

akselvoll.net

Magnus Akselvoll's personal blog.

Disclaimer: The postings on this site are my own and don't necessarily represent my employer's positions, strategies or opinions.

29 May 2014

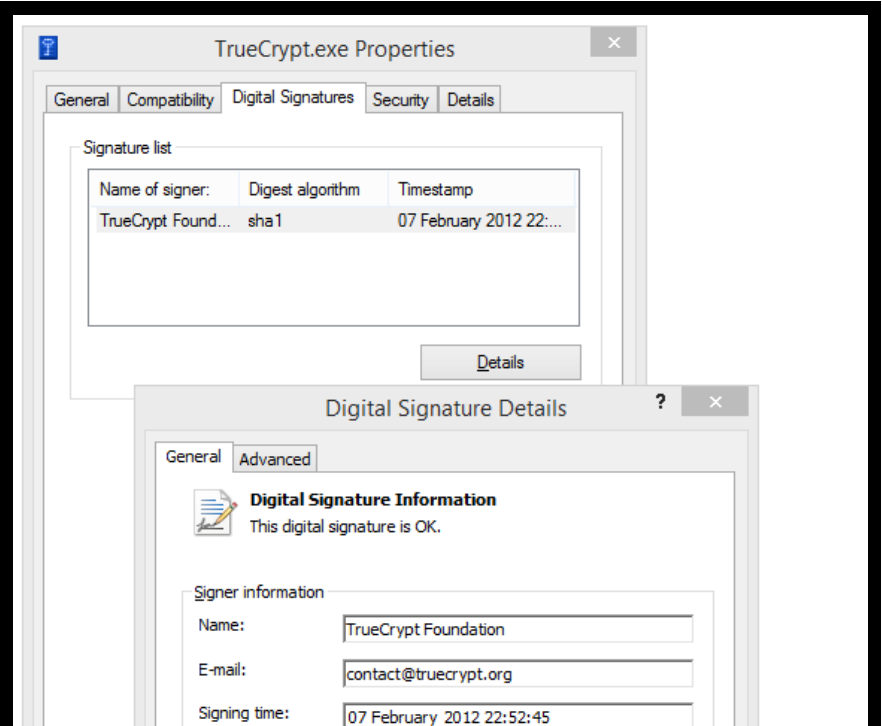
How to securely download TrueCrypt 7.1a

Now that TrueCrypt has [unexpectedly closed down the project](#), I recommend that no new users start using it. However, if you already use TrueCrypt and are not ready to migrate to anything different yet, you should stick to version 7.1a, since there are reports suggesting that version [7.2 may be compromised](#). *EDIT: Version 7.2 is a read-only version to let you migrate to other platforms. The reports on suspicious network activity are still not confirmed. In short, you want version 7.1a.*

But how do you download version 7.1a, now that TrueCrypt closed their site? Who do you trust? The answer is math! Trust the digital certificate used to sign the installation set, not the site you download it from. The way to do this is listed below.

Step 1 - Find the trusted certificate

On a computer that has version 7.1a installed and that you are quite confident that has not been taken over by evil martians, right click the file "C:\Program Files\TrueCrypt\TrueCrypt.exe" (or wherever you installed it) and select Properties. Go to the tab Digital Signatures, click Details, View Certificate and then scroll to Thumbprint in the Details tab.



