Martus

Helping human rights advocates protect, manage, and effectively utilize information

Partnership with Benetech, a non-profit organization that develops and supports Martus, secure information management software for human rights monitoring.
Benetech creates and develops new technology solutions that serve humanity, empower people, and address social justice questions. Benetech has several initiatives. The Global Literacy Program centers on Bookshare, a program for people with vision and reading disabilities. As part of this project, Benetech has formed the world's largest accessible digital library of scanned material. The Environmental Program has created a project management tool called Miradi especially for environmental conservation projects. The Human Rights Program at Benetech produces Martus, a free and open source secure documentation software that allows users to encrypt, search, analyze, and back up their data to a secure network of servers. Providing the capacity to securely document stories of human rights abuses, Martus protects the identities of witnesses and promotes the safety of human rights defenders. Currently available in 12 languages, Martus has been downloaded in over 100 countries, and Benetech has trained Martus users in over 40 of those. The demand for Martus technology and training is rapidly growing. Our Mobile Martus app for Android was released in September 2013, which is exciting and provides capacity for unobtrusive, secure mobile data collection. Martus is the Greek word for witness. And Benetech’s most recent initiative is Benetech Labs, an incubator project to identify big ideas and possible solutions to today’s major challenges. It’s where we begin to develop new technology—or enhancements to our existing technology—so that, ultimately, we can launch successful, useful, relevant tech tools for social good.
Benetech is based in Palo Alto, California and is a non-profit organization. Benetech is funded through the support of foundation and government grants as well as donations from individuals. The Human Rights Program is composed of six full time staff as well as associated engineers and trainers that develop Martus, provide support to Martus users, and conduct outreach and training on Martus to those who would like to learn to use the program. The Benetech Human Rights Program released the first version of Martus in 2003 and has trained and supported Martus users all over the world since then.

You can contact the Benetech Human Rights Program with questions or for assistance with troubleshooting Martus at any time by emailing help@martus.org or info@martus.org.
Information is a human rights advocates greatest asset, but it must be protected and properly utilized. To better understand why Benetech developed Martus, let’s start in Guatemala. This is a picture of the National Police Archives in Guatemala containing millions of pages of police records that detail many of the happenings during Guatemala’s long internal conflict in the 1980s and 1990s, including about torture, killings, detentions, and other illegal practices committed by state authorities, largely against the Mayan peoples of Guatemala. You may have heard in the news that one of Guatemala’s former leaders was sentenced for his role in carrying out genocide during this time. The National Police Archive, and the information accidentally discovered within it nearly 10 years ago, was instrumental in providing the evidence necessary for the verdict. But, as one can see, this pile of evidence is vulnerable to theft, loss, and easy destruction. In paper form, it is also not easily searchable or possible to analyze. The National Police Archives painstakingly preserved and digitized this warehouse full of information and safely stored samples of the data in Martus in order to be able to preserve it, secure it, make it searchable, analyze it, and transform it into powerful evidence. That evidence helped provide the proof that led to a verdict of a prison sentence of 80 years for genocide and crimes against humanity for Guatemala’s former leader. One of the keys was securing the data, and that’s where Martus came in.
Benetech designed Martus to serve organizations and situations like the National Police Archives, in which human rights advocates and defenders need to preserve, backup, and secure their information—keeping unauthorized viewers out while at the same time being able to get their information back in the event of a theft or attack. When Benetech asked its human rights partners what they would need from an information management program designed specifically for human rights, they gave Benetech this wish list. They said that the program would need to be:

- Easy to use
- Affordable
- Easy to customize
- Flexibility with data sharing
- Backup servers for safeguarding information
- Ability to search and report on information
- A way to publicize public data on the Internet

Benetech designed Martus to serve organizations and situations like the National Police Archives, in which human rights advocates and defenders need to preserve, backup, and secure their information—keeping unauthorized viewers out while at the same time being able to get their information back in the event of a theft or attack. When Benetech asked its human rights partners what they would need from an information management program designed specifically for human rights, they gave Benetech this wish list. They said that the program would need to be:

- Easy to use
- Affordable
- Easy to customize
- Offer flexibility with data sharing
- Include backup servers for safeguarding information
- Provide the ability to search and report on information
- Provide a way to publicize public data on the Internet
So, Benetech created Martus to meet all these needs:

- In its efforts to make Martus as widely accessible as possible, Martus is absolutely free and can be downloaded on the https://martus.org website.

