Analysis of OKCoin PDF Files

A report pertaining to a commercial arrangement between OKEX Technology, Pty. Ltd. and Mr. Roger Ver in relation to the bitcoin.com domain name

Author: Ben McGinnes

Date: **28/05/2015**

Email:	ben@adversary.org
OpenPGP Key:	0x321E4E2373590E5D
Key Type:	RSA 4096 [SC] / RSA 3072 [S] / ELG-E 4096 [E]
Subkey (sign):	0x7FF2D37135C7553C
Subkey (encrypt):	0xC98BAA1862E4484D

Report URL:	http://okbounty.adversary.org/OKCoinPDFanalysis.pdf
Evidence URL:	http://okbounty.adversary.org/OKCoinPDFevidence.zip

Contents

Introduction and Disclaimer

On the 24th of this month several documents were uploaded to DropBox[1] by OKCoin[2] staff and an announcement regarding their intentions was made on the Reddit message board.[3] Though I am not a subscriber of that site, the timing of that post happened to coincide with my checking the real time stream of the #bitcoin-news[4] channel on the Freenode IRC network.[5]

Though the names of both parties involved in the dispute these documents relate to are passingly familiar to me, this has been entirely through market and news reports until now. In the case of OKCoin, this has been primarily just seeing the name appear in the live market data on #bitcoin-market[6] or other ticker data posted to #bitcoin-otc[7] or other Bitcoin related channels. With regards to Mr. Roger Ver, I have read one or two articles regarding his recent visa troubles when attempting to return to the United States. Beyond that, each of their businesses are of little familiarity. I have not been following the news regarding the current dispute and since becoming aware of it, I have only read one article on that at CoinDesk.[8]

My own trading over the past three or four years would be best described as being somewhat sporadic. Occasionally engaging a local exchange in Australia or trading directly in #bitcoin-otc.

I have not used the OKCoin trading platform for that purpose. Though, having said that, I do have an account there. That account was opened when I first visited the OKCoin website over the weekend, during an initial attempt to determine whether the Reddit post was legitimate. I was also curious about the deployment of that site. Upon receiving that confirmation I began the investigation which has resulted in this report. I have no personal stake or investment in either the OKCoin exchange or in any of Mr. Ver's enterprises. Nor do I have any involvement in any of the related companies or investments of either those two parties or those of Mr. Changpeng Zhao, the former CTO of OKCoin.

While I do not have any type of personal or commercial relationship with OKCoin, I have corresponded with Mr. Jack Liu regarding certain technical aspects of the documents and the manner in which they were transmitted between OKCoin, Mr. Zhao and Mr. Ver.

Regarding the legal issues of this situation, I have no direct opinion and while I am familiar with many aspects of Australian law, they have no bearing or relevance on this case. This report deals purely with the technical aspects of the PDFs cited by the parties involved and whether or not they are legitimate documents with a verifiable origin. The results of this technical analysis do raise questions regarding the one of these documents, particularly with regards to identity and motive. I cannot directly answer these questions, nor do I seek to. What I can do is demonstrate what the precise nature of each document is and show that the conclusions I have reached are independently verifiable.

1 https://www.dropbox.com/sh/7dudlieancb1tr0/AAA0xmqujCZsvaQ0f_Uf-03Da?dl=0
2 https://www.okcoin.com/
3 https://www.reddit.com/r/Bitcoin/comments/372nux/okcoin_offers_20000_usd_reward_for_disproving_mr/
4 http://webchat.freenode.net/?channels=#bitcoin-news
5 http://freenode.net/
6 http://webchat.freenode.net/?channels=#bitcoin-market
7 http://webchat.freenode.net/?channels=#bitcoin-otc
8 http://www.coindesk.com/roger-ver-and-okcoin-at-war-over-bitcoin-com-domain-name/

While the purely technical conclusions do leave certain questions open, there is enough information available just in the nature of these documents to disprove some of the claims which have been made by one party regarding another, as the following sections will demonstrate. It should be noted, though, that while certain specific claims can be disproved, that does not equate to confirmation that those who have made those claims did so with malicious or duplicitous intent. As I have written previously, this report draws no conclusions regarding the motives or intentions of any of the parties involved.

This report is produced entirely in my capacity as an individual IT professional and is not in any way related to my roles with other organisations or projects; including, but not limited to the GNU Privacy Guard and Pirate Party Australia.

The Documents

Seven PDF documents were posted to the DropBox folder Sunday the 24th of May, 2015. Those documents were:

1. A – Refuting allegations of forgery allegations Star Xu.pdf[9]
2. B – Mr. Ver Taking Private Dispute Public.pdf[10]
3. C – Refuting allegations of intent to money launder.pdf[11]
4. D – Bitcoin.com Operating Challenges.pdf[12]
5. E – Bitcoin.com_v7 (final) (counter-signed).pdf[13]
6. F – Bitcoin.com_v8.pdf[14]
7. G – print version.pdf[15]

The first four documents were produced very recently by an OKCoin employee, Alfred Lim. An analysis of these files is not necessary, but some aspects of them were checked during the course of the investigation as a comparison to the two documents at the centre of this dispute. Mr. Lim's documents were all produced with Microsoft Word.

