The Dark Web Big Three



Pat Baker OtakuSystems LLC

twitter: otakusystems info@otakusystems.com

Penguicon 2019

About Me

Philosophy, Information Assurance (CyberSecurity), Intelligence Analyst

OtakuSystems LLC otakusystems.com twitter: @otakusystems

Technologist, Futurist, Philosopher, Geek

- Seeker of wisdom and knowledge -

- Disclaimer -

Not responsible for any damage done to you, your friends, your accounts, your pet goldfish, etc. All information is for educational or general knowledge purposes. Information held within may or may not be legal by your country, state or business.

If it's not legal then should you do it?

- Being Watched changes how you move and how you think -

What is Deep Web?



Surface Web

<10% of Internet

Indexed Internet

- >90% of Internet
- Unindexed Internet



G

You Tube

G**m**ail

f 🛄 in

E.

Dark Web (Darknet)

Subset of Deep Web Hidden Services

Security /Privacy

- Why do we need it?
- Do you have anything to hide?
- If not doing anything wrong then why worry?
- I have a VPN so I am safe?

How internet works







The Good Stuff







Tor





Tor

- Tor general
- History
- Overview
- Hidden Services
- Attacks
- Questions

What is Tor?

- Tor is a distributed anonymous communication service using an overlay network (Tor Cloud) that allows people and groups to improve their anonymity including governments and websites from tracking them, or to connect to those Internet services blocked by their local Internet providers on the Internet.
- Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site.
- Designed for anonymity, not security, plain text going in will still be plain text going out.

Tor is not

 A web encryption system, data not encrypted going into Tor will not get encrypted leaving the network.

• A web browsing security replacement.

History



Tor - history

- Defined core development in the 1990 by Unites States Naval Research Laboratories, and other unnamed government groups.
- Funded and further developed by DARPA.
- EFF took over funding after 2006, created "The Tor Project", still assists with project.
- Designed for anonymity not security, plain text going in will be plain text coming out.

Organizations using Tor

- EFF Electronic Frontier Foundation
- News Organizations
 - Reporters without boarders,
 - US International Broadcasting Bureau
- The Washington Post
- The Guardian
- The Facebook

Overview



Tor - parts

- Tor directory server
 - Holds the node lists
- Tor entrance node
 - First connection in the Tor network
- Tor relay node
 - Relays between Tor nodes in network
- Tor exit node
 - Connects to the requested site for you

- Circuit Based
 - Connections between you and the site, start and finished along the same route.
- Hidden sites
 - Sites within the Tor network you will need Tor to access them.
- Bridge relay
 - Used for places that block Tor know links, connects to non public listed Tor nodes. (bridges.torproject.org)

Tor Design

- Use of TCP protocols to send data packets
- Use of data encryption between nodes of the Tor network
- Does some data integrity checking at end point of streams
- Cloud type architecture

Tor Design

- Tor packets or 'cells' in the Tor cloud are the same size, 512 bytes, (1024 bytes in future)
- TSL and SSH PKI Session key exchanges.
- Node to Note key exchanges.
- Circuit nodes exchange multiple packets, may be different node types at same time.

Tor – How it works





Routing path













Tor software bundle

- Go to https://www.torproject.org for the Tor bundle, this includes software and browser.
- Linux, Mac, Win, Raspberry Pi, source, some OS's have depos with Tor package in them
- Use the Tor installed browser.

Tor Hidden Service



Tor – Hidden Service

- Sites that are not available to the normal DNS and INTERNET services.
- Uses an address example: "4gy7jw64hjtk.onion" to access the hidden site.
- If the hidden service server is misconfigured then it may leak location data of itself and you.

Tor Hidden Service

 Tor hidden service let users publish web sites and other services without needing to reveal the location of the site, it uses an encrypted hash table service key system.

 Generally they are relayed connections to your running web server within the Tor network. Site to IntroPoints still use the three hop layout.





Hidden Service












Tor hidden service

There also is an option of 'single onion': the hidden service introduction protocol acts as the exit node for the web site. In place of multi nodes, (over three), its just one hop from introduction to site, not 5,6,7,etc hops.

Configure hidden service

- Have a web server running, VirtualHosts will work also.
- Install Tor on your server class machine.
- Edit the file torrc. (location will depend on OS)
- Remove the # from
- HiddenServiceDir /var/lib/tor/hidden_services
- HiddenServicePort 80 127.0.0.1:80

Configure hidden service

• HiddenServicePort is used to specify virtual port, IP address for redirection connections to this virtual port.

• **HiddenServiceDir** the directory that Tor will store the information about the hidden service, this includes the generated hostname.