- Martus is also open-source, which means that the program’s source code is published and freely available for anyone to use, review, or build upon, as well as verify that the software does exactly what it says it does. Open source software means you don’t have to trust the developers— you can verify that you both have the *real* software and that it actually does what it says it does. You can contrast this with Skype for example. Skype uses encryption and it’s free, but it is owned by Microsoft, we can’t see the code behind the software, and therefore we can’t verify that it does what it says it does. Contributing to and drawing on the open source community is an important part of who Benetech is.

- Martus prioritizes security and uses standard encryption, like that which is often used by banks or sites like Google.com. Encryption is a way to obscure data so that it is only readable by authorized people.

- Finally, Martus offers a way to store, standardize, organize, search, and share digital information, making it a useful tool to transform *information* into useful *evidence*.
These are some of the logos of the many organizations that have worked with the Benetech Human Rights Program over the last ten years. We look forward to working with you!
The following screenshots offer a quick visual overview of the functionality of Martus, but an in-person training can provide more examples of how Martus can be used successfully for your project.
Martus data entry format templates are customizable, so you can shape your form to match the data you are collecting and any interview/intake forms you are already using. Martus allows various field types, including text fields, drop down menus, checkboxes, grids (tables), date and date range fields, among others.
For each Martus bulletin, you can attach as many files you would like, of any size, and of any file type. This includes video files, but remember, when backing up to the server, sending a video over the internet will be expensive and will take a long time (imagine uploading a 1gb video file to Dropbox or Google Drive – same thing when ending a Martus bulletin with a 1gb file attached).

Examples:

- Photos
- Scanned images
- Text files
- Spreadsheets
On your computer, all of the data in your Martus account is stored encrypted, so that only you or someone you designate can read it. You can choose to publish some of this information to the Martus public search engine if you like, or ensure that all of your data NEVER shows up on the search engine. In Martus, a red border around a bulletin section means that information is PRIVATE, which means it will never show up on the Martus search engine. If the border around a section is grey, then once sealed and saved on the server, the information in that section will be available on the open internet. This includes attachments within the bordered areas—any attachments inside a grey/Public section will appear on the Martus search engine once the bulletin has been saved to a Martus server. On every bulletin, there is a section that can be Public or Private, and a section that is ALWAYS Private. Most Martus users do not ever make any data public, but some do.
Martus: Secure by Design

Martus uses a well-established form of encryption also used by:

- Banks
- Commercial websites
- Security products such as PGP
  - (Pretty Good Privacy: http://www.pgpi.org/doc/overview/)

