connect to Tor which is offline of course, thus no connection was possible.

Now start Tor. Try again. Hopefully this time you will have more success and it should connect to the news server and start downloading headers.

Note: It can sometimes take a considerable time to connect when using the Tor network. This is normal, but means patience is a virtue here.

Go to a multimedia group and start to download a large file. While the download is in progress, close Tor. You should see an immediate error about connection to server closed unexpectedly. Good.

Re-start Tor. Re-establish the connection with the server and start over. This time close FreeCap. Notice the download will continue. Do not panic! It is still accessing via Tor. Prove this for yourself by closing Tor and notice the download again stops immediately and there is the same Winsock error. However, do not normally close any of these programs until you are ready to go offline. Always close the news reader first to ensure no data is being accessed which might just possibly jump across and appear in the clear.

The usual way to open each of these programs is go online with your ISP. Open Tor, open Freecap, start Stunnel from within FreeCap. Then last of all open your news reader. Test the system from time to time to satisfy yourself all is as it should be. Closing down is the reverse of this procedure.

If you have got this far, you have succeeded in creating a secure and truly anonymous network connection for both your browser and your Usenet posting/downloading.

Note: It is imperative that Stunnel be started only from within FreeCap and thus be socksified. Otherwise it will simply connect directly with your news provider, bypassing the Tor proxy network. Certainly it is an encrypted connection but totally useless from an anonymity point of view. Your ISP will know exactly where you are connected. Your news server could also log your ISP address!

46. What if no exit server exists on Tor with port 563 (or 119) enabled?

Since choosing to use SSL via port 563, I have not experienced any bother whatsoever in connecting to Usenet.

If you would prefer to subscribe to a Secure Shell host, then you need to use Putty as the SSH client.

Putty is here: http://www.tucows.com/preview/195286.html

You will still need Stunnel to allow the NNTPS (encrypted) connection into your news provider and FreeCap to act as a bridge between Stunnel and Tor. Tor is the socks proxy that hides your true IP from the

Secure Shell host server. Putty will channel everything through port 22, which should not be a problem.

See the above example stunnel.conf file.

The sequence is: Agent > Stunnel > Freecap > Tor > SSH server > news server (or wherever).

This is the route to go for the strongest anonymity. It is especially recommended for hard anonymous posting to Usenet. For lurking, the requirements are not as critical and it is sufficient to just go Agent > Stunnel > Freecap > Tor > news server.

Contrast that with the usual newby connection of Agent > news server, or worse, Outlook Express > server.

47. How do I configure Putty?

Open Putty. Load one of your SSH servers, but do not yet open the connection.

Go down left hand column to Proxy. Click on Socks5

Enter 127.0.0.1 into Proxy Hostname and 9050 into Port.

Click on Yes for "Do DNS name lookup at Proxy end."

Go down to Tunnels.

Input 563 for local port. Then input "secure.news.easynews.com:563" (or whatever name your news provider has assigned you) in the destination host box (without the quotes) and click on ADD.

Your entry will then look something like this:

L563   secure.news.easynews.com:563

Go back up to the opening screen in Putty and click on Save.

48. Can I post binaries anonymously to Usenet with this system?

Absolutely. If you choose to use Agent, it will always use your news provider as the posting host. This is why I recommend you subscribe anonymously to this news provider - see further down regarding anonymous subscriptions.

If you are into heavy posting then you should use Power Post or something similar that allows you to choose whole folders of files for posting.

If you use Quicksilver for posting to Usenet it will always use one of the mail2news gateways. All data from your desktop is encrypted through to the first remailer and then on through the Mixmaster remailers and onto Usenet. The one and only down side is that the

anonymous remailer network does not readily accept large files, such as binaries. The remailer network was set up to transmit text files, not binaries.

Agent can ensure that text files are included within the body of the message, rather than being sent as an attachment. To do this ensure you are in the posting frame and the focus is in the message frame. Go File > "Insert text file" > and navigate to your chosen text file.

This better suits the remailer network which does not normally accept attachments.

To post binaries use Agent or Power Post or similar and post via your socksified Stunnel and Tor.

A warning: If you post illegal material, you may find your anonymous account closed without warning and no possibility of any refund! Of course no such opportunity exists when you channel through the remailer network, which is precisely why so many choose to use it.

