<u>IN THE HIGH COURT OF JUSTICE</u> **Claim No: IL-2021-000019**

<u>BUSINESS AND PROPERTY COURTS OF ENGLAND & WALES</u>

<u>INTELLECTUAL PROPERTY LIST (ChD)</u>

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE **<u>Claimant</u>**

-and-

DR CRAIG STEVEN WRIGHT

<u>Defendant</u>

FIFTH EXPERT REPORT
OF MR PATRICK MADDEN

RightClick Forensic

INTRODUCTION AND SUMMARY OF FINDINGS

1. This is my Fifth Report in these proceedings. I have approached it in the same way as my previous reports and with the same duties in mind. I have been instructed to prepare this report in relation to the most recently-admitted set of additional documents which Dr Wright has had permission to admit, and some aspects of Dr Wright's recently-admitted evidence commenting on matters of authenticity. Since the Court gave permission for the introduction of further documents, I have again done a lot of analysis in a short time. This has again involved a great deal of steps, checks, and avenues of investigation.

2. Although there were relatively few individual documents and relevant topics in Dr Wright's evidence, analysing them has required me to revisit the broader set of original disclosure documents and has been much more onerous than it first appeared.

3. This means I have had very little time to prepare this report, while also preparing to give evidence and attending the trial. If my reporting is brief and to the point in some parts, I ask the Court to understand that this is the reason.

4. For the purposes of this statement I have been provided with copies of:

   a. Dr Wright's Eleventh Witness Statement

   b. Dr Wright's Thirteenth Witness Statement

   c. The Sroz Friedberg Summary report dated 29/01/2024

   d. The Stroz Friedberg Summary report dated 02/02/2024

   e. Additional Documents ID_006471 through ID_006493

   f. Additional Documents ID_006564 through ID_006568

   g. The chain of custody information provided by Shoosmiths on 9 February 2024.

5. This report is divided into the following sections:

   a. Comments in Dr Wright's Eleventh Witness Statement relating to his MYOB accounts.

   b. Comments in Dr Wright's Eleventh Witness Statement relating to certain emails he analyses relating to Abacus Seychelles.

   c. The new disclosure, including the Papa Neema emails and their attachments.

   d. A check of a TulipTrading domain name not previously featured in disclosure.

e. Dr Wright's account of using the BDOPC.raw image as a virtual machine.

Summary of findings

6. In summary, I have found as follows:

a. The **MYOB software** does not behave as Dr Wright suggests in his evidence. The software appears to accurately record the database version updates. I confirmed my previous findings. The software used is correctly recorded. When updating from the pre 2016 .MYO file format to the newer post 2016 MYOX file format, the MYO file is not overwritten and lost but imported into a new MYOX file. The old MYO is retained. Updates applied periodically within the same file format are applied to the live file. It is relevant to note, that the MYOB software, like many accounting packages, regularly prompts and reminds the user to make frequent backups.

b. I do not agree with Dr Wright that the 2014 **Abacus emails** he refers to in his Eleventh Witness Statement have been fabricated. I found no reason to doubt these emails (which I have already mentioned in my First Report). On further analysis in preparing this report, I have found positive reasons to consider them to be authentic.

c. I have analysed the **papa neema** emails and consider that they do not match the time zones of sending from Kenya. I have also made various observations about the attachments. Several messages in the chain are missing from disclosure and so could not be analysed.

d. I also noticed that Dr Wright's most recent disclosure documents list an email address **craig@tuliptrading.net**. I noticed that was not one of the disclosed sources of documents in Dr Wright's disclosure, and I therefore checked the registration of the domain, which also appears to have been registered by Dr Wright around the same date as the documents referring to the purchase of the Tulip Trading company as an aged shelf company in October 2014.

e. In my opinion, the **BDOPC.raw image** was not used as (or with) the virtual machine for which Dr Wright has disclosed an incomplete set of configuration files.

MYOB DOCUMENTS

7. In Wright 11 (Section IV starting at paragraph 298 and running through to Paragraph 312 {CSW/1/55}-{CSW/1/58}), Dr Wright advances his explanation for the anomalous timestamps and other irregularities found within the two MYOB database files examined by Dr Placks and myself in our previous reports.

8. Both Dr Placks and myself confirmed for ourselves, and agreed, that the documents {ID_004077}, {ID_004078} and {ID_004079} produced from the March 2020 backup included within the disclosure dataset contain subtle but distinct content differences to the records extracted from the Live accounts to which Dr Placks was provided access (which we referred to as the "**New MYOB**" files).

9. Revisiting the analysis of my Second Report {G/3/1}, Dr Wright's explanation does not explain all of the conflicts that arise. It is not necessary for me to revisit the documents and conduct analysis, as the information is already apparent from my previous analysis as I explain further below.

Filetypes

10. Both database files analysed were the more recent .MYOX file format, and not the ".MYO" file format associated with earlier versions of the MYOB software. This is relevant because:

a. I understand that the MYOX file format was introduced in version 19.11.3 which was released in April 2016 (Source: Appendix PM42 paragraph 40, {H/209/11}-{H/209/12}).

b. The MYOB software records information very differently depending on which file format it is using, and I explained this at Paragraph 40 of Appendix PM42 to my Second Report.

c. Without repeating all that analysis, most notably there was no recording of session ID (UUIDs) in older versions of MYOB before 2016, whereas that information is recorded in new files, and the equivalent of the "Session Security Log" also did not record the same level of information in the older formats as compared to newer formats.

d. Therefore, if sessions had been created in older versions of the software prior to 2016, they would not have recorded session ID or session security logging information in the same way as a more modern version.

e. However, Dr Wright's MYOB files do contain session ID and session security information consistent with all the sessions being conducted with modern versions of the MYOB software, even those which are dated to years before the release of that software in 2016.

f. Had the content been imported from the previous MYO file format into the newer MYOX format, it would have been imported without all the audit information that is available. When an older file is opened in newer software, some records are updated or converted, but these records are not.

g. Therefore, the presence of this information in the MYOB files is consistent with them all being authored in post-2016 software, and is not consistent with them being authored in older versions of the software. This is to say that the information was not entered into an earlier version of the software and migrated into the newer version of the software.

Data not imported

11. It is also clear that the records were not imported into MYOB from another file. The records recorded within the Databases do not record a single date of entry or single session, but are added individually and iteratively as a human user would, whereas an import would be expected to write the records all at once in a single session.

12. As part of my analysis leading up to my Second Report, I analysed how the MYOB software behaved when importing data from an older MYO file into an MYOX file format.

13. Contrary to Dr Wright's explanation, the program does not upgrade the MYO file to an MYOX file. It is necessary to import the content of the MYO file into a new MYOX database. The Pre-existing MYO file remains in its original format, and a copy is imported into the new database.

14. When that is done, there is a specific entry created and logged within the Session Security log that indicates when such an import took place. There are no such entries in the MYOX databases provided for analysis. Also, all of the entries (and most anomalously of these, even those dated before April 2016) include a full SessionID as would be expected only for entries generated in the newer versions of the software which was released after April 2016.

Sequence of logins

15. Dr Wright's explanation also does not account for the time and date anomalies observed in the session security logs, in particular:

a. The extremely long login – an "*Administrator*" (which is the account that is later associated with Dr Wright's email address) logged in with a session UUID "6d01ea93-97e5-4cca-9b67-b1a709db1902" which was apparently logged in for 12 years, 9 months, 6 days and 6 minutes (signed in date 31 August 2010, signed out date 06 June 2023).

b. The out of order records in the file, which I explain below.

16. The table below is a subset of the information in Exhibit PM42.5 {H/214/1} produced with my Second Report. As I explained previously, when viewed within the MYOB software, they are sorted in time order, but viewing them in database format allows them to be sorted in the order that they were recorded in the database, ordered by "Record ID".

17. Doing so reveals that the sequence of entries does not flow forward in time, but jumps around:

Record ID	SessionId	DateOcurred	Event Type	UserName
1	b8ebb9d4-34cf-4e96-b7df-0de5edaa6772	15/08/2009 16:16	0	Administrator
2	b8ebb9d4-34cf-4e96-b7df-0de5edaa6772	15/08/2009 17:47	2	Administrator
3	ba9365e9-dffe-4e4a-a40e-28e617743f0a	13/10/2009 15:25	0	Administrator
4	ba9365e9-dffe-4e4a-a40e-28e617743f0a	13/10/2009 15:39	2	Administrator
5	fc472414-0c22-453d-911e-c86fdd09bb15	14/01/2010 01:40	0	Administrator
6	fc472414-0c22-453d-911e-c86fdd09bb15	14/01/2010 01:45	2	Administrator
7	3fa0e56a-97c4-4744-b8f2-7b3e22a3ccd0	14/01/2010 03:46	0	Administrator
8	3fa0e56a-97c4-4744-b8f2-7b3e22a3ccd0	14/01/2010 03:50	2	Administrator
9	ada42f94-3259-4b4d-aaeb-ab52856a5fb1	06/06/2023 18:18	0	Administrator
10	ada42f94-3259-4b4d-aaeb-ab52856a5fb1	06/06/2023 18:19	2	Administrator
11	c89a062a-f37f-4f19-bc34-c0b5bea6ba4a	30/06/2010 18:19	0	Administrator
12	c89a062a-f37f-4f19-bc34-c0b5bea6ba4a	30/06/2010 18:33	2	Administrator
13	ba8d548d-4716-46c0-8fbf-913c19f7ea57	01/07/2010 18:34	0	Administrator
14	ba8d548d-4716-46c0-8fbf-913c19f7ea57	01/07/2010 19:05	2	Administrator
15	4788e222-a514-4272-98a4-61a9d392139d	31/07/2010 08:06	0	Administrator
16	4788e222-a514-4272-98a4-61a9d392139d	31/07/2010 08:24	2	Administrator
17	a7deefac-324b-4c66-9eb9-9ee49ae0f44a	06/06/2023 19:28	0	Administrator
18	6d01ea93-97e5-4cca-9b67-b1a709db1902	31/08/2010 19:29	0	Administrator
19	6d01ea93-97e5-4cca-9b67-b1a709db1902	06/06/2023 19:35	2	Administrator
20	2021d86c-6123-4ad5-b788-e189f1cff6d3	31/08/2010 19:36	0	Administrator
21	2021d86c-6123-4ad5-b788-e189f1cff6d3	31/08/2010 19:46	2	Administrator
22	979e890b-bb77-4387-a7a6-df7e79555774	28/02/2011 05:24	0	Administrator
23	979e890b-bb77-4387-a7a6-df7e79555774	28/02/2011 05:47	2	Administrator
24	557e6b64-c5d0-4e9f-b2dd-b9dd9aab05a5	25/03/2011 06:25	0	Administrator
25	557e6b64-c5d0-4e9f-b2dd-b9dd9aab05a5	25/03/2011 06:32	2	Administrator
26	7c9d49b4-3a49-4da4-a9dc-6edfe6eb8ab5	04/07/2011 04:47	0	Administrator
27	7c9d49b4-3a49-4da4-a9dc-6edfe6eb8ab5	04/07/2011 05:11	2	Administrator
28	75e9a884-986f-47df-93c4-8f745645d157	04/08/2011 06:13	0	Administrator
29	75e9a884-986f-47df-93c4-8f745645d157	04/08/2011 06:14	2	Administrator
30	322cc7d7-7857-4eda-bf8f-de8e33e22246	05/08/2011 14:11	0	Administrator
31	322cc7d7-7857-4eda-bf8f-de8e33e22246	05/08/2011 14:26	2	Administrator
32	f4979318-9e43-4fd8-a300-6855132205b2	06/08/2011 03:45	0	Administrator
33	f4979318-9e43-4fd8-a300-6855132205b2	06/08/2011 03:55	2	Administrator
34	77885e63-fa7d-4dad-8f44-576e9229d7ca	08/10/2011 04:55	0	Administrator
35	77885e63-fa7d-4dad-8f44-576e9229d7ca	08/10/2011 04:56	2	Administrator
36	82206fa7-c168-4108-aef4-e1312e0af46a	22/08/2012 07:21	0	Administrator
37	82206fa7-c168-4108-aef4-e1312e0af46a	22/08/2012 07:23	2	Administrator
38	7f9c960d-34df-40ba-a55f-1cf41fb3c254	22/05/2013 17:36	0	Administrator
39	7f9c960d-34df-40ba-a55f-1cf41fb3c254	22/05/2013 17:39	2	Administrator
40	16d4e4a2-1457-4803-ac33-9b28a00ce36b	05/02/2020 07:10	0	Administrator
41	42970b29-e8e9-4489-9c2b-42d585f5153b	15/04/2020 03:11	0	Administrator
42	a2ef72d1-dd89-448c-9138-ecd9313af178	07/06/2023 05:20	0	Administrator
43	a2ef72d1-dd89-448c-9138-ecd9313af178	07/06/2023 05:26	2	Administrator
44	e9107c87-d764-4f75-8554-ca19a1a3e00e	07/06/2023 05:26	0	Administrator
45	e9107c87-d764-4f75-8554-ca19a1a3e00e	07/06/2023 05:31	2	Administrator

18. It is noteworthy that the four entries dated 06 June 2023 that are out of sequence (Record IDs 9, 10, 17 and 19) are one day before 07 June 2023 after which there are no further timestamps that are out of sequence in the remaining 459 records.

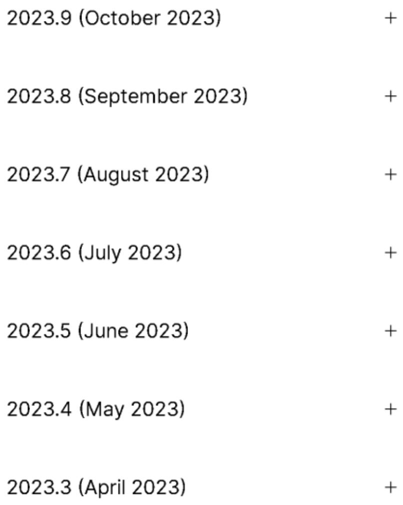
<u>Software version recording</u>

19. At Paragraph 56 of my Second Report, I have produced the content of the DbVersionInfo records table within the New WIIL MYOB file. I reproduce this table below:

Record ID	Change Ctr	DateCreated	Feature SetMask	Product Version	Schema Major Version	Schema Minor Version
1		15/08/2009 17:16	0	2023.4.1.6	251	1
2		14/06/2023 19:21	0	2023.5.1.4	252	1
3		02/08/2023 10:01	0	2023.6.1.3	253	1
4		02/08/2023 10:01	0	2023.6.1.3	254	1
5		30/08/2023 17:57	0	2023.7.1.3	255	1
6		21/09/2023 17:02	0	2023.8.1.2	256	1

20. This table logs the different program versions used to open the database, and tracks the dates of progressive updates applied. As observed in my Second Report, the first record is dated 15 August 2009 at 17:16, which correlates with the timestamp applied to the first recorded log on to the database; however, (in stark contradiction) that entry is authored with the software product version dating to "2023.4.1.6".

21. The versions of MYOB software currently available on their website is as follows:



2023.9 (October 2023) +

2023.8 (September 2023) +

2023.7 (August 2023) +

2023.6 (July 2023) +

2023.5 (June 2023) +

2023.4 (May 2023) +

2023.3 (April 2023) +

22. By downloading the installation files for each of these versions[1] and cataloguing the timestamps of their internal Digital Signatures, it is possible to see when each was created and to see that they increment consistently upward over time, in the way that is to be expected:

Download Program Version	Timestamp of the Digital signature in the software
2023.4.1.6	10/05/2023 07:36
2023.5.1.4	05/06/2023 03:01
2023.6.1.4	04/07/2023 11:05
2023.7.1.5	08/08/2023 07:32
2023.8.1.2	01/09/2023 11:25

23. It can be seen that the BDVersionInfo versions are updated at a time that follows the update of each release.

24. Notably, the use of later software has not caused the earlier records to be updated. These reflect the version of the software used to author the entries at those times, not the version of the software used to view them later.

25. This is in contrast to paragraph 302 onwards of Dr Wright's Eleventh Witness Statement {CSW/1/56}, where he appears to suggest that the version of the software to which Alix Partners were provided access in 2019 would not be reflective of the file's status in 2023. While software updates may occur and affect the general appearance of the program windows used to view the files, it cannot be responsible for the differences in content of the database itself, in which the past activity is logged.

26. I have considered the update process described by Dr Wright. Though it is not entirely clear, I believe that the process described by Dr Wright in paragraph 305 {CSW/1/57} relates primarily to offline local files, and not online stored databases. However, this does not affect my analysis or conclusions.

27. Similarly, paragraphs 308 to 312 {CSW/1/58} did not contain any information which affects my conclusions or analysis.

[1] I note that in two cases, the sub-version number available now does not quite match the sub-version used in Dr Wright's MYOB file (for example, Dr Wright's file used 2023.6.1.3 but the version currently available for download is 2023.6.1.4. I do not think this makes a difference to the analysis, as the analysis is based on the versions used and the consistent ordering in time.

Conclusion on MYOB

28. As demonstrated above, Dr Wright's explanation does not account for how a 2023 version of the software can exhibit an August 2009 database creation date. The various updates recorded thereafter appear to be correctly timestamped. In my opinion the explanations provided do not explain the functioning of MYOB's product and do not account for the anomalies observed, which are consistent with backdating of the accounting records concerned.

ABACUS EMAILS: ID_001414 AND RELATED DOCUMENTS

29. From Paragraph 42 to 53 of his Eleventh Statement {CSW/1/8}-{CSW/1/11}, Dr Wright discusses his own analysis regarding the document {ID_001414} within his disclosure dataset. Dr Wright refers to {ID_001414} as an example of a 'fabricated' email from Ira Kleiman, and refers to two pieces of evidence to support this:

a. DNS Records for the domain abacus-offshore.com, and

b. The DKIM authentication header for {ID_001414}.

Already found to be not-altered in first report

30. {ID_001414} is an email from the original disclosure dataset, VOL001. On Page 18 of Appendix PM14 {H/73/16}, I showed a picture of the content of that email in the form of {ID_001396}, which is a duplicate of the same email.

31. I analysed {ID_001396} from paragraphs 52 to 55 of Appendix PM14 {H/73/18}-{H/73/19}, and concluded that I found no technical irregularities in it, and that it did not appear to have been altered.

32. However, {ID_001396} is not a hash-identical copy. It contains some internal differences which are not relevant to this analysis, but I compared the two closely to make sure that there were no other differences which are relevant. I found that:

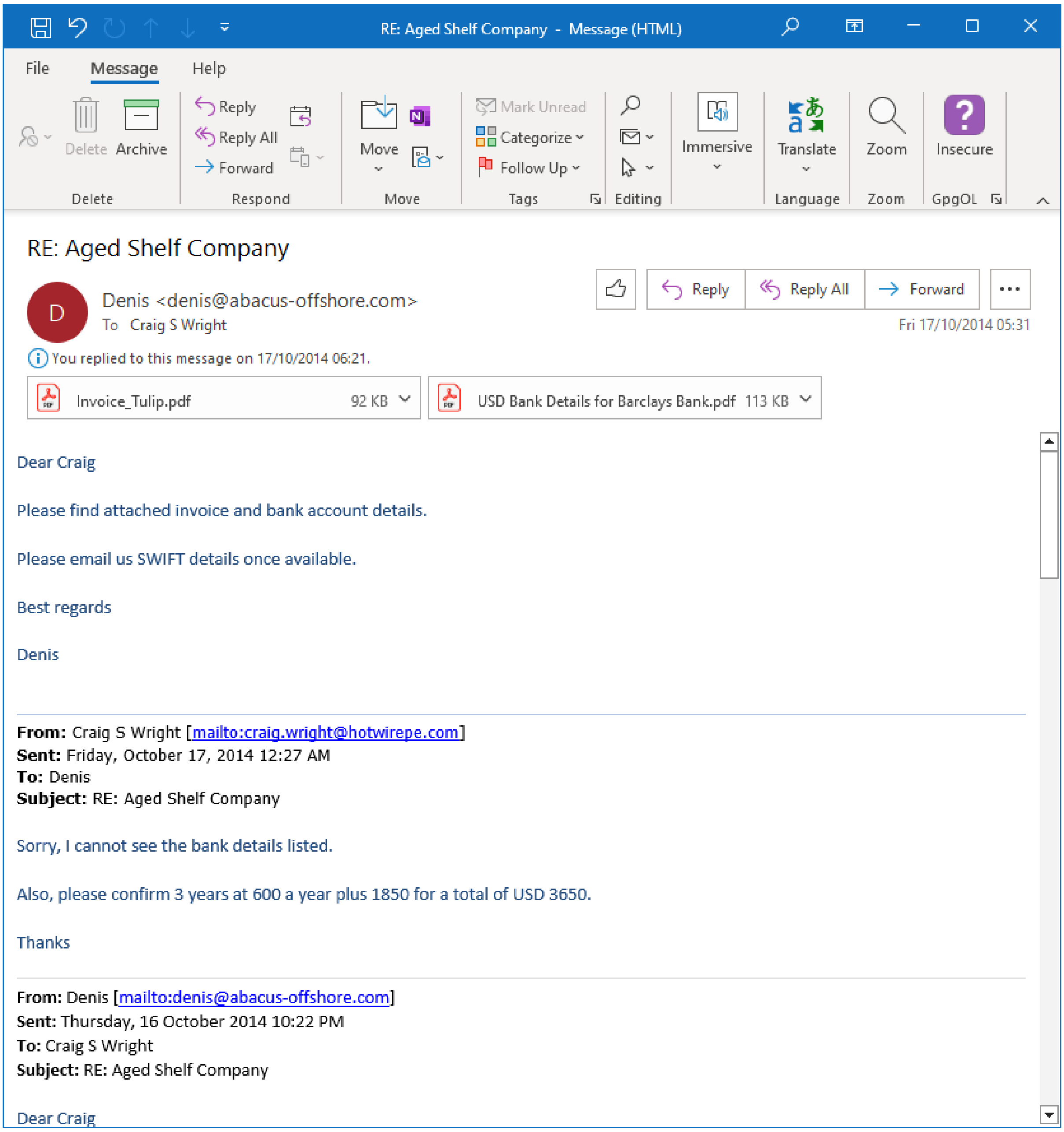
a. The transmission headers are identical between the two emails;

b. The message bodies are identical between the two emails;

c. The two attachments are identical between the two emails;

d. There are differences between the two documents in relation to Outlook specific metadata, and presentation.