Configure hidden service

- Save torrc and restart Tor service.
- Note the "private_key" keep that hidden or others will be able to impersonate you.
- Change to the HiddenServiceDir location and note the "hostname" that was generated.
- Ex: 56dfge6hest5d8sde.onion

Tor Attacks



Tor Attacks

- Who is running the nodes?
- Use of packet analysis tools
- Node database servers
- Your web site misconfiguration
- Your web browser misconfiguration

Bad Entry Node



Bad Exit Node



MIM from Exit Node



Tor – quick demo



Papers about tor

 http://cacr.uwaterloo.ca/techreports/2013/ cacr2013-09.pdf

 http://security.stackexchange.com/questions/ 79395/in-depth-tor-encryption-design-details

https://blog.torproject.org/category/tags/attacks

Points about Tor

- It will be slow at times
- Some ISP and countries frown on Tor usage and hosting hidden services
- Bad people use it as well as good people
- Streaming services not good

Help the project

• Run a Tor relay

• Give money \$\$\$\$ to The Tor Project

Spread the word about Tor

Questions

You got questions? (I may have answers)



I2P

What is it Services History Parts of the service How it works Install General Demo

What it is

Anonymous network layer (implemented as a Mix Network) that allows for censorship-resistant, peer to peer communication. Anonymous connections are achieved by encrypting the user's traffic (by using end-to-end encryption), and sending it through a volunteer-run network of roughly 55,000 computers distributed around the world -wikipedia.

Services

- Email/Messaging
- IRC (internet Relay Chat)
- Eepsites
- Torrents
- File Storage
- Search Engine's (legwork.i2p, seeker.i2p)
- stats.i2p, no.i2p (eepsite registration service)

I2P Router Console	x	+

(i) 127.0.0.1:7657/home

12P	12P ROUTER	CONSOLE									
Version: 0.9.31-0 Uptime: 3 min											
BANDWIDTH IN/OUT											
3 Sec: 0.13 / 1.64 KBps	Welcome to I2P! Please I	Welcome to 12PI Please have patience as 12P boots up and finds peers.									
Total: 0.27 / 1.57 KBps Used: 79.96 KB / 335.46 KB	/ 1.57 KBps While you are waiting, please adjust your bandwidth settings on the configuration page.										
Wetwork: Firewalled	Also you can setup your browser to use the I2P proxy to reach eepsites. Just enter 12/1.0.0.1 (or localhost) port 4444 as a http proxy into your browser settings. Do not use SOCKS for this. More information can be found on the I2P browser proxy setup page. Once you have a "shared clients" destination listed on the left, please check out our FAQ. Point your IRC client to localhost:6668 and say hi to us on #i2p.										
LOCAL TUNNELS											
흥 shared clients 🛛 🔹	* WELCOME TO 12P										
	@	<u>@</u>					2				
	Addressbook	Configure Bandwidth	Configure UI	Customize Home Page	Email	Help	Manage Plugins	Router Console	Torrents		
	Web Server										
	HIDDEN SERVICES OF INTEREST										
	١		1	Ŷ	2	•	X	?			
	anoncoin.i2p	Dev Forum	diftracker	echelon.i2p	exchanged.i2p	git.repo.i2p	I2P Bug Reports	I2P FAQ	I2P Plugins		
	F	WIKI	0		()	1		*			
	I2P Technical Docs	I2P Wiki	Open4You	Pastebin	Planet I2P	Postman's Tracker	Project Website	stats.i2p	The Tin Hat		
	Trac Wiki										

I2P - History

- Generally first defined and software created in 2003 using peer-to-peer protocol.
- I2P Invisible Internet Project.
- Initial lead developers/creators were jrandom, zzz, killyourtv, and complication.
- Censorship-resistant, peer-to peer communication.

I2P - Terminology

- Inbound tunnels send message data to the tunnel creator.
- Outbound tunnels send message data from the tunnel creator.
- Peers the people you are connected to, for exchange of data packets.
- Address Book stores eepsite to address links, can be edited manually, updated by connections peers



- Eepsites the hidden sites accessible by I2P clients, more designed as static sites, no web server install required.
 I2P has web server function build into its operations.
- Address book stores links and sites:
- projekt.i2p/hosts.txt (http://udhdrtrcetjm5sxzskjyr5ztpeszydbh4dpl3pl4utgqqw2v4jna. b32.i2p/hosts.txt)

Eepsite

eepsites are websites that are hosted anonymously within the I2P network. Eepsite names end in .i2p, such as ugha.i2p or forum.i2p. EepProxy can locate these sites through the cryptographic identifier keys stored in the hosts.txt file found within the I2P program directory. Typically, I2P is required to access these eepsites.

.i2p

'I2p' is a pseudo-top-level domain which is only valid within the I2P overlay network scope. .i2p names are resolved by browsers by submitting requests to EepProxy which will resolve names to an I2P peer key and will handle data transfers over the I2P network while remaining transparent to the browser.