The same encryption methods that major banks and commercial websites use to protect their data are employed by Martus. PGP is an open source standard that has been around for many years, and Martus uses the same methods.
Martus encrypts private bulletin data in multiple ways. It encrypts the DATA on your machine, before it's ever sent to a server. And, it encrypts the CONNECTION itself, so that snooping attackers cannot see what information is being sent or received by either end. Even if they were able to decrypt the connection (very very hard), all they would see is encrypted data being sent to or received from the server. And the data also stays encrypted on the servers so that nobody, including Benetech or server operators, can read the data.
This is a VERY basic example of encryption, illustrating the IDEA of encryption. THIS IS NOT THE TYPE OF ENCRYPTION MARTUS USES. If it did, the encryption could be cracked instantly. Instead, Martus uses very, very advanced encryption methods that change the original data into something unreadable and indecipherable without the decryption key.
This is what your data encrypted inside Martus looks like. Data encrypted in Martus can only be decrypted and viewed inside Martus and only by the Martus account in which it was created, or anyone that you have authorized to decrypt and read it. If you try to open the encrypted files on your computer that contain the data in your Martus bulletins outside of Martus, this is what you will see. You can see that there is data, but you can’t read it. In the event that an attacker or authority were to gain access to the Martus server, this is also what they would see: there is data, but it's unreadable.
Benetech makes two servers available for free to all Martus users. There is no limit to the amount of data you are allowed to back up on the server, and the servers “mirror” each other several times a day, so there is always a backup of your backup.
Martus 4.3 and above allows for the option of communicating with Martus servers over Tor. Tor is a free and open-source tool that provides internet users with greater anonymity online and a better ability to circumvent censorship. In most cases, when you send or receive information over the internet, you establish a fairly direct connection to the sites or servers you are contacting. For example, if you send an email through Gmail, it is easy for those along the way to see that you are connecting to Gmail.com and for Google, who administers the servers, to see information about your computer and where it is located. Instead, Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world and obscuring the trail using encryption. Thus, it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. If you need or want to obscure your connection to the Martus server, or to circumvent censorship in order to connect to the backup Martus servers, using Martus over Tor can help you do this. Using Tor will also make sending and receiving bulletins from the Martus servers slower.
You may choose to share data with other Martus users. When sending data in Martus, the sender is the Field Desk and the receiver is the Headquarters. A Field Desk may also be a Headquarters, and a Field Desk may configure as many Headquarters accounts as she likes.
Data is shared with other Martus users through the servers. Data is encrypted on your computer, the encrypted data is sent to the server, someone you trust and have authorized downloads that encrypted data, and it is decrypted on that person’s computer. Never was the plain, unencrypted message available throughout the interchange.
End to end encryption means that your data is encrypted locally on your computer and only the encrypted data is sent over the internet. The encrypted data is then downloaded by the recipient and decrypted on their computer back to plain text they can read. At no point during the transit of that data from one computer to the server to another computer is the data ever unencrypted. Martus makes this easy and automatic. End-to-end encryption requires that the keys to decrypt the data are not stored on the server facilitating the exchange. This means that if an unauthorized person, whether a server admin under bribe or threat, or another user or hacker were to gain access to the data on the server, they cannot decrypt the data. It also means that you cannot access your Martus account and view your data through an online web portal, which would require that your keys be stored on the server where your data is stored. This would significantly reduce the security of your data. It’s also why some companies have been able to give away their users’ emails or data to inquiring authorities. In those cases, even if the data is encrypted on their servers, they also hold the keys, rendering the encryption little protection from legal subpoenas. But Benetech can’t give away your unencrypted data because Benetech doesn’t have the keys to decrypt it, and they don’t want them!

This slide shows that WITHOUT end to end encryption, people “in the middle” could read what is being sent (or the data could be read if your computer is stolen/confiscated, since the data isn’t encrypted there either).
And WITH end to end encryption, people “in the middle” cannot read anything (and also can’t read what’s on the computers at either end because the files are encrypted there as well)...
You can choose if and how you share information with other accounts. There is no pre-established organization of a Martus system. Individuals, organizations, and groups must think through their information flow or desired information flow, and trainers support users to configure their Martus accounts to match the flow of information required. These are some of the ways that Martus accounts can be configured to send and/or receive data from others. Martus uses the language of “HQ: Headquarters” to describe accounts that receive data, and “FD: Field Desks” to describe accounts that send data.
Choose different configurations based on the needs of your organization

One account can be both a Field Desk and a Headquarters account.
This may seem complicated, but it is a rather typical information flow. Several field desks report to a regional manager, who shares with the Executive Director, or something similar. Martus is flexible with regard to data sharing and can be set up to match your organization's current information flow.
You can see various field types here, including drop downs, checkboxes, grids (tables) and date range fields.
Why customize?

- Organize information in a consistent way
- Especially helpful if you are working with other people
- Make sure you have collected all of the useful pieces of information
- Facilitate data entry
- Prevent inconsistency and errors

There are benefits to customization, including minimizing typing errors (which impact searching and reporting), and standardizing data across accounts.
Martus offers a robust search function, including using multiple search criteria, saving searches, specifying a field (or multiple fields) or searching all fields for text.