33. The document {ID_001396} presents as follows:



RE: Aged Shelf Company

Denis <denis@abacus-offshore.com>
To Craig S Wright

Reply Reply All Forward

Fri 17/10/2014 05:31

You replied to this message on 17/10/2014 06:21.

Invoice_Tulip.pdf 92 KB

USD Bank Details for Barclays Bank.pdf 113 KB

Dear Craig

Please find attached invoice and bank account details.

Please email us SWIFT details once available.

Best regards

Denis

From: Craig S Wright [mailto:craig.wright@hotwirepe.com]
Sent: Friday, October 17, 2014 12:27 AM
To: Denis
Subject: RE: Aged Shelf Company

Sorry, I cannot see the bank details listed.

Also, please confirm 3 years at 600 a year plus 1850 for a total of USD 3650.

Thanks

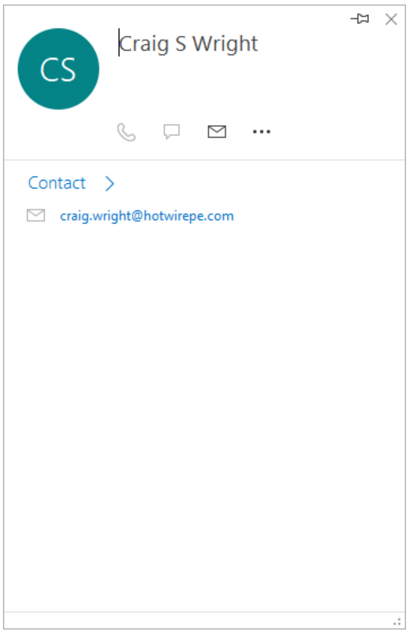
From: Denis [mailto:denis@abacus-offshore.com]
Sent: Thursday, 16 October 2014 10:22 PM
To: Craig S Wright
Subject: RE: Aged Shelf Company

Dear Craig

34. I observe that,

a. it includes an indication that “You replied to this message on 17/10/2014 at 06:21”

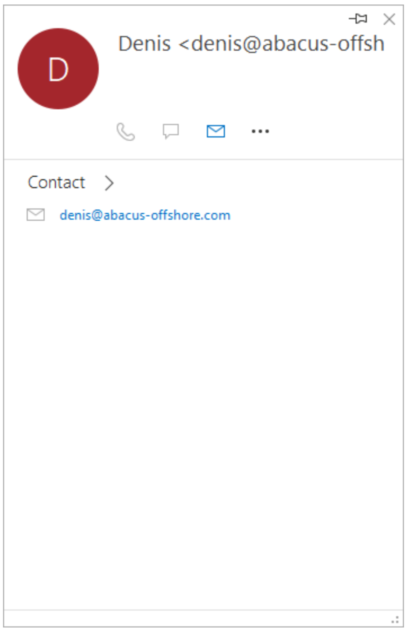
b. the email addresses for sender and recipient present normally, and that they present an address popup window when hovered over as shown below:



Craig S Wright

Contact

craig.wright@hotwirepe.com

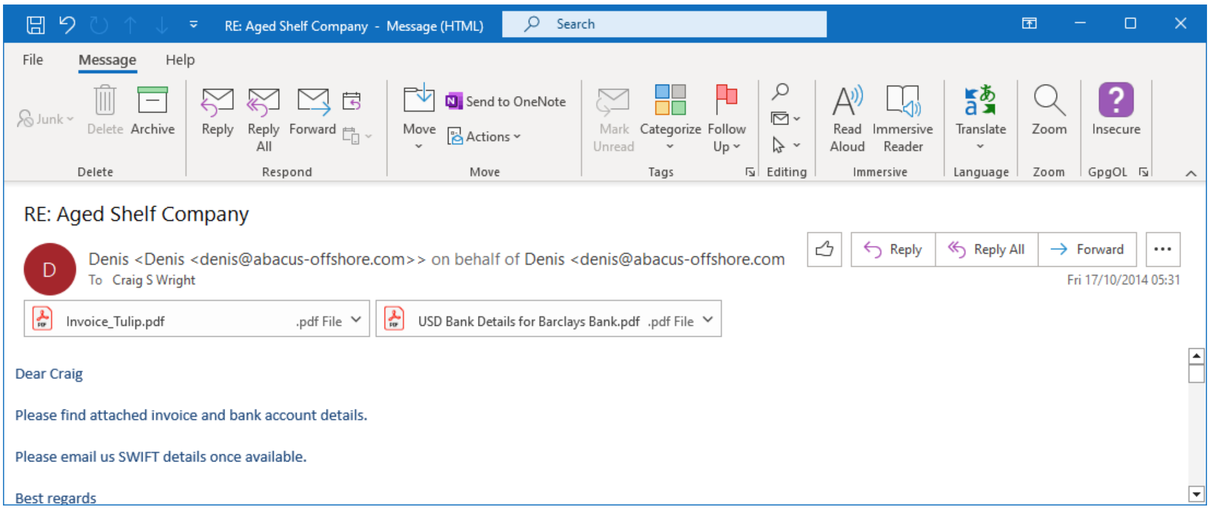


Denis <denis@abacus-offsh

Contact

denis@abacus-offshore.com

35. By contrast the email message {ID_001414} exhibits some abnormalities. As shown below it exhibits the irregular "on behalf of" characteristic seen with some other email documents within the disclosure dataset:



RE: Aged Shelf Company

Denis <Denis <denis@abacus-offshore.com>> on behalf of Denis <denis@abacus-offshore.com

To Craig S Wright

Fri 17/10/2014 05:31

Invoice_Tulip.pdf .pdf File

USD Bank Details for Barclays Bank.pdf .pdf File

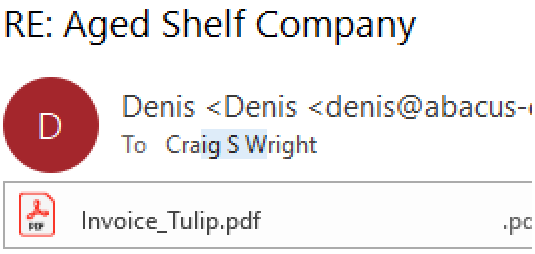
Dear Craig

Please find attached invoice and bank account details.

Please email us SWIFT details once available.

Best regards

36. While both email addresses in the 'From' field produce an address popup window, the recipient address is unavailable and is selectable as plain text as below, a characteristic also seen with some other irregular emails:



RE: Aged Shelf Company

Denis <Denis <denis@abacus-

To Craig S Wright

Invoice_Tulip.pdf .pc

37. Returning to {ID_001396}, inspecting the Outlook specific metadata I confirmed the internal metadata timestamps as follows. The PR_Creation_Time and PR_Last Modification timestamps are consistent with the email message having been exported from MS Outlook into an individual MSG file just under an hour after it was authored and sent:

Record	GMT timestamp
PR_CLIENT_SUBMIT_TIME	04:30, 17/10/2014
PR_CREATION_TIME	05:22, 17/10/2014
PR_LAST_MODIFICATION_TIME	05:22, 17/10/2014
PR_MESSAGE_DELIVERY_TIME	04:30, 17/10/2014

38. The manner in which this was conducted has preserved the content of the email message, and other metadata pertinent to the message, such as the record that the email had been replied to just under an hour after it was sent ("You replied to this message on 17/10/2014 at 06:21").

39. While I discuss the content of the message in more detail below, I cannot find a reason to doubt the authenticity of this document.

40. The same cannot be said for ID_001414, which has the following timestamps recorded in the file:

Record	GMT timestamp
PR_CLIENT_SUBMIT_TIME	04:30, 17/10/2014
PR_CREATION_TIME	22:43, 08/08/2019
PR_LAST_MODIFICATION_TIME	22:43, 08/08/2019
PR_MESSAGE_DELIVERY_TIME	04:30, 17/10/2014

41. I observe that in addition to the anomalous presentation of the email sender and recipient fields, and the omission of the Replied to record, {ID_001414} has also had some other timestamps removed or obscured.

42. Considering these points {ID_001414} appears to have been handled poorly and not to be a good forensic copy of the email, and I do not consider that the .MSG file is an ideal contender for forensic examination. Had it not been for the presence of {ID_001396} within the disclosure dataset, I would have assessed the .MSG file {ID_001414} as unreliable and likely contaminated during the preservation or processing stages.

Chain of custody information

43. The chain of custody information provided in relation to these two files is as follows:

Document ID	Devices/accounts from which obtained	Date of collection	Collector
ID_001396 AP ref: F0030927-0001-01	Unknown	Date unknown: Data collected by ATO and provided to eLaw/LaxonLex. 21 May 2019 - Data transferred to AlixPartners via Box from eLaw as a production set and loaded directly to Relativity	eLaw
ID_001414 AP ref: E0030531-0001-01	Laptop – ASUS R552J – System Serial Number - DAN0CY467767442 with 1500 GB capacity Custodian: Bobby Wilson, Hotwire PE	4 February 2019	AlixPartners Note: Contains encrypted Bitlocker partition protected with unknown credentials, other partitions (including user partition) are not encrypted and appear readable; HW0327 BOBBY WILSON HOTWIREPE. Drive removed from laptop and imaged using a Tableau TD2u write blocker to encrypted disk. Laptop remained on site.

44. Of these,

a. For {ID_001414}, the information provided indicates that the anomalous timestamps are likely the result of handling errors after collection, and may relate to how the emails were handled after the imaging of the drive. It appears to have been exported in a way that did not preserve it forensically intact, causing metadata to be overwritten and/or lost.

b. For {ID_001396}, the information provided indicates that it was collected by the ATO which I understand to be in connection with earlier litigation, and the metadata does seem to have been preserved.

Dr Wright's analysis of the Transmission header of the email

45. I do not agree with Dr Wright's analysis of this email (in either of its forms) for the reasons set out below.

46. The portion of the email message that Dr Wright used for his analysis is the Transmission header. I have established that this was identical between {ID_001396} and {ID_001414}. Although {ID_001414} exhibits differences in other areas, those do not affect Dr Wright's analysis or mine.

47. Dr Wright has not shown the plain text of the Transmission header of the email message, but has used a method available in MS Outlook. This is that he has opened the document using MS Outlook, and he has clicked on "File" and the "Properties" to produce a copy of the screenshot

that follows paragraph 43 on his Eleventh Witness Statement {CSW/1/8}. This is an acceptable way to view a Transmission header.

48. I agree that the Transmission header indicates that the email was transmitted by abacus-offshore.com using Google email infrastructure. There are several indicators of this within the Transmission header.

49. The below extract from the Transmission header relates to the first hop or transmission step that the email undertook. This record is the equivalent to that found in many email messages sent by Dr Wright's email accounts within the disclosure dataset. Highlight added to aid review.

```
Received: from LP1SEYAB ([41.79.60.178])          by mx.google.com with ESMTPSA
 id q5sm189766wja.49.2014.10.16.21.30.36          for
 <craig.wright@hotwirepe.com>          (version=TLSv1
```

50. Looking at the highlighted portions:

a. It was authored on a computer named "LP1SEYAB" that was assigned the Internet IP address "41.79.60.178". This is consistent with the apparent origin.

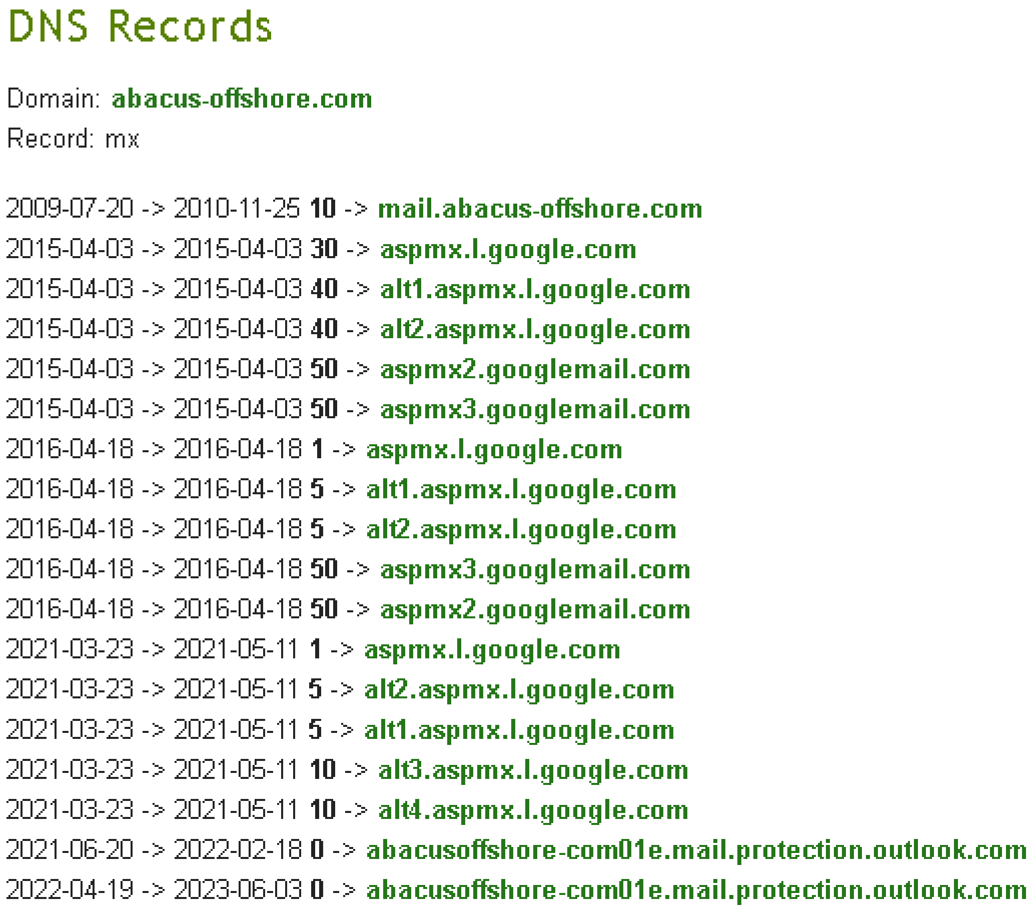
b. I observe that the first external server to handle the message is recorded as "mx.google.com", which is consistent with an email sent via Google infrastructure.

c. I note that the highlighted timestamp, 21:30.36 on 16 October 2014 recorded with a -0700 PDT timezone elsewhere in the header.

<u>Dr Wright's analysis of DNS records</u>

51. Dr Wright has visited the website of dnshistory.org to inspect the records held for the "abacus-offshore.com" domain. I produce below a more easily read list of the records that DNS History hold for the domain.

52. The "MX" Record for a domain is used to indicate where (to what server) email for the specified email domain should be sent.



DNS Records

Domain: **abacus-offshore.com**
Record: mx

```
2009-07-20 -> 2010-11-25 10 -> mail.abacus-offshore.com
2015-04-03 -> 2015-04-03 30 -> aspmx.l.google.com
2015-04-03 -> 2015-04-03 40 -> alt1.aspmx.l.google.com
2015-04-03 -> 2015-04-03 40 -> alt2.aspmx.l.google.com
2015-04-03 -> 2015-04-03 50 -> aspmx2.googlemail.com
2015-04-03 -> 2015-04-03 50 -> aspmx3.googlemail.com
2016-04-18 -> 2016-04-18 1 -> aspmx.l.google.com
2016-04-18 -> 2016-04-18 5 -> alt1.aspmx.l.google.com
2016-04-18 -> 2016-04-18 5 -> alt2.aspmx.l.google.com
2016-04-18 -> 2016-04-18 50 -> aspmx3.googlemail.com
2016-04-18 -> 2016-04-18 50 -> aspmx2.googlemail.com
2021-03-23 -> 2021-05-11 1 -> aspmx.l.google.com
2021-03-23 -> 2021-05-11 5 -> alt2.aspmx.l.google.com
2021-03-23 -> 2021-05-11 5 -> alt1.aspmx.l.google.com
2021-03-23 -> 2021-05-11 10 -> alt3.aspmx.l.google.com
2021-03-23 -> 2021-05-11 10 -> alt4.aspmx.l.google.com
2021-06-20 -> 2022-02-18 0 -> abacusoffshore-com01e.mail.protection.outlook.com
2022-04-19 -> 2023-06-03 0 -> abacusoffshore-com01e.mail.protection.outlook.com
```

53. The records presented there are broken down into time periods:

a. The first line covers a period from 20 July 2009 to 25 November which did not relate to Google.

b. There is then a gap covering some 4 years and five months.

c. The second to sixth lines show that on 03 April 2015 onwards, there were several records active all relating to Google.

d. Further gaps follow, and the same Google servers are present on further snapshots, dated 18-04-2016 and 23-03-2021.

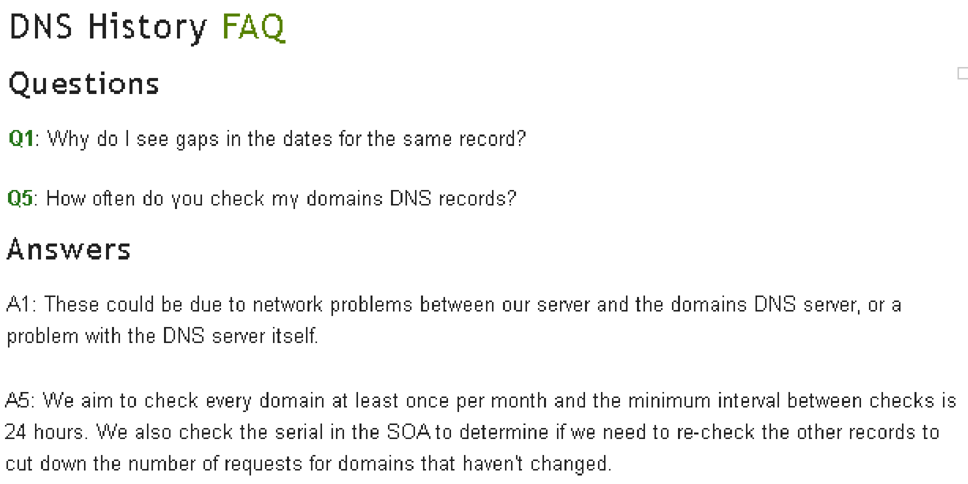
e. By 2021, Abacus appears to have moved to an Outlook.com mail server.

54. The records provided are not a complete record of servers used at all times, but are informed by snapshots taken by the relevant service. The presence of gaps does not indicate that there was no mail sever in use at the time, merely that the mail server at that time is not known.

55. This is a common approach taken for such a server history, and such records cannot be assumed to be a complete audit trail. Different vendors of DNS history information offer services such as

collating such a catalogue of historic information, gathered by performing periodical checks of each address record, and recording what the settings were at the time of a check. If a check is not conducted, or fails to complete for whatever reason, the recorded records would be expected to be incomplete.

56. This is also highlighted on the FAQ page of that website, a screenshot of which is below (showing the relevant questions and answers, which are numbers 1 and 5). This explains that it is possible for there to be gaps in records due to network issues or problems with servers:



DNS History FAQ

Questions

Q1: Why do I see gaps in the dates for the same record?

Q5: How often do you check my domains DNS records?

Answers

A1: These could be due to network problems between our server and the domains DNS server, or a problem with the DNS server itself.

A5: We aim to check every domain at least once per month and the minimum interval between checks is 24 hours. We also check the serial in the SOA to determine if we need to re-check the other records to cut down the number of requests for domains that haven't changed.

57. As such, although Dr Wright concludes that Abacus had not yet moved to Google servers by 2014, in my opinion that is an unsafe assumption. What these records indicate is that Abacus appears to have adopted Google mail servers at some point between 20 July 2009 and 3 April 2015.

58. That is consistent with the content of {ID_001396} and {ID_001414} and not a reason to call its content into doubt.

59. I note that in the Stroz Friedberg report dated 02 February 2024 {AB-D/5/4} they state that:

a. “The screenshot does indicate that for the ‘abacus’ domain in question the MX server used was changed on 2015-04-03 to google.com and prior to that date was a likely a private email server.”, and

b. “While the MX records do display the dates of DNS record changes and updates, we can only observe from the MX DNS records for ‘abacus-offshore.com’ that between 2009-07-20 and 2010-11-25 the domain used was ‘mail.abacus-offshore.com’ and starting on 2015-04-03 they began using the domain ‘aspmx.l.google.com’.

60. I do not agree with that summary for the reasons set out above. The server used was changed at some point on or before 2015-04-03 (rather than starting on that date). It is not possible to determine what the MX Record configuration was in the gap period before 2015, as it is not recorded.

61. I also note that the work undertaken by Stroz Friedberg does not appear to have been based on access to the actual email item, or the Transmission header, and it appears from their statement that they were only provided with the conclusions expressed in Dr Wright's Eleventh Witness Statement. If that is the case, it would heavily restrict their ability to analyse it.

Dr Wright's screenshot of MX data

62. In Paragraph 48 of his Eleventh Witness Statement (CSW/1/10), Dr Wright introduces a screenshot from the website osint.sh that he describes as being *"…the mx or mail exchange DNS records associated with the Abacus email domain*". To be clear, the records shown are not MX records and do not relate to the delivery of email. The records shown are the DNS record for the domain as shown in the address bar "osint/sh/dnshistory/"

63. These records also exhibit an absence of records between 25 November 2010 and 03 April 2015.

64. I observe that there is a further gap in the period from November 2016 to April 2021, which cannot be reliably accounted for from these records.