49. what about sending Email?

I recommend Quicksilver. Quicksilver now supports a direct route through to Tor, providing you specify it. To ensure this go > Tools > POP Accounts > Proxy > input 127.0.0.1 in the Proxy Server window and 9050 in the Proxy Port window and choose 5 for Socks Level from the drop down options. Obviously, you must also input your POP3 userid and password in the POP Accounts section.

There is no need to worry about socksifying it through Stunnel and FreeCap. Here are sample templates for this. Just copy and paste them into a Quicksilver template.

This one is for Usenet, name it Panta-news:

```
Fcc: outbox
Tor: 127.0.0.1:9050,4a; nowhere.invalid;
Host: panta-rhei.dyndns.org:2525
From: kwiktime <kwiktime@kwiktimemail.net>
From: urnym.goes.here
Chain: panta,*,*,*; copies=2
References:
To: mail2news_nospam@anon.lcs.mit.edu,
 mail2news_nospam@freedom.gmsociety.org
Newsgroups:
X-No-Archive: yes
X-Hashcash:
Subject:
```

...and this one is for Email, name it Panta-Email:

```
Fcc: outbox
Tor: 127.0.0.1:9050,4a; nowhere.invalid;
Host: panta-rhei.dyndns.org:2525
From: kwiktime <kwiktime@kwiktimemail.net>
From: urnym.goes.here
Chain: panta,*,*,*; copies=2
To:
X-Hashcash:
Subject:
```

Notice that in both cases truly excellent anonymity is assured because in addition to the anonymity offered by Tor, your messages are further anonymized by passing across the Mixmaster remailer network. It should be truly impossible for your ISP to be able to even discern that you are posting or sending Emails. This is because you are not using your ISP's SMTP server to sendmail or to post.

Hashcash is a requirement for panta-rhei, banana and dizum. Without the Hashcash token your message will be either randomnly sent to another remailer or lost. To use Hashcash you must get the Hashcash zipped file from here: http://www.panta-rhei.dyndns.org/downloads/

Unzip and install in a convenient folder. After installation go > Start > Programs > Universal Hashcash Minter and copy or drag and drop the shortcuts shown into your desktop, or wherever. Now all you need to do is click on the shortcut to mint tokens, copy one of these tokens to the clipboard so you can paste it into the header of your Quicksilver template. Then delete that token from the list of availables.

Hashcash is being forced on remailer admins to help minimize junk mail. Without it, some might simply close. We all benefit from the remailer network and this is the price we have to pay for this service.

To read more about Hashcash go here: http://www.hashcash.org/

A further refinement when using Quicksilver is to ensure that when you ask it to update the remailer listing, it always uses Tor. To ensure this, on the Tool Bar go > Remailer Documents > Proxy > in Proxy Host type 127.0.0.1 and Port 9050 and Socks Level 5.

50. Why is the remailer network so secure and anonymous?

Although not perfect (nothing is), it does offer a level of anonymity well above and beyond what simple anonymous services (such as Hotpop) offer. It uses the Mixmaster remailers and has protocols to ensure your messages are very difficult to trace and decrypt. Remember, by using Quicksilver in the recommended way, you are not just using Mixmaster, but also using the Tor network which then sends all data on to the Mixmaster remailer service.

Mixmaster is the type II remailer protocol and the most popular implementation of it. Remailers provide protection against traffic analysis and allow sending email anonymously or pseudonymously.

Mixmaster consists of both client and server installations and is designed to run on several operating systems including but not limited to *BSD, Linux and Microsoft Windows. It does not use PGP, but RSAREF with its own keys and key formats.

In the above cases, this anonymity is further reinforced by using the Tor network to anonymize you from the panta-rhei or banana first remailer in the Mixmaster network. Double anonymity - excellent.

51. How do I receive Email with Quicksilver?

You can set up Quicksilver to look for Emails on any POP server such as Fastmail.fm or hotpop.com. All your mail is then recovered via the Tor network which helps you remain anonymous.

