

Cryptome

21 May 2010

Wikileaks Security Measures

Wikileaks has reopened with a sophisticated offering of security measures for submissions and communications. It has compiled an impressive range of communications security to assure privacy and protection of those making submissions. It is worth study for a view of the current state of the art -- and an indication of weaknesses in the art.

A security given is that any system is subject to successful attack and no promise of absolute protection should be made. And that any promise of such protection should be considered with skepticism.

Instead, it is recommended that along with promises of security there should be an admission that no system is attack-proof, and in particular emphasize that the biggest risk is that an unknown breach has occurred and deliberately withheld to encourage continued trust.

The history of security -- communications and more generally, national security -- is rich with deception about highly trusted systems being secretly compromised, some failures later revealed, others never.

A test of the effectiveness of security is to subject it the strongest attack, sometimes called beta testing, where highly skilled attackers set out to breach a security system to reveal its weaknesses. Nearly all such attacks are successful in the earliest stages and contribute lessons learned to enhance security, the best never cease.

To aid Wikileaks in its increasingly sophisticated and evolving submissions and communications security, this provides a summary of its security measures on 21 May 2010 for beta attack.

Cryptome has observed flaws in every feature of Wikileaks security. All are derived from the fundamental design and operation of the Internet, digital communications and other offline means of communications to allow covert interception, tracking and identification of users.

WikiLeaks

“ ... could become as important a journalistic tool as the Freedom of Information Act. ”

— Time Magazine

Get involved

Contact • Donate • Contribute • Follow

Submit documents

Country • Region • Language

Br

Latest Tweets

- Thu, 20 May 2010 11:43:44 wikileaks: 5 websites that could change the news
- Thu, 20 May 2010 03:01:02 wikileaks: WikiLeaks works to expose governme
- Thu, 20 May 2010 00:34:19 wikileaks: WikiLeaks, les fuites en avant | Libera

In the News

- WikiLeaks in the news (Google) (/wiki/Special:Jump/aHR0cDovL25ld3MuZ2/aGw9ZW4mYW1wO25lZD1lbiZhbXA7cT13aWtpbGVha3MmYW1wO2lll
- WikiLeaks in blogs (Icerocket) (/wiki/Special:Jump/aHR0cDovL2Jsb2dzLmljZXJvY2tldC5jb20vc2VhcmNoP3RhYj1ibG9nJmF
- WikiLeaks on Twitter (Icerocket) (/wiki/Special:Jump/aHR0cDovL2Jsb2dzLmljZXJvY2tldC5jb20vc2VhcmNoP3RhYj10d2l0dGV

Recent Analyses

- Kundus-Bericht im Internet veröffentlicht
- Is the Internet Filter Australia's Berlin Wall
- TSA to Conduct Full Review After Leak of Sensitive Information
- TSA puts 5 on leave after security manual hits Internet
- Five Transportation Security underlings put on leave after airport screening fil
- US Lawmakers Want to Criminalize Whistleblower Sites Over TSA Leak
- Rätsel um Maut-Vertrag geht weiter
- Schadenersatz-Klage gegen Toll-Collect auf der Kippe
- Staatlich garantierte Abzocke
- Wikileaks' Dokumentation zum 11. September - „Bitte, geh nicht aus dem Ge
- The morning of 9/11, before they realized the world had changed
- Website Wikileaks publishes '9/11 messages'
- Die einsame Entscheidung des Oberst Klein
- Big Pharma caught spying on the WHO
- Toll Collect Verträge, 2002

(more)

WikiLeaks:Submissions

From WikiLeaks

WikiLeaks accepts *classified, censored or otherwise restricted* material of *political, diplomatic or ethical significance*. WikiLeaks *does not accept* rumour, opinion or other kinds of first hand reporting or material that is already publicly available.

Submitting confidential material to WikiLeaks is safe, easy and protected by law. We have several methods, but the best for most submissions is:

**Click here to securely submit a file online
(<https://secure.wikileaks.org/>)**

(bank grade encrypted submission, no logs kept and protected under Swedish and Belgium press secrecy laws)

Over 100,000 articles catalyzed world-wide. Every source protected. No documents censored. All legal attacks defeated.

All staff who deal with sources are accredited journalists. All submissions establish a journalist-source relationship. Online submissions are routed via Sweden and Belgium which have first rate journalist-source shield laws. In Sweden, not only does the law provide protection against any official inquiry into journalists' sources, but it allows a source whose identity has been revealed without permission to initiate criminal prosecutions against an unfaithful journalist who has breached his or her promise of confidentiality.

WikiLeaks records no source identifying information and there are a number of submission mechanisms available to deal with even the most sensitive national

security information.

WikiLeaks is the winner of the 2008 Economist Index on Censorship Freedom of Expression award and the 2009 Amnesty International human rights reporting award (New Media).