65. By my reading of his statement, it appears that Dr Wright is attaching a correlation between the change in DNS records to "GoDaddy.com" with the change in MX Records to the Google services as a firm indication of the date when the configuration changes were made.

66. While it is not uncommon practice to migrate multiple services at the same time, it is also not necessary to do so. As a result it cannot safely be assumed that because one service was migrated, the other must have been at the same time.

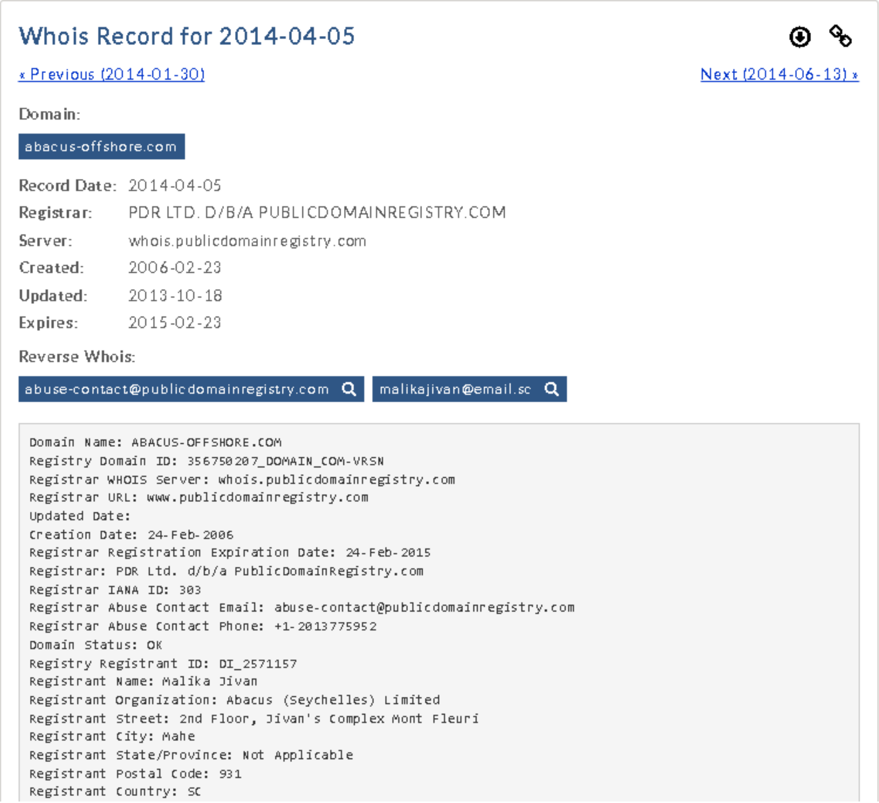
Cross checking with other records

67. Considering these gaps, I investigated the historic MX and DNS records for the domain with other available resources. I have been unable to locate any records that can be used to confirm when the MX records were changed to redirect email to the Google servers as opposed to the private "mail.abacus-offshore.com" server. However, some related and more reliable information can be obtained by looking at the domain registrar information, which can be purchased from the website DomainTools. I have done this in relation to the domain "abacus-offshore.com", and found as follows:

a. The domain registrar information was created in February 2006 and has been updated multiple times since then, as also seen in the following two screenshots:

b. Up to 13 June 2014 the registrar was recorded as being "PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM".

c. This then changed at some point between 05 April 2014 and 13 June 2014, when the domain registrar was changed to GoDaddy.



Whois Record for 2014-04-05

« Previous (2014-01-30) Next (2014-06-13) »

Domain:

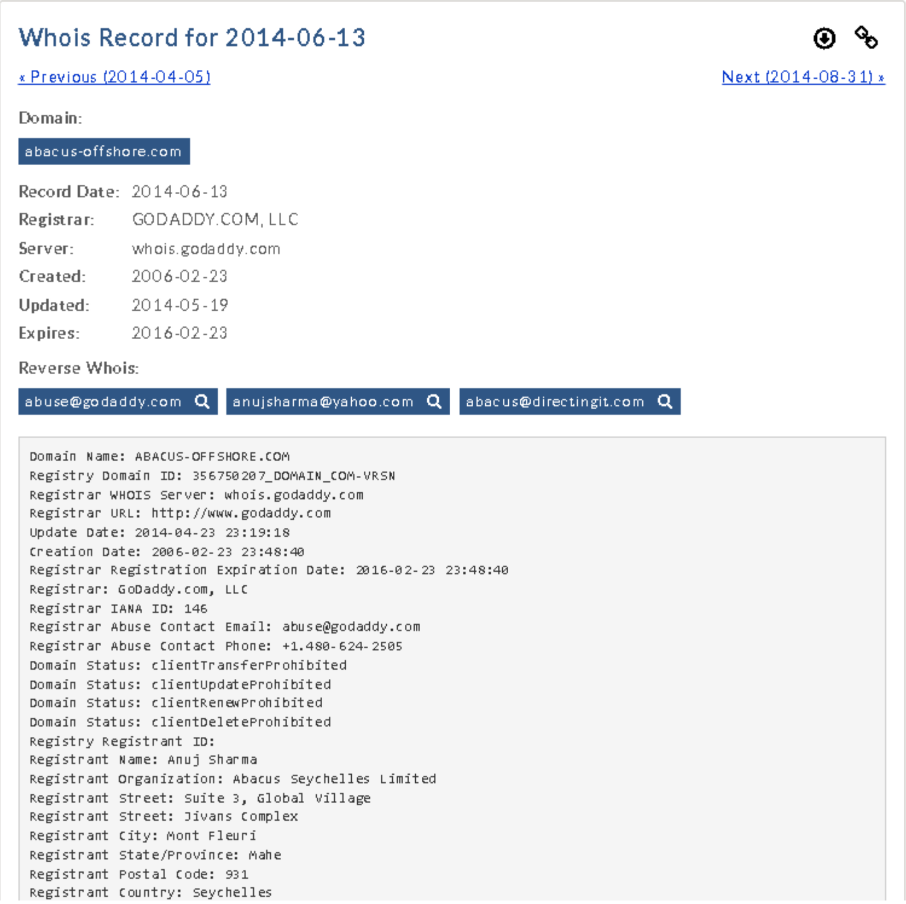
abacus-offshore.com

Record Date: 2014-04-05
Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Server: whois.publicdomainregistry.com
Created: 2006-02-23
Updated: 2013-10-18
Expires: 2015-02-23

Reverse Whois:

abuse-contact@publicdomainregistry.com malikajivan@email.sc

```
Domain Name: ABACUS-OFFSHORE.COM
Registry Domain ID: 356750207_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date:
Creation Date: 24-Feb-2006
Registrar Registration Expiration Date: 24-Feb-2015
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1-2013775952
Domain Status: OK
Registry Registrant ID: DI_2571157
Registrant Name: Malika Jivan
Registrant Organization: Abacus (Seychelles) Limited
Registrant Street: 2nd Floor, Jivan's Complex Mont Fleuri
Registrant City: Mahe
Registrant State/Province: Not Applicable
Registrant Postal Code: 931
Registrant Country: SC
```



Whois Record for 2014-06-13

« Previous (2014-04-05)

Next (2014-08-31) »

Domain:

abacus-offshore.com

Record Date:	2014-06-13
Registrar:	GODADDY.COM, LLC
Server:	whois.godaddy.com
Created:	2006-02-23
Updated:	2014-05-19
Expires:	2016-02-23

Reverse Whois:

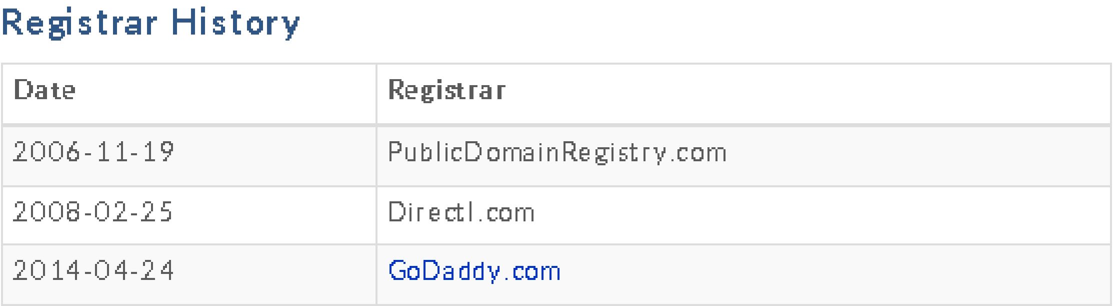
abuse@godaddy.com

anujsharma@yahoo.com

abacus@directingit.com

```
Domain Name: ABACUS-OFFSHORE.COM
Registry Domain ID: 356750207_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2014-04-23 23:19:18
Creation Date: 2006-02-23 23:48:40
Registrar Registration Expiration Date: 2016-02-23 23:48:40
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.480-624-2505
Domain Status: clientTransferProhibited
Domain Status: clientUpdateProhibited
Domain Status: clientRenewProhibited
Domain Status: clientDeleteProhibited
Registry Registrant ID:
Registrant Name: Anuj Sharma
Registrant Organization: Abacus Seychelles Limited
Registrant Street: Suite 3, Global Village
Registrant Street: Jivans Complex
Registrant City: Mont Fleuri
Registrant State/Province: Mahe
Registrant Postal Code: 931
Registrant Country: Seychelles
```

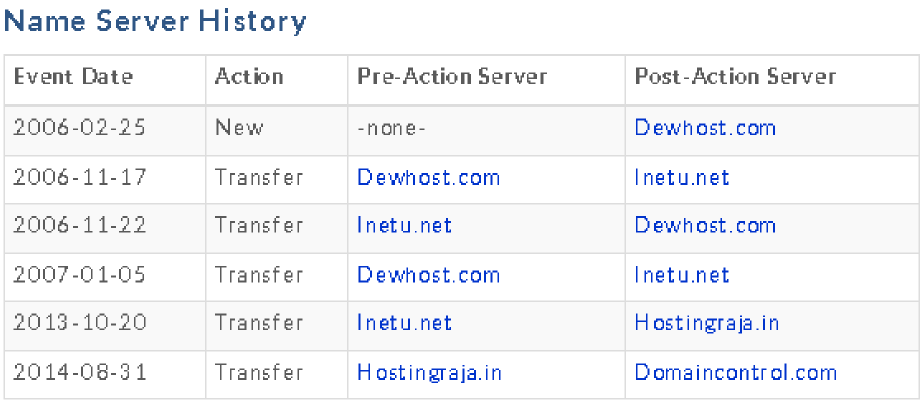
68. Domain Tools has further information indicating that the registrar history was updated to GoDaddy.com by 24 April 2014 as follows. At the time of writing, GoDaddy is still the active registrar:



Registrar History

Date	Registrar
2006-11-19	PublicDomainRegistry.com
2008-02-25	Directl.com
2014-04-24	GoDaddy.com

69. DomainTools has also recorded a Name Server change with a record dated 31 August 2014:

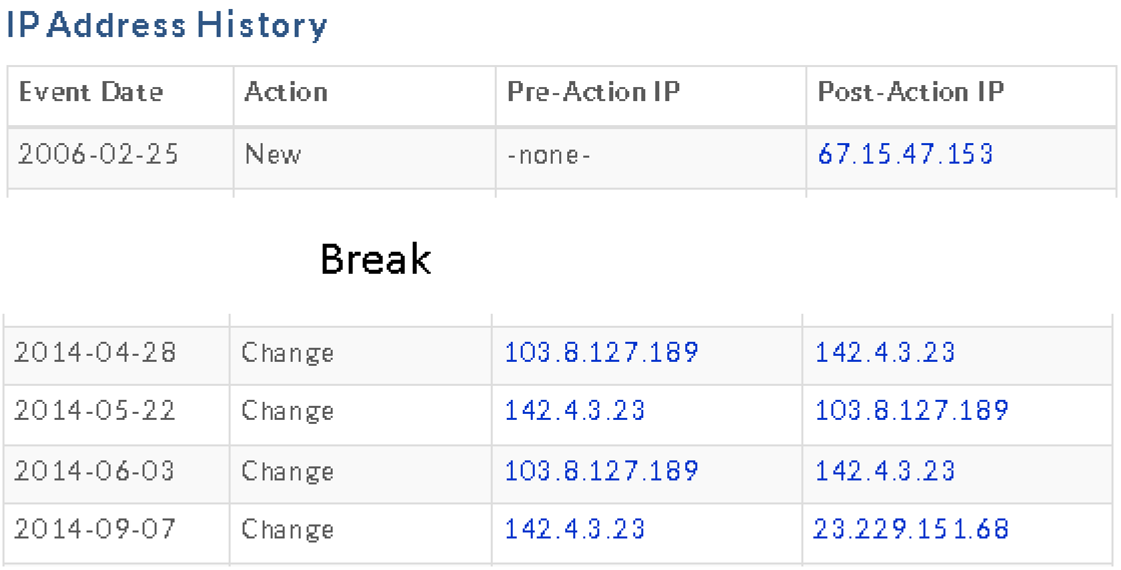


Name Server History

Event Date	Action	Pre-Action Server	Post-Action Server
2006-02-25	New	-none-	Dewhost.com
2006-11-17	Transfer	Dewhost.com	Inetu.net
2006-11-22	Transfer	Inetu.net	Dewhost.com
2007-01-05	Transfer	Dewhost.com	Inetu.net
2013-10-20	Transfer	Inetu.net	Hostingraja.in
2014-08-31	Transfer	Hostingraja.in	Domaincontrol.com

70. The server "Domaincontrol.com" is associated with GoDaddy and is therefore consistent with the other records. The available records indicate that the Name Server records were changed from "Hostingraja.in" to "Domaincontrol.com" on 31 August 2014.

71. The IP Address history recorded by Domain Tools lists the following (I have inserted a break where I have excluded a volume of irrelevant changes):



IP Address History

Event Date	Action	Pre-Action IP	Post-Action IP
2006-02-25	New	-none-	67.15.47.153

Break

Event Date	Action	Pre-Action IP	Post-Action IP
2014-04-28	Change	103.8.127.189	142.4.3.23
2014-05-22	Change	142.4.3.23	103.8.127.189
2014-06-03	Change	103.8.127.189	142.4.3.23
2014-09-07	Change	142.4.3.23	23.229.151.68

72. The last IP address shown, 23.229.151.68, relates to GoDaddy.com and is therefore consistent with the other records.

73. This therefore indicates that the change to GoDaddy infrastructure to which Dr Wright refers in his Eleventh Witness Statement, (and which I understand he is relating to the change in MX Records to the Google services) took place at least as early as April 2014, and not in 2015 as Dr Wright suggests. If Dr Wright is correct that the use of Google mail servers took place at the same time as the change to GoDaddy servers, that is entirely consistent with the emails in question being authentic.

74. While I reiterate that these services are different services to MX records and so do not relate directly to the mailing server, they do provide information against which to check the MX records. All the records that are available indicate that a general infrastructure change for Abacus took place around approximately July or August 2014.

75. Based on the information available, the use of Google infrastructure to send the email (whether the copy {ID_001396} or the copy {ID_001414}) would have been expected to result in the observed characteristics and do not call its authenticity into doubt. This is therefore consistent with the authenticity of the email {ID_001396} (which is materially the same as {ID_001414}), but it has not been possible to obtain a reliable indicator of when the MX records for "abacus-offshore.com" themselves changed during the period of the long gap in Dr Wright's screenshot record.

76. It has however been possible to verify the authenticity of the emails themselves by other means as I explain further below.

DKIM Signatures

77. At paragraph 50 of his Eleventh Witness Statement {CSW/1/10}, Dr Wright suggests that the DKIM field of the email {ID_001414} would not verify, such that it must be an inauthentic email. I consider this to be an unsound conclusion regarding the DKIM signatures.

78. A DKIM signature, "DomainKeys Identified Mail", is a method for email verification at the time of receipt of an email.[2] DKIM, like SPF (which I have explained in Appendix PM21 {H/104/7}), are primarily used to detect spam or spoofing. While they can be useful for forensic analysis in certain circumstances, there are considerations that need to be born in mind:

a. The primary use of DKIM signatures is at the time an email is transmitted. This verification involves checking a cryptographic signature in the DKIM field against a public key from the originating mail server, allowing verification.

b. Dr Wright's tests would have amounted to testing the DKIM signature from 2014 against the current public key. As many domains deploy key rotation, or simply change their keys periodically, a DKIM signature check conducted today may very well be conducted against mismatched keys hosted on the domain server. The public key for a mail server can therefore be expected to change from time to time, and it cannot be relied upon as a given that the

[2] https://www.cloudflare.com/en-gb/learning/dns/dns-records/dns-dkim-record/

DKIM of an email from 2014 can be reliably tested against the public key of the current infrastructure in 2024.

c. To corroborate this, using the same online resource https://mxtoolbox.com/EmailHeaders.aspx I checked a known authentic email from a similar time period. That produced a similar failed result, even though I knew it to be genuine. This is to be expected for the reasons given above.

79. There are also further reasons not to doubt the validity of the header of these emails. A search of the disclosure dataset indicates that the same domain and selector are present in email messages between nCrypt staff during 2016. These messages would therefore also fail a DKIM verification today, even though they likely would not have done on the day they were sent and received. Specifically,

a. The DKIM of {ID_001414} is as follows, which indicates the domain "d" and selector "s" parameters:

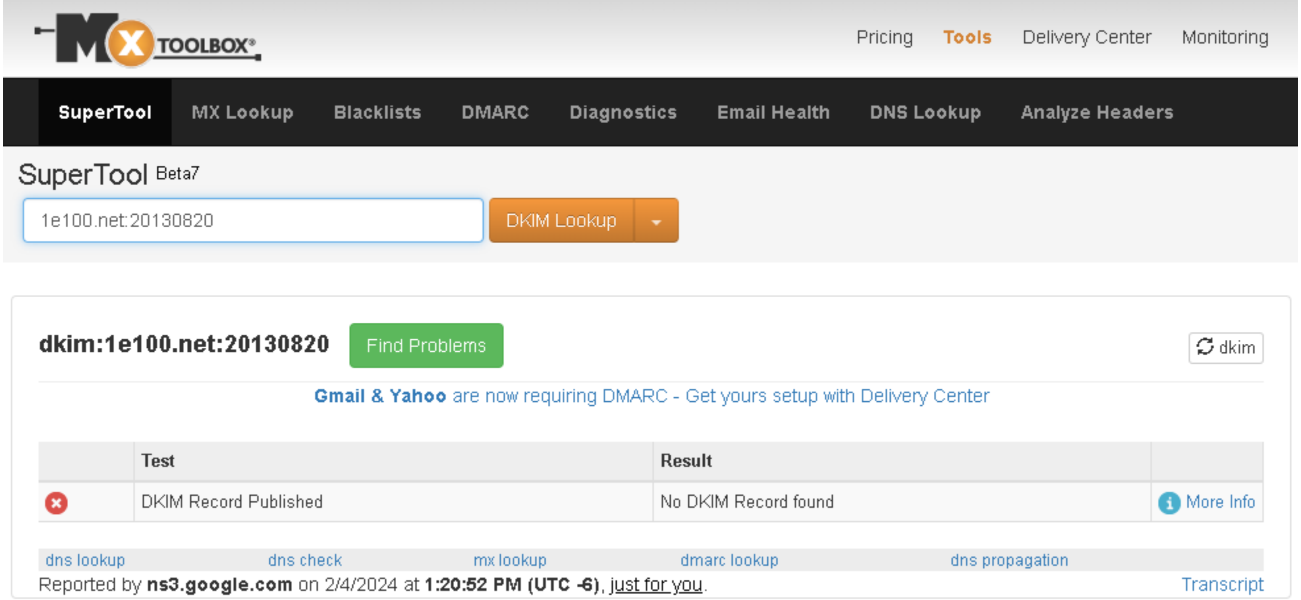
```
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20130820;
        h=x-gm-message-state:from:to:references:in-reply-to:subject:date
         :message-id:mime-version:content-type:thread-index:content-language;
        bh=5pe+o5xRaNRptRmDN6fK/k8qbMzR051m3QnKOp6xKBo=;
        b=JdDqKvlhAlmC91BMy2Fg9L5vs93D105ZS3r2ytXwW/KkUO49wG1dL4sfHFvKwzmCfc
         LUFVBLK/AylGAF/sSz3oP21lEqMWD4766NZ9kZgalhEiUeH9VO3P406cqSwq8owLRbcQ
         dRIjStrq1wRJXtUJ3Opvm9tjqVP7BHL1ud4dqhx5xrFHK6yzRxJ+AWmhBM1h2TDQPJ9g
         3cSQHySyhP7/IprcrvR2xESMGKeROxeszBwIIRJIaLj3285JIoVRuiF9SmoPxuK89cFM
         X3BJo5pt/jTE3eLRXAFcpIt0/ZoPxNyPGyU5KK46RCFzG2NViSmTf1V6VTytuL7ToylQ
         DyqA==
```

b. The relevant part of the email message for this demonstration is highlighted in Yellow. "1e100.net" is a name associated to Google services.

c. Returning to the DKIM check, I note that the pair highlighted in yellow above, features in more than 100 nCrypt email messages within the disclosure dataset.

d. From the handful of emails from Abacus-offshore.com in the disclosure dataset, all exhibit similar characteristics indicating a Google Infrastructure.

e. A specific DKIM lookup for these, conducted using a specific tool for DKIM record checking on the same website MX toolbox, produces the following result:



dkim:1e100.net:20130820

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

	Test	Result	
☒	DKIM Record Published	No DKIM Record found	More Info

Reported by **ns3.google.com** on 2/4/2024 at **1:20:52 PM (UTC -6)**, just for you.

f. This indicates that the Google servers will no longer validate this record for an old email. This is not unusual.

