Hi Ross,

On Sep 15, 2009, at 17:01 , Ross Ulbricht wrote:

> Dear Arto,
>
> Thank you for being open to my questions. I don't want to bother
> you too much, but I find this topic fascinating and very
> applicable. The impression I get is that the technology is getting
> close but not quite there yet.

I'd say that the technology is here, it's just not evenly distributed yet. There is a lot of incidental complexity throughout that could still be gotten rid of.

> What do you think of Tor browsing and Tor hidden services? Is it
> as anonymous as they say it is? The hidden services part sounds
> interesting, but I have been unsuccessfull in actually accessing
> any of the existing ones yet including eCache.

I use Tor on a regular basis. (And I have it set up on my mobile phone, too: http://www.cl.cam.ac.uk/research/dtg/android/tor/)

There exist a number of theoretical attacks and compromises on Tor security, but in practice you don't need to worry about them. To use Tor effectively you do need, however, to take into account the points at http://www.torproject.org/download.html.en#Warning

My experience with the hidden services, particularly eCache, has been frequent inaccessibility. I don't think this is a problem with the Tor network itself, but rather, for whatever reason, the hidden service providers themselves have not taken sufficient steps to ensure availability. (I suspect a whole lot of hidden services are being run from the private computer of their operators, over an ADSL line or such, which isn't conductive to uptime.)

eCache hasn't been available for a while, so it should probably be assumed to be defunct at the moment.

> With Pecunix, I understand it is a goldbacked digital currency.

Yes. They store the gold in secure facilities with Via Mat in Switzerland. Anglo Far-East Bullion Company serves as the bullion custodian.

> Can I anonymously and securely deposit funds?

In principle, yes. You would only need to find somebody who already has Pecunix and is willing to transfer some to you in exchange for cash (or other forms of remuneration). No trace of the transaction would thus exist outside the Pecunix system itself.

In practice, however, the individual-to-individual (or peer-to-peer) exchange market is underdeveloped at the moment; in-exchanges are currently dominated by larger digital gold exchangers, who are companies that provide this service professionally. Many of these

GOVERNMENT
EXHIBIT
270
14 Cr. 68 (KBF)

companies require personally identifying KYC information, so in practice you would, typically, leave a one-way trace in the bank transfer to your exchanger.

Of course, any digital gold that you actually *earn* in the free digital economy is already inside the closed system and thus won't leave anything but a transaction record on a secured server in Panama.

> Can I anonymously and securely withdraw funds in the form of fiat
> currency or gold?

Yes. The usual way to withdraw anonymous fiat cash is by obtaining an anonymous debit card that can be reloaded via digital currency payments. These are usually generically-branded Visa or Maestro cards that have no name on the front or on the magnetic strip, so they are not, in of themselves, traceable back to you.

Gold currencies like Pecunix or C-Gold also allow you to obtain your gold in physical form. This is called "bailing out" a gold coin or bar. Usually, however, they have a minimum quantity (such as 1 kilogram) that may be out of reach for the casual account holder.

> I can see how it would work as a closed system, but is there a way
> to integrate it with the rest of the economy securely?

This is the essential service that digital gold exchangers provide: they ensure convertibility between digital currencies, keeping the free digital economy liquid as a whole. There exist automated exchangers that will let you instantly convert between digital currencies with very low transaction fees, so in practice you can rather easily convert your gold to whatever funds you need at the moment (including fiat-based payment systems such as PayPal and Moneybookers, despite this being forbidden by the TOS of such payment systems).

> I would love to be able to set up an online storefront that
> couldn't be traced back to me (tor hidden services?)

Hidden services are one way to do this, but you can get a pretty secure setup in more conventional ways, too. For example, there exist a number of domain name registrars and hosting providers that accept anonymous digital currencies (including Pecunix). If you take care to not "leak" any personal information (including your real IP address) at any point, you can, in practice, set up a "proper" .com site that cannot be traced back to you.

The best-known service provider in this realm is probably Katz Global. Have a look at their domain trust services, anonymous shared hosting services, and anonymous SSL certificate services. On the downside they are, naturally, more expensive than run-of-the-mill service providers, and their services also attract some unsavory types (scammers, phishers, etc) who abuse the services for illegitimate (from an agorist POV) purposes, which can in turn affect how people perceive your site ("their domain is anonymously hosted at Katz, ergo they *must* be scammers!")