Google+



google.com/+MagnusAkselvoll

Tech, Photography, Norway, Málaga

Follow

1.734 followers

Climate Málaga

27°
19°



Wednesday 26° 21°



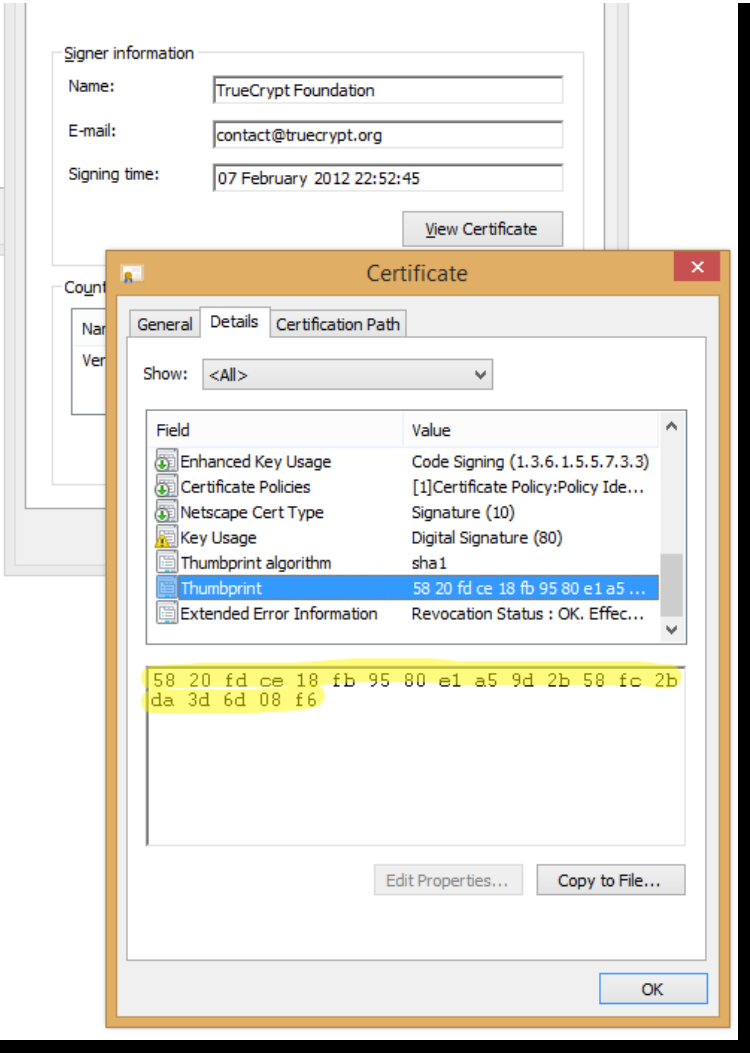
Thursday 29° 19°



Friday 30° 20°



tiempo.com [+info](#)



Take note of this thumbprint. For me it was "58 20 fd ce 18 fb 95 80 e1 a5 9d 2b 58 fc 2b da 3d 6d 08 f6", but don't trust me, do it yourself.

As an added step of security, you should go to the Certification Path tab, click the topmost certificate in the chain, click View Certificate and find the thumbprint for that as well. For me this was "b1 bc 96 8b d4 f4 9d 62 2a a8 9a 81 f2 15 01 52 a4 1d 82 9c".

Step 2 - Download TrueCrypt 7.1a

It doesn't matter where you find it. Sure, don't go to the darkest places of the web and get your computer infected with all kinds of malware, but my point is that you will check the validity of the file after you download it. I downloaded from here: http://filehippo.com/download_truecrypt/11601

Edit: You can also download from [this BitTorrent Magnet link](#). Once again, I checked it to be valid, but you really have to validate yourself.

Edit: Grc.com has a [good page](#) explaining the trustworthiness of TrueCrypt 7.1a and offers download links.

Step 3 - Verify the signature

Now go to the file you downloaded, and repeat the process.



Google™ Custom Search

Made using

[Blogger](#)

[El Tiempo](#)

[Google Apps](#)

[Hover](#)