80. It is therefore not surprising that a 10 year old email can no longer be validated using current server information. The same can be said for the SPF checks conducted. As the domain has been migrated to an MS Office 365 environment, it is not possible to conduct a current SPF lookup.

Cross check against other messages in the disclosure dataset

81. The dataset includes an email message {ID_001405} which has a duplicate (though not hash identical): {ID_001418}. This email is related to {ID_001414} (and {ID_001396}), and provides corroboration for it as follows:

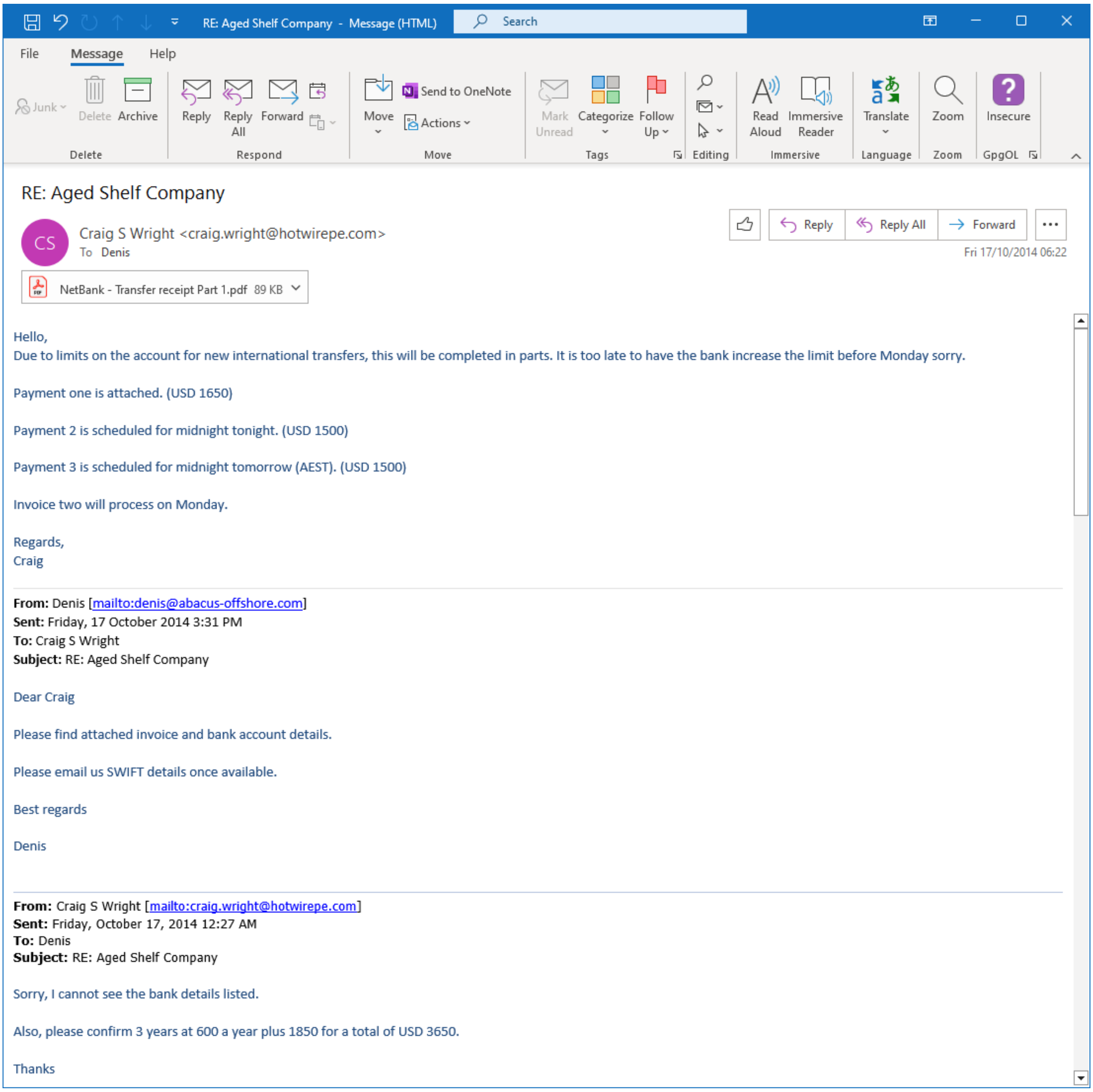
a. {ID_001418} is an email reply to {ID_001414}, sent by Dr Wright's email address, as I show below. The email itself presents as a reply to Denis by "Craig S Wright" "craig.wright@hotwirepe.com" and discusses the same subject as the rest of this email conversation.

b. As well as presenting as a reply to {ID_001414},{ID_001418} contains in its header a Reference key referring to the Mail ID of {ID_001414}, consistent with it being a reply. This information is common to both {ID_001405}and {ID_001418};

c. The Transmission header of {ID_001418} also indicates that the email was received into the mailbox "craig@rcjbr.org". In common with other emails in the dataset, from the Transmission header it is apparent that Dr Wright's RCJBR email address was included as

BCC Blind Copy recipient to {ID_001418}. This is consistent with the email being sourced from Dr Wright's RCJBR inbox.

d. I observe that the PR_CREATION_TIME and the PR_LAST_MODIFICATION_TIME for {ID_001405} are both recorded as being 17/10/2014 at 05:22. This is consistent with the email message being produced as an MSG item out of MS Outlook at this time. This time matches the equivalent records for {ID_001396} and therefore is consistent with both items being exported from MS Outlook at this time.



RE: Aged Shelf Company

Craig S Wright <craig.wright@hotwirepe.com>
To Denis
Fri 17/10/2014 06:22

NetBank - Transfer receipt Part 1.pdf 89 KB

Hello,
Due to limits on the account for new international transfers, this will be completed in parts. It is too late to have the bank increase the limit before Monday sorry.

Payment one is attached. (USD 1650)

Payment 2 is scheduled for midnight tonight. (USD 1500)

Payment 3 is scheduled for midnight tomorrow (AEST). (USD 1500)

Invoice two will process on Monday.

Regards,
Craig

From: Denis [mailto:denis@abacus-offshore.com]
Sent: Friday, 17 October 2014 3:31 PM
To: Craig S Wright
Subject: RE: Aged Shelf Company

Dear Craig

Please find attached invoice and bank account details.

Please email us SWIFT details once available.

Best regards

Denis

From: Craig S Wright [mailto:craig.wright@hotwirepe.com]
Sent: Friday, October 17, 2014 12:27 AM
To: Denis
Subject: RE: Aged Shelf Company

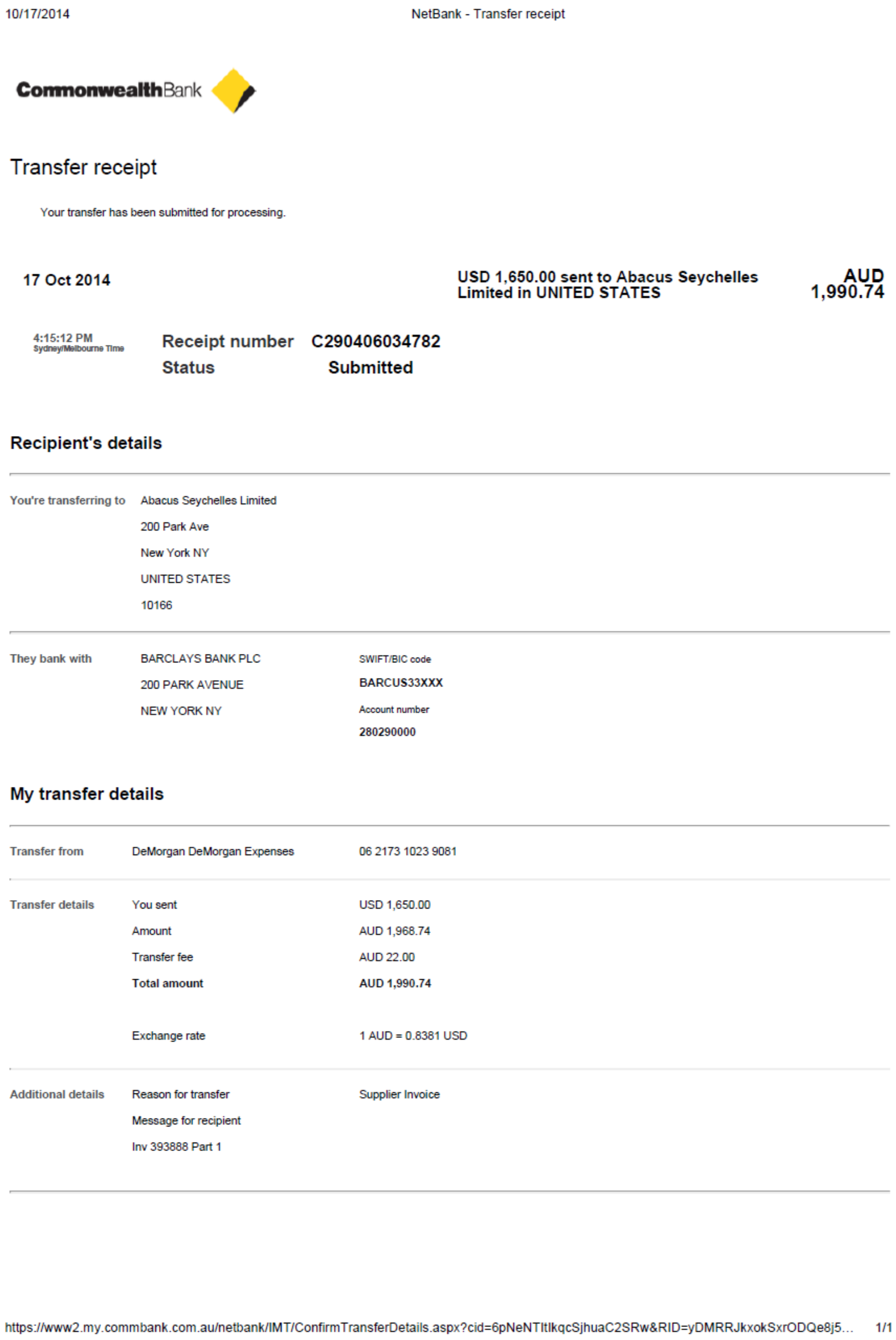
Sorry, I cannot see the bank details listed.

Also, please confirm 3 years at 600 a year plus 1850 for a total of USD 3650.

Thanks

Content of {ID_001418} / {ID_001405}

e. The attachment to the email is a PDF file that presents as follows:



10/17/2014 NetBank - Transfer receipt

CommonwealthBank

Transfer receipt

Your transfer has been submitted for processing.

17 Oct 2014	**USD 1,650.00 sent to Abacus Seychelles Limited in UNITED STATES**	**AUD 1,990.74**

4:15:12 PM
Sydney/Melbourne Time

Receipt number	C290406034782
Status	Submitted

Recipient's details

You're transferring to	Abacus Seychelles Limited 200 Park Ave New York NY UNITED STATES 10166	
They bank with	BARCLAYS BANK PLC 200 PARK AVENUE NEW YORK NY	SWIFT/BIC code **BARCUS33XXX** Account number **280290000**

My transfer details

Transfer from	DeMorgan DeMorgan Expenses	06 2173 1023 9081
Transfer details	You sent	USD 1,650.00
	Amount	AUD 1,968.74
	Transfer fee	AUD 22.00
	Total amount	**AUD 1,990.74**
	Exchange rate	1 AUD = 0.8381 USD
Additional details	Reason for transfer	Supplier Invoice
	Message for recipient Inv 393888 Part 1	

https://www2.my.commbank.com.au/netbank/IMT/ConfirmTransferDetails.aspx?cid=6pNeNTItlkqcSjhuaC2SRw&RID=yDMRRJkxokSxrODQe8j5... 1/1

f. I observe that there are two indications of the date being 17 October 2014 and that the “Additional details” section of the transfer receipt includes the text “Inv 393888 Part 1”. This matches the invoice number attached to {ID_001396} (and thereby {ID_001414})

82. The Internet header of {ID_001405} does not include a DKIM signature. This is not itself irregular and is consistent with the hotwirepe.com domain not utilising DKIM at the time. The email <u>does</u> however include a contemporaneous SPF authentication as shown below:

```
Received-SPF: pass (google.com: domain of craig.wright@hotwirepe.com designates
108.166.43.114 as permitted sender) client-ip=108.166.43.114;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of craig.wright@hotwirepe.com designates 108.166.43.114 as
permitted sender) smtp.mail=craig.wright@hotwirepe.com
```

83. This is consistent with {ID_001418} / {ID_001405} being authentic:

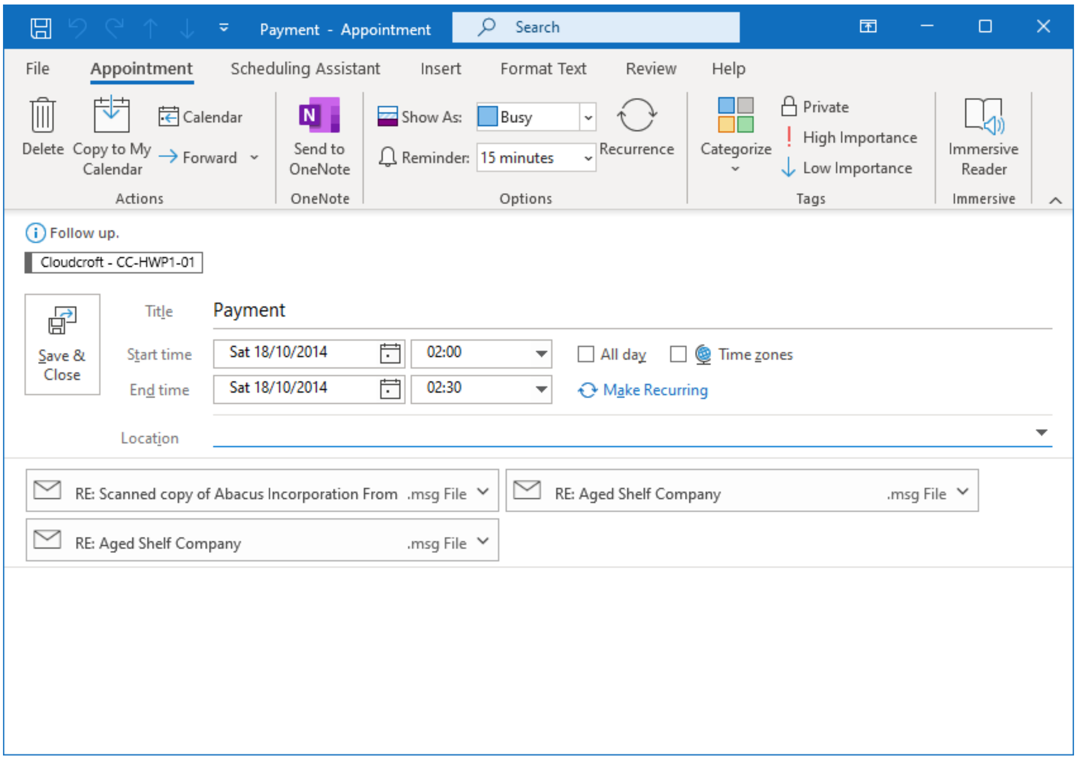
a. This indicates that an email account in the name of Dr Wright "craig.wright@hotwirepe.com" did reply to {ID_001414} at the time.

b. That email reply passed SPF verification at the time of sending via Dr Wright's infrastructure.

c. I have assessed the embedded timestamps found inside the Transmission header and found these to be consistent with the messages in the chain.

d. I have also found no other reason to doubt the authenticity of {ID_001405} (although the copy of it as {ID_001418} exhibits similar irregularities to {ID_001414}, these do not affect the analysis).

84. Another MSG file found within the disclosure dataset that relates to these messages is {ID_001399} with a non-electronic duplicate {ID_001411}. {ID_001399} presents as an MS Outlook Appointment as shown below:



Show As: Busy
Reminder: 15 minutes

Follow up.
Cloudcroft - CC-HWP1-01

Title: Payment
Start time: Sat 18/10/2014 02:00 □ All day □ Time zones
End time: Sat 18/10/2014 02:30
Location:

RE: Scanned copy of Abacus Incorporation From .msg File
RE: Aged Shelf Company .msg File
RE: Aged Shelf Company .msg File

85. The three messages attached to it relate to {ID_001396} (and thereby {ID_001414}), {ID_001405} (and thereby {ID_001418}), and {ID_001400} (and thereby {ID_001412}). I discuss {ID_001400} and {ID_001412} after {ID_001399}, as follows:

a. {ID_001399} is an example of an Outlook MSG file that is not itself an email. It is an appointment record. The topic / title of the appointment is “Payment”. It indicates an appointment time of 02:00 to 02:30 in the UTC timezone.

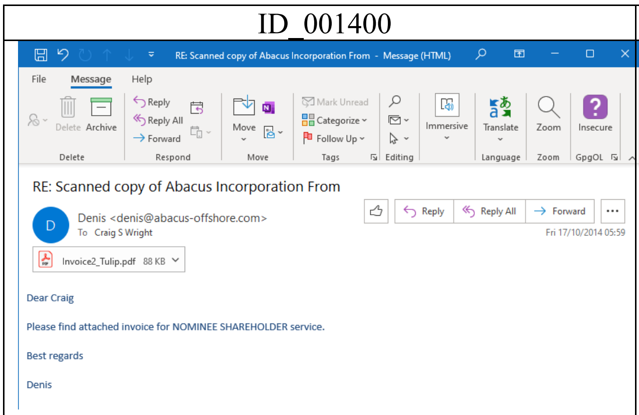
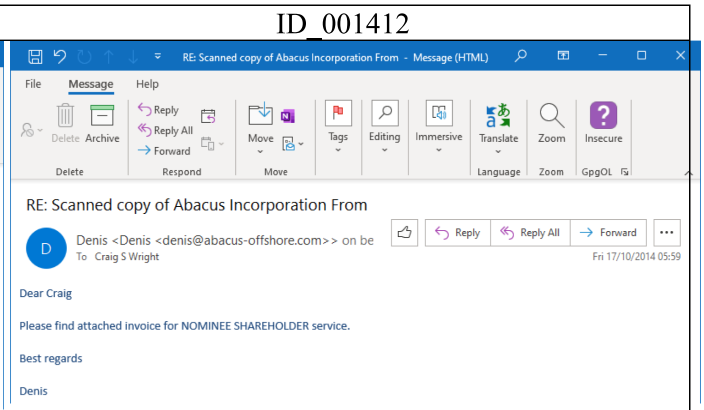
b. At face value the document appears to be a reminder to make the follow-up payment which is being discussed in {ID_001396} ({ID_001414}).

c. As the item is not an email, it does not have a Transmission header, or other items typical of an email. It does have Outlook MSG file metadata which indicates a R_CREATION_TIME of 05:21 on 17/10/2014. This correlates with the timestamps observed for {ID_001396} and {ID_001405}.

d. The appointment has been assigned a categorisation of “Cloudcroft - CC-HWP1-01”. I am unaware of the significance of this, or when this was applied to the appointment.

e. {ID_001400} and {ID_001412} share a similar relationship to the other document pairs described above in that they relate to the same email message but with one copy, {ID_001412} exhibiting some anomalous characteristics.

f. A major difference is that while {ID_001400} openly displays that it has an attachment, the attachment of {ID_001412} does not present on the face of the email in Outlook. A comparison is shown below:

ID_001400	ID_001412
 RE: Scanned copy of Abacus Incorporation From - Message (HTML) File Message Help Delete Archive Reply Reply All Forward Move Mark Unread Categorize Follow Up Immersive Translate Zoom Insecure Respond Tags Editing Language GpgOL RE: Scanned copy of Abacus Incorporation From Denis <denis@abacus-offshore.com> To Craig S Wright Fri 17/10/2014 05:59 Invoice2_Tulip.pdf 88 KB Dear Craig Please find attached invoice for NOMINEE SHAREHOLDER service. Best regards Denis	 RE: Scanned copy of Abacus Incorporation From - Message (HTML) File Message Help Delete Archive Reply Reply All Forward Respond Move Tags Editing Immersive Translate Zoom Insecure Language GpgOL RE: Scanned copy of Abacus Incorporation From Denis <Denis <denis@abacus-offshore.com>> on be To Craig S Wright Fri 17/10/2014 05:59 Dear Craig Please find attached invoice for NOMINEE SHAREHOLDER service. Best regards Denis

g. While the attachment is still embedded within the MSG file, it is not made available on the face of the document. I have not had sufficient time to investigate the cause of this, but consider that it is likely a result of the disclosure handling of the document.

h. Through this analysis I reach the opinion that I find no reason to doubt the authenticity of this collection of email messages {ID_001396}, {ID_001399}, {ID_001400} and {ID_001405}.

Conclusion on ID_001414 and related emails

86. In summary,

a. Dr Wright is correct that {ID_001414} and some related emails display anomalies. However, these anomalies likely relate to how the message was handled.

b. The content of these messages (including their Transmission headers and sender/recipient information) are confirmed by comparison with other documents in the disclosure dataset which do not exhibit the same anomalies.

c. {ID_001396} is a copy of {ID_001414} which does not display the same anomalies, and which I have already found that there is no reason to doubt.

d. It is apparent that Dr Wright's email account "craig.wright@hotwirepe.com" was used to reply to the message of {ID_001414} at the time. This is logged in the content of {ID_001396} and the reply messge itself {ID_001405}. The reply message {ID_001405} does not display the same anomalies and does include an SPF check indicating that it was verified at the same time, which is another indicator of authenticity.

e. While their respective copies {ID_001414}, {ID_001418}, {ID_001411} and {ID_001412} exhibit a number of anomalous traits, these can likely be attributed to the disclosure processing, or how they were handled before on account of the former set of documents. Such anomalies as appear do not affect analysis, as they do not affect the Transmission header of the emails.

f. I consider the conclusions reached by Dr Wright in his Eleventh Witness Statement in relation to {ID_001414} and its related emails to be speculative and unsound.