> where my customers could buy my products (revealing their identity
> only to me) and transferring funds to me anonymously and securely
> (Pecunix?). I suppose this is the ideal. What are the key pieces
> that are currently missing that would make this a reality?

I think the single biggest hurdle is the difficulty of getting existing fiat currency funds "uploaded" into the free digital economy, as described above. This overly high barrier to entry discourages "ordinary" people from opening e.g. a Pecunix account, which in turn limits the potential customer base for merchants, which in turn discourages potential merchants (such as yourself) from entering this market.

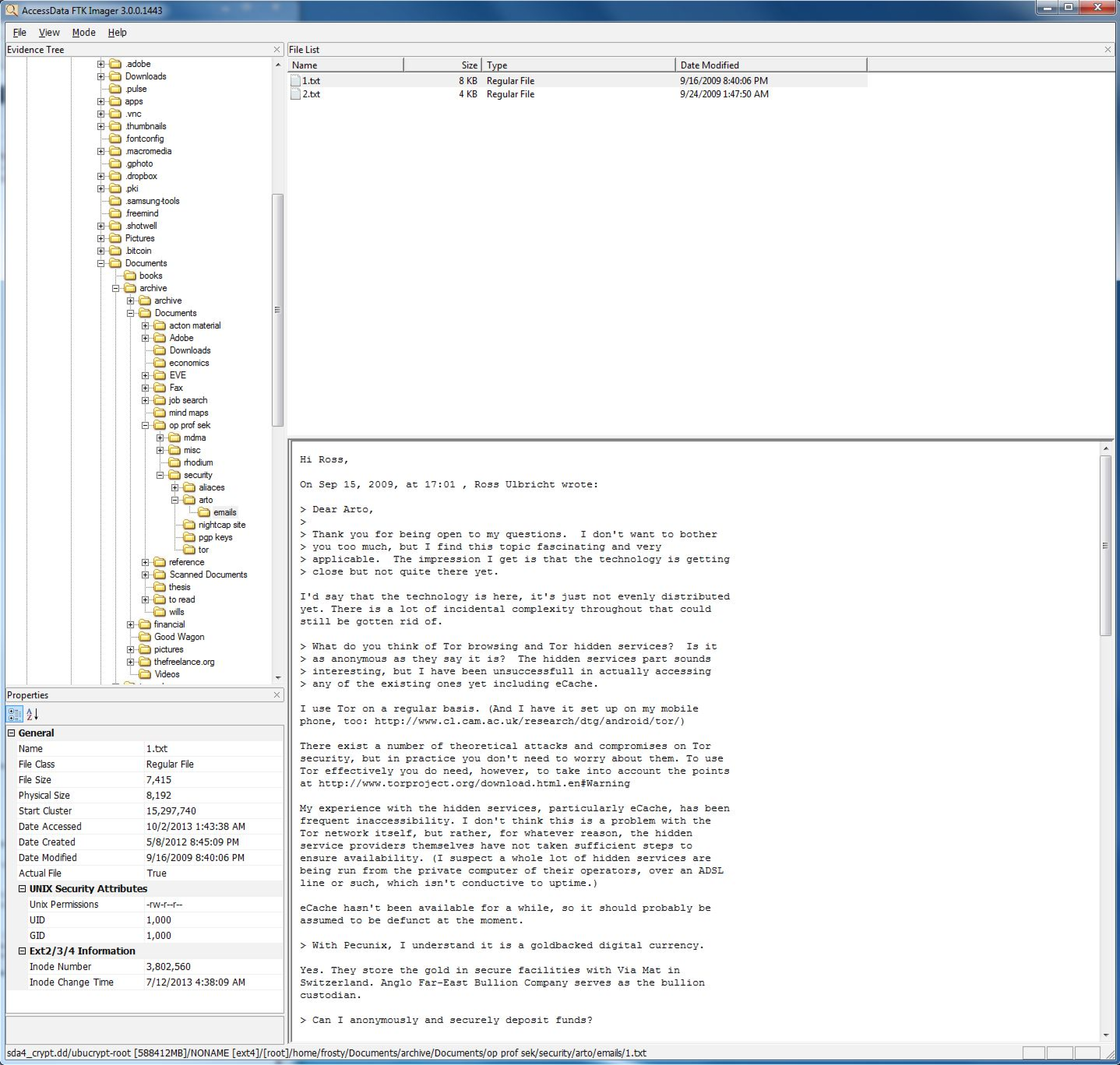
I am attempting to help solve this problem with the Drupal-based Agora software I'm developing, with the intention of making it easy to proliferate spot markets for digital currency exchange. Efforts like Agora will hopefully eventually decentralize the digital exchange market so that you will be able to find trustworthy people in your neighborhood with whom you can meet up with to take care of business (you give them cash, they give you Pecunix), all without having to jump through any gov-regulated KYC hurdles, and all without having to deal with the legacy banking cartel.