EepProxy

The EepProxy program handles all communication between the browser and any eepsite. It functions as a proxy server that can be used by any web browser.

Peers, I2P nodes

Other machines using I2P that are connected to user's machine within the network. Each machine within the network shares the routing and forwarding of encrypted packets.

Tunnels

A connection is established between the user's machine and another peer. Data to and from the user, along with the data for other peers (routed through the user's machine), pass through these tunnels and are forwarded to their final destination (may include more jumps). Connections will disconnect and reconnect or disconnect and reconnect to other peers and nodes at times.

netDb

The distributed database that holds information on I2P nodes and I2P eepsites. This database is split up among routers known as "floodfill routers". When a user wants to know how to contact an eepsite, or where more peers are, they query the database.



Crypto at tunnels

- The network itself makes use of a significant number of cryptographic techniques and algorithms includes:
 - 2048bit ElGamal encryption,
 - 256bit AES in CBC mode with PKCS#5 padding,
 - 1024bit DSA signatures, SHA256 hashes,
 - 2048bit Diffie-Hellman negotiated connections with station to station authentication, and ElGamal / AES+SessionTag.







How it works


Crypto at tunnels



General networking

- I2PTunnel is an application embedded into I2P that allows arbitrary TCP/IP applications to communicate over I2P by setting up "tunnels" which can be accessed by connecting to pre-determined ports on localhost.
- SAM (Simple Anonymous Messaging) is a protocol which allows a client application written in any programming language to communicate over I2P, by using a socket-based interface to the I2P router.
- BOB (Basic Open Bridge) router protocol.



12P Services

Susimail SusiDNS Torrents Webserver

12P NETWORK PEERS

NTCP connections: 5 limit: 120 timeout: 15m

Peer	Dir	Idle	In/Out	Up	Skew	Send	Recv	Out queue	Backlogged?	Reading?
🚺 -9jw	out	25/3735	0,60/0,00KBps	45m	-75	114	230	No messages	false	No
🔳 WBNt	out	155/395	0,00/0,00KBps	Sm	05	21	4	No messages	false	NO
🔚 1нок	out	1265/325	0,00/0,00KBps	18m	-115	38	19	No messages	false	No
INIT INIT	out	6465/3405	0,00/0,00KBps	2 1 m	65	112	53	No messages	false	NO
📕 wVBh	out	35/7225	0,31/0,00KBps	13m	15	3	73	No messages	false	NO
5 peers			0.91/0.00KBps	20m	-2200ms	288	379			

UDP connections: 14 limit: 180 timeout: 30m

Peer	Dir/Intro	Idle V^ / V^	In/Out VA / VA	Up VA	skew VA	Cwnd VA	Ssthresh VA	Rtt VA	Dev VA	Rto VA	Mt
5 CF-3	out	1775/1775	0,00/0,00KBps	14m	15	11K/0/18/0	4K	650	82	978	1350
🔳 D5-A	out	45/45	0,00/0,00KBps	14m	05	10K/0/11/0	4K	561	52	769	135
II HFLm	out [2 failures]	17625/8855	0,00/0,00KBps	5 4m	45	8K/0/18/0	4K	526	44	702	135

I2P Internals I2PTunnel Tunnels Profiles NetDB Logs Jobs Graphs Stats Configuration Help

General Ident: (view) Version: 0.7.6-0 Uptime: 56m Now: 11:06:35 (64s skew) Reachability: Firewalled

Shutdown

Peers Active: 10/32 Fast: 8 High capacity: 5 Well integrated: 1 Known: 99

Bandwidth in/out

12P)
-----	---

I2P TUNNEL SUMMARY

RO	UTER IN	FO	Ι.	
Version		0.9.37-0-		E
Uptime:		2~trusty+1 19 hours		Û
BAND	VIDTH IN	I/OUT		4
3 Sec:	63.31	/ 63.06 KBps		-
5 Min: Total:	56.69 43.86	/ 56.38 KBps / 42.39 KBps		
Used:	3.0	2GB / 2.92GB		
		•••		
				1
	Network: (ОК		1
	PEERS			1
Active:		1515 / 3496		1
High Capacit	y:	150		4
Integrated: Known:		1549 3297		
-	UNNELS			
Exploratory:		12		1
Client: Participating		2 318		-1
Share Ratio:		9.09		-1
LOC	AL TUNN	IELS		-
📕 shared cli	ents	*		
Acce	pting Tun	nels		
		()		С
R		v		Û
121	SERVIC	ES		-
Email To	orrents We	b Server		
100		1		