THE PAPA NEEMA EMAIL MESSAGES

87. I next analyse the emails relating to discussion with the 'papa neema' email address.

88. I understand that the manner in which these email messages have been disclosed is that they were emailed from “craig@tuliptrading.net” to Shoosmiths on 25 January 2024 and this in turn was forwarded to KLD. This is that the collection was not performed by KLD being given access to the source mailbox itself. The selection of what email messages were or were not submitted was collated by the custodian of the “craig@tuliptrading.net” email mailbox.

89. Unlike any of my other analysis, I have seen some evidence relating to these already in the form of the Twentieth Witness Statement of Philip Nathan Sherrell {P1/20/1}. I was not involved in preparing that statement or its analysis, and I have conducted my own analysis to draw my own conclusions.

90. The four email documents {ID_006564}, {ID_006566}, {ID_006567}, and {ID_006568} were included in disclosure dataset. The four email messages are all sent items from the address “papa.neema@gmail.com” and from the Transmission headers have been produced from the Mailbox “ramona@rcjbr.org”.

91. The table below summarises their prominent properties:

ID	ID_006564	ID_006566	ID_006567	ID_006568
From	Denis Mayaka <papa.neema@gmail.com >	Denis Mayaka <papa.neema@gmail.com >	Denis Mayaka <papa.neema@gmail.com >	Denis Mayaka <papa.neema@gmail.com >
To	Craig Wright <craig@rcjbr.org>	Craig Wright <craig@rcjbr.org>	Ramona Watts <ramona@rcjbr.org>, Craig Wright <craig@rcjbr.org>	ramona@rcjbr.org, Craig Wright <craig@rcjbr.org>
CC	STEFAN@taal.com, Ramona Watts <ramona@rcjbr.org>	STEFAN@taal.com, Ramona Watts <ramona@rcjbr.org>		
Date	Sun, 10 Sep 2023 15:09:52 +0100	Sun, 10 Sep 2023 15:10:41 +0100	Fri, 29 Sep 2023 17:25:19 +0100	Fri, 29 Sep 2023 17:45:54 +0100
Subject	Re: Requested invoices	Re: Requested invoices	Fwd: papa.neema@gmail.com	Re: papa.neema@gmail.com
Attachment	"C Wright.zipx" "TimeDoc 2.zip" "TimeDoc 2.pdf"		"WhatsApp Unknown 2023-09-10 at 15.21.45.zip"	

92. I note that a number of these emails are chains, but the underlying emails are present only as forwarded or replied-to messages within the message body in the email chains, and have not been provided thorough disclosure. It is not therefore possible to conduct a thorough analysis of these messages.

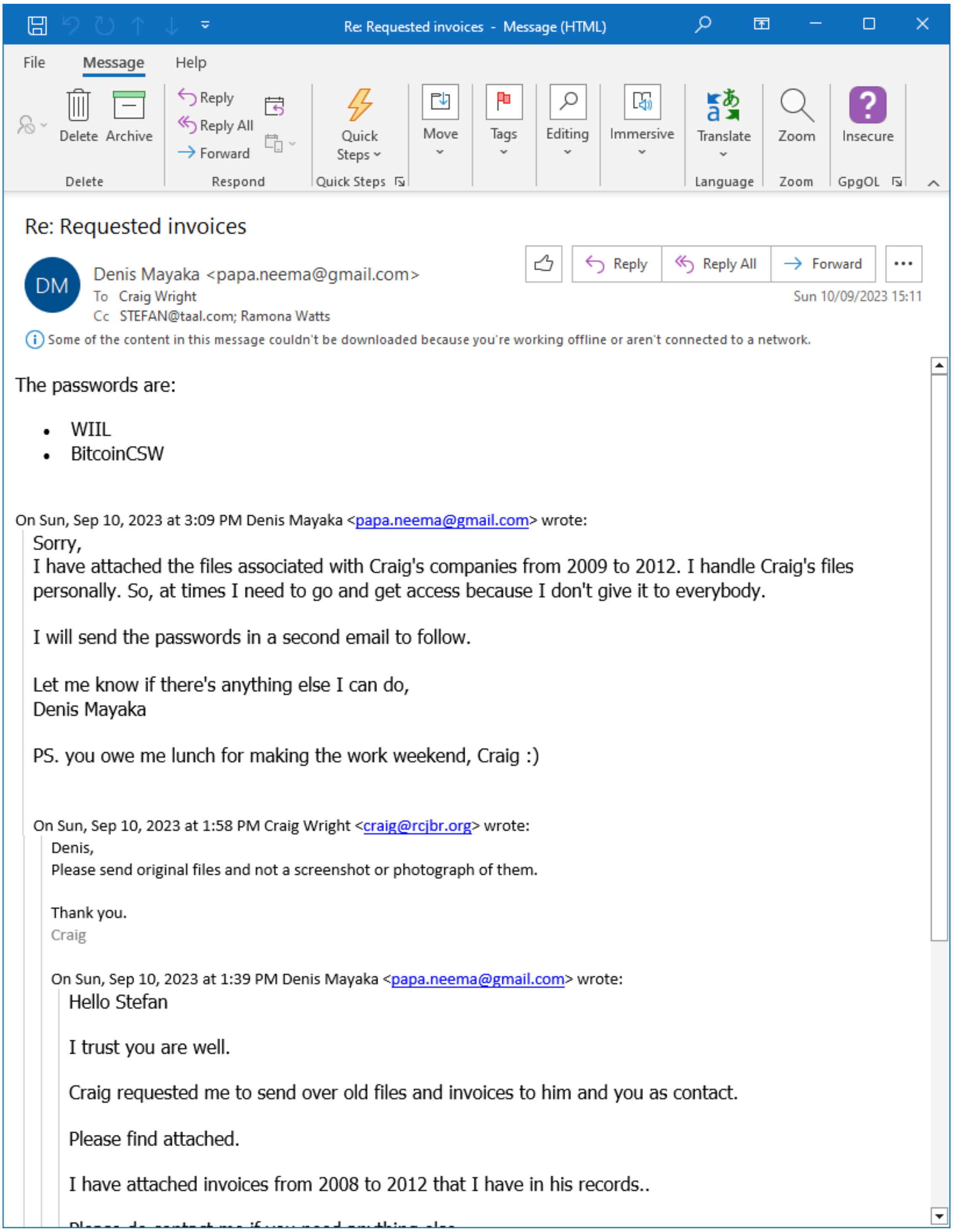
Timezones in the Papa Neema emails.

93. The recorded timezone offset on all four messages is +0100 which is consistent with the UK, Portugal, and parts of West Africa. It is not consistent with Kenya, but is consistent with UK time.

94. An email sent from a computer configured as if it was in Kenya would present a timezone offset of +0300 as per the sample below extracted from a test message to illustrate:

```
Date: Sat, 10 Feb 2024 23:16:36 +0300
```

95. I further observe that the time increments in the message bodies of forwarded emails also do not follow what would be expected where one party is in the UK, and the other in Kenya. Taking {ID_006566} as an example:



Re: Requested invoices

DM Denis Mayaka <papa.neema@gmail.com>
To Craig Wright
Cc STEFAN@taal.com; Ramona Watts
Sun 10/09/2023 15:11

Some of the content in this message couldn't be downloaded because you're working offline or aren't connected to a network.

The passwords are:

- WIIL
- BitcoinCSW

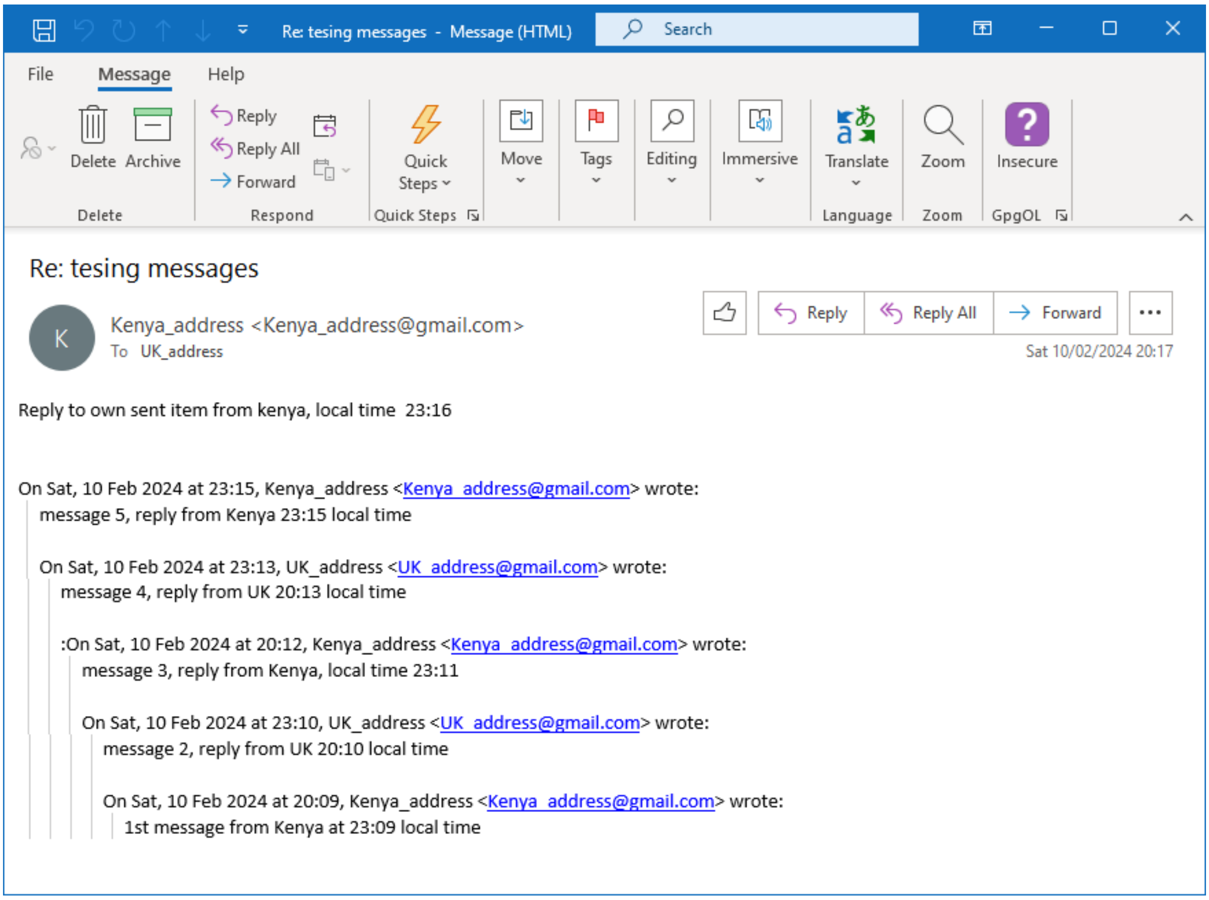
On Sun, Sep 10, 2023 at 3:09 PM Denis Mayaka <papa.neema@gmail.com> wrote:

> Sorry,
> I have attached the files associated with Craig's companies from 2009 to 2012. I handle Craig's files personally. So, at times I need to go and get access because I don't give it to everybody.
>
> I will send the passwords in a second email to follow.
>
> Let me know if there's anything else I can do,
> Denis Mayaka
>
> PS. you owe me lunch for making the work weekend, Craig :)
>
> On Sun, Sep 10, 2023 at 1:58 PM Craig Wright <craig@rcjbr.org> wrote:
>
> > Denis,
> > Please send original files and not a screenshot or photograph of them.
> >
> > Thank you.
> > Craig
> >
> > On Sun, Sep 10, 2023 at 1:39 PM Denis Mayaka <papa.neema@gmail.com> wrote:
> >
> > > Hello Stefan
> > >
> > > I trust you are well.
> > >
> > > Craig requested me to send over old files and invoices to him and you as contact.
> > >
> > > Please find attached.
> > >
> > > I have attached invoices from 2008 to 2012 that I have in his records..
> > >
> > > Please do contact me if you need anything else.

96. It can be observed that the time increments that both conversation partners were in the same timezone.

97. I produce below an illustrative sample where I have sent several messages back and forth and finished with a reply to a sent item from a Kenyan time zone. When conducting the tests I entered the text to record local time and set country into the message body so this can be compared to the reply snippet. This indicates what would be expected when conversation partners are in different

timezones, conversing over a short period of time. It can be seen how the clock appears to slip backwards and forwards through the chain.



Re: tesing messages

Kenya_address <Kenya_address@gmail.com>
To UK_address

Sat 10/02/2024 20:17

Reply to own sent item from kenya, local time 23:16

On Sat, 10 Feb 2024 at 23:15, Kenya_address <Kenya_address@gmail.com> wrote:
message 5, reply from Kenya 23:15 local time

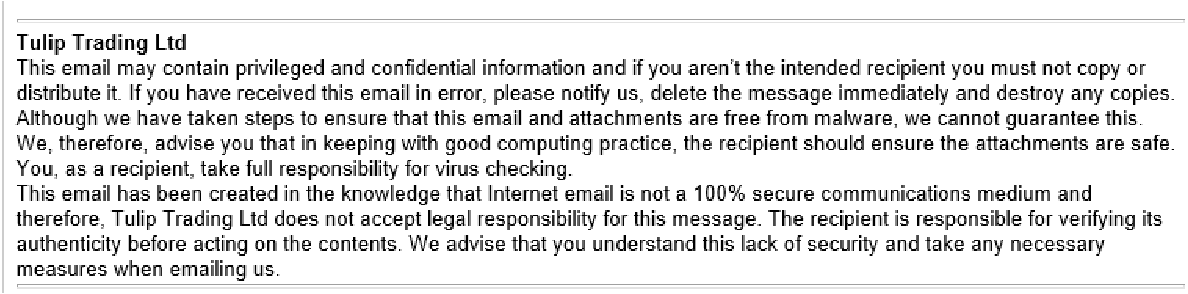
On Sat, 10 Feb 2024 at 23:13, UK_address <UK_address@gmail.com> wrote:
message 4, reply from UK 20:13 local time

:On Sat, 10 Feb 2024 at 20:12, Kenya_address <Kenya_address@gmail.com> wrote:
message 3, reply from Kenya, local time 23:11

On Sat, 10 Feb 2024 at 23:10, UK_address <UK_address@gmail.com> wrote:
message 2, reply from UK 20:10 local time

On Sat, 10 Feb 2024 at 20:09, Kenya_address <Kenya_address@gmail.com> wrote:
1st message from Kenya at 23:09 local time

98. I therefore consider that the papa.neema@gmail.com account was being operated in a +0100 timezone, and not +0300 as would be expected in Kenya. I also observe that three of the email messages, {ID_006564}, {ID_006566}, and {ID_006568} include a signature block for "Tulip Trading Ltd" as illustrated below:

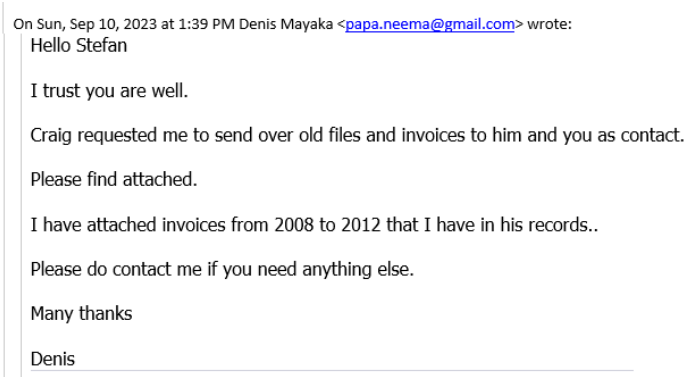


Tulip Trading Ltd
This email may contain privileged and confidential information and if you aren't the intended recipient you must not copy or distribute it. If you have received this email in error, please notify us, delete the message immediately and destroy any copies. Although we have taken steps to ensure that this email and attachments are free from malware, we cannot guarantee this. We, therefore, advise you that in keeping with good computing practice, the recipient should ensure the attachments are safe. You, as a recipient, take full responsibility for virus checking.
This email has been created in the knowledge that Internet email is not a 100% secure communications medium and therefore, Tulip Trading Ltd does not accept legal responsibility for this message. The recipient is responsible for verifying its authenticity before acting on the contents. We advise that you understand this lack of security and take any necessary measures when emailing us.

99. The email messages themselves appear to be authentic to their purported timestamps, but are not consistent with sending from Kenya. The content of the attached files I address below.

ID_006564

100. The email message contains three attachments "C Wright.zipx", "TimeDoc 2.zip", and "TimeDoc 2.pdf". The Message also includes a chain history in the message body. The first of which includes the content below:



On Sun, Sep 10, 2023 at 1:39 PM Denis Mayaka <papa.neema@gmail.com> wrote:

Hello Stefan

I trust you are well.

Craig requested me to send over old files and invoices to him and you as contact.

Please find attached.

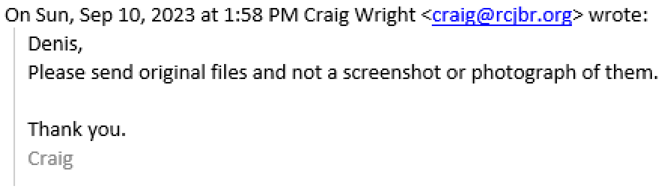
I have attached invoices from 2008 to 2012 that I have in his records..

Please do contact me if you need anything else.

Many thanks

Denis

101. This appears to indicate that there should have been some attachments to this previous email message in the chain. The reply message shown below suggests that the provided files were either screenshots or photographs:



On Sun, Sep 10, 2023 at 1:58 PM Craig Wright <craig@rcjbr.org> wrote:

Denis,
Please send original files and not a screenshot or photograph of them.

Thank you.
Craig

102. There are no reliable indications as to what the original attachments to this email message were and the 13:39 10 September 2023 email has not been included in the disclosed data. I note that {ID_006567} dated 29 September 2023 includes a series of photographs as attachments, and I have assumed that these are intended to be the same photographs, however it would be better if all the available relevant information were disclosed for analysis.

103. I address the content of the various attachments below.

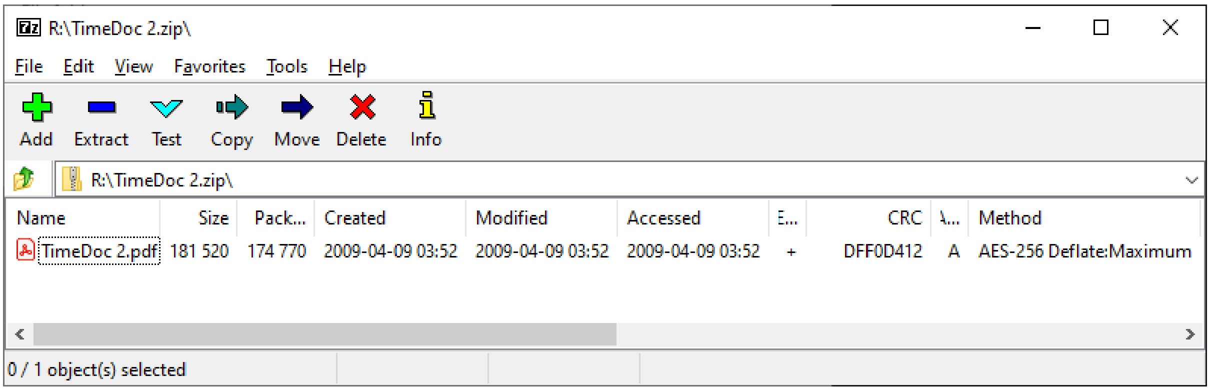
TimeDoc 2.zip and TimeDoc 2.pdf

104. This attachment, TimeDoc 2.zip is identical by MD5 hash to a file of the same name that is stored on the Samsung drive, in a folder named “BDO”. It is stored together with another Zip file named “TimeDoc.zip” The file timestamp properties of these three items are listed in the table below:

Name	Path	Size	Created	Modified	Accessed
BDO	\		31/10/2017 18:19:27	31/10/2017 18:20:26	31/10/2017 18:19:26
TimeDoc 2.zip	\BDO	174,952	31/10/2017 19:00:31	09/04/2009 13:53:10	31/10/2017 19:00:30
TimeDoc.zip	\BDO	174,463	31/10/2017 19:00:31	09/04/2009 13:39:40	31/10/2017 19:00:30

105. These timestamps are consistent with the two zip files being copied into the BDO folder with the computer clock set to 31 October 2017 at 19:00:31. (I also note that this date is a date which I have identified in my Fourth Report as being associated with backdated activity {G/6/13}).