WikiLeaks has a history breaking major stories in every major media outlet and robustly protecting sources and press freedoms. **No source has ever been exposed and no material has ever been censored.** Since formation in early 2007, WikiLeaks has been victorious over every legal (and illegal) attack, including those from the Pentagon, the Chinese Public Security Bureau, the Former president of Kenya, the Premier of Bermuda, Scientology, the Catholic & Mormon Church, the largest Swiss private bank, and Russian companies. WikiLeaks has released more classified intelligence documents than the rest of the world press combined.

Contents

- 1 Examples
 - 1.1 War, killings, torture and detention
 - 1.2 Government, trade and corporate transparency
 - 1.3 Suppression of free speech and a free press
 - 1.4 Diplomacy, spying and (counter-)intelligence
 - 1.5 Ecology, climate, nature and sciences
 - 1.6 Corruption, finance, taxes, trading
 - 1.7 Censorship technology and internet filtering
 - 1.8 Cults and other religious organizations
 - 1.9 Abuse, violence, violation
- 2 Submissions via secure upload
- 3 Submissions via our discreet postal network
 - 3.1 High risk postal submissions
 - 3.2 Postal addresses of our trusted truth facilitators
 - 3.3 Australia

Examples

War, killings, torture and detention

- Changes in Guantanamo Bay SOP manual (2003-2004) - Guantanamo Bay's main operations manuals
- Of Orwell, Wikipedia and Guantanamo Bay (/wiki/Special:Jump/aHR0cDovL3RoZWxlZGUiYmxvZ3Mubnl0aW1lcy5jb20vMjAwNy8xMi8x) - In where we track down and expose Guantanamo Bay's propaganda team
- Fallujah jail challenges US - Classified U.S. report into appalling prison conditions in Fallujah
- U.S lost Fallujah's info war - Classified U.S. intelligence report on the battle of Fallujah, Iraq
- US Military Equipment in Iraq (2007) - Entire unit by unit equipment list of the U.S army in Iraq
- Dili investigator called to Canberra as evidence of execution mounts - the Feb 2008 killing of East Timor rebel leader Reinado
- Cómo entrenar a escuadrones de la muerte y aplastar revoluciones de El Salvador a Iraq - The U.S. Special Forces manual on how to prop up unpopular government with paramilitaries

Government, trade and corporate transparency

- Change you can download: a billion in secret Congressional reports - Publication of more than 6500 Congressional Research Reports, worth more than a billion dollars of US tax-funded research, long sought after by NGOs, academics and researchers
- ACTA trade agreement negotiation lacks transparency - The secret ACTA trade agreement draft, followed by dozens of other publications, presenting the initial leak for the whole ACTA debate happening today
- Toll Collect Verträge, 2002 - Publication of around 10.000 pages of a secret contract between the German federal government and the Toll Collect consortium, a private operator group for heavy vehicle tolling system
- Leaked documents suggest European CAP reform just a whitewash - European farm reform exposed
- Stasi still in charge of Stasi files - Suppressed 2007 investigation into infiltration of former Stasi into the Stasi files commission
- IGES Schlussbericht Private Krankenversicherung, 25 Jan 2010 - Hidden report on the economics of the German private health insurance system and its rentability

Suppression of free speech and a free press

- The Independent: Toxic Shame: Thousands injured in African city, 17 Sep 2009 - Publication of an article originally published in UK newspaper The Independent, but censored from the Independent's website. WikiLeaks has saved dozens of articles, radio and tv recordings from disappearing after having been censored from BBC, Guardian, and other major news organisations archives.
- Secret gag on UK Times preventing publication of Minton report into toxic waste dumping, 16 Sep 2009 - Publication of variations of a so-called super-injunction, one of many gag-orders published by WikiLeaks to expose successful attempts to suppress the free press via repressive legal attacks
- Media suppression order over Turks and Caicos Islands Commission of Inquiry corruption report, 20 Jul 2009 - Exposure of a press gagging order from the Turks and Caicos Islands, related to WikiLeaks exposure of the Commission of Inquiry corruption report
- Bermuda's Premier Brown and the BCC bankdraft - Brown went to the Privy council London to censor the press in Bermuda
- How German intelligence infiltrated Focus magazine - Illegal spying on German journalists