**Searching in Martus**

<table>
<thead>
<tr>
<th>Field(s) to search</th>
<th>Compare how?</th>
<th>Search for...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any Field</td>
<td>Contains</td>
<td>prison or jail</td>
</tr>
<tr>
<td>Last Saved</td>
<td>=&gt;</td>
<td>Jan 1 2004</td>
</tr>
</tbody>
</table>

- **Search “Any Field”** - for a full text search
- **Search on a specific standard or custom field** – to focus your search
- **Use AND/OR search functionality** - to sharpen your search.
- **Save Search specifications** - to use them again later
Martus also offers reporting, which allows users to gather certain parts of their data to be presented together. There are two reporting formats (page report and tabular report).

- Select which fields and order of appearance
- Filter bulletins by search criteria
- Choose to print full bulletin information, summary counts, or both
- Select public bulletins, private, or both
Table reports have one row per bulletin; Page reports display fields in the order they appear in the bulletins (you can print all fields or only a subset)
Bar and Pie charts summarize any bulletin field you select, and only those that match the search criteria you define.
Mobile Martus for Android allows for more unobtrusive use of Martus – e.g. you can take a photo with your phone (or other mobile device) and very quickly back it up securely to be retrieved at a later point; especially useful if you are in a place where you are worried about your phone being confiscated etc.

“Write-only” means that you can send bulletins to the server, to be retrieved and viewed by you or another user in the Martus client on your computer, but you cannot see the bulletins you created on the phone. Technically speaking, this is because only the part of the key used to encrypt the data (called the public key) is stored on the phone, but the part of the key used to decrypt (or read) that data (called the private key) remains only on the desktop HQ account connected to your Mobile account.

You can “send to Martus” using the standard “share” functionality with other apps that create files (e.g. Gallery for photos/video)

Data is encrypted on the phone and during transmission to server, after which the bulletin data is removed from the phone (the original attachment, e.g. photo in your Gallery, is not removed automatically by Martus but you can delete it after sending to Martus)
Tor can help you if you are working in a place where certain internet activity is blocked, and makes it harder for folks doing surveillance to recognize your activity.

As with the Martus client on a computer, Mobile Martus will accept, encrypt, and send any kid of attachment – images, videos, voice notes, text, etc.
This photo was sent securely to the Martus servers using the “Share” or “Send to” feature inside the Gallery.
Tails (The Amnesic Incognito Live System) is a portable operating system that can be installed to a USB stick, DVD or SD card and booted from virtually any computer. It provides extra security by ensuring the underlying file system can’t be altered, running all internet traffic through the Tor network, only ever writing to RAM (and wiping RAM at shutdown), and providing state-of-the-art encryption software out of the box. It’s entirely free and open source, and when using Tails on a USB or SD card, users can install and run Martus.

Tails is not necessary for all Martus users, but can provide the highest level of accessible, usable security to those who need it.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amnesic</strong></td>
<td>Wipes all traces on shutdown</td>
</tr>
<tr>
<td><strong>Locked down</strong></td>
<td>File system is read-only</td>
</tr>
<tr>
<td><strong>Incognito</strong></td>
<td>All internet traffic is anonymized</td>
</tr>
<tr>
<td><strong>Portable</strong></td>
<td>Install to USB stick, DVD or SD card</td>
</tr>
</tbody>
</table>
Martus is available in 12 languages (English, Spanish, Russian, Arabic, Burmese, Farsi, Vietnamese, Thai, French, Khmer, Nepali, Armenian), with others being planned (e.g. Chinese).

The map above shows just some of the locations where Martus users live and work...
One of Benetech’s long time partners and Martus Users is the Network for Human Rights Documentation – Burma, a network of a dozen organizations that collaborate using Martus to produce information about human rights violations inside Burma.
Another example of a long-time partner is the Guatemalan National Police Archive, discussed above, which has been a Martus user since 2006.
Some other tools that Martus users might be interested in using to protect their data and communications:

- PGP for email encryption
- Pidgin/Adium/Cryptocat for encrypted chat
- Jitsi for encrypted VOIP
- Tor for anonymous browsing
- Whole disk encryption

For whole disk encryption, please see "Disk Encryption" recommendations on https://prism-break.org.
Welcome to the Martus Community!

Thank you!

info@martus.org
help@martus.org