106. Viewed in 7Zip, the file "TimeDoc 2.zip" presents as follows

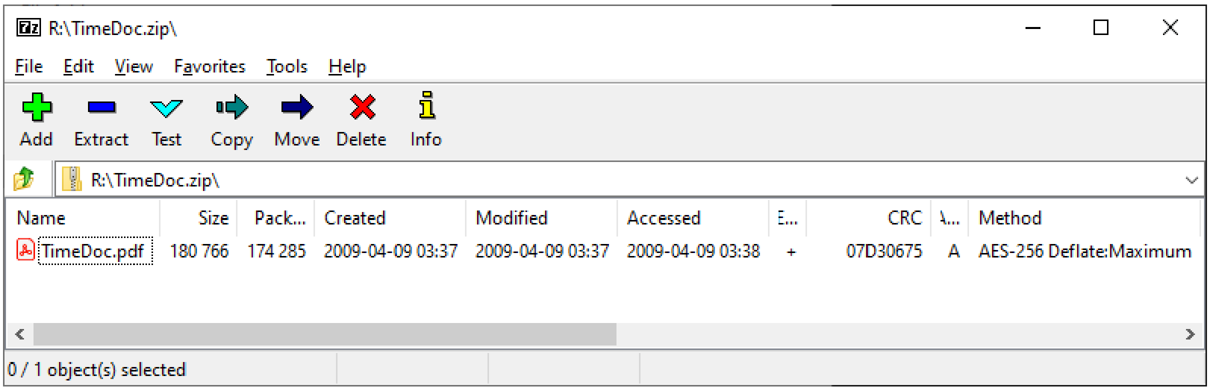


Name	Size	Pack...	Created	Modified	Accessed	E...	CRC	A...	Method
TimeDoc 2.pdf	181 520	174 770	2009-04-09 03:52	2009-04-09 03:52	2009-04-09 03:52	+	DFF0D412	A	AES-256 Deflate:Maximum

0 / 1 object(s) selected

107. The Zip file is encrypted. I have been provided with the password "Bitcoin11" to decrypt the content.

108. Another Zip file on the Samsung drive "TimeDoc.zip" presents as follows when opened in 7Zip.



Name	Size	Pack...	Created	Modified	Accessed	E...	CRC	A...	Method
TimeDoc.pdf	180 766	174 285	2009-04-09 03:37	2009-04-09 03:37	2009-04-09 03:38	+	07D30675	A	AES-256 Deflate:Maximum

0 / 1 object(s) selected

109. I am unaware of the password for this second zip file and am therefore unable to access the content of the file.

110. Returning to the attachments to the email {ID_006564}, The file "TimeDoc02.pdf" is CRC32 hash identical to the file within the zip of similar name and also attached to the same email. This indicates that the email has attached to it both the PDF file itself, and an encrypted zip of the same PDF file "TimeDoc 2.pdf".

111. The PDF file "TimeDoc 2.pdf" itself is also password-protected. The password for this file was provided in the email {ID_006566}.

112. The password protected status of a document does not make it a more reliable document, or prohibit it from manipulation or backdating.

a. Password protecting a document can reduce the risk of accidental contamination or the updating of internal metadata timestamps to a more recent date by bad handling, but it will not protect the document in circumstances where the password for the document is known.

b. The file timestamps for a password protected file are also not protected any further because the file is password protected.

113. The Document {ID_006565}, "TimeDoc 2.PDF" presents in manner that is generally similar to the Control Copy Bitcoin Whitepaper but is different in several observable ways.

a. It is dated to 9 April 2009, which is after the publication of the 2008 and 2009 versions of the Bitcoin White Paper.

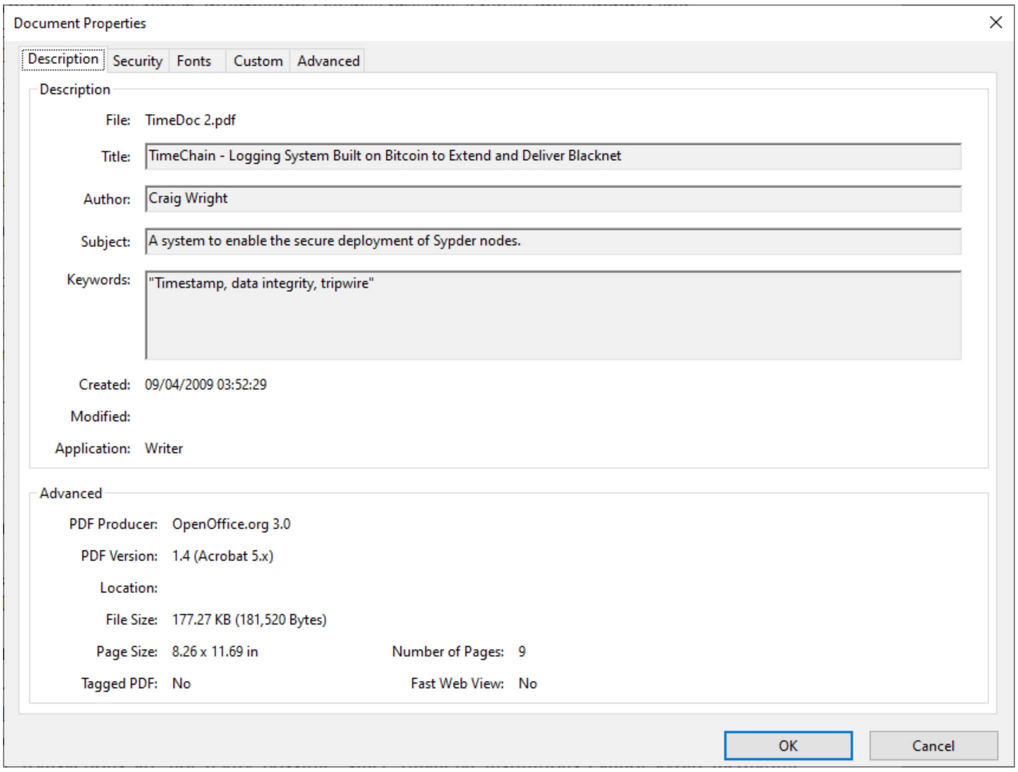
b. The text font sizes differ between the documents, with the text being larger in {ID_006565},

c. The paper sizes are different, with {ID_006565} being 8.26 x 11.69 Inches, while {ID_000865} (control Copy BWP) is 8.5 x 11.00 Inches.

d. {ID_006565} has several of the metadata property fields populated with content where {ID_000865} did not.

e. The text of the document is also different.

114. The Adobe reader Properties tab indicates the following information for the file {ID_006565}:



Description

File: TimeDoc 2.pdf

Title: TimeChain - Logging System Built on Bitcoin to Extend and Deliver Blacknet

Author: Craig Wright

Subject: A system to enable the secure deployment of Sypder nodes.

Keywords: "Timestamp, data integrity, tripwire"

Created: 09/04/2009 03:52:29

Modified:

Application: Writer

Advanced

PDF Producer: OpenOffice.org 3.0

PDF Version: 1.4 (Acrobat 5.x)

Location:

File Size: 177.27 KB (181,520 Bytes)

Page Size: 8.26 x 11.69 in Number of Pages: 9

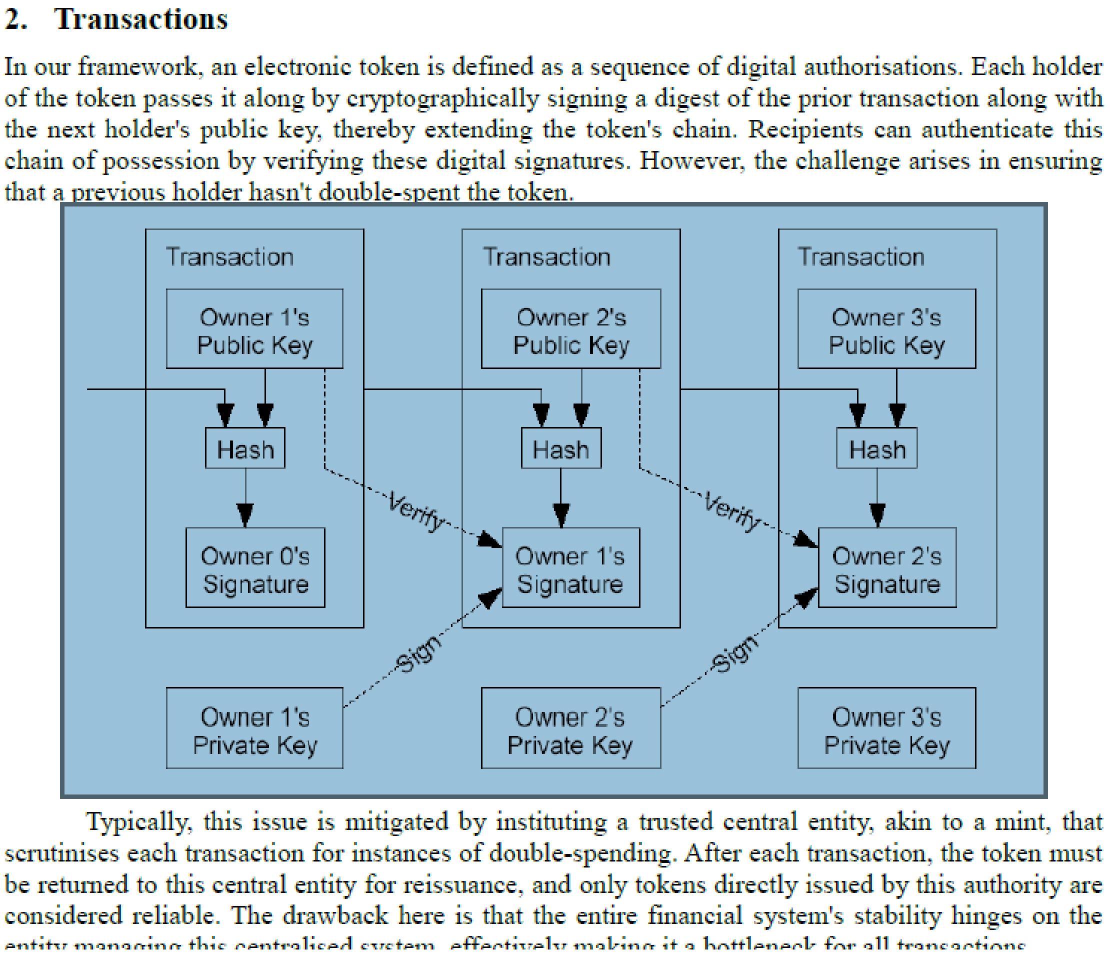
Tagged PDF: No Fast Web View: No

115. I note that the Timestamp within the embedded metadata stream is recorded with a +10:00 timezone offset:

```
/CreationDate (D:20090409135229+10'00')
```

116. It can be observed that this indicates the use of a version of OpenOffice listed which is more recent than the Bitcoin White Paper itself, but this itself is not unusual and the version is contemporary to the date of the file.

117. The 5 diagrams in {ID_006565} are not vector diagrams (e.g. with selectable text) as found in {ID_000865}, but are embedded as picture items:



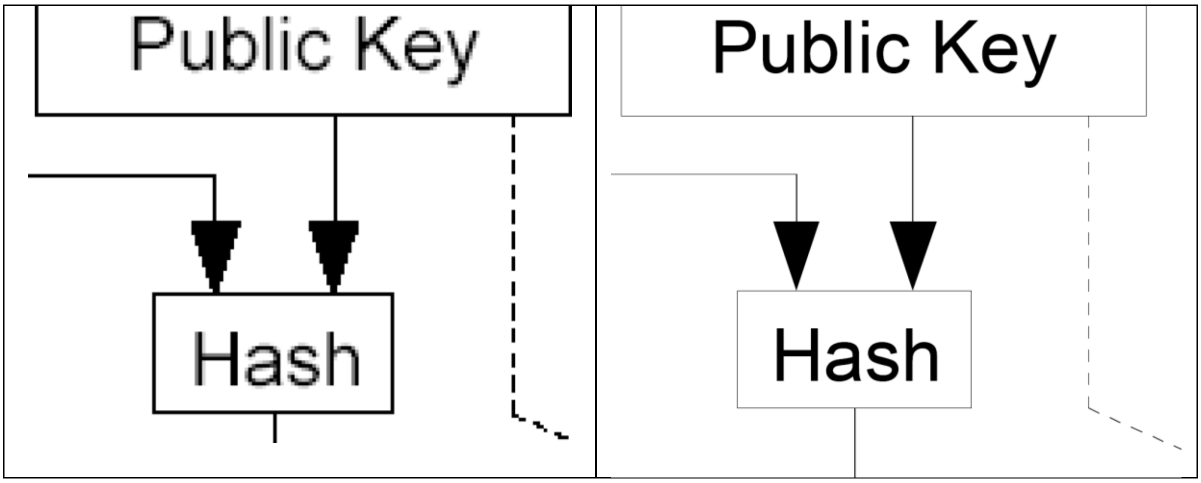
2. Transactions

In our framework, an electronic token is defined as a sequence of digital authorisations. Each holder of the token passes it along by cryptographically signing a digest of the prior transaction along with the next holder's public key, thereby extending the token's chain. Recipients can authenticate this chain of possession by verifying these digital signatures. However, the challenge arises in ensuring that a previous holder hasn't double-spent the token.

Typically, this issue is mitigated by instituting a trusted central entity, akin to a mint, that scrutinises each transaction for instances of double-spending. After each transaction, the token must be returned to this central entity for reissuance, and only tokens directly issued by this authority are considered reliable. The drawback here is that the entire financial system's stability hinges on the entity managing this centralised system, effectively making it a bottleneck for all transactions.

118. On closer inspection, the pictures are of a low resolution and are very pixelated compared to the equivalent diagrams in {ID_000865} as compared in the table below:

ID_006565	Bitcoin White Paper



119. The content of {ID_006565} would be relatively trivial to recreate e.g. by taking screenshots, as the diagrams are all embedded as picture items, and the only other content is plain text.

Summary on {ID_006565}

120. Other than the visual observations I make above, I do not comment on or consider the content of the document of as this is outside of my expertise, though I have seen the comments made in the Twentieth Witness Statement of Philip Nathan Sherrell.

121. While I have found no anachronistic metadata characteristics within this document itself in the time available to me, I have made several observations that bring it into contrast with the BWP control copy {ID_000865}. This is to say that the document has been assembled in a different manner to {ID_000865} and does not appear to have been produced from the OpenOffice document used to create {ID_000865} (and it also does not appear to come from {ID_000254}, a document which I understand is said to be related).

122. The same OpenOffice document could not have been used without undergoing significant changes to the formatting and style of the document as well as its content, and the diagrams have been replaced with relatively low-quality static pictures instead of flowchart-style graphic drawings.

123. I also note that the OpenOffice software version 3.0 that was used to author {ID_006565} is still available for download today from Internet resources[3], and it would have been possible to create a document identical to ID_006565 by downloading and running that software on a computer (or

[3] This is available via the same FTP site that I referenced in PM23 at page 9 in respect of the availability of OpenOffice 2.4: https://ftp5.gwdg.de/pub/openoffice/archive/stable/3.0.0/

virtual computer) with a backdated clock. The manner in which the email message to which the document was attached has been disclosed is less than ideal and does not allow me a full picture for forensic analysis.

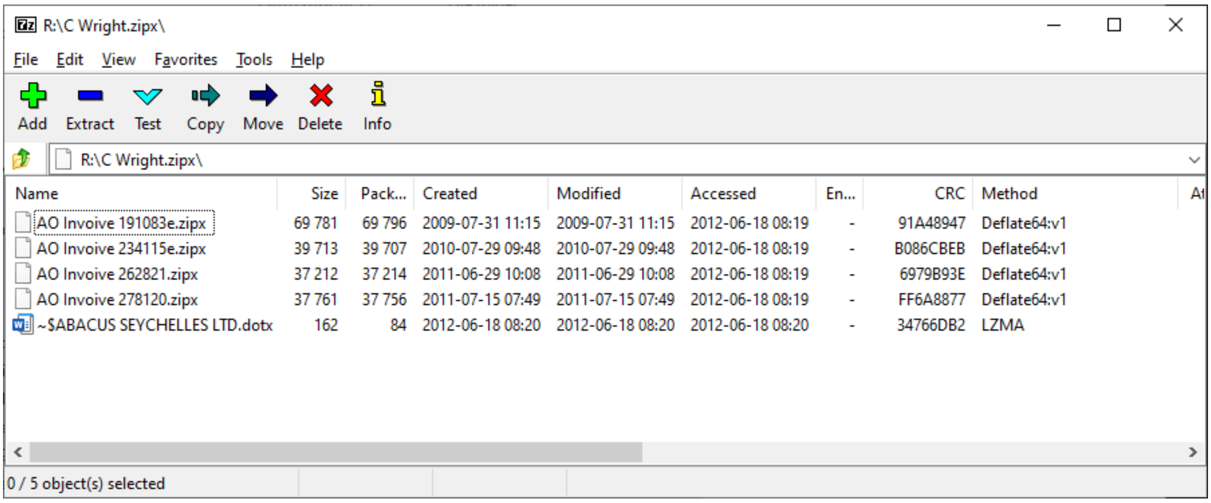
124. The copy of the ZIP file that was created on the Samsung drive has been attributed with timestamps of 31 October 2017, a date I have attributed with significant backdating behaviour on the Samsung drive {G/6/13}.

125. Finally, I point out that the presence of password protection does not indicate that this document is more or less likely to be authentic, and is not a factor I considered in my analysis.

126. I therefore consider that the authenticity of this document {ID_006565} should be considered at least as unreliable, without further supporting evidence. It may be possible to come to a more concluded view if I was provided access to the computing systems used to author and store this document and the emails associated with it.

The attachment "C Wright.zipx"

127. The next attachment is a Zip file that contains five files. When opened in 7Zip it presents as follows:



Name	Size	Pack...	Created	Modified	Accessed	En...	CRC	Method	At
AO Invoive 191083e.zipx	69 781	69 796	2009-07-31 11:15	2009-07-31 11:15	2012-06-18 08:19	-	91A48947	Deflate64:v1	
AO Invoive 234115e.zipx	39 713	39 707	2010-07-29 09:48	2010-07-29 09:48	2012-06-18 08:19	-	B086CBEB	Deflate64:v1	
AO Invoive 262821.zipx	37 212	37 214	2011-06-29 10:08	2011-06-29 10:08	2012-06-18 08:19	-	6979B93E	Deflate64:v1	
AO Invoive 278120.zipx	37 761	37 756	2011-07-15 07:49	2011-07-15 07:49	2012-06-18 08:19	-	FF6A8877	Deflate64:v1	
~$ABACUS SEYCHELLES LTD.dotx	162	84	2012-06-18 08:20	2012-06-18 08:20	2012-06-18 08:20	-	34766DB2	LZMA	

0 / 5 object(s) selected

Lock file

128. The last file listed "~$ABACUS SEYCHELLES LTD.dotx" is an MS word lock file:

a. The lock file is typically a hidden file in Windows and indicates that a file with a similar name (but without a leading ~) is locked for editing.

b. Inside the file it has recorded the name of "denis Mayaka" as the registered user. I observe that "denis" is typed with a lower case "d" while "Mayaka" has a Capital "M", though this does not affect my analysis itself.

c. The lock file is also typically created in the same location as the document file itself. In this instance a template .dotx file.

d. Lock files are typically deleted when the document to which they relate has been closed, and only remain when an error occurs and a document is not properly closed.

e. I consider it somewhat unusual that this lock file is included in the zip file without the template itself. It is possible that this could have happened through normal computer use, but the circumstances are still somewhat unusual.

129. Although a lock file indicates that a main document file (to which it relates) is being edited or opened, there is no accompanying file "ABACUS SEYCHELLES LTD.dotx" to which this lock file relates included in the Zip archive. I also note that there is no "AO invoive" file with 18 June 2012 timestamps attributed to the lock file.

130. The Last Accessed timestamps for all of these files is captured in the Zip file as being 18 June 2012 at 18:08. This is the same time captured by the zip file as being the Created and Modified time of the lock file, and indicates the setting of the computer clock at the time that the zip was created.

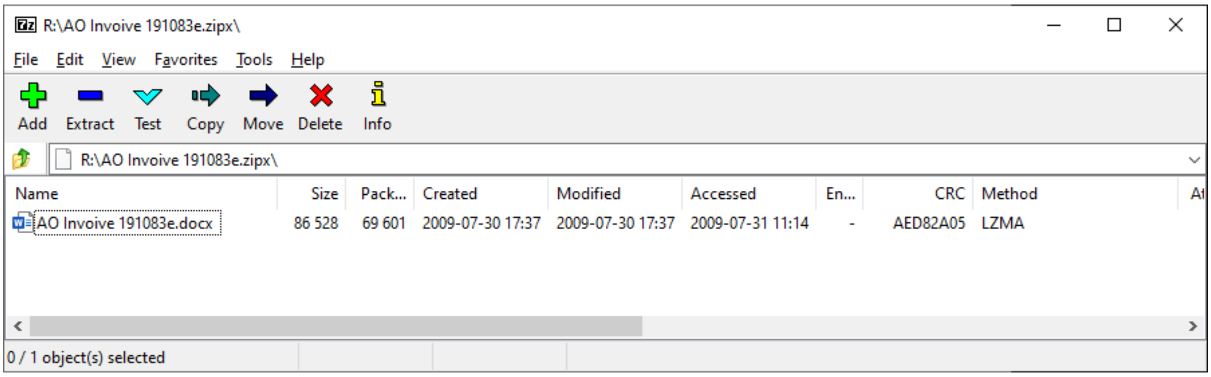
131. I have considered two possible ways of how this could have occurred:

a. If the user had the template .DOTX file open at the time, while preparing the content of this zip incorrectly selected the lock file when intending to select the template file. However, this all occurred with the clock set around 11 months after the previous invoice in the folder was Last Modified, which is unusual.

b. The lock file may have remained in the folder if MS Word did not successfully exit and remove the lock file. The template file is removed from the folder, and any other files that may have been created in the folder. The user creates a zip file of the folder, expecting only the four ZIP files to be included, but it incidentally also captures the lock file.

Invoices in Zip files

132. Turning to the four Zipx files. Each of these contains a single .DOCX file as demonstrated with one of the zips presented in 7Zip below:



R:\AO Invoive 191083e.zipx\

Name	Size	Pack...	Created	Modified	Accessed	En...	CRC	Method	At
AO Invoive 191083e.docx	86 528	69 601	2009-07-30 17:37	2009-07-30 17:37	2009-07-31 11:14	-	AED82A05	LZMA	

0 / 1 object(s) selected

133. All four documents have been password protected and digitally signed. These are not actually DOCX files as shown in their file extensions: they are .DOC files with an incorrect extension, though this is not itself an issue. The table below lists the file timestamps captured in the zipx files.

