

# **A comparison between the early days of the public Internet and the darknet Freenet**

**First draft**  
**14/03/2011**  
**Megan Hoogenboom**

## **Elements:**

The early days of the public Internet  
The commercialisation of the public Internet  
The beginning of Freenet  
The structure of Freenet  
Comparison between early public Internet and the Freenet Darknet (conclusion)  
Future of darknet's like Freenet

(This first draft of my final thesis has also elements implemented I want to add at a later stadium, to make the parts that are already wrote more clear.)

## **The early days of the public Internet**

As a result of the adoption of Part 68 of Title 47 of the Code of Federal Regulations by the FCC in 1977, all costumers of a telephone and telephone line could finally attach any devise they wished to the network. Before this was held back by AT&T, which was the monopoly of telephones at that time, because of commercial benefits. The network could now be opened for earlier developed networking systems, opened up by ARPANET created by ARPA, The Advanced Research Projects Agency, which was part of the Department of Defence of the US (Griffiths 2002, <http://www.let.leidenuniv.nl/history/ivh/chap2.htm>). In 1978 Ward Christensen and Randy Suess developed a new piece of software; the Computer Bulletin Board System, BBS (Gilbertson 2010, <http://www.wired.com/thisdayintech/tag/ward-christensen/>). This small program was only available if one person received a phone call, and would shut down if the caller hung up. While they were connected the one who made the call could send commands to the computer on the other end of the line. Users could also upload and store files, this was the forerunner of contemporary web forums. BBS was later joined by FidoNet, created by Tom Jennings. This program allowed users to communicate on a bigger scale: global. The PC was getting more common because of these networking abilities, which was the beginning of the World Wide Web or Public Web (Ryan 2010). These first systems were developed by hobbyists/enthusiasts or people of the Homebrew community. Not late after that companies joined in, and made the technology more available to home users. At the end of 1980 and the beginning of 1990 the competition and commercialisation of the web slowly began. Also, on universities and within companies people were getting more PC's and were connecting them via LAN with TCP/IP protocol, which was freely distributed. At the same time, ARPANET funded by the Defence Communications Agency, DCA, adopted the TCP/IP protocol, in which they moved the network of DCA from a networking protocol to an internetworking protocol. This was the foundation of the internet today. The ARPANET was officially decommissioned in 1990, after it had formed the temporary backbone for a new system called NSFNET (<http://www.nsf.gov/about/history/nsf0050/internet/launch.htm>). This was meant to be a high-speed national networking system, build by MERIT and became operational in 1988 (MERIT timeline [http://www.merit.edu/about/history/timeline\\_1980.php](http://www.merit.edu/about/history/timeline_1980.php)). After this all, Tim Berners-Lee developed in 1990 the hypertext language HTML. He wanted it to be part of a world wide web of information, where the document format wouldn't make a different, it would al be able to be called up by a URI. The HTML came along with the first browser and editor to view and create HTML files. This was the beginning of the world wide web, and the browser.

The personal webpages got a slow start after the introduction of the browser. Different browers were developed and people started to buy and use PCs and office computers. The www was missing one essential element in the 1990s to 2002s, a search engine. The public Internet of the 1990s and early 2000s was referred to with the metaphor "I go get Web" (Vander Wal 2006 [http://personalinfocloud.com/2006/01/the\\_come\\_to\\_me\\_.html](http://personalinfocloud.com/2006/01/the_come_to_me_.html)). As this metaphor implies, in these times one should know where he wanted to go, and in this way find the content. The public Internet slowly moved to the "Come to me Web", the web where the content and information comes to the users and one can modify what information he wants to receive.

## **The commercialisation of the public Internet**

- surveillance

In the first chapter of this Thesis I talked about how the Internet came to be, and how the first intentions were open, and formed out of a collaboration of multiple people. Not too much later, after the Internet became more common, companies became aware of this medium and its opportunities. Ian Clarke wrote in his first paper on Freenet, about the possibility of tracking and privacy on the public Internet. He states that any information on the public Internet can be lead back to a server, and thus, a person (Clarke 1999). The danger of this issue is that this immediately decreases the freedom and free-speech of the users. The public Internet is often thought of as an anarchic medium, were one can be free and say and publish whatever one wishes, but as examples of early illegal mp3 distribution public websites have showed, it is not (Biddle, England, Peinado, Willman 2002).