0.9.37-0-	Exp	loratory tur	inels							*≜ @
2~trusty+1 19 hours	砂	Expiration	Usage	G	ateway		Participa	ants		Endpoint
/OUT	*	34 sec	23 KB	🛃 nJwo 2	2519999397 📘	📕 jOue 198743669	96	🚍 HjOe 1265163317 ℕ	local	3735610456
63.06 KBps	*	68 sec	19 KB	🔲 CQpe 🗄	1073185248	📲 0Af0 285868557	75 0		local	655890280
42.39 KBps GB / 2.92GB	*	104 sec	26 KB	📕 Lpv 📕	2476222915	₩ d8Qv 371189558	38 N		local	1018207893
	*	2 min	8 KB	🛃 HUkp 2	2714308280 N	xNcA 29692348	93		local	2654780568
	*	7 min	7 KB	📕 Iz3w 2	2525581920	▶ ByBn 314988357	79		local	2285697774
к	*	7 min	4 KB	📕 dFru 3	3479725263 N	💻 5-p- 275417278	34		local	1902648878
	*	8 min	0 KB	🖸 g1B0 2	2892080383 N	sx41 166523842	20 0		local	258927127
1515 / 3496	*	8 min	0 KB	Z-2U 3	3075149464	DTmA 271627761	L4 O	💻 PmV1 2245620176 🚺	local	2043852065
150	-	25 sec	33 KB	local	3029332593	📕 lhzv 298516951	11	№ 05kK 280487838		z9Z7 O
3297	*	95 sec	43 KB	local	3556501683	Ryv0 28233264	14	🛏 Yrt6 893226615 N		6zER L
10	*	6 min	8 KB	local	3471682893	■ gdPf 128664053	39 0	🔜 9vym 437436918 N		G-xC L
12	*	6 min	18 KB	local	2270585671	MVi3 207525130)9 N	🔯 LpJR 370833394 N		RTFd
318 9.09	•	6 min	8 KB	local	2097865713	📕 08u6 233148988	33 N	🚟 YONu 3359808217	9	8DX- N
ELS	*	7 min	3 KB	local	1299847427	₩ ~5AF 313811311	L7 N	📕 QXRN 1914004824		P907 L
*					Lifetime	bandwidth usage: 22	2.4MB in, 30.	1MB out		
els										
U	Clie	nt tunnels f	for shared	l clients						*≜ @
	劯	Expiration	Usage	G	ateway		Participa	ants		Endpoint
Samor	*	4 min	0 KB	0102	2125126113	KGRq 287954963	34	🚟 EI1D 1569150283 💽	local	1535309059
Server	-	2 min	3 KB	local	1417719256	📕 keQm 152942931	.5 N	🕮 0-wf 2898257525		g3Yo

- Packet based connection to other peers for exchanging data.
- 127.0.0.1:7657/ localhost and port accessed by client software.
- Itoopie the logo, a person putting on a mask.



Eepsites overview

- Eepsites setup, its easier to just convert the default page.
- Encoded base64 and shorter b32 address
- Depending on your OS the sites document will step you through it.

Base64 address (legwork.i2p)

h-Qo-

- ~IFHGvc067ASKg~X~zyUIPyppCz3d3AszMmZIVAoIXttaokLhGh5P nKZzReapqIQuVjyP-
- Anlryo8uCNIPyWYXDgimA2~QQN2dkyWR3a9dNcNHGwIcdU20E mISJdVg0gT~jvxkHO6i-94i-PTk1M70MwZfhHK7T-
- S1~jrFIG0ZbW2J8AjsHbOUWRW7NGr3eCawfpIqJ6Ys44nZZeHWe cd4sATBp7gMOSCEdU1H8btw-
- 9H1HdfTLUJ1hm2omMjOeXk9sVrMsIn3L0ZMgcppBmFnI52YgNJB AnrmiZjVIxKI-V5CLAB1SNhso1ZxD3Pjrh~z4PxvW61qjOZAVHZjtaWwxWs6iwkYOF0BFmbtOftBGCH-JtqUcYtgU-
- ~QqSkLTAK309QKwGYhNQ5USZvyX5~GJ0cGliJ10jf0fl9rAoXAge c1YtEDyHl3vDj~yVfFfHuCOyBwW4z5DGJ7hngh4z8KNn9qc0aDsC h30Xt~fv6F-svrfOfVqPuz3EQ6BQAEAAcAAA==