Diplomacy, spying and (counter-)intelligence

- U.S. Intelligence planned to destroy WikiLeaks, 18 Mar 2008 - Classified (SECRET/NOFORN) 32 page U.S. counterintelligence investigation into WikiLeaks. Has been in the worldwide news.
- CIA report into shoring up Afghan war support in Western Europe, 11 Mar 2010 - This classified CIA analysis from March, outlines possible PR-strategies to shore up public support in Germany and France for a continued war in Afghanistan. Received international news coverage in print, radio and TV.
- U.S. Embassy profiles on Icelandic PM, Foreign Minister, Ambassador - Publication of personal profiles for briefing documents for U.S. officials visiting Iceland. While lowly classified are interesting for subtle tone and internal facts.
- Cross-border clashes from Iraq O.K. - Classified documents reveal destabilizing U.S. military rules
- Tehran Warns US Forces against Chasing Suspects into Iran - Iran warns the

United States over classified document on WikiLeaks

- Inside Somalia and the Union of Islamic Courts - Vital strategy documents in the Somali war and a play for Chinese support

Ecology, climate, nature and sciences

- Draft Copenhagen climate change agreement, 8 Dec 2009 - Confidential draft "circle of commitment" (rich-country) Copenhagen climate change agreement
- Draft Copenhagen Accord Dec 18, 2009 - Three page draft Copenhagen "accord", from around Friday 7pm, Dec 18, 2009; includes pen-markings
- Climatic Research Unit emails, data, models, 1996-2009 - Over 60MB of emails, documents, code and models from the Climatic Research Unit at the University of East Anglia, written between 1996 and 2009 that lead to a worldwide debate
- The Monju nuclear reactor leak - Three suppressed videos from Japan's fast breeder reactor Monju revealing the true extent of the 1995 sodium coolant disaster

Corruption, finance, taxes, trading

- The looting of Kenya under President Moi - \$3,000,000,000 presidential corruption exposed; swung the Dec 2007 Kenyan election, long document, be patient
- Gusmao's \$15m rice deal alarms UN - Rice deal corruption in East Timor
- How election violence was financed - the embargoed Kenyan Human Rights Commission report into the Jan 2008 killings of over 1,300 Kenyans
- Financial collapse: Confidential exposure analysis of 205 companies each owing above EUR45M to Icelandic bank Kaupthing, 26 Sep 2008 - Publication of a confidential report that has lead to hundreds of newspaper articles worldwide
- Barclays Bank gags Guardian over leaked memos detailing offshore tax scam, 16 Mar 2009 - Publication of censored documents revealing a number of elaborate international tax avoidance schemes by the SCM (Structured Capital Markets) division of Barclays
- Bank Julius Baer: Grand Larceny via Grand Cayman - How the largest private Swiss bank avoids paying tax to the Swiss government
- Der Fall Moonstone Trust - Cayman Islands Swiss bank trust exposed
- Over 40 billion euro in 28167 claims made against the Kaupthing Bank, 23

Jan 2010 - List of Kaupthing claimants after Icelandic banking crash

- Northern Rock vs. Wikileaks - Northern Rock Bank UK failed legal injunctions over the £24,000,000,000 collapse
- Whistleblower exposes insider trading program at JP Morgan - Legal insider trading in three easy steps, brought to you by JP Morgan and the SEC

Censorship technology and internet filtering

- Eutelsat suppresses independent Chinese-language TV station NTDTV to satisfy Beijing - French sat provider Eutelsat covertly removed an anti-communist TV channel to satisfy Beijing
- Internet Censorship in Thailand - The secret internet censorship lists of Thailand's military junta

Cults and other religious organizations

- Church of Scientology's 'Operating Thetan' documents leaked online - Scientology's secret, and highly litigated bibles
- Censored Legion de Cristo and Regnum Cristi document collection - Censored internal documents from the Catholic sect Legion de Cristo (Legion of Christ)
- US Department of Labor investigation into Landmark Education, 2006 - 2006 investigative report by the U.S. Department of Labor on Landmark Education

Abuse, violence, violation

- Report on Shriners raises question of wrongdoing - corruption exposed at 22 U.S. and Canadian children's hospitals.
- Claims of molestation resurface for US judo official
- Texas Catholic hospitals did not follow Catholic ethics, report claims - Catholic hospitals violated catholic ethics

If you want to send us a message of your own, as opposed to a document, please see Contact.

Submissions via secure upload

Fast, easy and automatically encrypted with the best banking-grade encryption. We

keep no records as to where you uploaded from, your time zone, browser or even as to when your submission was made (if you choose a non-zero *publishing delay*, we set the file time record to be the release date + a random time within that day).

If you are anonymously submitting a **Microsoft word file (".doc") that you have edited at some stage**, please try to send a PDF document (".pdf") instead, as Word documents may include your name or the name of your computer, see **Word file redaction** for further information. If you have no means to produce a PDF file your document will be converted by WikiLeaks staff.

The process your document will undergo is outlined for **understanding submissions**.

Click here to securely submit a file online
(<https://secure.wikileaks.org/>)

Submissions via our discreet postal network

Submissions to our postal network offer the **strongest form of anonymity** and are good for bulk truth-telling.