The fifth and sixth documents are the focus of this investigation and are at the centre of the current allegations made by Mr. Ver against OKCoin in general and OKCoin's CEO, Mr. Star Xu, in particular. The main points of contention regarding these two documents relate to Mr. Ver's claim

9 https://www.dropbox.com/sh/7dudlieancb1tr0/AADu8LOYE3FMXh0-H9QkadVda/A%20-%20Refuting%20allegations%20of%20forgery%20allegations%20Star%20Xu.pdf?dl=0

10 https://www.dropbox.com/sh/7dudlieancb1tr0/AACJCskLShpZK5UBgQGLzdKGa/B%20-%20Mr.%20Ver%20Taking%20Private%20Dispute%20Public.pdf?dl=0

11 https://www.dropbox.com/sh/7dudlieancb1tr0/AABHBQpZZRvPKP0czOxh1_-xa/C%20-%20Refuting%20allegations%20of%20intent%20to%20money%20launder.pdf?dl=0

12 https://www.dropbox.com/sh/7dudlieancb1tr0/AACXq471bXk0iV1XceDF15EKa/D%20-%20Bitcoin.com%20Operating%20Challenges.pdf?dl=0

13 https://www.dropbox.com/sh/7dudlieancb1tr0/AADoyQyzkyz89tSEYawPFooBa/E%20-%20Bitcoin.com_v7%20%28final%29%20%28counter-signed%29.pdf?dl=0

14 https://www.dropbox.com/sh/7dudlieancb1tr0/AACqHVW-LQmD1ks5pulvg6HTa/F%20-%20Bitcoin.com_v8.pdf?dl=0

15 https://www.dropbox.com/sh/7dudlieancb1tr0/AAABg1R-n07cov4GLc4tGPx_a/G%20-%20print%20version.pdf?dl=0

that he never received a copy of the sixth document, which is sometimes referred to as document F and sometimes referred to as v8 (or the eighth version of the contract between OKCoin and Mr. Ver), and thus never signed it. Mr. Ver also alleges that document F is a forgery produced by or produced at the order of Mr. Xu. It was this last accusation, with its potential to adversely affect both Mr. Xu's professional reputation and that of OKCoin, which prompted the decision to publicly disclose the documents and to place a bounty for proof that document F was not created recently, but was actually created at the time OKCoin has previously stated, in December, 2014.

The seventh document is a scan of a physically signed contract between Mr. Ver and OKCoin. The authenticity of the scanned file is not in question, though the physical contract is apparently pending additional forensic analysis to verify that nothing was added to or removed from the contract after it was signed.

Throughout the rest of this report I will refer to each document by the letter assigned to it by Alfred Lim as this will be the most readily identifiable part of each filename utilised by any other external party seeking to reproduce the results of my analysis. I do encourage anyone to do so, particularly members of the press reporting on this and any similar cases in the future. Most of the rest of the report deals with documents E and F.

The Allegations

There are a number of allegations in the current dispute which are best left to the parties directly involved in it or to the relevant legal authorities with jurisdiction over the matters. There are, however, some allegations and assertions which can be resolved through this analysis. Those allegations are:

- That document F was produced in an identical and with the same software packages as document E.
- That the signature attributed to Mr. Ver in document F is a duplicate of the signature on document E.
- Mr. Ver's claim that document F has a forged timestamp.
  - That the December, 2014 timestamp in document F is false and that the document was produced by Mr. Xu.
  - That document F was actually produced sometime during May, 2015.

Signatures and Terminology

The signatures on documents E and F have caused some considerable consternation as well as a certain degree of confusion, at least by some of the parties involved. The confusion needs to be addressed first.

It is clear, both from the recent article at CoinDesk and some of the correspondence in relation to this matter, that some people involved are not aware of the technical differences between a digital signature and an electronic signature. The term digital signature has been used when referring to these documents when electronic signature would be far more accurate.

For reference; a digital signature is one produced by a cryptographic hash algorithm such as SHA256 or SHA512. A digital signature can be validated via the same mathematical algorithm which produced it and is a major component of cryptography.[16] An electronic signature, however, is simply a means by which a physical, hand-written signature can be applied to a document.[17] This usually involves a scan or photograph of the signature which is subsequently copied into a particular document.

Electronic signatures are extremely vulnerable to forgery as when they are used it is simply a matter of someone later copying them out of an existing document to paste into some other document. It is for this reason which some PDF software vendors, particularly Adobe, combine the electronic signatures of their users with a corresponding digital signature. That way if a document is tampered with, it will be quite obvious that this occurred. Furthermore, the lack of any kind of digital signature remaining with the electronic one or a broken digital signature would signal to a reader that the signature on question was not actually valid.