Name	File Created (zip)	File Modified (zip)	File Accessed (zip)
AO Invoive 191083e.docx	30/07/2009 17:37:00	30/07/2009 17:37:35	31/07/2009 11:14:07
AO Invoive 234115e.docx	29/07/2010 09:43:28	29/07/2010 09:45:14	29/07/2010 09:45:04
AO Invoive 262821.docx	29/06/2011 09:59:18	29/06/2011 10:05:31	29/06/2011 10:04:40
AO Invoive 278120.docx	15/07/2011 07:49:35	15/07/2011 07:47:21	15/07/2011 07:49:35

134. I produce at **Exhibit PM-R 5.1** a schedule listing the prominent metadata properties for the four invoices[4].

Spelling mistake across four invoices

135. I observe that all four documents share a spelling mistake in the filename “Invoive” rather than “Invoice”:

a. This is an apparent mistake that is not repeated within the content of the documents or their properties.

b. I consider it irregular that four separate files created and put into four separate zip files at yearly intervals over a two year period can exhibit such a consistent spelling mistake.

c. It is correct that the letters “V” and “C” are adjacent to each other on a keyboard, and that the spelling mistake is therefore an easy one to make on occasion.

d. However, in this example, the mistake would need to have been repeated four times over the course of two years, and captured contemporaneously in each of the four occasions when the

[4] The file “AO Invoive 191083e.doc” includes two copies of the same digital signature, but I have reported on the details of the signature only once

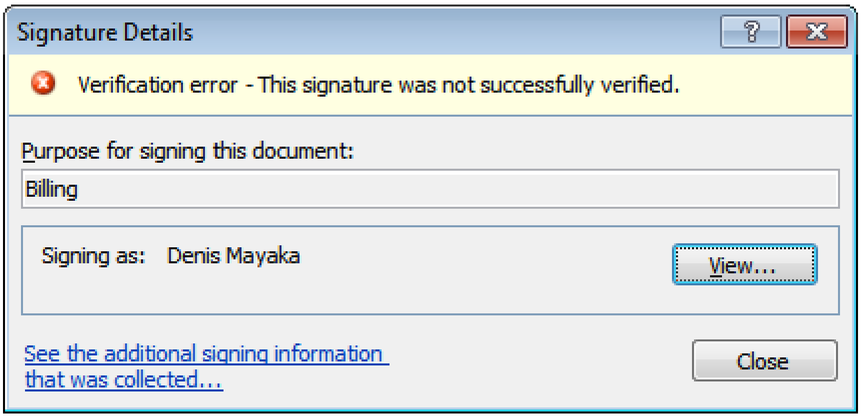
individual files were captured into the individual zip files, unless the documents were created one from another.

Signature dates vulnerable to clock manipulation

136. I share the opinion of Stroz Friedberg in their report dated 29 January 2024 {F/170/3} (although I note that Stroz Friedberg's analysis appears to have been carried out in December 2023), that the digital signatures found in the four documents cannot be relied upon for an accurate timestamp, and that these can be manipulated or backdated by changing the clock time on the computer concerned.

137. I have also checked for myself the same points independently, which I did before reading the report of Stroz Friedberg. This has allowed me to make several further observations as follows:

a. Each of the signatures includes information about the signatures, but also an additional section that captures information about the computer used at the time the signature was added to the document. This additional information can be accessed by clicking on the option in the bottom left of the Signature Details window. Demonstrated below in respect of "AO Invoive 191083e.docx":


Signature Details

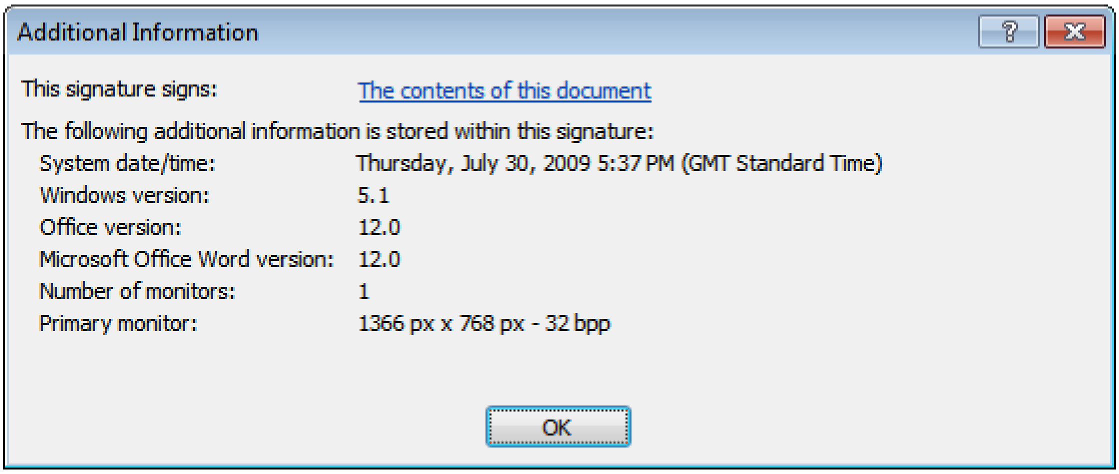
Verification error - This signature was not successfully verified.

Purpose for signing this document:
Billing

Signing as: Denis Mayaka

?
View...
See the additional signing information that was collected...
Close

b. Viewing this presents with the following information:



This signature signs: The contents of this document

The following additional information is stored within this signature:

System date/time: Thursday, July 30, 2009 5:37 PM (GMT Standard Time)
Windows version: 5.1
Office version: 12.0
Microsoft Office Word version: 12.0
Number of monitors: 1
Primary monitor: 1366 px x 768 px - 32 bpp

c. I observe that this system timestamp is recorded as being a GMT timestamp. It correlates with the File Created and File Modified timestamps being “17:37”, as captured by the ZIPx file created on 31 July 2009. This is consistent with all these file timestamps being stored as GMT.

d. This is consistent across all four of the invoice documents, whereby the file timestamps captured in the zip file correspond to the GMT system date captured by the application of the digital signature to the documents.

e. The computer-specific records are also consistent, indicating a computer running Windows XP (version 5.1) and MS Word 2007 with a monitor with a screen resolution of 1366 x 768px.

Content match between two invoices

138. I observe that although “AO Invoive 278120.docx” exhibits the highest invoice number, and is the most recently modified according to the timestamps, it features the same date at face value as the first invoice “AO Invoive 191083e.docx”. These two documents also feature the same description “Registration of a Seychelles International Company” and other content, with the only differences between them being the bill-to address, company detail and cost.

Metadata of invoices and inherited spelling error

139. The Table below lists the Internal metadata properties for the four documents. None of the files have a recorded Author or Last Saved By field, which is therefore not included in this table:

Name	Title	Comments	Template	Subject	Word Created	Word Modified

AO Invoive 191083e.docx	Abacus Offshore - Accounts	Wright International Investments Limited	Normal.dotm	Invoice 191083	30/07/2009 18:36	30/07/2009 18:37
AO Invoive 234115e.docx			Abacus Inv.dotx		29/07/2010 10:45	29/07/2010 10:45
AO Invoive 262821.docx			Normal.dotm		29/06/2011 10:57	29/06/2011 11:04
AO Invoive 278120.docx	Tulip Trading	Setup and Registration of Seychelles International Company by Niminee and bearer shares.	0 ABACUS SEYCHELLES LTD.dotx	# Bill to: Craig Wright	15/07/2011 08:41	15/07/2011 08:47

140. I observe that in addition to sharing a face value invoice date, “AO Invoive 191083e.docx” and “AO Invoive 278120.docx” are the only two to have metadata property fields such as Title, Comments and Subject populated. The two intermediate documents have no information recorded in these fields.

141. “AO Invoive 191083e.docx”and “AO Invoive 262821.docx” also both have a recorded template of “Normal.dotx” while the other two have custom template files listed, which for “AO Invoive 278120.docx” is the template filename “0 ABACUS SEYCHELLES LTD.dotx”. This template filename is consistent with the filename of the lock file discussed previously in this report.

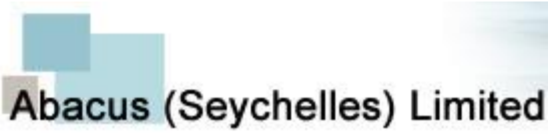
142. I observe that the use of a template file was not consistent between the four documents, but I make no direct conclusion from this in itself, but comment that the spelling mistake present in the four filenames spanning two years is irregular in consideration of the use of a template. When saving a file based on the use of a custom Word template, the user would be prompted to type a new filename at each point. The presence of a repeated typing mistake at this point appears unusual, and tends to support that the documents were not created in that way. However, from the limited information available I cannot make a firm conclusion regarding this spelling mistake, but I do observe it as unusual.

143. The varying pattern in recorded template files, and how only the first and last files have the metadata fields, is consistent with the files not being copied and pasted to create subsequent files, but a more complicated editing practise. I therefore cannot attribute the repeated spelling mistake in the filename to an inherited error from the previous file.

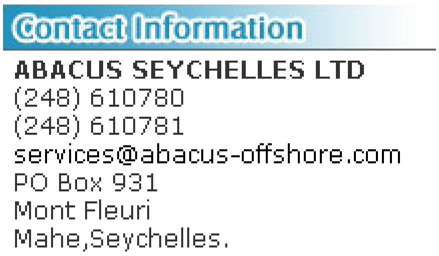
Logo in invoices

144. I have looked into the logo in the top right-hand corner of the documents. This is the same logo which is also mentioned in the Twentieth Witness Statement of Philip Nathan Sherrell. This

matches the dimensions of a logo file available from a Web Archive snapshot of the Abacus Offshore website from 2010[5]. The dimension are 284 x 67 pixels:



145. The same Web Archive snapshot also includes the same address and contact details listed in the invoices:



Contact Information

ABACUS SEYCHELLES LTD
(248) 610780
(248) 610781
services@abacus-offshore.com
PO Box 931
Mont Fleuri
Mahe,Seychelles.

Periods of validity of the digital Signature Timestamps

146. I next compared the timestamps for the signing of these four documents against the periods of validity of the digital signatures. Across the four files, there are two digital signatures that are used. I do not repeat all of the information presented in the Stroz Friedberg report, but summarise the timestamp information in the table below:

Name	File Created (zip)	File Modified (zip)	Signed	System Date	Serial Number	Valid From	Valid To
AO Invoive 191083e.docx	30/07/2009 17:37:00	30/07/2009 17:37:35	Denis Mayaka	30/07/2009 17:37	57286a0e29e6df80 4f7c03206b4d6286	30 July 2009 17:34:16	30 July 2010 23:34:16
AO Invoive 234115e.docx	29/07/2010 09:43:28	29/07/2010 09:45:14	Denis Mayaka	29/07/2010 09:45	57286a0e29e6df80 4f7c03206b4d6286	30 July 2009 17:34:16	30 July 2010 23:34:16
AO Invoive 262821.docx	29/06/2011 09:59:18	29/06/2011 10:05:31	Denis Mayaka	29/06/2011 10:04	101497bdcdb696ba 49e3265e061aa42e	29 June 2011 10:05:23	28 June 2012 16:05:23
AO Invoive 278120.docx	15/07/2011 07:49:35	15/07/2011 07:47:21	Denis Mayaka	15/07/2011 07:47	101497bdcdb696ba 49e3265e061aa42e	29 June 2011 10:05:23	28 June 2012 16:05:23

[5] https://web.archive.org/web/20100806115027/http://www.abacus-offshore.com/index.asp

147. I observe that the first digital signature had a validity period from 30/07/2009 to 29/07/2010. The valid-from date is the same date as the first invoice. The valid-to (expiry) date is just one day later than the second invoice.

148. There is then a void period of approximately 11 months between the two signatures from 30 July 2010 at 23:35 until 29 June 2011 at 10:05 when the second digital signature is created.

149. The creation of the second digital signature also correlates with the creation of the third invoice file “AO Invoive 262821.docx”.

150. This is therefore consistent with these signatures being created for the purpose of these invoices specifically, with the dates aligning closely. While this itself does not indicate the signatures to be inauthentic, it does provide possible context for their creation. No other documents in the disclosure dataset are signed in this manner using these keys.

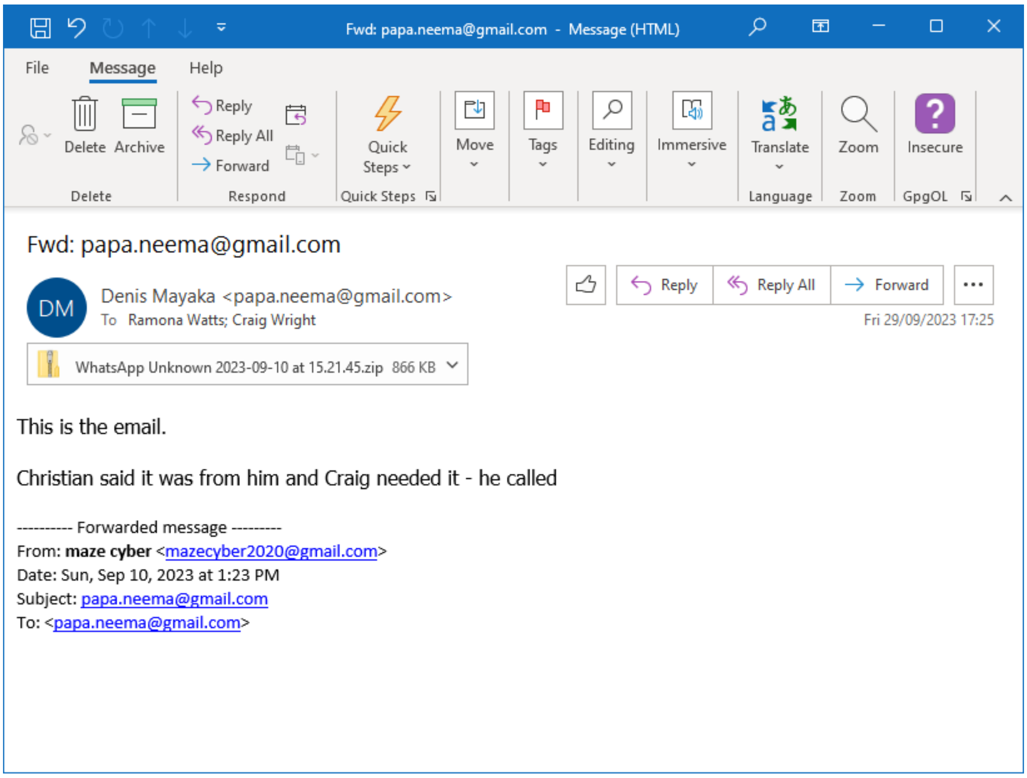
Doc file format

151. I note that it is somewhat unusual to issue invoices in docx format. This format is normally used for documents that need to be edited, with PDF being a more common file format for sending or publishing files in their final form. The invoices provided by Abacus Offshore in the 2014 email exchanges were all PDF files.

152. While the application of the digital signatures to the documents do cause a notice to be applied that the document is considered finalised and that any changes will remove the digital signatures, it does not prevent editing which is still easily done within MS Word.

Attachment - WhatsApp Unknown 2023-09-10 at 15.21.45.zip

153. This is the attachment file to {ID_006567} as seen in the screenshot below:



Fwd: papa.neema@gmail.com

DM Denis Mayaka <papa.neema@gmail.com>
To Ramona Watts; Craig Wright
Fri 29/09/2023 17:25

WhatsApp Unknown 2023-09-10 at 15.21.45.zip 866 KB

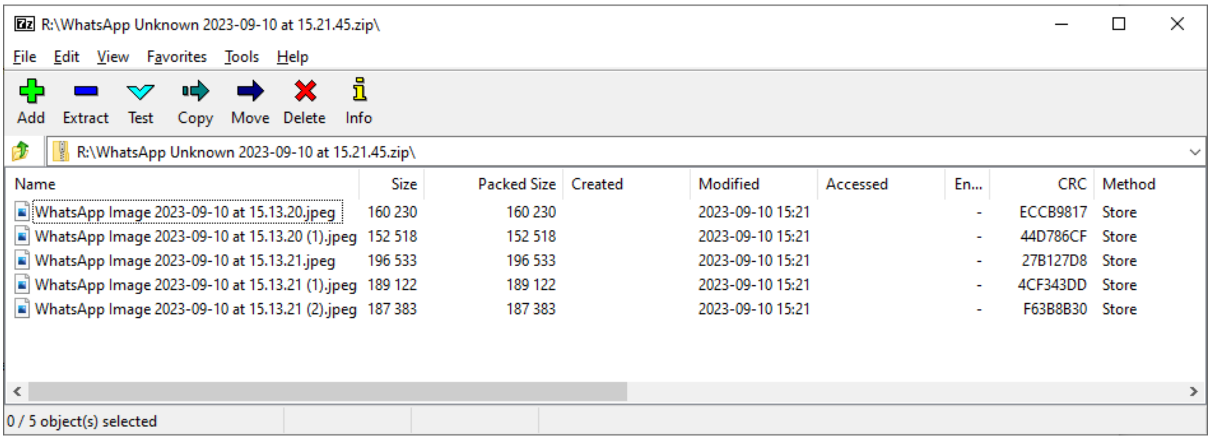
This is the email.

Christian said it was from him and Craig needed it - he called

---------- Forwarded message ---------
From: **maze cyber** <mazecyber2020@gmail.com>
Date: Sun, Sep 10, 2023 at 1:23 PM
Subject: papa.neema@gmail.com
To: <papa.neema@gmail.com>

154. The forwarded email message from “mazecyber2020@gmail.com” has not been provided, and therefore is not available for analysis.

155. The attached zip file presents in 7Zip as follows:

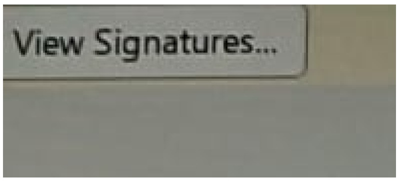

R:\WhatsApp Unknown 2023-09-10 at 15.21.45.zip\
File
Edit
View
Favorites
Tools
Help
Add
Extract
Test
Copy
Move
Delete
Info
R:\WhatsApp Unknown 2023-09-10 at 15.21.45.zip\

Name	Size	Packed Size	Created	Modified	Accessed	En...	CRC	Method
WhatsApp Image 2023-09-10 at 15.13.20.jpeg	160 230	160 230		2023-09-10 15:21		-	ECCB9817	Store
WhatsApp Image 2023-09-10 at 15.13.20 (1).jpeg	152 518	152 518		2023-09-10 15:21		-	44D786CF	Store
WhatsApp Image 2023-09-10 at 15.13.21.jpeg	196 533	196 533		2023-09-10 15:21		-	27B127D8	Store
WhatsApp Image 2023-09-10 at 15.13.21 (1).jpeg	189 122	189 122		2023-09-10 15:21		-	4CF343DD	Store
WhatsApp Image 2023-09-10 at 15.13.21 (2).jpeg	187 383	187 383		2023-09-10 15:21		-	F63B8B30	Store

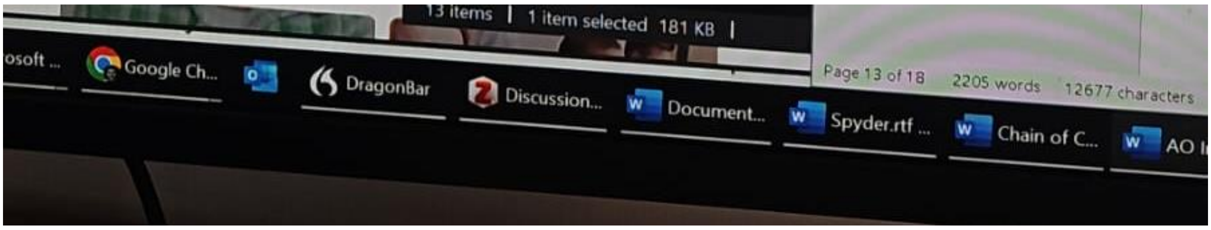
0 / 5 object(s) selected

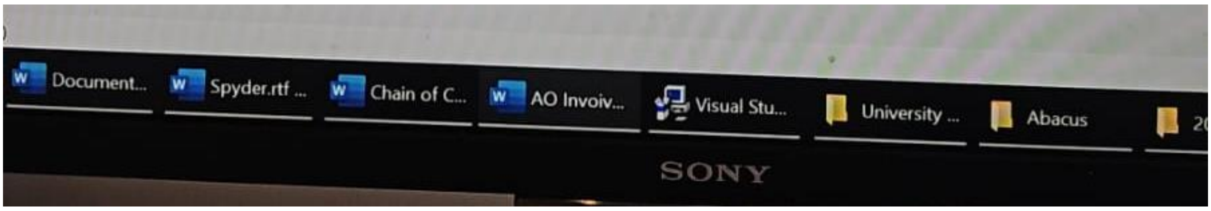
156. The five picture files shown are photographs of a computer screen that is displaying content consistent with the four invoices provided as MS word documents.

157. One of the pictures includes a reference to a digital signature:

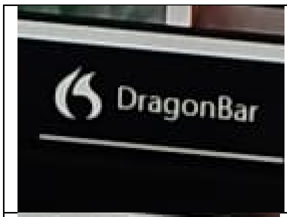
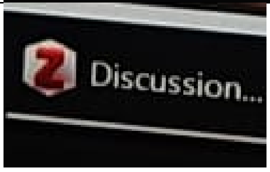
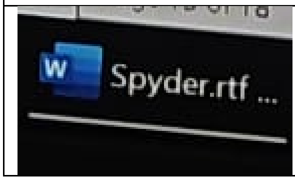


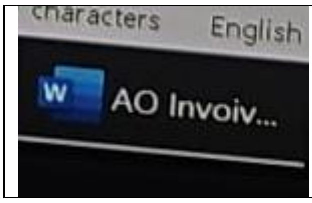
158. Others include a view of the taskbar on the computer, which have also been shown in the Twentieth Witness Statement of Philip Nathan Sherrell:





159. I observe that this indicates the following programs and documents open. Having formed the view myself, I agree with the Twentieth Witness Statement of Philip Nathan Sherrell, that these correspond to the applications and documents discussed there, including the following:

	DragonBar is consistent with various versions of the software Dragon Naturally Speaking. Dragon dictation software has featured in many of the documents analysed.
	This is consistent with Zotero (https://www.zotero.org/download/) The two documents “The King.rtf” and The King 2.rtf” retained embedded references to this software Zotero 6 for Windows Your personal research assistant Download
	“Spyder.rtf” is the name of a content empty RTF document on the Samsung drive that I have addressed in my Fourth Report.