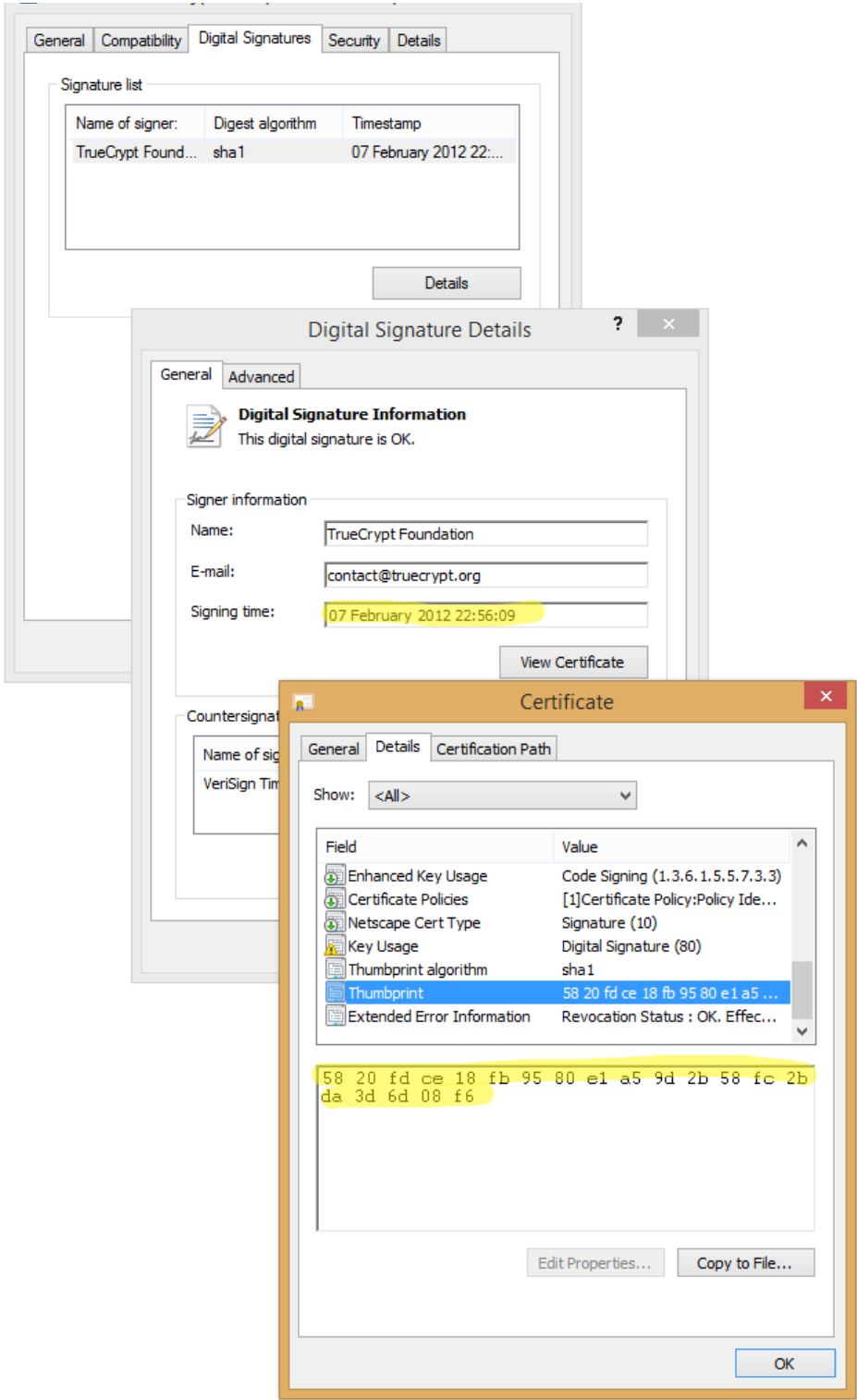
[internetVista®
monitoring](#)

Subscription



(Click to
subscribe)

asphalt aurgi backblaze backup birds blogger bus
canon car cheese chrome cinema consumer
crashplan crosswalk education emt eos fail firefox
fon.com fonera foobar2000 fun google handicraft
hardware ie invites itunes last.fm lightroom livedrive
malaga marmalade media moon movistar mozy
music networks nokia norway pdf Philadelphia
photo politics programming puzzle recipe
security software spideroak spotify starter
sync tech techo tips travel truecrypt Urende
video walnuts windows wordpress



Verify that the **Thumbprint is exactly the same** and that the **Signing time is in Febryary 2012**. Also, if you checked the certificate chain previously, verify the thumbprint for the root certificate as well.

If any of these checks fail, delete the file you downloaded. No ifs or buts, no trusting someone else saying that exactly this version is trustworthy. Only trust the file if it was signed around the time the original version was signed and with the exact same certificate. Do not trust certificate names or anything but the thumbprint.

I still think you should take TrueCrypts advice and migrate away from the software, but you probably don't have to rush. Until then, use a trusted version of 7.1a.

Posted by [Magnus Akselvoll](#) at [09:52](#)   +6 Recommend this on Google

Labels: [security](#), [software](#), [truecrypt](#)

3 comments:



Anonymous [29/5/14 19:24](#)

Nice one. Just checked from my local copy of 7.1a installer...thumbs match !!

[Reply](#)



Anonymous [2/6/14 05:04](#)

I have looked at my thumbs but can't see the numbers on them.
I washed my hands about an hour ago so could that have washed the numbers off too?
Please help.

[Reply](#)

▼ [Replies](#)



Magnus Akselvoll  [2/6/14 16:57](#)

This is a common problem caused by an aluminium compound the NSA adds to all commercially available hand soap to hide these numbers from us. But don't worry, you can easily recover the numbers by holding your thumbs firmly against a hot iron just long enough to see the first sign of smoke.

And please do not buy any industrial hand soap from here on. Make it yourself from recycled bacon fat or simply stop washing.

[Reply](#)

Comment as:

Select profile...



[Home](#)

[Older Post](#)



Subscribe to: [Post Comments \(Atom\)](#)