Go > Tools > POP Accounts > Proxy > 127.0.0.1 for Proxy Server, 9050 for Port and Socks level 5. Ignore the two lower lines. This will route your Email path through Tor. You can choose to ensure that quicksilver only downloads PGP encrypted mail and to delete or leave on the server. Very flexible.

52. What about P2P and IRC?

P2P using eMule or whatever is very risky from a privacy view point, unless you know what you are doing. I believe some have used it in conjunction with Find.not, but you will have to do your own research about this. I am sorry I cannot help as I have never tried it.

The Tor Website claims you can use Tor for IRC and IM, but again, I have never used Tor in this fashion myself.

53. How do I get access to the premium (paid for) services?

Apply on their sites. But always access via Tor and ensure you subscribe anonymously. The easiest way is by means of a prepaid Debit Card.

54. I want a Pre-paid Debit Card, how and where do I get one?

Go here: http://www.money-around-the-world.com/ But only after you have configured your browser to route via Tor - most important this!

They will accept many forms of payment. Pecunix is now my preferred way using two different accounts back to back.

The Debit Card is acceptable to many more web sites, especially news providers, than Pecunix (or my earlier choice, e-Gold). Note this card is solely for Net use. It is a virtual card. You get Emailed the card details, you do not receive a physical card through snail mail. Thus the name and address you supply need only match the name and address you have used when creating your second Pecunix account. Naturally, this is the

same address you must use when using your card to subscribe to a Web site. But this name and address is your choice! If in the United States, the Zip code must match your choice of address. But so far as I can tell, that is the only check that is made. Just take an address out of the phone book, but change the name and house number.

Of course the Email address you offer, must be accurate, secure and most importantly, anonymous.

55. Are there any disadvantages to this type of card?

Cost. They charge you 50 US Dollars, plus 6 percent of the value you wish to load into the card. At the end of the year, you need to re-apply for another. It can only be used for Web purchases.

Its truly big advantage is it can be purchased anonymously. No online identity checks or credit checks and no need to offer a genuine postal address.

But be certain to use an accurate and anonymous Email address.

56. What about funding my Pecunix account?

This can be a disadvantage if you choose a market maker unwisely. Some will want to identify you as per the latest Government homeland security bills. However, if you choose an Asian market maker, you can pay directly into one of their branches with a fake identity. Remember this is your initial Pecunix account. The name you use must be different to your second account. The second Pecunix account receives its funding by you transferring money from one account to another. To Pecunix it would seem as if you were sending money to someone else with no connection with you. Ensure you setup Firefox to delete all data, including cookies when you shut down Firefox. In Firefox, Tools > Options > privacy > ensure "Always clear my private data when I close Firefox" is checked. Whilst in the options tab, go > Content > uncheck both Java and Javascript boxes.

This is probably the single most important item to be meticulous about.

57. What is so bad about Microsoft Internet Explorer?

MSIE is a dangerous program designed by MS to allow remote servers to access your computer's registry. Although designed for use by MS to allow easy updating of the Windows Operating System, this feature could be used by any site to access your IP address, even your machine ID and your personal Credit Card details or worse, far worse, your saved passphrases. This can be done even if you have logged onto a site through a chain of proxies. In other words Microsoft Internet Explorer is an absolute no-no as far as anonymity is concerned.

Be wary also of Windows Media Player. It creates a unique ID number in the form of a 128-bit GUID (Globally Unique Identifier) which will uniquely identify your computer to the world at large. It is stored in

the Windows Registry here:

HKEY_CURRENT_USER\Software\Microsoft\WindowsMedia\WMSDK\General\UniqueID

This ID number can be retrieved by any web site through the use of JavaScript. Hence the reason why it MUST be disabled. The ID number is called a supercookie because it can be retrieved by any web site. This supercookie can be retrieved by any site to track you and web sites can share this information with each other, allowing them to create a sophisticated profile about your Internet usage. Worse, cookie blockers cannot block its use!

The easy way to fix the problem is in Windows Media Player > Tools > Options > Player. In the "Internet settings" section, uncheck the box next to "Allow Internet sites to uniquely identify your Player."

Or you can ensure that Windows Media Player is not enabled at all. To do this go Start > Settings > Control Panel > Add/Remove Programs > Set Program Acess and Defaults > Custom > clear the button for both Real Player (another bad one) and Windows Media Player and also clear the button where it says "Enable access to this player" for both of them. I choose both of the above methods as I believe in belts and braces when it comes to privacy.