Steps:

1. First place your leak onto a floppy disk, CD, DVD or a USB Flash Drive. If you are using a floppy disks, please create two as they are often unreliable. If you only have paper documents, we will scan them if they are of significant political or media interest (if you are unsure whether this may be the case, please **contact us** first).
2. Post your information to one of our trusted truth facilitators listed below. You may post to whatever country you feel most suitable given the nature of the material and your postal service. If your country's mail system is unreliable, you may wish to send multiple copies, use DHL, FedEx or another postal courier service.

WikiLeaks truth facilitators will then upload your submission using their fast internet connection. If you use a floppy disk, be sure to send two for increased reliability.

You can use whatever return address you like, but make doubly sure you have written the destination correctly as postal workers will not be able to return the envelope to you.

After receiving your postal submission our facilitators upload the data to WikiLeaks and then destroy the mailed package.

High risk postal submissions

If your leak is extremely high risk, you may wish to post away from your local post office at a location that has no witnesses or video monitoring.

Many CD and DVD writers will include the serial number of the DVD or CD writer onto the CD/DVDs they write. If the post is intercepted this information can in theory be used to track down the manufacturer and with their co-operation, the distributor, the sales agent and so on. Consider whether there are financial records connecting you to the CD/DVD writer sale if your adversary is capable of intercepting your letter to us and has the will to do this type of expensive investigation.

Similarly, CD and DVD media themselves include a non-unique manufacturing "batch number" for each group of around 10,000 CD/DVDs made.

Although we are aware of **no instances** where the above has been successfully used to trace an individual, anti-piracy operations have used the information to trace piracy outfits who sell tens or hundreds of thousands of counterfeit CDs or DVDs.

If you suspect you are under physical surveillance give the letter to a trusted friend or relative to post. On some rare occasions, targets of substantial political surveillance have been followed to the post office and have had their posted mail seized covertly. In this rare case if you are not intending to encrypt the data and if the police or intelligence services in your country are equipped to perform DNA and/or fingerprint analysis you may wish to take the appropriate handling precautions.

Postal addresses of our trusted truth facilitators

You may post to any country in our network.

Pick one that best suits your circumstances. If the country you are residing in has a postal system that is unreliable or frequently censored, you may wish to send your material to multiple addresses concurrently. For unlisted postal addresses, please **contact us**.

Australia

```
To: "WL" or any name likely to evade postal censorship in your  
BOX 4080  
University of Melbourne  
Victoria 3052  
Australia
```

Retrieved from "<https://88.80.17.76:43443/wiki/WikiLeaks:Submissions>"

Categories: Pages needing translation | Vital pages

WikiLeaks:Contact

From WikiLeaks

(Redirected from Contact)

Submission inquiries

Please see Document Submissions for general advice.

Electronic

If you want to electronically submit a document, please refer to the online document submission system. Using this link, you will be provided with more information on how to safely and anonymously submit documents for publication, that you can consider depending on your situation.

Onion routing

Contents

- 1 Submission inquiries
 - 1.1 Electronic
 - 1.2 Postal mail
- 2 General inquiries
 - 2.1 General office
 - 2.2 Direct contact
 - 2.3 Press inquiries
 - 2.4 Legal inquiries
- 3 Specialized inquiries
 - 3.1 WikiLeaks expert groups
 - 3.1.1 WikiLeaks analysts
 - 3.1.2 WikiLeaks artists
 - 3.1.3 WikiLeaks coders
 - 3.1.4 WikiLeaks lawyers
 - 3.1.5 WikiLeaks tech
 - 3.1.6 WikiLeaks writers
 - 3.2 WikiLeaks in your country
 - 3.2.1 Australia
 - 3.2.2 France
 - 3.2.3 Germany
 - 3.2.4 Iceland
 - 3.2.5 Kenya
 - 3.2.6 United Kingdom
 - 3.2.7 United States

See our Tor
Instructions for
connecting to
WikiLeaks through
an additional
anonymization layer.

Postal mail

Post

To: Pick any
name likely to
evade postal
censorship in
your country.
BOX 4080
University of
Melbourne
Victoria 3052
Australia

General inquiries

General office

`wl-office@sunshinepress.org`

Press inquiries

Direct contact

To chat with us, please see the WikiLeaks
Chat page. Talk to "office".

Legal inquiries

wl-press@sunshinepress.org

Get notified about our press releases:

Email address:

Subscribe

(Disclaimer)

For any legal requests, please see:
WikiLeaks legal pages.