Base32 address (legwork.i2p)

cuss2sgthm5wfipnnztrjdvtaczb22hnmr2ohnaqqqz 3jf6ubf3a.b32.i2p

SERVICES MANAG	iER		
T STATUS MESSAGES			
Tunnels ready for client: HTTP Client ready, listening on 127. Client ready, listening on 127. Tunnels ready for client: Stand Client ready, listening on 127.	Proxy on 127.0.0.1:4444 0.0.1:4444 0.0.1:6668, delaying tunnel open until required dard client on 127.0.0.1:7659 0.0.1:7659		
			Refresh Clear
∉ GLOBAL TUNNEL CONT	ROL		
			Tunnel Wizard Stop All Start All Restart All
I2P HIDDEN SERVICES			
Name	Туре	Points at	Preview Status Control
I2P webserver	HTTP server	127.0.0.1:7658	No Preview 🗱 ¥ 🖗 Start
Hostname: mysite.i2p Description: My eepsite			
Wy forum	HTTP server	127.0.0.1:80	No Preview 🛛 🗱 🖗 Start
Destination: ctp2l6pd2aql3 Description: My forum	zxwvpy4gfdf2uqesnnsc6bdau7mmks5s4lp64tq.b32.i2p		
			New hidden service: HTTP
I2P CLIENT TUNNELS			
Name	Туре	Interface	Port Status Control
I2P HTTP Proxy	HTTP/HTTPS client	127.0.0.1	4444 🛛 🖗 🖈 Stop
Outproxy: false.i2p Description: HTTP proxy fo	r browsing eepsites and the web		

HIDDEN SERVICES MANAGER

Name		Туре				
I2P webserver		HTTP server				
Description		Auto Start Tunnel				
My eepsite		Automatically start tunnel when router starts				
Target						
Host: 127.0.0.1		Port: 7658 Use SSL to connect to target				
Website Hostname						
mysite.i2p (leave blank for outproxies)						
Local destination		Private key file				
x~qfmzvg090qtZeCF5GA~9rTx17gRJP7pk52sPx97Ih~A5-\	YV8198uEM9gM5sG3xm-e6Mb7zyIcg	eepsite/eepPriv.dat				
x-qfmzvg090qtZeCF5GA-9rTx17gRJP7pk52sPx97Ih-A5-1 Note: In order to enable QR code generation or re- mynewserver.i2p	rV8198uEW9gW5sG3xm-e6Mb7zyIcg gistration authentication, configure the Website Hostn	eepsite/eepPriv.dat ame field (for websites) or the Name field (everything else) above with an .i2p suffixed hostname e.g.				
x-qfmzvg090qtZeCF5GA-9rTx17gRJP7pk52sPx97Ih-A5- Note: In order to enable QR code generation or re- mynewserver.i2p ADVANCED NETWORKING OPTION Tunnel Options	rV8198uEM9gM5sG3xm-e6Mb7zyIcg gistration authentication, configure the Website Hostn	eepsite/eepPriv.dat ame field (for websites) or the Name field (everything else) above with an .i2p suffixed hostname e.g.				
x-qfmzvg090qtZeCF5GA-9rTx17gRJP7pk52sPx97Ih-A5- Note: In order to enable QR code generation or re- mynewserver.i2p ADVANCED NETWORKING OPTION Tunnel Options Length	rV8198uEM9gM5sG3xm-e6Mb7zyIcg gistration authentication, configure the Website Hostn	eepsite/eepPriv.dat ame field (for websites) or the Name field (everything else) above with an .i2p suffixed hostname e.g. Variance				
x-qfmzvg090qtZeCF5GA-9rTx17gRJP7pk52sPx97Ih-A5- Note: In order to enable QR code generation or re- mynewserver.i2p ADVANCED NETWORKING OPTION Tunnel Options Length 3 hop tunnel (high anonymity)	rV8198uEW9gW5sG3xm-e6Mb7zyIcg gistration authentication, configure the Website Hostn IS	eepsite/eepPriv.dat ame field (for websites) or the Name field (everything else) above with an .i2p suffixed hostname e.g. Variance 0 hop variance (no randomization, consistent performance)				
x-qfmzvg090qtZeCF5GA-9rTx17gRJP7pk52sPx97Ih-A5- Note: In order to enable QR code generation or re- mynewserver.i2p ADVANCED NETWORKING OPTION Tunnel Options Length 3 hop tunnel (high anonymity) Count	rV8198uEW9gW5sG3xm-e6Mb7zyIcg gistration authentication, configure the Website Hostn IS	eepsite/eepPriv.dat ame field (for websites) or the Name field (everything else) above with an .i2p suffixed hostname e.g. Variance Variance I 0 hop variance (no randomization, consistent performance) Variance				
 x-qfmzvg090qtZeCF5GA-9rTx17gRJP7pk52sPx97Ih-A5- Note: In order to enable QR code generation or remynewserver.i2p ADVANCED NETWORKING OPTION Tunnel Options Length 3 hop tunnel (high anonymity) Count 2 inbound, 2 outbound tunnels (standard bandwidth a 	rV8198uEW9gW5sG3xm-e6Wb7zyIcg	eepsite/eepPriv.dat ame field (for websites) or the Name field (everything else) above with an .i2p suffixed hostname e.g. Variance Ø hop variance (no randomization, consistent performance) Backup Count Ø backup tunnels (Ø redundancy, no added resource usage)				