After the previous, the next big hurdle is establishing useful metrics for reputability (i.e. trustworthiness). This is probably more of a social problem than a technological one, but technology can make it easier. The existing PGP web-of-trust might turn out to be part of the solution.

> Once again I really appreciate your willingness to discuss these
> matters with me.

No problem. I will dig up and forward you a couple of earlier in-depth answers to questions much like yours, which should help round out the information given here.

Best regards,
Arto



```
.adobe
Downloads
.pulse
apps
.vnc
.thumbnails
.fontconfig
.macromedia
.gphoto
.dropbox
.pki
.samsung-tools
.freemind
.shotwell
Pictures
.bitcoin
Documents
    books
    archive
        archive
        Documents
            acton material
            Adobe
            Downloads
            economics
            EVE
            Fax
            job search
            mind maps
            op prof sek
                mdma
                misc
                rhodium
                security
                    aliaces
                    arto
                        emails
                    nightcap site
                    pgp keys
                    tor
            reference
            Scanned Documents
            thesis
            to read
            wills
        financial
        Good Wagon
        pictures
        thefreelance.org
        Videos
```

Name	Size	Type	Date Modified
1.txt	8 KB	Regular File	9/16/2009 8:40:06 PM
2.txt	4 KB	Regular File	9/24/2009 1:47:50 AM

General	
Name	1.txt
File Class	Regular File
File Size	7,415
Physical Size	8,192
Start Cluster	15,297,740
Date Accessed	10/2/2013 1:43:38 AM
Date Created	5/8/2012 8:45:09 PM
Date Modified	9/16/2009 8:40:06 PM
Actual File	True
UNIX Security Attributes	
Unix Permissions	-rw-r--r--
UID	1,000
GID	1,000
Ext2/3/4 Information	
Inode Number	3,802,560
Inode Change Time	7/12/2013 4:38:09 AM

```
Hi Ross,

On Sep 15, 2009, at 17:01 , Ross Ulbricht wrote:

> Dear Arto,
>
> Thank you for being open to my questions.  I don't want to bother
> you too much, but I find this topic fascinating and very
> applicable.  The impression I get is that the technology is getting
> close but not quite there yet.

I'd say that the technology is here, it's just not evenly distributed
yet. There is a lot of incidental complexity throughout that could
still be gotten rid of.

> What do you think of Tor browsing and Tor hidden services?  Is it
> as anonymous as they say it is?  The hidden services part sounds
> interesting, but I have been unsuccessfull in actually accessing
> any of the existing ones yet including eCache.

I use Tor on a regular basis. (And I have it set up on my mobile
phone, too: http://www.cl.cam.ac.uk/research/dtg/android/tor/)

There exist a number of theoretical attacks and compromises on Tor
security, but in practice you don't need to worry about them. To use
Tor effectively you do need, however, to take into account the points
at http://www.torproject.org/download.html.en#Warning

My experience with the hidden services, particularly eCache, has been
frequent inaccessibility. I don't think this is a problem with the
Tor network itself, but rather, for whatever reason, the hidden
service providers themselves have not taken sufficient steps to
ensure availability. (I suspect a whole lot of hidden services are
being run from the private computer of their operators, over an ADSL
line or such, which isn't conductive to uptime.)

eCache hasn't been available for a while, so it should probably be
assumed to be defunct at the moment.

> With Pecunix, I understand it is a goldbacked digital currency.

Yes. They store the gold in secure facilities with Via Mat in
Switzerland. Anglo Far-East Bullion Company serves as the bullion
custodian.

> Can I anonymously and securely deposit funds?
```

sda4_crypt.dd/ubucrypt-root [588412MB]/NONAME [ext4]/[root]/home/frosty/Documents/archive/Documents/op prof sek/security/arto/emails/1.txt