If you want to join our global press freedoms defense team as a lawyer, please contact

wl-lawyers@sunshinepress.org

Specialized inquiries

WikiLeaks expert groups

WikiLeaks analysts

wl-analysts@sunshinepress.org

WikiLeaks artists

wl-art@sunshinepress.org

WikiLeaks coders

wl-coders@sunshinepress.org

WikiLeaks lawyers

wl-lawyers@sunshinepress.org

WikiLeaks tech

wl-tech@sunshinepress.org

WikiLeaks in your country

Australia

wl-australia@sunshinepress.org

France

wl-france@sunshinepress.org

Germany

wl-germany@sunshinepress.org

Iceland

wl-iceland@sunshinepress.org

Kenya

wl-kenya@sunshinepress.org

WikiLeaks writers

`wl-writers@sunshinepress.org`

United Kingdom

`wl-uk@sunshinepress.org`

United States

`wl-usa@sunshinepress.org`

Retrieved from "<http://www.wikileaks.org/wiki/WikiLeaks:Contact>"

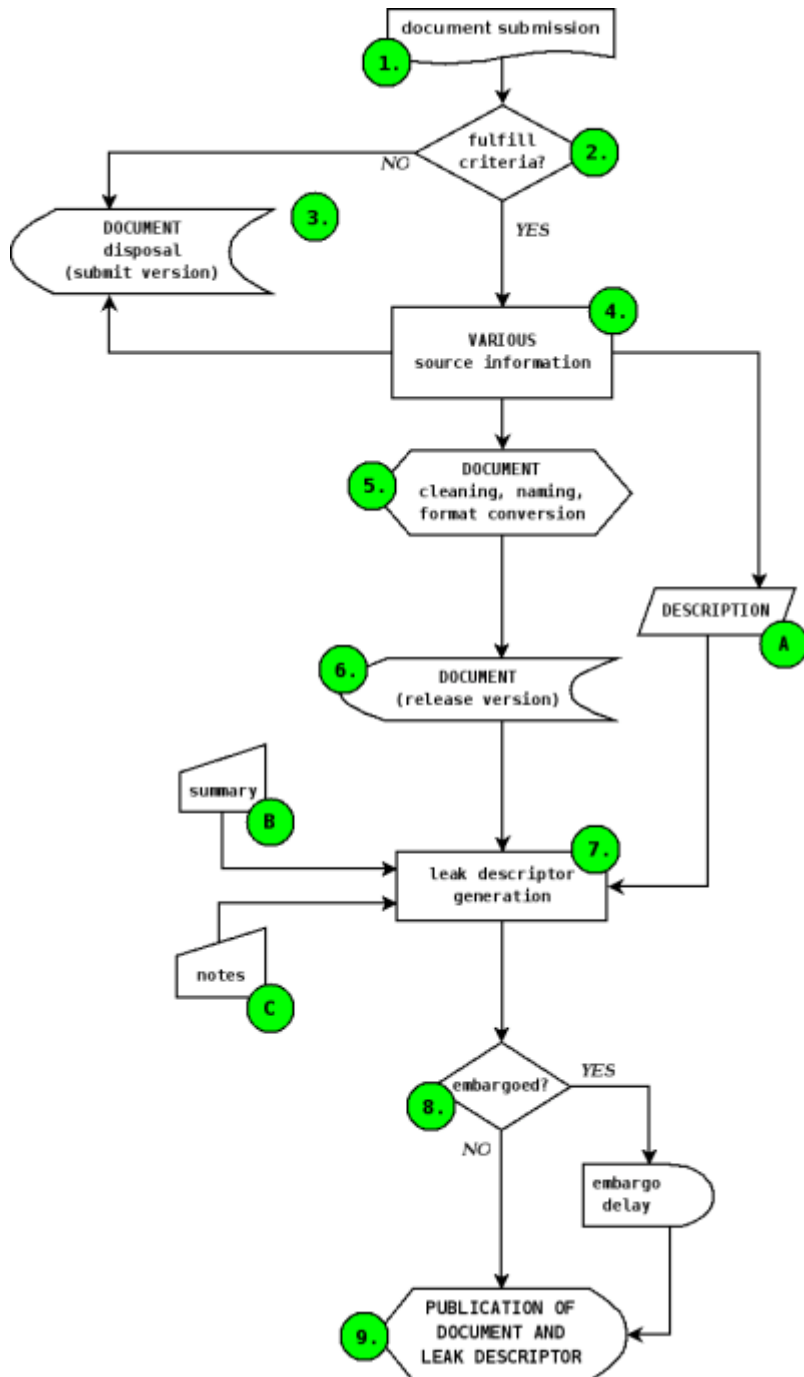
Category: Vital pages

WikiLeaks:Understanding submissions

From WikiLeaks

This page is intended to provide an insight into processing of documents at Wikileaks, from submission to the release to the public. While the chart does not include all details, it presents all relevant steps a submission goes through before publication. It has been created in an effort to enhance the understanding of the general public and the media of Wikileaks operations. All files are processed in cryptographically secure, isolated environments making use of AES256, *US DoD TOP SECRET*-approved encryption for long-term storage as well as system swap memory.