The details regarding the implementation of digital signatures within PDF documents is covered in section 12.8 of ISO 32000-1:2008, which is published by the International Organization for Standardization,[18] but made freely available in its entirety by Adobe Systems[19] on their PDF Reference page.[20]

Though the term digital signature has been used a fair bit in relation to these documents, neither document E nor F contain digital signatures. They only contain electronic signatures and as such it is quite possible for someone with access to the documents or to one of the documents to attempt a forgery based on that fact. Which is a conclusion to which Mr. Ver appears to have reached.

With regards to actual digital signatures, there may or may not have been OpenPGP signatures attached to correspondence between Mr. Ver and Mr. Zhao in December, 2014. If such correspondence exists or did exist, that correspondence is not currently publicly available so any digital signatures produced by the GNU Privacy Guard or other OpenPGP implementations cannot be independently verified. The CoinDesk news site makes reference to copies of correspondence between Mr. Ver and OKCoin which has been signed with an OpenPGP key, but does not provide

16 https://en.wikipedia.org/wiki/Digital_signature
17 https://en.wikipedia.org/wiki/Electronic_signature
18 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502
19 http://wwwimages.adobe.com/content/dam/Adobe/en/devnet/pdf/pdfs/PDF32000_2008.pdf
20 http://www.adobe.com/devnet/pdf/pdf_reference.html

any of the details of those signatures or the public key or keys used to make the signatures. Though that information is not available, document B includes an image of an email from Mr. Ver dated Sunday the 17th of May, 2015, which includes a signature.asc attachment and is often displayed by MIME capable mail clients which do not provide support for OpenPGP signatures and encryption in the standard PGP/MIME format.

There are currently six OpenPGP keys on the public key servers listed for Changpeng Zhao, of which five existed during the course of his time working at OKCoin. The sixth appears to have been generated shortly after Chinese New Year and shortly following his departure from OKCoin. The fifth was generated on the 20th of December, 2014 with a an email address at the bitcoin.com domain name. The oldest key is from 1998.

There are currently fourteen OpenPGP keys on the public key servers listed for Roger Ver and all of them existed prior to December, 2014. The oldest key is from 2011, most likely around the time of Mr. Ver's initial involvement with Bitcoin.

The PDF Structure

The File Identifier

Initial examination of the documents utilised one of the most basic, and frequently overlooked, tools available on every POSIX compliant operating system; the strings command. Note that in this usage there is no difference between the output of the unadorned strings command and using it with the -a flag. This is due to the way in which PDFs store their metadata internally. As these PDFs do not employ any built-in encryption, the strings command and other tools can be very useful in analysing them.

Even before utilising the strings command, there were a few things which stood out. Documents A, B, C and D are all PDF version 1.5 files, all produced by Microsoft Word 2010. Document G was made with Preview on OS X 10.10.2 via Quartz PDFContext and is a PDF version 1.3 file. Document E was made with RunePDF on OS X 10.9.5 via Quartz PDFContext and is a PDF version 1.3 file. Document F was made with RunePDF on OS X 10.9.5 via Quartz PDFContext and is a PDF version 1.4 file.

This discrepancy prompted a closer look at documents E and F, along with the others, to see if there were other structural differences between the two that were not simply related to content.

This is the last six lines of document E[21] when run through strings:

```
trailer
<< /Size 62 /Root 40 0 R /Info 1 0 R /ID [ <8ee9c05377ffe77f875475dccbc6d3a0>
<8ee9c05377ffe77f875475dccbc6d3a0> ] >>
startxref
323682
%%EOF
```

This is the last six lines of document G[22] when run through strings:

```
trailer
<< /Size 19 /Root 12 0 R /Info 1 0 R /ID [ <27de23be7b0d1e45d39b44b275618acd>
<27de23be7b0d1e45d39b44b275618acd> ] >>
startxref
143270
%%EOF
```

This is the equivalent last seven lines of document F[23] when run through strings:

```
trailer
<</Size 57 /Root 35 0 R /Info 1 0 R /ID [(
LK)(
LK)]>>
startxref
147568
%%EOF
```

21 http://okbounty.adversary.org/evidence/strings/Estrings.txt
22 http://okbounty.adversary.org/evidence/strings/Gstrings.txt
23 http://okbounty.adversary.org/evidence/strings/Fstrings.txt

The final number at the end is the size of the file in bytes, but it is the data in the trailer section that is interesting. The bit that is missing from document F is the file identifier. According to section 14.4 of the standard the /ID tag must be a unique identifier, independent of the file's name. In order to achieve this the standard recommends using a digital hashing algorithm to hash the following material:

- The current time.
- A string representation of the file's location, usually a pathname.
- The size of the file in bytes.
- The values of all entries in the file's document information dictionary.

The standard suggests, but does not require, using MD5 as the hashing algorithm and as a consequence MD5 is the most commonly implemented algorithm used for this purpose.[24] While MD5 is broken cryptographically, for a purpose such as this it may still serve.