ď



e Edit View Higtory Bookmarks	Tools Geb
🔁 - C X 💩 🗋 MpJ	/127.0.0.117957/ndex.jp
12P Router Console - home	
12P	I2P ROUTER CONSOLE
12P SERVICES	
Addressbook Torrents Webmail Webserver	2009-10-12: 0.7.7 Released
12P INTERNALS	12P version 0.7.7 contains several anonymity improvements. The use of session keys for crypto was completely reworked, and 12PSnark now uses its own tunnels for tracker communication. Work continues on improving the router console, including conformance to HTML standards and better support of UTF-8.
Tunnels Peers Profiles NetDB Logs Jobs Graphs Stats	Work also continues on increasing speeds, both by reducing the number of session keys transferred, by improving the methods of dropping messages during overload, and by reducing drops by high-bandwidth routers. There is a new unsigned update option for those of you that would like automatic udpates to bleeding-edge development versions.
GENERAL Local Identity	The release also contains several changes to reduce memory and CPU usage, and a large assortment of bug fixes. Upgrading is recommended. Please give the developers feedback on IRC #i2p or ferum.i2p and get involved!
Version: 0.7.7-0 Uptime: 23h	News last updated 23h ago
OK	Welcome to 1201
Restart Shutdown	
PEERS	If you've just started 12P, the Active: numbers on the left should start to grow over the next few minutes and you'll see a "shared clients" local destination listed on the left (if not, see below). Once those show up, you can
Active: 204/664 Fast: 12 High capacity: 29 Integrated: 15 Known: 1000	 browse "eepsites" - on I2P there are anonymously hosted websites - tell your browser to use the HTTP prexy at 127.0.0.1 port 4444, then browse to an eepsite: inproxy.tino.i2p and perv.i2p: sites tracking active eepsites forum.i2p: a secure and anonymous connection to forum.i2p2.de mount i2p: i2p and mirror i2p.anoidat i2p: secure and anonymous connections to wave i2p2 de
BANDWIDTH IN /OUT	 eepsites.i2p: an anonymously hosted search engine of eepsites
In It was a series	 ugha.12p: ugha's eepsite, a wiki that anyone can edit, and lots of links
5m: 11.43/11.06K/s	 fprexy,tino.i2p: Freenet proxy
Total: 19.91/20.13K/s	echelon.i2p: software archive and information for I2P
Used: 1.60G8/1.61GB	 paste.I2p2.I2p: secure and anonymous paste service.
TUNNELS IN/OUT	There are many more eepsites - just follow the links from the ones you see, bookmark your favorites, and visit them often!
Exploratory: 3/3 Client: 8/7 Participating: 219	 browse the web - there is currently an HTTP "outproxy" in I2P hooked up to your own HTTP proxy on port 4444 - simply set your browser's proxy to use it (as above) and go to any normal URL - your requests will be bounced through the I2P network.
CONCESTION	 transfer files - there is an integrated port of the Snark BitTerrent client.
Job lag: 3ms Nessage delay: 642ms Tunnel lag: 2059ms Backlog: 0	 use anexymous email - postman has created a mail system compatible with normal mail clients (POP3 / SMTP) that allows email within 12P as well as mail from and to the normal internet) get your account al hq.pestman.i2p. We bundle susimall, a web based anonymity-oriented pop3/smtp client configured to access postman's mail services. chat anonymously - fire up your own IRC client and connect to the server at 127.0.0.1 pert 6668. This points at one of two anonymously hosted IRC servers, but neither you nor they know where the other is. blog anonymously - check out Syndie and lats mere.
Accepting Tunnels	
LOCAL DESTINATIONS	Want your own eepsite?
shared clients ¥	We've bundled some software to let you run your own eepsite - a Jetty instance listening on http://127.0.0.1:7658/. Simply place your files in the eepsite/docroot/ directory (or place any standard JSP/Serviet .ver files in the experimentation of the standard stand

I2P – Install

- https://geti2p.net select the version for your operating system. You need java as well.
- ./i2prouter starts i2p and opens the browser console, if issues then try using "./sh runplain.sh" as normal user not as an admin.
- The i2p website has full documentation for most install questions.

Browser Setup

- HTTP Proxy:127.0.0.1, Port:4444
- Add Local host of 127.0.0.1 to the 'No Proxy for' box
- Set to Socks v5

I2P – quick demo



links

- https://www.youtube.com/watch?v=nydXb8IZr0
- https://thetinhat.com/tutorials/darknets/ i2p.html
- https://medium.com/@mhatta/how-to-setup-untraceable-websites-eepsites-on-i2p-1fe26069271d

links

 https://www3.cs.stonybrook.edu/~mikepo/ papers/i2p.imc18.pdf

Questions

You got questions? (I may have answers)

Freenet

What is it? History Parts of the service How it works Install General Demo



• A peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the Web without fear of censorship.