Wikileaks document flow



1. A document is submitted to WL using the correct Document Submission page.

2. The document is checked against the submission criteria. If matching, processing continues.

3. None-matching documents are safely disposed of.

4. Information from the source is processed into according channels.

5. The document is cleaned from compromising metadata (according to NSA and WL-internal standards), renamed to the WL naming standard, and eventually converted to an appropriate file type.

6. A release version of the document is produced and moved to the final destination.

7. The leak descriptor is compiled from various

information sources, including description (A) by the submitter, notes (B) by WL staff editors and a summary (C) by volunteers and/or staff. The document is tied to related organisations, countries, its cryptographic identity and other information.

8. A final check verifies if the document has been embargoed by the submitter. In case of an embargo date set, an according publication delay will be established.

9.
The document is published via the leak descriptor page and available to the public.

Retrieved from "http://wikileaks.org/wiki/WikiLeaks:Understanding_submissions"

WikiLeaks:Tor

From WikiLeaks

Report a problem on this page

The following method requires some technical ability. If you are used to installing new software and configuring proxy servers you should have the required skills, otherwise you may wish to use one of our other submission methods. Don't let the technology defeat you!

Tor or The Onion Router is a cryptographic technique first implemented by US navy research to permit intelligence agents to use the internet without being traced, by encrypting and routing communications through many different internet servers. Subsequently Tor has been developed by US University MIT (/wiki/Special:Jump/aHR0cDovL21pdC5lZHUv) and the California internet rights watchdog the Electronic Frontier Foundation (/wiki/Special:Jump/aHR0cDovL2VmZi5vcmcv) and subsequently incorporated into Wikileaks.

Using our anonymous access package (see below) you can prevent internet spies knowing that your computer has connected to Wikileaks.

Most Wikileakers do not need this extra security and there are simpler and possibly safer alternatives for once-off high-risk leaks (see Submissions). But for those who are at risk and want to access Wikileaks from the comfort of their homes or offices or need to bypass Internet censorship, Tor (Onion Routing) is an excellent solution.

When you have installed our Tor access package (see below), you may then connect to Wikileaks via our anonymous address (the ".onion" is short for "Onion Routing", but you do not need to be concerned with this detail).

Then whenever you want to establish an encrypted anonymous (even to internet spies) connection to Wikileaks goto our magic link:

<http://gaddbiwdftapg1kq.onion/>

(this link will only work once you have installed and configured Tor.)

To upload a document anonymously using tor:

<http://gaddbiwdftapglkq.onion/wiki/Special:Leak>
(**this link will only work once you have installed and configured Tor.**)

Unless your memory is superb you may wish to write that address down — you may wish to destroy the paper after you are finished with it.

Without Tor, when you access a Wikileaks site the usual way, e.g via <https://wikileaks.org/> all your data is encrypted, but internet spies maybe able note how long your computer spent talking to Wikileaks servers. See Connection Anonymity for further discussion.

Wikileaks Tor uses **fully encrypted end-to-end anonymous connections**. Accidental misconfiguration is impossible and at no stage does your communication leave the encrypted network.

The cost of this anonymity is speed, with page loads taking on average 15 seconds but sometimes as many as 60. File uploads to our servers tend to happen at 5 to 30 kilobytes per second.