Runecats Software, the producers of RunePDF, confirmed that their product did not directly manage or influence the generation of this identifier beyond the ability of content creators to set values for parts of the document information dictionary. This function is handled by the underlying Quartz 2 Core Framework within Apple's OS X operating systems. I further confirmed this with the comparison to document G and additional PDFs produced on a system running OS X 10.9.5 here, albeit not with RunePDF. The same structure with an MD5 hash is present in those cases as well, though some other software which does not rely on Quartz to produce PDFs had a little variation.

This is the last 11 lines of document A[25] when run through strings:

```
trailer
<</Size 57/Root 1 0 R/Info 15 0
R/ID[<224349EC63687D49BEC6124DAAD42A9E><224349EC63687D49BEC6124DAAD42A9E>] >>
startxref
326785
%%EOF
xref
trailer
<</Size 57/Root 1 0 R/Info 15 0
R/ID[<224349EC63687D49BEC6124DAAD42A9E><224349EC63687D49BEC6124DAAD42A9E>] /Prev
326785/XRefStm 326417>>
startxref
328083
%%EOF
```

It is unclear why Microsoft Word repeats itself here with an increase in file size, but does not appear to make much difference. It is, at least, consistent across those four documents made by Alfred Lim.

While this is the last 9 lines of a document produced using LibreOffice 4.4.3.2[26] and 4.3.7.2:

```
trailer
<</Size 313/Root 311 0 R
```

24 ISO 32000-1:2008, p. 551.

25 http://okbounty.adversary.org/evidence/strings/Astrings.txt

26 Two versions were used due to a bug in LibreOffice introduced in version 4.4.0 which prevents styles and formatting being honoured when exporting to PDF. The same is true with the writing and production of this report. https://bugs.documentfoundation.org/show_bug.cgi?id=88941

```
/Info 312 0 R
/ID [ <5AFAFAE11157366EDAACFD66917DECE6>
<5AFAFAE11157366EDAACFD66917DECE6> ]
/DocChecksum /D31543A8FE73DEA1DF0DDCF03F6A775F
startxref
140604
%%EOF
```

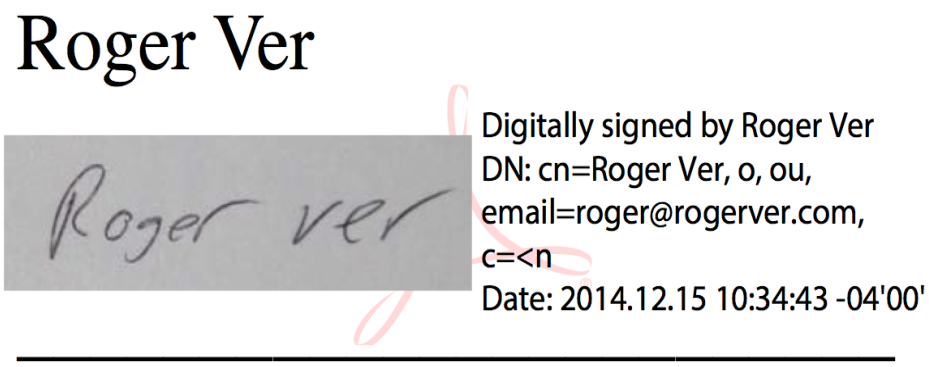
Both Microsoft Office and LibreOffice use MD5 as well, but in upper case instead of lower.

The lack of any hashed object for the file identifier for document F is a very clear indication that something non-standard had occurred with that document. Particularly by comparison to the other contract file, document E.

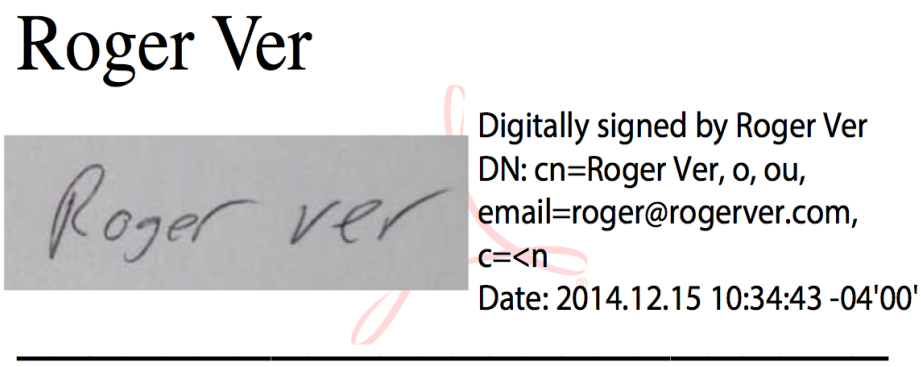
The Electronic Signature

As observed by CoinDesk, the signatures for Mr. Ver in documents E and F appear to be identical.

This is the signature as it appears in document E:[27]



This is the signature as it appears in document F:[28]



Right down to the same timestamp. Note, though that the signature is stated as being a digital signature with the Adobe watermark indicating the signature was made with Adobe Acrobat. Yet opening either document E or F in several PDF readers and editors, including Adobe Acrobat Reader DC, Preview for OS X, PDFpenPro 6.3.2 and Master PDF Editor all give no indication that there is an actual digital signature present to validate.