## The beginning of Freenet

- from surveillance to anonymity
- from censorship to freedom
- How Freenet is an answer to the public Internet
- Bring back elements of the first chapter:
  - AT&T, the monopoly of this company vs. the monopoly of certain companies on the public Internet.
  - the open structure of the beginning of the public Internet and the beginning of Freenet
  - The ideas of multiple Freenet developers and users to create a wireless Freenet-network, the similarities with the ARPANET and the PRNET (one of the first networks, using radio waves).

## The structure of Freenet

- anonymity

From the beginning of the Internet, it had a lot to do with networking people. The first connections were merely connections between people who knew each other. In the public web, or www, one can also connect to strangers, or visit strangers webpages, blogs or read their tweets. With applications like Facebook users are going back to connecting to their friends, sometimes on the other side of the world and sometimes friends from your home town. These networks offer hardly any privacy, as it is known that Facebook makes good profit from the sharing of information of their users.

Twitter also stores all the information of their users, as an example there is the case of Dutch hacker and one of the founders of XS4ALL, one of the first Dutch Internet providers, Rop Gonggrijp (Documentary on Wikileaks and Rop Gonggrijp <http://tegenlicht.vpro.nl/nieuws/2011/januari/Biografie-Rop-Gonggrijp.html>). He worked as a hacker for Wikileaks, as he quotes it on his website: “I have done work for Wikileaks, last when I helped produce the Iraqi helicopter video in late March, early April.” Because of this, apparently, he received a message from Twitter that they had “received legal process requesting information regarding your Twitter account, @rop\_g” (<http://rop.gonggrijp.jp/?p=442>). The DOJ wanted the IP address of Gonggrijp and requested this from Twitter, who in their case only warned their user that this information will be given to the DOJ. This example clearly states that a commercial company will work together with a government to reveal information of their users, they don't protect their costumers with any privacy of anonymity.

Ian Clarke developed the idea and startingpoint of the Freenet project at the University of Edinburgh. The project was later further enhanced and improved on Sourceforge, by multiple people. The software was, and is, distributed freely. As Clarke puts it Freenet is “a Distributed, Decentralised Information Storage and Retrieval System” (Clarke 1999 <http://www.google.nl/url?sa=t&source=web&cd=1&ved=0CBsQFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Bjsessionid%3DB30FB9379166109B4196703534062450%3Fdoi%3D10.1.1.32.3665%26rep%3Drep1%26type%3Dpdf&rct=j&q=%E2%80%9Ca%20Distributed%2C%20Decentralised%20Information%20Storage%20and%20Retrieval%20System%E2%80%9D&ei=k894TYDrK4OEOOrDswKkH&usq=AFQjCNFP0nvo2ic7KP0ypKhiNVcvP0r7uA&sig2=QsVEQrR6fQRnnpXVUVF8Aw>). Freenets architecture works “as a peer-to-peer network of nodes that query one another to store and retrieve data files which are named by location-independent keys. Each node maintains its own local datastore which it makes available to the network for reading and writing, as well as a dynamic routing table containing addresses of other nodes and the keys that they are thought to hold. It is intended that most users of the system will run nodes, both to provide security guarantees against inadvertently using a hostile foreign node and to increase the storage capacity available to the network as a whole” (Clarke, Sandberg, Wiley, Hong 2000). Unlike other anonymity programs and software, Freenet enables its users to store files anonymous. This also means that one can publish websites and build databases, all in an online-anonymous environment.

Freenet is a software program that needs to be installed on one's computer. This software runs in a browser, and after answering a few questions, i.e. to verify the level of security, risk or anonymity, it is installed and ready to use. The world of Freenet is a hidden online world, only accessible through the installing of the

software (Beckett 2009). Thus, via Google, or any other public Internet search engine, no content of Freenet can be found or retrieved. Freenet runs on the same browser but uses a different part of the web than the public Internet, figure 1.