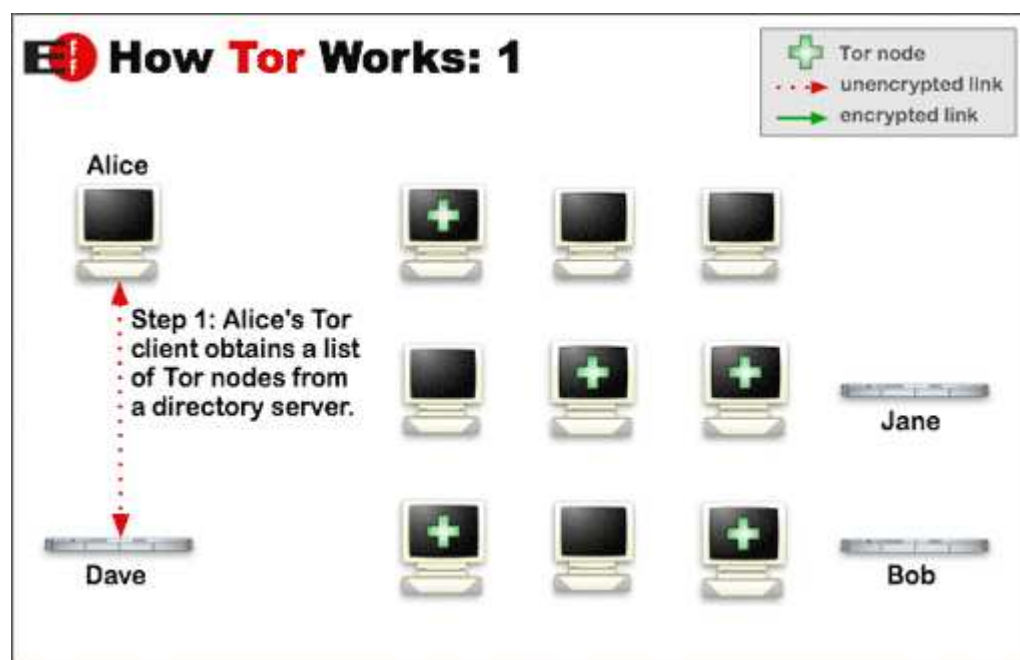
Installing Tor

1. If you don't have it already, install the Firefox (</wiki/Special:Jump/aHR0cDovL2ZpcmVmb3guY29tLw==>) web-browser. Other web-browsers will work with Tor, but you will have to configure the "proxy servers" manually. Under windows at least, this will be performed automatically if you have firefox.
2. Goto <http://tor.eff.org/> and download, install and configure Tor.
3. start Firefox.
4. Visit <http://gaddbiwdftapglkq.onion/wiki/Special:Leak>

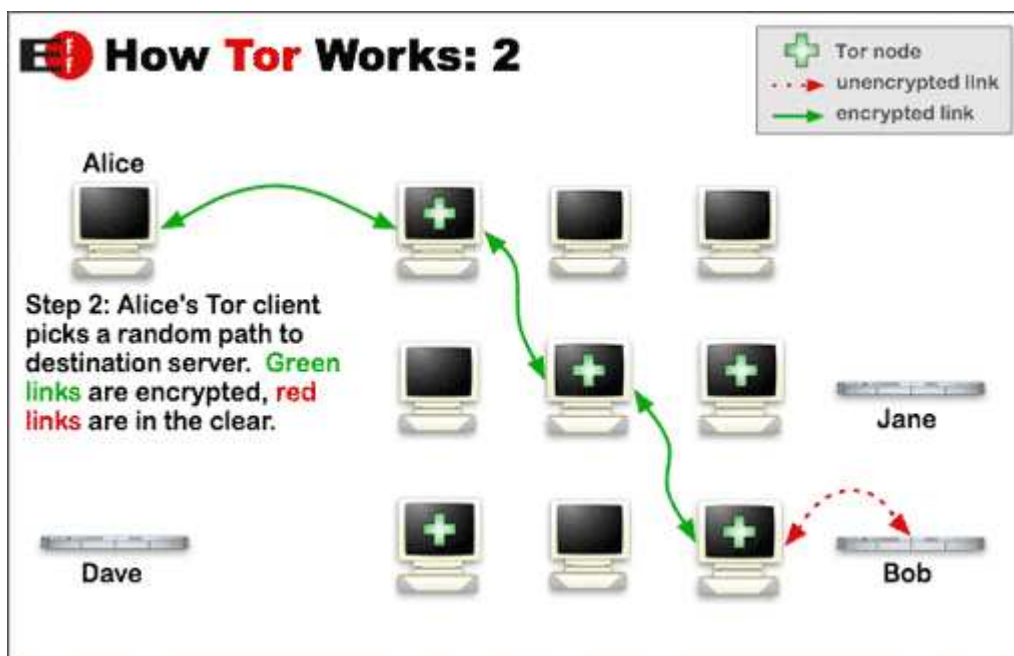
Tor is usually **VERY SLOW**. Page load times of 5-60 seconds are normal. Please be patient.