- Peer to peer connections.
- Sites or parts of sites are stored encrypted, local to the users.

Freenet Services

- Email client
- Chat clients
- File exchange
- Web Sites, (jsite)
- Social Sites
- Search Engines

- No general connection to non freenet sites, all sites are dark web sites.
- All sites are in the freenet cloud
- Sites are stored local to the use or parts are stored on nodes and grabbed as needed
- Web based screens, java required



History

- Created in 1999 by Ian Clarke at the University of Edinburgh as a student project to create a distributed decentralized information storage and retrieval system with strong anonymity protections.
- Ian Clarke's resulting unpublished report "A distributed decentralized information storage and retrieval system" (1999) provided foundation for the seminal paper written in collaboration with other researchers, "Freenet: A Distributed Anonymous Information Storage and Retrieval System" (2001)

History

 Wikipedia says he received a "B" grade on the project, so decided to release to Internet for further expansion, turned into "freenet".

Function

 Small World network principle, connections of connections. You are connected to small groups of people that are connected to other groups of people, circle of trust.

• Think of "Six Degrees of Separation" or the "Keven Bacon" connection for site searching.

Small-world network (wikipedia)

A small-world network is a type of mathematical graph in which most nodes are not neighbors of one another, but the neighbors of any given node are likely to be neighbors of each other and most nodes can be reached from every other node by a small number of hops or steps. Specifically, a small-world network is defined to be a network where the typical distance L between two randomly chosen nodes (the number of steps required) grows proportionally to the logarithm of the number of nodes N in the network, that is:

 $L \propto log \ N$

while the clustering coefficient is not small. In the context of a social network, this results in the small world phenomenon of strangers being linked by a short chain of acquaintances. Many empirical graphs show the small-world effect, e.g., social networks, forms the underlying architecture of the Internet, wikis such as Wikipedia, and gene networks. It is the inspiration for many network-on-chip architectures in contemporary computer hardware





Parts

- Nodes/Super Nodes you and other users of Freenet.
- Local cache kept in memory until restart, increases access to returning locations.
- Packet based connections to exchange data.

Parts

- Datastore located on your machine and holds encrypted pieces of data for you and others.
- Containers 2meg zipped file collections.
 Contains most or all of the files required to load for the freesite to display.
- Keys site access associations, think if them as the URL of Freenet. CHK@SVbD9~HM5nzf3AX4yFysior=3xd..

Link references

lastGoodVersion=Fred,0.7,1.0,1010 sig=7c7edc8c5250e42ac4cb161b216b70de7019221f1b331f0f92bd67439[...]609660f0d4 identity=5tBtS3R59nf0Tvc1be~V0sSfkWir8EW38YeocP0gsYM myName=FreenetTestInstall location=0.02970997399122577 testnet=false version=Fred,0.7,1.0,1016 physical.udp=83.255.75.223:13762 ark.pubURI=SSK@M1wjFha2tujY0500QF~5Fqz5anVEiIzI9VrA8IrhAsQ,5M[...],AQACAAE/ark ark.number=0 dsaPubKey.y=JhlWYVx8rA0y0x1Fb3y9TfqXDYiIsnkEka8PLsePerpCELTIn[...]laHe2bk1007Dg dsaGroup.p=AIYIrE9VNhM38qPjirGGT-PJjWZBHY0q-JxSYyDFQfZQe0hrx4[...]ofeLdX7xhehuk dsaGroup.g=UaRatnDByf0QvTlaaAXTMzn1Z15LDTXe-J~g0qXCv0zpz83CVn[...]Fuqt8yZe1PDVg dsaGroup.q=ALFDNoq81R9Y1kQNVBc5kzmk0VvvCWosXY5t9E9S1tN5 End

Example web site link

http://localhost:8888/ freenet:USK@cJNO6G0[..]joM,AQACAAE/ watergate2/1/
Parts

- Key types
 - CHK Content Hash Keys static content.
 - SSK Signed Subspace Keys -changes over time.
 - USK Updateable Subspace Keys links to SSK.
 - KSK Keyword Signed Keys the Freenet sites.

How it works



Websites - jsite

- JSITE a graphical application that you can use to create, insert and manage your own Freenet sites.
- Websites HTML coding static to the location stored, stored on node then copied over to you, no web site server used.