Either the digital component was not included originally or the signature in both documents has been doctored to remove that component. Regardless of whether there was a digital signature originally accompanying the electronic one or not, the lack of one meant there would be no alert or error messages indicating there was something wrong with the file.

27 http://okbounty.adversary.org/evidence/electronicsigs/E-RVsig.png
28 http://okbounty.adversary.org/evidence/electronicsigs/F-RVsig.png

The Timestamp

Finally there is the matter of the timestamp in document F; whether or not it has been modified in any way and, if so, whether there is any evidence of that. For this reason we need to return to the data from the strings command. The metadata for the document creation details is available at the end of the body section within the PDF structure, following the stream of the document's contents and immediately preceding the cross-reference table.[29]

```
50 0 obj
16745 endobj
51 0 obj
(Untitled)
endobj
52 0 obj
(Mac OS X 10.9.5 Quartz PDFContext)
endobj
53 0 obj
(RunePDF)
endobj
54 0 obj
(D:20141216104501Z00'00')
endobj
55 0 obj
endobj
56 0 obj
endobj
```

The timestamp is recorded in UTC by Quartz PDFContext and this format is reflected in other documents, such as document G.

```
13 0 obj
(print version.jpg)
endobj
14 0 obj
(Mac OS X 10.10.2 Quartz PDFContext)
endobj
15 0 obj
(Preview)
endobj
16 0 obj
(D:20150524074708Z00'00')
endobj
17 0 obj
endobj
18 0 obj
endobj
```

To change the creation date or apparent creation date of a PDF is, at best, difficult and not supported by most applications. There is, however, one metadata manipulation tool which can do it, possibly the only one. That tool is Phil Harvey's ExifTool.[30]

---

29 *Hidden Data and Metadata in Adobe PDF Files: Publication Risks and Countermeasures*, pp. 2-6. Enterprise Applications Division of the Systems and Network Analysis Center (SNAC), Information Assurance Directorate, National Security Agency, 2008. https://www.nsa.gov/ia/_files/app/pdf_risks.pdf

30 http://www.sno.phy.queensu.ca/~phil/exiftool/

So what happens when ExifTool is used to manipulate the creation date?

```
bash4-4.3$ exiftool "-CreateDate+=0:0:9 0:0:0" F_-_Bitcoin.com_v8.pdf
    1 image files updated
bash4-4.3$ ls
F - Bitcoin.com_v8.pdf             F_-_Bitcoin.com_v8.pdf_original
F_-_Bitcoin.com_v8.pdf             F_original_timestamp.png
bash4-4.3$ ls -l
total 1824
-rw-r--r--@ 1 ben  staff  148837 26 May 02:02 F - Bitcoin.com_v8.pdf
-rw-r--r--  1 ben  staff  149246 28 May 02:37 F_-_Bitcoin.com_v8.pdf
-rw-r--r--@ 1 ben  staff  148837 26 May 02:02 F_-_Bitcoin.com_v8.pdf_original
-rw-r--r--@ 1 ben  staff  476929 28 May 02:30 F_original_timestamp.png
bash4-4.3$ rm -f F_-_Bitcoin.com_v8.pdf_original
bash4-4.3$ mv F_-_Bitcoin.com_v8.pdf F\ -\ Bitcoin.com_v8mod.pdf
bash4-4.3$ ls -l
total 1528
-rw-r--r--@ 1 ben  staff  148837 26 May 02:02 F - Bitcoin.com_v8.pdf
-rw-r--r--  1 ben  staff  149246 28 May 02:37 F - Bitcoin.com_v8mod.pdf
-rw-r--r--@ 1 ben  staff  476929 28 May 02:30 F_original_timestamp.png
bash4-4.3$ exiftool F\ -\ Bitcoin.com_v8.pdf
ExifTool Version Number         : 9.96
File Name                       : F - Bitcoin.com_v8.pdf
Directory                       : .
File Size                       : 145 kB
File Modification Date/Time     : 2015:05:26 02:02:37+10:00
File Access Date/Time           : 2015:05:28 02:58:38+10:00
File Inode Change Date/Time     : 2015:05:28 02:30:57+10:00
File Permissions                : rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 2
Title                           : Untitled
Producer                        : Mac OS X 10.9.5 Quartz PDFContext
Creator                         : RunePDF
Create Date                     : 2014:12:16 10:45:01Z
Modify Date                     : 2014:12:16 10:45:01Z
bash4-4.3$ exiftool F\ -\ Bitcoin.com_v8mod.pdf
ExifTool Version Number         : 9.96
File Name                       : F - Bitcoin.com_v8mod.pdf
Directory                       : .
File Size                       : 146 kB
File Modification Date/Time     : 2015:05:28 02:37:53+10:00
File Access Date/Time           : 2015:05:28 02:58:49+10:00
File Inode Change Date/Time     : 2015:05:28 02:37:53+10:00
File Permissions                : rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 2
Title                           : Untitled
Producer                        : Mac OS X 10.9.5 Quartz PDFContext
Creator                         : RunePDF
Create Date                     : 2014:12:25 10:45:01Z
Modify Date                     : 2014:12:16 10:45:01Z
bash4-4.3$ ls -l
total 2480
```

```
-rw-r--r--@ 1 ben  staff  148837 26 May 02:02 F - Bitcoin.com_v8.pdf
-rw-r--r--@ 1 ben  staff  149246 28 May 02:37 F - Bitcoin.com_v8mod.pdf
-rw-r--r--@ 1 ben  staff  485345 28 May 03:03 F_changed_timestamp.png
-rw-r--r--@ 1 ben  staff  476929 28 May 02:30 F_original_timestamp.png
bash4-4.3$
```