58. Surely all this is totally over the top for the majority of users?

It is certainly over the top for 99 per cent of users for 99 per cent of the time. If, however, you are the one in a hundredth and you do not much like the idea of being at risk for 1 per cent of the time, then no, it is not over the top at all.

In any case, using these tactics helps create smoke which in turn helps protect those who really do need all the protection and security they can get.

Remember this Faq is intended to help many different people. Some may be living in deprived conditions, in countries where human rights abuses are a daily fact of life. There are many more undemocratic countries than democratic ones.

59. What about backing up my Data?

Create another encrypted container using TrueCrypt on an external hard drive. Open this partition and copy some innocuous data from your normal plaintext drive. Now close this container and create a hidden container, following the instructions in the documentation that comes with TrueCrypt. Now copy all your secret data across into this secret container.

Restoring is just as simple. Just open the secret container and copy into your TrueCrypt partition.

60. Are there any other hints?

A few items that may be of interest if you run Windows XP, although not of any value as snoop protection. To make your system run faster do this: Right-click on the Start menu button > Properties > Start Menu > Classic Start menu > Customize > Advanced Start > scroll down to "Show Small Icons in Start menu" and uncheck the box. Click OK, again OK. Now right-click on your Desktop > Properties > Appearance > effects. Uncheck everything. Click OK in the Display Properties dialog and OK again. You have just got rid of much of the Windows kludge. It will run faster and will seem more enthusiastic about everything.

A further small improvement in securing your TrueCrypt drive is to ensure it is mounted as removable media. Go > Settings > Preferences > Ensure "Mount volumes as removable media" is checked. This will disable Write behind disk caching and disable cross drive connected Recycle Bins.

.....

I am aware that this Faq has grown over the years and will seem very daunting to someone new to the Net. My suggestion is to take it one step at a time. Experiment with PGP. Generate a few keys, test them out by sending Email to yourself. Only when you understand what you are doing should you then go on to the next step. I would suggest this might be by investing in a new hard drive and experiment with encrypting it using TrueCrypt.

Only then should you try installing VMWare and attempting to create a virtual machine. Again, take it one step at a time. Do not over-reach yourself.

Despite my attempts at thoroughness, this Faq still falls woefully short of a truly comprehensive explanation of all that is required for true Net privacy and anonymity. Hopefully individuals will take time to read and learn more as they go along.

My key is on the key servers. This is my key fingerprint:

F463 7DCB C8BD 1924 F34B 8171 C958 C5BB

Remember, anybody can call themselves by my Nic, but there can only be one key fingerprint like the above - mine. It thus ensures you are reading a Faq prepared by me and no one else.

I have no objection to anyone hosting a copy of this Faq on their Website. I only request they try and ensure it is the latest version.

Links to items specifically mentioned or recommended in the Faq:

VMWare Workstation 6: http://www.vmware.com/products/ws/

PGP: http://www.panta-rhei.dyndns.org/downloads/PGP/pgp658ckt08.zip

(This is the version I prefer)

TrueCrypt: http://www.truecrypt.org/

Tor: http://tor.eff.org/index.html.en

Stunnel is used for NNTP secure connections to your news provider.

Stunnel requires the executive file plus 2 others.

Stunnel: http://www.stunnel.org/download/binaries.html

stunnel-4.05.exe
stunnel-4.05.exe.asc (digital signature file optional but recommended)

OpenSSL Libraries (required files - scroll down the page:

libssl32.dll
libeay32.dll

libssl32.dll.asc (optional)
libeay32.dll.asc (optional)

Privoxy Home page: http://www.privoxy.org/

Putty: http://www.tucows.com/preview/195286.html

or here:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
Quicksilver: http://www.quicksilvermail.net/

Mixmaster: (required by Quicksilver) can be downloaded after
installing Quicksilver, just go > Window > Update Wizard and
follow the onscreen steps

POP Email services: http://www.emailaddresses.com/email_pop.htm

Hashcash Zip file: http://www.panta-rhei.dyndns.org/downloads/

Hashcash site: http://www.hashcash.org/

Kremlin: http://kremlinencrypt.com/download.php

Windows Washer is here: http://www.webroot.com

Pecunix:

Virtual Debit Cards: http://www.money-around-the-world.com/

Agent: http://www.forteinc.com/main/homepage.php

Zonealarm: http://www.zonelabs.com/store/content/home.jsp

Other links that might be of interest:

Free Email: http://www.emailaddresses.com/email_pop.htm

UUDeview: http://www.fpx.de/fp/Software/UUDeview/

Jstrip: http://www.davidcrowell.com/

BLJoin: http://www.all4you.dk/FreewareWorld/links.php?id=8866

(Recommended to decode and join binary files)

SSL Proxy info: http://www.jestrix.net/tuts/sslsocks.html#intro

WinHex: http://www.winhex.com/winhex/order.html.

(Will show you what is on your hard drive)

ACDSee: http://www.acdsystems.com/english/products/acdsee/index

Thumbs Plus: http://www.cerious.com

VuePro: http://www.hamrick.com

News Providers: http://www.exit109.com/~jeremy/news/providers/

Freenet: http://freenet.sourceforge.net/

In case you need convincing:

http://www.gn.apc.org/duncan/stoa_cover.htm

Useful programs:

Partition Magic: http://www.powerquest.com/

HJSplit: http://www.freebyte.com/hjsplit/

Mastersplitter: http://www.tomasoft.com/mswin95.htm

PowerPost: http://www.cosmicwolf.com/

Quickpar: http://www.pbclements.co.uk/QuickPar/

SmartPar: http://www.smr-usenet.com/tutor/smartpar.shtml

WinAce: http://www.winace.com/

WinRAR: http://www.rararchiver.com/

YProxy: http://www.brawnylads.com/yproxy/

Media Player Classic: http://sourceforge.net/projects/guliverkli/

Some anonymity sites:

http://www.worldnet-news.com/software.htm

http://www.skuz.net/potatoware/index.html

http://www.skuz.net/potatoware/jbn/index.html

http://packetderm.cotse.com/

http://www.cotse.com/refs.htm

http://freeyellow.com/members3/fantan/pgp.html

http://www.all-nettools.com/privacy/

http://Privacy.net/

http://www.geocities.com/CapeCanaveral/3969/gotcha.html

http://www.junkbusters.com/ht/en/links.html

http://www.skuz.net/potatoware/privacy.txt

Other additional useful sites:

Beginner's Guide to PGP:

http://www.stack.nl/~galactus/remailers/bg2pgp.txt

PGP for beginners:

http://axion.physics.ubc.ca/pgp-begin.html#index

Faq for PGP Dummies: http://www.skuz.net/pgp4dummies/

The PGP Faq: http://www.cryptography.org/getpgp.txt

The SSH home page: http://www.ssh.com/products/ssh/

Anonymous Posting:

http://www.skuz.net/Thanatop/contents.htm

Anonymity Info: http://www.dnai.com/~wussery/pgp.html

Nym Creation:

http://www.stack.nl/~galactus/remailers/nym.html

General info:

http://www.stack.nl/~galactus/remailers/index-pgp.html

Revision 22.3

-----BEGIN PGP SIGNATURE-----
Version: 6.5.8ckt http://www.ipgpp.com/

iQEVAwUBRsRtMWToeXEUpganAQG9WQgAhQQ359LIV2HiOIi8G0DGLlt/+Rp57eHu
JrouYyw937dQkdwH8aezNJPNW1piFEgYkjhLXNqVSLhS3a3pM26D/dE0VMajsndn
0yoilcHyVjyGPxqZw0zwrizw26tpEvkIDba//3J3jpVzhoTj/siPkf6s9OlvoSfJ
Wqrdg2u8Cmja/ZTWB/53jiioc4MHt6n2jAPgDdtoxo/K56IUFQetpGDwdhq2g0vT
t6qdRIXqq2+u0hFYineNjtSeL6VHoioW5LZM+yDP65q3cNzF2CuHhhNZrS4TFTB0
b2icfhMZP9XmaxT3K3SEcNyp61YoUoPaV3mFxDsdYol1MhfHf3pSRw==
=Bpth
-----END PGP SIGNATURE-----