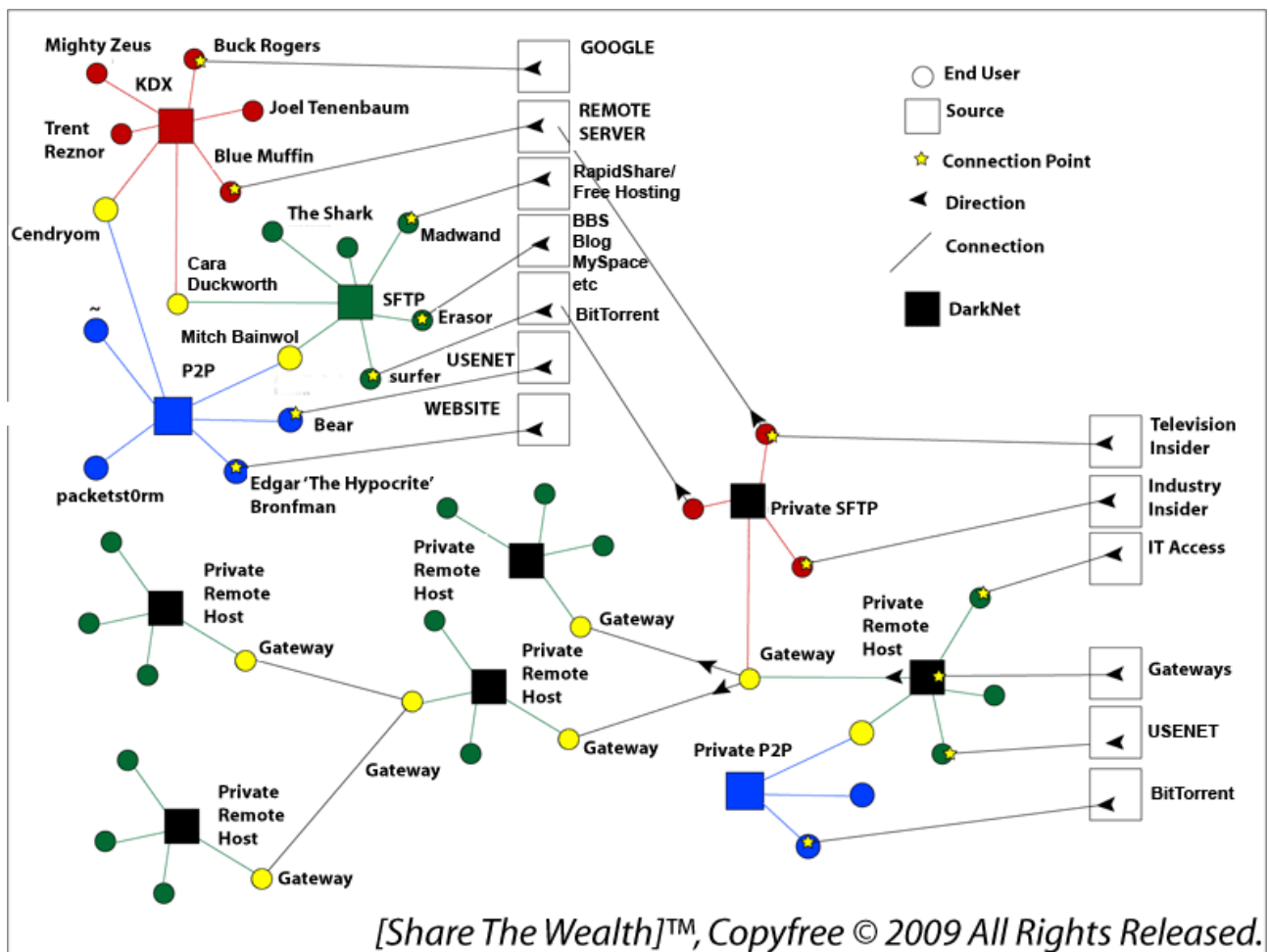


Figure 1: this figure illustrates how darknets operate in the web. Via different gateways the web can be entered, and sometimes some are connected, but some are a dead end or closed network. The illustration also shows, that searching with Google only gives one the small amount of public information available. As a summary, Google can not, or will not, search the whole Internet for content. (Source: <http://www.p2pnet.net/story/25817>)

Freenet is a peer-to-peer network containing nodes, these nodes query each other to be able to store and retrieve content. This content is named by location-independent keys. For reading and writing the notes contain and maintain their own local datastore and a dynamic routing table, this holds information on the addresses of other nodes and keys they are thought to hold (Clarke, Sandberg, Wiley, Hong 2000). All users are expected to run nodes, in order for the system can guarantee security. Freenet users are also obliged to share disk space, thus there is no central server. To make sure the user who is requesting content and the specifications of this content are extremely difficult to determine, the nodes are encrypted and routed through other nodes (Freenet <http://freenetproject.org/whatis.html>). Freenet works four different keys, these keys represent the kind of URI Freenet works with:

- CHK - Content Hash Keys are for files with static content, like an .mp3 or a PDF-document. It contains three elements: the hash of the file, the description key that unlocks the file and the used cryptographic settings.
- SSK - Signed Subspace Keys are usually for sites that are going to change over time. For example, a website that may need news to be updated or information to be corrected, added or deleted. They contain out of five parts: public key hash, document decryption key, cryptographic settings, a user selected name and the current version of the site.

- USK - Updateable Subspace Keys are useful for linking to the latest version of a SSK site. Note that USKs are really just a user-friendly wrapper around SSKs, which hide the process of searching for more recent versions of a site.
- KSK - Keyword Signed Keys allow you to save named pages in Freenet. They are not secure against spamming or name hijacking. But can be easily remembered, because of the simple and readable URI. (<http://freenetproject.org/understand.html>)

All of these keys are the URIs to Freesites and/or files on Freenet. These Freesites are the websites of Freenet. With the Freenet software of jSite, it is fairly easy to publish your own Freesite on Freenet. Once one has build a HTML website, within a directory, with jSite it takes only a few clicks to publish it. Also, the software will give you the keys needed, and the URI. Updating via jSite is also possible. Freenet doesn't, yet, support flash, only Java, in which it is build, HTML and coding.

Because of this whole system the Freesites have a certain look to them. It is so easy to create and publish a HTML Freesite, people have done this with only the content and hardly any design. The design has become less important and the content is the basic assumption. Although there are Freesites that look and feel like websites on the public Internet, while surfing Freenet most Freesites are distinctly different than websites.

## **Comparison between early public Internet and the Freenet Darknet**

### **Future of darknet's like Freenet**

- A virtual circle: A new place for freedom is created > people start to build elements to filter content, like search engines > some pages are being excluded, index pages don't index everything anymore and some areas are becoming more and more in the background > (or government/police shuts the website down, because of vulnerable content or because of copyright issues.) > areas are moved to new places for freedom.
- Freenet users want elements of the public Internet on Freenet: social communities and twitter-like application on Freenet (in development): <https://github.com/sanity/tahrir>

## **Annotated Bibliography**

A History of the Internet and the Digital Future. By Ryan, J., 2010.

In this book Johnny Ryan portraits the history of the public Internet. From the far most beginning, the development of the telephone and the telephone-line, to the point we are now and what the future might bring. The book has a clear chronological order in the history and how the public Internet became what it is today. Although there are a few elements missing, I would like to have seen implemented in the book. One is the big importance of users creating personal HTML pages, and later moving to blogs and twitter, which illustrates the commercialisation of the public Internet. The second thing I missed in the book, are the splitting of the Internet, into the public Internet and several darknets.

Control and Freedom, Power and Paranoia in the Age of Fiber Optics. By Chun, W. H. K., January 2006.

Wendy Chun talks about how the public Internet became a commercial medium based on control while it was founded by people who wanted it to be a medium for freedom. This control also connects to the paranoia of this day and age.

In the chapter about pornography she talks about how the pornography changed the public Internet. Pornography opened doors to several elements that are now broadly used on the public Internet, but also frustrated a lot of people. People who are afraid of their children looking at indecent pictures. It caused the shift from open to closed and from private to public. This is an interesting book to read next to texts and books about the public Internet and darknets.

The World Wide Web: Past, Present and Future. By Berners-Lee, T., 1996.

Tim Berners-Lee illustrates in this text, first hand, the development the Internet has gone through. He stood at the beginning of the Internet, and gives a personal view in the text. In he beginning of the text he writes that the goal of the web was to be a shared information space through which people, and machines, could communicate. It was supposed to be a flexible medium. I found in this text a lot of similarities between the beginning of the Internet and Freenet, for instance that the Internet, in the beginning, had only content about itself, just like Freenet, mostly, has now. He also adressed the first censorship that happened in the Internet, PICS, which was a decentralised solution to the freedom of the Internet.