How Tor works

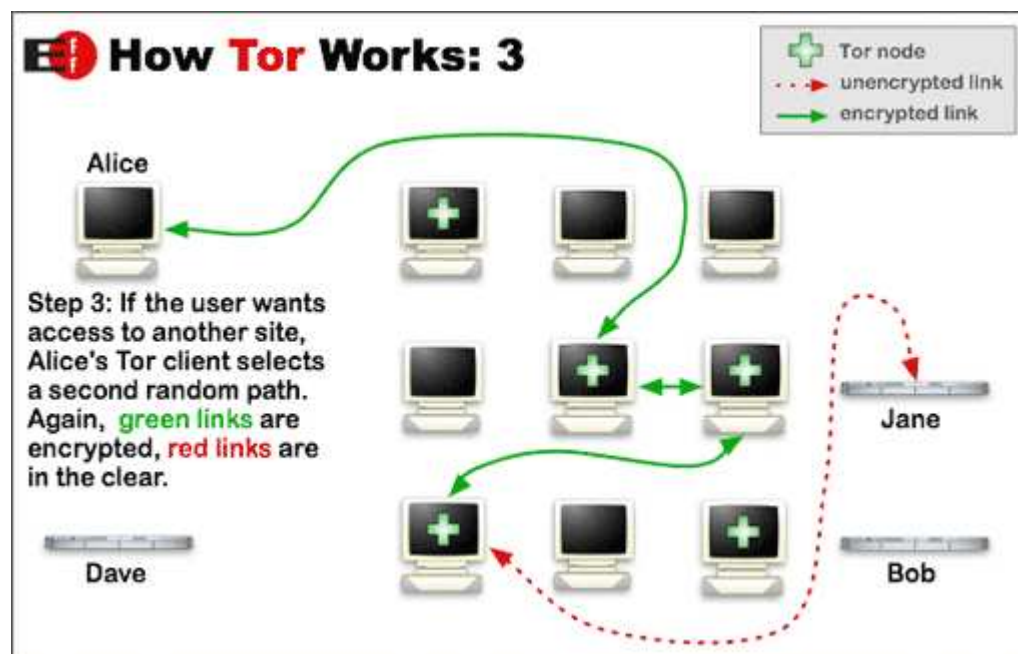
Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you—and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several servers that cover your tracks so no observer at any single point can tell where the data came from or where it's going.



To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through servers on the network. The circuit is extended one hop at a time, and each server along the way knows only which server gave it data and which server it is giving data to. No individual server ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.



Once a circuit has been established, many kinds of data can be exchanged. Because each server sees no more than one hop in the circuit, neither an eavesdropper nor a compromised server can use traffic analysis to link the connection's source and destination.



For efficiency, the Tor software uses the same circuit for connections that happen within the same minute or so. Later requests are given a new circuit, to keep people

from linking your earlier actions to the new ones.

Retrieved from "<http://wikileaks.org/wiki/WikiLeaks:Tor>"

WikiLeaks:Psiphon

From WikiLeaks

Report a problem on this page

(Redirected from Psiphon)

1. REDIRECT <http://psiphon.civisec.org/>

Retrieved from "<http://www.wikileaks.org/wiki/WikiLeaks:Psiphon>"

WikiLeaks trampoline

From WikiLeaks

To protect your privacy, all external links are redirected through this page.

The safest and recommended way to visit the page you requested is to copy the following address, and then paste to your browser's address bar.

`http://psiphon.civisec.org/`

Click here to proceed to the requested page immediately.

Retrieved from "<http://www.wikileaks.org/wiki/Special:Jump>"

Psiphon is under construction

February 24, 2010 in [Uncategorized](#) | [2 comments](#)

Welcome to Psiphon. We are currently remodeling the site. Please check back soon.

You can contact our staff by emailing info@psiphon.ca (<mailto:info@psiphon.ca>)

thanks,
The Psiphon Team



WikiLeaks accepts **classified, censored** or otherwise **restricted** material of **political, diplomatic or ethical significance**.

WikiLeaks **does not accept** rumour, opinion or other kinds of first hand reporting or material that is already publicly available.

If your submission matches this criteria we will publish and keep published the document you submitted. The information you submit will be technically anonymized and we do not retain any information on you. We will never cooperate with anyone seeking to identify you.

[Read the full disclaimer here.](#)

Please choose a file for upload:

To upload multiple files please compress them as a file archive.

Please split files larger than 200MB into smaller files. Thanks.

To explicitly set an embargo date for the upload uncheck the checkbox and enter the desired release date. Please enter the date in the format YYYY/MM/DD.

No embargo, defaults to on:

The upload will not be released until:

 / /

Since it seems that you have no JavaScript enabled you can see the progress of your upload if you click on the link. This will open the progress indicator in a new window.

[CLICK HERE](#) the get the upload progress indicator.

To submit the document press the **Upload** button. After your upload is finished you can provide additional information about the content.

Courage is contagious.



Disclaimer

You

Submit a document for us to publish and, in order to maximize its impact, distribute it to a network of investigative journalists, human rights workers, lawyers and other partners.

We

We will publish and keep published the document you submitted, provided it meets our criteria. Your data is stored decentralized, encrypted and as a preserved historical record in full by the public.

The information you submit will be cleaned by us to not be technically traceable to your program, your word installation, scanner, printer.

We also anonymize any information on you at a very early stage of the WikiLeaks services; neither we nor our partners know who you are nor do they keep any information about your visit.

We will never cooperate with anyone trying to identify you as our source. In fact we are bound not to do so, and any investigation into you as our source is a crime in various jurisdictions and will be prosecuted.

You can continue with your upload by following this [link](#).

Courage is contagious.