Now viewing the modified file in a GUI PDF viewer will display a creation date of Christmas Day, 2014, even with a modified date of the 16th of December, 2014. It does look very thorough, especially if the modified date is adjusted to match.

That is, of course, until looking at the raw text data with the strings command again:

```
bash4-4.3$ strings F\ -\ Bitcoin.com_v8.pdf > F_original_strings.txt
bash4-4.3$ strings F\ -\ Bitcoin.com_v8mod.pdf > F_changed_strings.txt
bash4-4.3$ diff F_original_strings.txt F_changed_strings.txt
1985a1986,2010
> %BeginExifToolUpdate
> 1 0 obj
> /Title 51 0 R
> /Producer 52 0 R
> /Creator 53 0 R
> /CreationDate (D:20141225104501Z)
> /ModDate 54 0 R
> /Keywords 55 0 R
> /AAPL:Keywords 56 0 R
> endobj
> xref
> 0000000000 65535 f
> 0000148859 00000 n
> trailer
> /Size 57
> /Root 35 0 R
> /Info 1 0 R
> /ID [ (
> LK) (
> LK) ]
> /Prev 147568
> %EndExifToolUpdate 148837
> startxref
> 149027
> %%EOF
bash4-4.3$
```

The changed date has been inserted between the cross-reference table and the trailer section, while to original data at the end of the body remains intact and cannot be removed or modified. What happens is that it is ignored by PDF readers and not displayed, as is also the case with data objects of a version more advanced than those versions supported by the software rendering it.[31] This is explained further in the National Security Agency's *Hidden Data and Metadata in Adobe PDF Files: Publication Risks and Countermeasures* paper.[32]

31 From PDF version 1.6 this behaviour changed to remove such data rather than hiding it, but that does not apply to any of the documents examined in this report.

32 https://www.nsa.gov/ia/_files/app/pdf_risks.pdf

Conclusions

On page four of this report the allegations this investigation sought to resolve were listed. Once again they were:

- That document F was produced in an identical and with the same software packages as document E.
- That the signature attributed to Mr. Ver in document F is a duplicate of the signature on document E.
- Mr. Ver's claim that document F has a forged timestamp.
  - That the December, 2014 timestamp in document F is false and that the document was produced by Mr. Xu.
  - That document F was actually produced sometime during May, 2015.

The result of the investigation results in the conclusions that document F was either created with an entirely different software package or modified after the fact. Most likely the latter and it was this modification which resulted in the file identifier being removed from the trailer section of the PDF structure. Though the specific tool used has not yet been identified, the most likely explanation is that it was something used to manipulate the signature data in that file.

Though it is possible that the signatures attributed to Mr. Ver might have been applied by him to both documents at the same time, this is more than a little unlikely. Especially when considered in conjunction with the the evidence of document F being manipulated following its creation. It is far more likely that the two points are inextricably linked.

Finally there is the matter of whether or not the timestamp for document F has been modified. As demonstrated, while it is possible to change the creation date reported by most software, it is not possible to do so in a manner which cannot be detected. Since there is no evidence of that type of manipulation within the file, it is clear that the timestamp is accurate. The inability to remove the original metadata is further confirmed by Phil Harvey, the author of ExifTool and creator of the MIE metadata standard, on the ExifTool website.[33]

This evidence confirms the position of Star Xu and Jack Liu of OKCoin, as well as the timing of files transmitted as presented by Alfred Lim in document A. The accusations levelled against Mr. Xu by Mr. Ver are thus entirely without foundation.

While Mr. Ver has clearly been proven wrong with regards to his accusations against Mr. Xu and OKCoin, this should not be interpreted as a presumption of guilt. This report proves the veracity of the OKCoin position, it does not prove where the fault actually lies in this unfortunate affair.

Though the results of this investigation do mean a considerable narrowing of the field with regards to who modified document F and the precise nature of that modification; it is still not possible to state with absolute certainty who modified the file, why it was done or whether or not they were operating alone or in league with anyone else.

33 http://www.sno.phy.queensu.ca/~phil/exiftool/#limitations

Evidence and Files

All the evidence corroborating this report, along with the report itself is publicly available online. Additionally each file generated as part of this investigation has been digitally signed with my GPG key, in both ASCII armoured format and the GPG binary format, during the course of writing this report.