127.0.0.1:8888/USK@Isel-izgllc8sr~1reXOL	z1LNGLIY-voOnLWWOvagYO.xWfr4pv0YZgAOSI-B	7bolD 🗇 😴 🔣 🔻 Google
INKAGEDDON LINKALOG	LINKAGEDDON	LINKALOG LINKAGEDDO
Bookmark Me! Read Me		Read Me Bookmark Me!
ActiveLink versio	on of this page Check for new edition Download	TXT file of listed freesites
Welcome to Linkageddon. Here we aim to bring you a filtered with respect to their content so please read an	a comprehensive list of all available freesites, both old ar v description before you dive in.	d new. The links presented here are not currently
WARNING: Some of the freesites linked to here may c	contain material that is illegal in many countries and/or h	ghly offensive to a large number of people. Where
appropriate we try to use the treesite title and descripti reserve the right to edit those links for clarity.	ion embedded in a freesite by it's author, but if the title ai	nd/or description are absent or too misleading we
If you feel the title and/or description for a particular fre	eesite does not give sufficient warning about it's content nd suggestions compatible with the aims of this freesite v	then please feel free to comment to that effect on Sone will be taken into account for future edits
or to the relevant rivio board. Reasonable requests an	na suggestions companye with the arms of this neesler	and be taken into account for future curis.
Freenet in a box (en/de/fr/ar)	Freereader	Freereader
How to install freenet on a vps/rps Wie freenet auf einem	A few German RSS feeds reposted into Freenet via the	RSS feeds of a large number of security related blogs.
VPS / RPS installieren Comment faire pour installer freenet sur un VPS / RPS ، كيفية تثبيت في installer	Freereader plugin.	Updated: Feb 04
RPS	Updated: Feb 04	
Updated: Feb 04		Freenet graphs
	Index - Closed Loop Gain	These are automatically generated graphs of Freenet
Freenet fetch/pull stats	flog of OP90	stats.
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data	flog of OP90 Added: Feb 04	stats. Updated: Feb 04
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data over time.	flog of OP90 Added: Feb 04	stats. Updated: Feb 04
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data over time. Updated: Feb 04	flog of OP90 Added: Feb 04 Enzo's Freesite	stats. Updated: Feb 04 IRC Log
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data over time. Updated: Feb 04	flog of OP90 Added: Feb 04 Enzo's Freesite Links to some cool stuff on Freenet	stats. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data over time. Updated: Feb 04 IRC Log	flog of OP90 Added: Feb 04 Enzo's Freesite Links to some cool stuff on Freenet Updated: Feb 04	stats. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel.
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data over time. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet	flog of OP90 Added: Feb 04 Enzo's Freesite Links to some cool stuff on Freenet Updated: Feb 04	stats. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel. Updated: Feb 04
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data over time. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel.	flog of OP90 Added: Feb 04 Enzo's Freesite Links to some cool stuff on Freenet Updated: Feb 04 de.piratenpartei.ankuendigungen	stats. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel. Updated: Feb 04
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data over time. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel. Updated: Feb 04	flog of OP90 Added: Feb 04 Enzo's Freesite Links to some cool stuff on Freenet Updated: Feb 04 de.piratenpartei.ankuendigungen Announcements of the German Pirate Party - Postings	stats. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel. Updated: Feb 04 American Net Neutrality
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data over time. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel. Updated: Feb 04	flog of OP90 Added: Feb 04 Enzo's Freesite Links to some cool stuff on Freenet Updated: Feb 04 de.piratenpartei.ankuendigungen Announcements of the German Pirate Party - Postings from de.piratenpartei.ankuendigungen	stats. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel. Updated: Feb 04 American Net Neutrality Archiving News Articles Relevant to internet freedom in the United States of America
Freenet fetch/pull stats Some data and graphs of the retrievability of Freenet data over time. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel. Updated: Feb 04 TheSeeker's F'Log - Index	flog of OP90 Added: Feb 04 Enzo's Freesite Links to some cool stuff on Freenet Updated: Feb 04 de.piratenpartei.ankuendigungen Announcements of the German Pirate Party - Postings from de.piratenpartei.ankuendigungen Updated: Feb 03	stats. Updated: Feb 04 IRC Log Log of previous day's discussion on the official Freenet IRC development channel. Updated: Feb 04 American Net Neutrality Archiving News Articles Relevant to internet freedom in the United States of America Undated: Feb 03

Install

- https://freenetproject.org location of application and excellent documentation.
- Is a java based install and used java for its operation.
- The defaults will work but as you get more used to the system it is recommended to increase the security.

Demo





Interesting sites

 https://null-byte.wonderhowto.com/news/ anonymity-networks-dont-use-one-use-allthem-0133881/

Final Questions?



About Me

Philosophy, Psychology, Information Assurance CyberSecurity, Intelligence Analyst

OtakuSystems LLC otakusystems.com twitter: @otakusystems

Technologist, Futurist, Philosopher, Geek

- Seeker of wisdom and knowledge -