Analysis: The dark side of the web. By Andrews, S., 2010., 9 March & Uncovering the Dark Side of the world wide web. By Gibson, M., 2000.

These two small articles, written respectively by Andrews and Gibson, explain the basis of the dark side of the web. These articles hasn't got the content needed for research, but they were the first I read on this subject, and opened my eyes to other texts and books.

White Paper: The Deep Web: Surfacing Hidden Value. By Bergman, M. K., 2001.

Michael K. Bergman emplanes in this white paper the basic elements of the dark web, and darknets. The text is more a technical text on how big the dark web is, and on what content can be found there. Brightplanet's software is explained and used to retrieve content from the darkweb. They also qualify the retrieved content on several elements, to see what the real value of the dark web is. In the end, a proposal is made for two search engines: one that retrieves content from the surface web and another that searched the darknets and dark sides of the web.

The Darknet and the Future of Content Distribution. By Biddle, P. England, P. Peinado, M. and Willman B., 2002.

Peter Biddle, Paul England, Marcus Peinado and Bryan Willman investigated the darknet for this text. They explain really elaborate what a darknet is and where one can find them. They also make predictions about how the “darknet-genie will not be put back into the bottle”.

Freenet: A Distributed Anonymous Information Storage and Retrieval System. By Clarke, I. Sandberg, O. Wiley, B. Hong, T. W., 2000.

Ian Clarke, original founder of Freenet, Oskar Sandberg, Brandon Wiley and Theodore W. Hong describe in this text Freenet, the peer-to-peer network that keeps its users anonymous. They explain what the Freenet has become, and how the network works. They are very honest about that Freenet can not always guarantee ones anonymity and safety, but they do explain to keep this risk at a minimum. The text is very technological, but while reading it, the darknet Freenet gets more clear how it works and how it came to look like it does.

## References

- Ryan, J., 2010. A History of the Internet and the Digital Future. London, England: Reaktion Books LTD.
- Chun, W. H. K., January 2006. Control and Freedom, Power and Paranoia in the Age of Fiber Optics. London, England: The MIT Press.
- Berners-Lee, T., 1996 The World Wide Web: Past, Present and Future, w3,[online] August. Available at: <<http://www.w3.org/History.html>>
- Andrews, S., 2010. Analysis: The dark side of the web, PcPro, [online] 9 March. Available at: <<http://www.pcpro.co.uk/features/356254/the-dark-side-of-the-web>>
- Gibson, M., 2000. Uncovering the Dark Side of the world wide web. Financial Times, [online] 20 October. Available at: <<http://cryptome.org/dark-spy.htm>>
- Bergman, M. K., 2001. White Paper: The Deep Web: Surfacing Hidden Value, JEP the journal of electronic publishing, [online] August, volume 7, issue 1. Available at: <<http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104>>
- Biddle, P. England, P. Peinado, M. and Willman B., 2002. The Darknet and the Future of Content Distribution, [online] 18 November. Originally published [online]. Available at: <<http://www.crypto.stanford.edu/DRM2002/prog.html>>
- Microsoft Corporation, 2002 ACM Workshop on Digital Rights Management [online]. Available at: <[http://www.bearcave.com/misl/misl\\_tech/msdrm/darknet.htm](http://www.bearcave.com/misl/misl_tech/msdrm/darknet.htm)>
- Clarke, I. Sandberg, O. Wiley, B. Hong, T. W., 2000. Freenet: A Distributed Anonymous Information Storage and Retrieval System, [online] July 1. Available at: <<http://www.eecs.umich.edu/~zmao/eecs589/papers/freenet.pdf>>
- Seijdel J., 2010. Beyond Privacy, New Perspectives on the Private and Public Domains, Open, [online]. Available at: <<http://www.skor.nl/artefact-4808-nl.html?lang=en>>
- Mansfield-Devine, S., 2010. Going over to the dark side, Webvivant Computer Fraud & Security, [online]. Available at: <<http://www.webvivant.com/feature-darknets.html>>
- Howe, J., 2005. The Shadow Internet, Wired [online] Issue 13.01, January. Available at: <[http://www.wired.com/wired/archive/13.01/topsite.html?pg=1&topic=topsite&topic\\_set](http://www.wired.com/wired/archive/13.01/topsite.html?pg=1&topic=topsite&topic_set)>