File List URLs

http://okbounty.adversary.org/OKCoinPDFanalysis.pdf
http://okbounty.adversary.org/OKCoinPDFanalysis.pdf.asc
http://okbounty.adversary.org/OKCoinPDFanalysis.pdf.sig

http://okbounty.adversary.org/OKCoinPDFevidence.zip
http://okbounty.adversary.org/OKCoinPDFevidence.zip.asc
http://okbounty.adversary.org/OKCoinPDFevidence.zip.sig

http://okbounty.adversary.org/evidence/electronicsigs/E-RVsig.png
http://okbounty.adversary.org/evidence/electronicsigs/E-RVsig.png.asc
http://okbounty.adversary.org/evidence/electronicsigs/E-RVsig.png.sig
http://okbounty.adversary.org/evidence/electronicsigs/F-RVsig.png
http://okbounty.adversary.org/evidence/electronicsigs/F-RVsig.png.asc
http://okbounty.adversary.org/evidence/electronicsigs/F-RVsig.png.sig
http://okbounty.adversary.org/evidence/exifdata/exifdata/E_exifout_default.txt
http://okbounty.adversary.org/evidence/exifdata/exifdata/E_exifout_default.txt.asc
http://okbounty.adversary.org/evidence/exifdata/exifdata/E_exifout_default.txt.sig
http://okbounty.adversary.org/evidence/exifdata/exifdata/E_exifout_dict.txt
http://okbounty.adversary.org/evidence/exifdata/exifdata/E_exifout_dict.txt.asc
http://okbounty.adversary.org/evidence/exifdata/exifdata/E_exifout_dict.txt.sig
http://okbounty.adversary.org/evidence/exifdata/exifdata/F_exifout_default.txt
http://okbounty.adversary.org/evidence/exifdata/exifdata/F_exifout_default.txt.asc
http://okbounty.adversary.org/evidence/exifdata/exifdata/F_exifout_default.txt.sig
http://okbounty.adversary.org/evidence/exifdata/exifdata/F_exifout_dict.txt
http://okbounty.adversary.org/evidence/exifdata/exifdata/F_exifout_dict.txt.asc
http://okbounty.adversary.org/evidence/exifdata/exifdata/F_exifout_dict.txt.sig
http://okbounty.adversary.org/evidence/gpgkeys/benkey.asc
http://okbounty.adversary.org/evidence/gpgkeys/benkey.gpg
http://okbounty.adversary.org/evidence/gpgkeys/czkeys.gpg
http://okbounty.adversary.org/evidence/gpgkeys/rvkeys.gpg
http://okbounty.adversary.org/evidence/okcoin-source-files.zip
http://okbounty.adversary.org/evidence/okcoin-source-files.zip.asc
http://okbounty.adversary.org/evidence/okcoin-source-files.zip.sig
http://okbounty.adversary.org/evidence/strings/Astrings.txt
http://okbounty.adversary.org/evidence/strings/Astrings.txt.asc

http://okbounty.adversary.org/evidence/strings/Astrings.txt.sig
http://okbounty.adversary.org/evidence/strings/Bstrings.txt
http://okbounty.adversary.org/evidence/strings/Bstrings.txt.asc
http://okbounty.adversary.org/evidence/strings/Bstrings.txt.sig
http://okbounty.adversary.org/evidence/strings/Cstrings.txt
http://okbounty.adversary.org/evidence/strings/Cstrings.txt.asc
http://okbounty.adversary.org/evidence/strings/Cstrings.txt.sig
http://okbounty.adversary.org/evidence/strings/Dstrings.txt
http://okbounty.adversary.org/evidence/strings/Dstrings.txt.asc
http://okbounty.adversary.org/evidence/strings/Dstrings.txt.sig
http://okbounty.adversary.org/evidence/strings/Estrings.txt
http://okbounty.adversary.org/evidence/strings/Estrings.txt.asc
http://okbounty.adversary.org/evidence/strings/Estrings.txt.sig
http://okbounty.adversary.org/evidence/strings/Fstrings.txt
http://okbounty.adversary.org/evidence/strings/Fstrings.txt.asc
http://okbounty.adversary.org/evidence/strings/Fstrings.txt.sig
http://okbounty.adversary.org/evidence/strings/Gstrings.txt
http://okbounty.adversary.org/evidence/strings/Gstrings.txt.asc
http://okbounty.adversary.org/evidence/strings/Gstrings.txt.sig
http://okbounty.adversary.org/evidence/timestamps/F - Bitcoin.com_v8.pdf
http://okbounty.adversary.org/evidence/timestamps/F - Bitcoin.com_v8.pdf.asc
http://okbounty.adversary.org/evidence/timestamps/F - Bitcoin.com_v8.pdf.sig
http://okbounty.adversary.org/evidence/timestamps/F - Bitcoin.com_v8mod.pdf
http://okbounty.adversary.org/evidence/timestamps/F - Bitcoin.com_v8mod.pdf.asc
http://okbounty.adversary.org/evidence/timestamps/F - Bitcoin.com_v8mod.pdf.sig
http://okbounty.adversary.org/evidence/timestamps/F_changed_strings.txt
http://okbounty.adversary.org/evidence/timestamps/F_changed_timestamp.png
http://okbounty.adversary.org/evidence/timestamps/F_changed_timestamp.png.asc
http://okbounty.adversary.org/evidence/timestamps/F_changed_timestamp.png.sig
http://okbounty.adversary.org/evidence/timestamps/F_original_strings.txt
http://okbounty.adversary.org/evidence/timestamps/F_original_timestamp.png
http://okbounty.adversary.org/evidence/timestamps/F_original_timestamp.png.asc
http://okbounty.adversary.org/evidence/timestamps/F_original_timestamp.png.sig

Acknowledgements

I would like to thank the staff of Runecats, who make the RunePDF software package used by OKCoin for their timely responses to my queries regarding their software and its interaction with Apple's Quartz PDFContext.

I am also grateful to Adobe Systems Incorporated for publishing the entire PDF standard on their PDF References page, even after copyright for the standard passed to the International Organization for Standardization.

I almost don't believe I'm typing this, but thanks are also due to the Enterprise Applications Division of the Systems and Network Analysis Center (SNAC), Information Assurance Directorate, National Security Agency for their *Hidden Data and Metadata in Adobe PDF Files: Publication Risks and Countermeasures* paper. This document is one of the clearest descriptions of PDF metadata available anywhere, with relevant examples of the types of data and metadata to examine. It is certainly true that, of all organisations in this world, the NSA do know a fair bit about metadata.

About this Report

This report was written and produced with GNU Emacs 24.5, LibreOffice 4.4.3.2, LibreOffice 4.3.7.2, Preview 7.0 (826.4) and PDFpenPro 6.3.2 on OS X 10.9.5. It utilises the Times New Roman and Inconsolata fonts and renders best with them.

Additional tools and software used during the course of this investigation were the strings command, ExifTool 9.96, Adobe Acrobat Reader DC, Master PDF Editor 2.2.15, DragonDisk 1.05, GPG 1.4.19 and GPG 2.1.4.

Copyright and Licensing

34 http://creativecommons.org/licenses/by-nc-nd/4.0/

About the Author

I have been involved with the PGP, and later GPG, community since the Crypto Wars in the mid-1990s. Subsequently beginning my career in IT in the late '90s. During that time I have worked for one of Australia's largest ISPs (at the time), Connect.com.au; the country's oldest IT consulting firm, Cybersource;[35] the country's largest domain registrar and hosting provider, Melbourne IT;[36] a little time in the public service and a little over a year as a Systems Engineer at Sun Microsystems, prior to the purchase of that company by Oracle. In the latter case the customers tended towards government departments and significant enterprises, including handling both law enforcement and Department of Defines cases.[37] I am currently working as a consultant providing systems administration and security research services.

My non-paying positions over the years have included two years as Vice President of Linux Users of Victoria,[38] founding member of Open Source Victoria,[39] founding member of Open Source Industry Australia[40] and co-founder of CryptoParty with Asher Wolf and Nick Jaffe. I am also the current Treasurer of Pirate Party Australia.[41] The latter is reflected in the third and fourth UIDs on my current GPG key.[42]

I have been involved in a number of free and/or open source projects over the years. Most recently in porting the PyME bindings for the GPG Made Easy API from Python 2 to Python 3 and joining the GNU Privacy Guard team as a maintainer for that and additional API related projects. I am also a member of the recently reformed OpenPGP Working Group with the IETF to revise the OpenPGP standard.

In the Bitcoin community I am generally known by my IRC handle, Hasimir,[43] which I also used on the BitcoinTalk forum; albeit not for quite some time. On the Pirate IRC Network[44] I can usually be found as either Hasimir or Ben. Like almost everyone these days, I'm on Twitter too.[45]

The GPG key used in those places is the same one this document and the related evidence files are signed with. The master key has the fingerprint "`DB47 24E6 FA42 86C9 2B4E 55C4 321E 4E23 7359 0E5D`" and the signing subkey has the fingerprint "`B7F0 FE75 9387 430D D0C5 8BDB 7FF2 D371 35C7 553C`" (some incomplete OpenPGP implementations may display a warning that the signature does not match the master key; if you see this you should raise the matter as a bug with your OpenPGP vendor).

35 http://www.cyber.com.au/
36 http://www.melbourneit.com.au/
37 https://au.linkedin.com/in/benmcginnes
38 http://www.luv.asn.au/
39 http://www.osv.org.au/
40 http://www.osia.org.au/
41 http://pirateparty.org.au/
42 http://pool.sks-keyservers.net:11371/pks/lookup?op=vindex&search=0xDB4724E6FA4286C92B4E55C4321E4E2373590E5D
43 http://bitcoin-otc.com/viewratingdetail.php?nick=Hasimir
44 http://pirateirc.net/
45 https://twitter.com/benmcginnes