	"AO Invoiv…" is consistent with the filenames of the four invoice documents, Including the spelling error

FILES AND FOLDERS ON THE SAMSUNG DRIVE RELATED TO THE PAPA NEEMA EMAILS

Backdated, deleted "Denis" folder on the Samsung drive

160. At paragraph 51 of my Fourth Report {G/6/18}, I described some deleted content from the Recycle Bin of the Samsung drive. This includes a reference to a folder that had been named "Denis" that had been deleted from the Samsung drive.

161. At the time of writing that report, the possible relevance of this folder was not apparent to me. Having reviewed the content of the recently disclosed documents, I observe a correlation between this folder and others on the Samsung drive and other data.

162. There are three file system records on the Samsung drive that pertain to the "Denis" folder. It is no longer possible to recover the content of this deleted folder, but the properties of these deleted records are listed below:

Name	File Created	Last Written	Last Accessed	Full Path
Denis	31/10/2007 06:24:44	31/10/2007 06:24:44	31/10/2007 06:24:44	Samsung_T1
$R1X6LZZ	31/10/2007 06:24:44	31/10/2007 06:24:44	31/10/2007 06:24:44	Samsung_T1\$RECYCLE.BIN
$I1X6LZZ	31/10/2007 06:24:57	31/10/2007 06:24:58	31/10/2007 06:24:58	Samsung_T1\$RECYCLE.BIN

163. The first entry is an original filesystem record for the folder as it existed on the Samsung Drive. The second entry is the filesystem record for the folder once it had been sent to the Recycle Bin. The third entry is the Recycle Bin entry for the folder itself.

164. Like other deleted files on Dr Wright's Samsung Drive, this "Denis" folder also exhibits indications of backdating. In my Fourth Report I explained at paragraph 50 to 52 {G/6/18} - {G/6/19} how the Recycle Bin entries were created in a manner that is consistent with Windows 10 or later operating systems, but are dated to dates before that operating system existed.

165. While it is not possible to be sure whether the content of this folder relates to Denis Mayaka, I do note that its creation on the Samsung drive, and subsequent deletion is similar in character to several other seemingly related files and folders, such as "University" and "Spyder.rtf", both of which feature in the photographs attached to the Papa Neema emails.

166. This has led me to revisit certain aspects of the Recycle Bin content of the Samsung drive. I observed in my Fourth Report that there were multiple Recycle Bin entries with the dates 31 October 2007, or 31 October 2014 recorded for the content having been sent to the Recycle Bin. These Recycle Bin records could not have been created with an accurate clock, and therefore must be the result of clock manipulation and backdating.

167. I repeat in a more consolidated manner the information relating to the entry "$IFH6M1E.rar"which relates to the file "Prior PC.rar"

Name	File Created	Logical Size of Recycle Bin file	Internal Timestamp	original Path
$IFH6M1E.rar{SS}	31/10/2007 06:26:01	60	31/10/2007 06:26	E:\Prior PC.rar

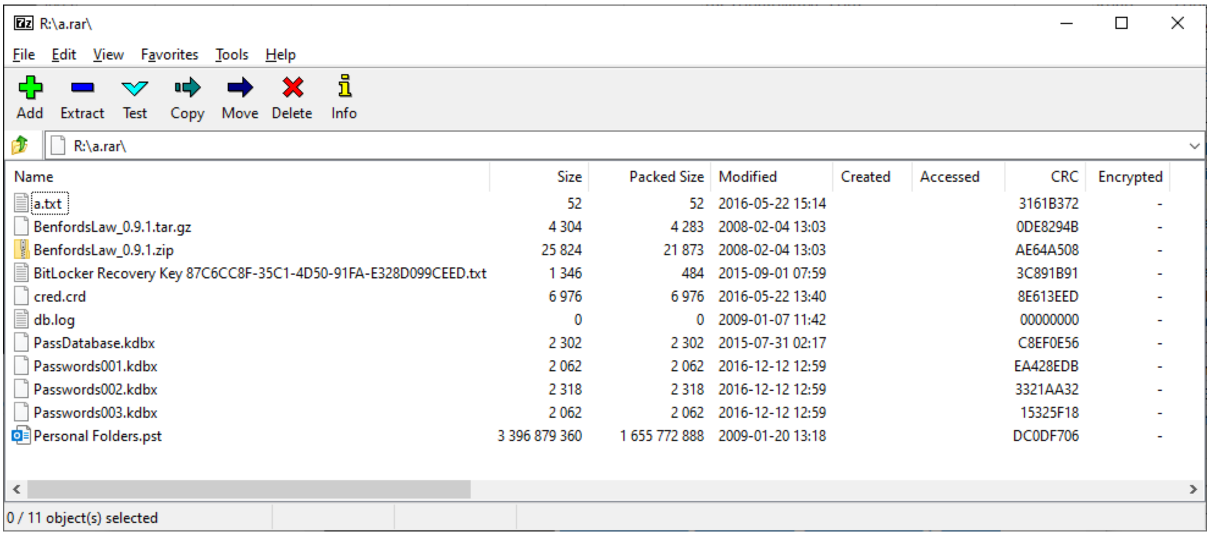
Name	File Created	Last Written	Last Accessed	Full Path
Prior PC.rar	31/10/2017 18:48:21	31/10/2017 18:47:56	31/10/2017 18:48:20	Samsung_T1
$RFH6M1E.rar	31/10/2017 18:48:21	31/10/2017 18:47:56	31/10/2017 18:48:20	Samsung_T1\$RECYCLE.BIN
$IFH6M1E.rar	31/10/2007 06:26:01	31/10/2007 06:26:02	31/10/2007 06:26:02	Samsung_T1\$RECYCLE.BIN

168. Quite anomalously, the file "Prior PC.rar" has file timestamps indicating 31 October 2017, but the Recycle Bin entry for the file is recorded has a timestamp of 31 October 2007 over a decade earlier. At face value, this would indicate that the file was sent to the Recycle Bin a decade before it was created.

169. According to these timestamps, "Prior PC.rar" (which was also not recoverable, but which was of a file size consistent with it being another disk image) was sent to the Recycle Bin just over a minute after the folder "Denis", indicating a link between them in the time of their deletion. I note that Dr Wright makes reference to "H:\PriorPC" at paragraph 20.1 of his Twelfth Witness Statement {CSW/7/5} in relation to the VMware configuration. The VMWare configuration files provided make no mention of the file "PriorPC" but as I noted, the provided information is an incomplete set of configuration files which does not allow for a full analysis.

Documents related to the TimeDoc files on the Samsung Drive

170. I observe that the folder "BDO" on the Samsung Drive, in which the two files "TimeDoc.zip" and "TimeDoc 2.zip" are located, also contains an archive file "a.rar". The three of these files share a created date of 31 October 2017 while the time varies between the files. The content of "a.rar" as opened in 7zip is shown below:



Name	Size	Packed Size	Modified	Created	Accessed	CRC	Encrypted
a.txt	52	52	2016-05-22 15:14			3161B372	-
BenfordsLaw_0.9.1.tar.gz	4 304	4 283	2008-02-04 13:03			0DE8294B	-
BenfordsLaw_0.9.1.zip	25 824	21 873	2008-02-04 13:03			AE64A508	-
BitLocker Recovery Key 87C6CC8F-35C1-4D50-91FA-E328D099CEED.txt	1 346	484	2015-09-01 07:59			3C891B91	-
cred.crd	6 976	6 976	2016-05-22 13:40			8E613EED	-
db.log	0	0	2009-01-07 11:42			00000000	-
PassDatabase.kdbx	2 302	2 302	2015-07-31 02:17			C8EF0E56	-
Passwords001.kdbx	2 062	2 062	2016-12-12 12:59			EA428EDB	-
Passwords002.kdbx	2 318	2 318	2016-12-12 12:59			3321AA32	-
Passwords003.kdbx	2 062	2 062	2016-12-12 12:59			15325F18	-
Personal Folders.pst	3 396 879 360	1 655 772 888	2009-01-20 13:18			DC0DF706	-

0 / 11 object(s) selected

171. The RAR file includes a Modified timestamp, but in this case not any Created or Accessed timestamps. The Modified timestamps range from January 2009 to December 2016.

172. I observed that the filenames and file capacities within "a.rar" match with two sets of files in the Samsung drive's Root directory. The files themselves have been deleted and overwritten, however. I list the properties of these below together with the properties of "a.rar", "TimeDoc.zip" and "TimeDoc 2.zip" in the top three rows in italics to differentiate them.

Name	Is Deleted	File Created	Last Written	Last Accessed	File Size	Full Path
a.rar		*31/10/2017 18:20:44*	*31/10/2017 18:20:26*	*31/10/2017 18:20:44*	*1,655,816,211*	*Samsung_T1\BDO*
TimeDoc 2.zip		*31/10/2017 19:00:31*	*09/04/2009 12:53:10*	*31/10/2017 19:00:30*	*174,952*	*Samsung_T1\BDO*
TimeDoc.zip		*31/10/2017 19:00:31*	*09/04/2009 12:39:40*	*31/10/2017 19:00:30*	*174,463*	*Samsung_T1\BDO*
a.txt	yes	31/10/2007 18:17:32	22/05/2016 15:14:00	31/10/2007 18:17:32	52	Samsung_T1
a.txt	yes	31/10/2007 18:17:32	22/05/2016 15:14:00	31/10/2007 18:17:32	52	Samsung_T1
BenfordsLaw_0.9.1.tar.gz	yes	31/10/2007 18:17:31	04/02/2008 13:03:02	31/10/2007 18:17:30	4,304	Samsung_T1
BenfordsLaw_0.9.1.tar.gz	yes	31/10/2007 18:17:31	04/02/2008 13:03:02	31/10/2007 18:17:30	4,304	Samsung_T1
BenfordsLaw_0.9.1.zip	yes	31/10/2007 18:17:31	04/02/2008 13:03:02	31/10/2007 18:17:30	25,824	Samsung_T1
BenfordsLaw_0.9.1.zip	yes	31/10/2007 18:17:31	04/02/2008 13:03:02	31/10/2007 18:17:30	25,824	Samsung_T1
BitLocker Recovery Key 87C6CC8F-35C1-4D50-91FA-E328D099CEED.txt	yes	31/10/2007 18:17:32	01/09/2015 07:59:38	31/10/2007 18:17:32	1,346	Samsung_T1
BitLocker Recovery Key 87C6CC8F-35C1-4D50-91FA-E328D099CEED.txt	yes	31/10/2007 18:17:32	01/09/2015 07:59:38	31/10/2007 18:17:32	1,346	Samsung_T1
cred.crd	yes	31/10/2007 18:17:32	22/05/2016 13:40:52	31/10/2007 18:17:32	6,976	Samsung_T1

cred.crd	yes	31/10/2007 18:17:32	22/05/2016 13:40:52	31/10/2007 18:17:32	6,976	Samsung_T1
db.log	yes	31/10/2007 18:17:28	07/01/2009 11:42:02	**31/10/2007 18:17:28**	0	Samsung_T1
db.log	yes	31/10/2007 18:17:28	07/01/2009 11:42:02	**31/10/2007 18:17:36**	0	Samsung_T1
PassDatabase.kdbx	yes	31/10/2007 18:17:28	31/07/2015 02:17:44	31/10/2007 18:17:28	2,302	Samsung_T1
PassDatabase.kdbx	yes	31/10/2007 18:17:28	31/07/2015 02:17:44	31/10/2007 18:17:28	2,302	Samsung_T1
Passwords001.kdbx	yes	31/10/2007 18:17:15	12/12/2016 12:59:20	31/10/2007 18:17:14	2,062	Samsung_T1
Passwords001.kdbx	yes	31/10/2007 18:17:15	12/12/2016 12:59:20	31/10/2007 18:17:14	2,062	Samsung_T1
Passwords002.kdbx	yes	31/10/2007 18:17:15	12/12/2016 12:59:24	31/10/2007 18:17:14	2,318	Samsung_T1
Passwords002.kdbx	yes	31/10/2007 18:17:15	12/12/2016 12:59:24	31/10/2007 18:17:14	2,318	Samsung_T1
Passwords003.kdbx	yes	31/10/2007 18:17:15	12/12/2016 12:59:26	31/10/2007 18:17:14	2,062	Samsung_T1
Passwords003.kdbx	yes	31/10/2007 18:17:15	12/12/2016 12:59:26	31/10/2007 18:17:14	2,062	Samsung_T1
Personal Folders.pst	yes	31/10/2007 18:17:15	**31/10/2014 18:18:20**	**31/10/2014 18:18:20**	3,396,879,360	Samsung_T1
Personal Folders.pst	yes	31/10/2007 18:17:15	**20/01/2009 13:18:50**	**31/10/2007 18:17:14**	3,396,879,360	Samsung_T1

173. The file-created date of the deleted files are all listed as being 31/10/2017 between 18:17:15 and 18:17:32 (17 seconds later). In the time available to me I have been unable to determine the cause of the file duplication, but I observe that it is not just a duplication of the filenames: each set points to a different set of file data locations on the disk, indicating that these files were written to the disk multiple times.

174. It is possible to see that the clock setting when these files were written to the disk was 31 October 2007. Since the archive "a.rar" has no Created or Accessed timestamps, these would be populated at the time of extracting from that archive using the clock setting at the time of extraction. It is possible that these files were either extracted from a.rar, or that they were first created on the drive and then added to the archive "a.rar". I consider extraction more likely, since the Created timestamps are all within 17 seconds of each other (consistent with the time likely taken to extract from an archive); however, it is not possible to be certain.

175. Further, the last modified and accessed timestamps for the PST file referred to above have then been updated to 31 October 2014 as emphasised in bold in the table above:

   a. Aside from being almost exactly 7 years later, this timestamp is also not captured inside "a.rar", so must not originate from that archive, and must be the clock setting on the computer used to access and modify them.

   b. This 31 October 2014 timestamp can also be attributed to a set of Recycle Bin entries that appear to correlate with these files.

c. The table I produced at paragraph 50 of my Fourth Report {G/6/18} features two sets of Recycle Bin entries that correlate with the content of these files in many ways, including matching the length of the original filepath length and the corresponding file capacities.

d. This is set out in more detail in **Exhibit PM-R 5.2**, which compares the file entry for the Root directory of the Samsung Drive; the $R Recycle Bin records, and the $I Recycle Bin records.

176. Comparing this information, it can be seen that the two sets of files in the Root directory of the Samsung drive are recorded as having been sent to the Recycle Bin on 31 October 2014. This date predates the release of Windows 10 and therefore must be the result of clock manipulation.

177. I note that there are no Recycle Bin entries that relate to the copy of "Personal Folders.pst" that had been last modified on 31 October 2014. This could be because the file was moved from the Samsung Drive onto another storage volume (which would not have cause it to be deleted into the Recycle Bin); or it may have been permanently deleted from the Samsung drive without first being sent to the Recycle Bin.

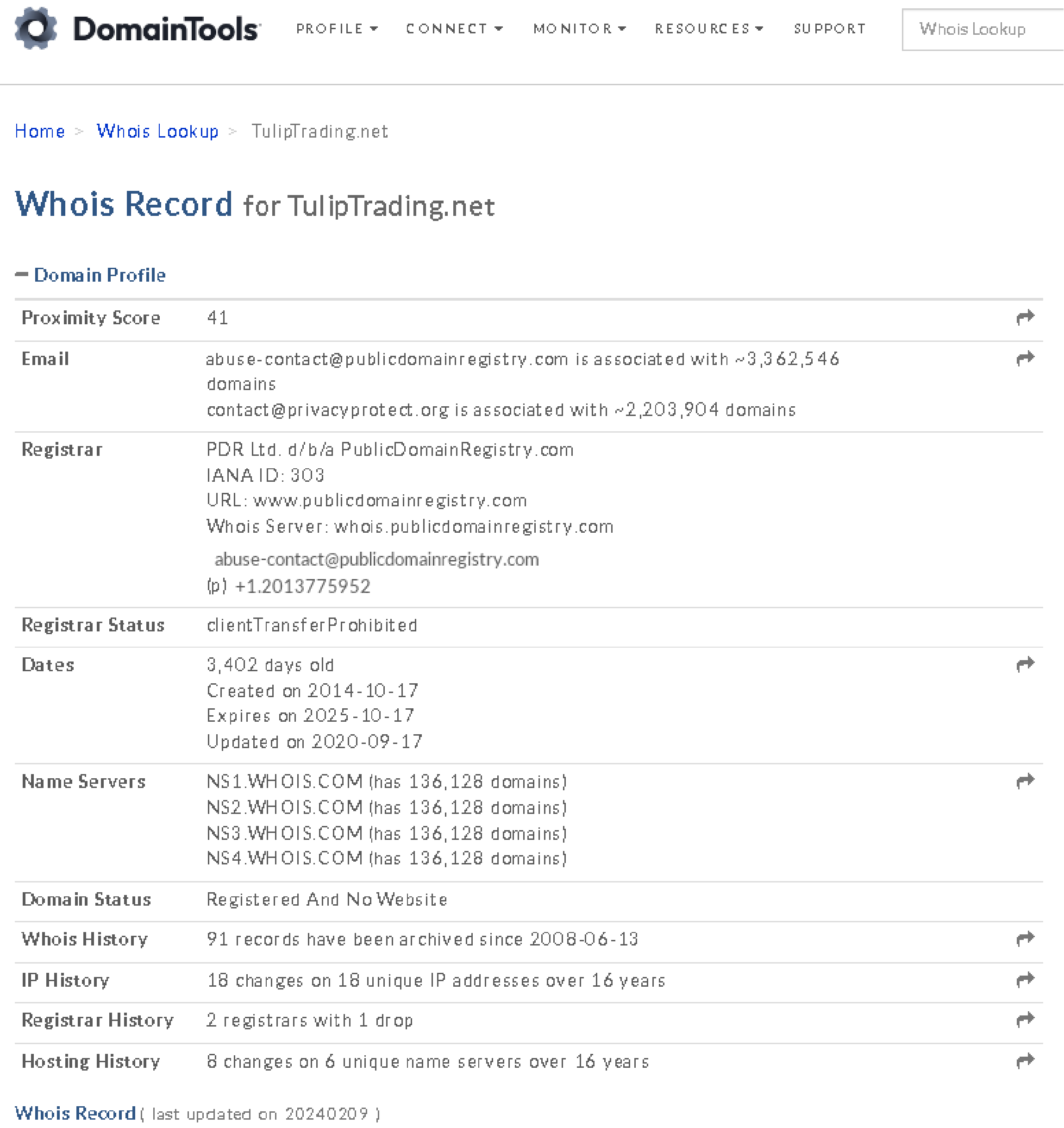
178. Overall, the collation of this data and the various other artefacts described in my Fourth and Fifth Reports present very significant anomalies regarding these 31 October dates, be they 2007, 2014, or 2017. As such, I consider that that any files bearing these dates on the Samsung Drive should not be accepted as reliable without supporting information.

<u>THE TULIPTRADING.NET DOMAIN</u>

179. I noticed that the email address "craig@tuliptrading.net" was listed as the source account of a handful of the most recently disclosed documents: {ID_006564}, {ID_006565}, {ID_006566}, {ID_006567}, and {ID_006568}. The email address is not listed in either the processed or irretrievable sources of documents for disclosure.

180. I had previously referred to registration records for various email domains referred to in disclosure (including in my First Report) but had not previously checked the domain 'tuliptrading.net' as it was not listed. I therefore checked it.

181. The domain registration information for the domain "tuliptrading.net" indicates that the current registration was created on 17 October 2014.



Home > Whois Lookup > TulipTrading.net

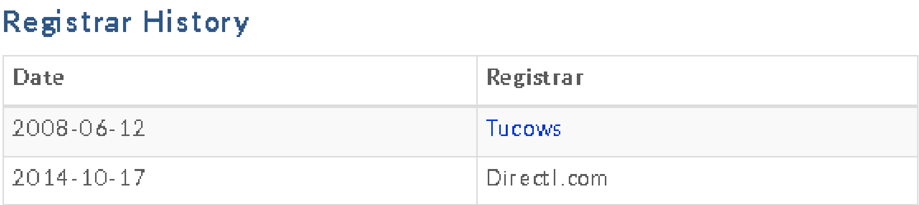
Whois Record for TulipTrading.net

− Domain Profile

Proximity Score	41
Email	abuse-contact@publicdomainregistry.com is associated with ~3,362,546 domains contact@privacyprotect.org is associated with ~2,203,904 domains
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: www.publicdomainregistry.com Whois Server: whois.publicdomainregistry.com abuse-contact@publicdomainregistry.com (p) +1.2013775952
Registrar Status	clientTransferProhibited
Dates	3,402 days old Created on 2014-10-17 Expires on 2025-10-17 Updated on 2020-09-17
Name Servers	NS1.WHOIS.COM (has 136,128 domains) NS2.WHOIS.COM (has 136,128 domains) NS3.WHOIS.COM (has 136,128 domains) NS4.WHOIS.COM (has 136,128 domains)
Domain Status	Registered And No Website
Whois History	91 records have been archived since 2008-06-13
IP History	18 changes on 18 unique IP addresses over 16 years
Registrar History	2 registrars with 1 drop
Hosting History	8 changes on 6 unique name servers over 16 years

Whois Record (last updated on 20240209)

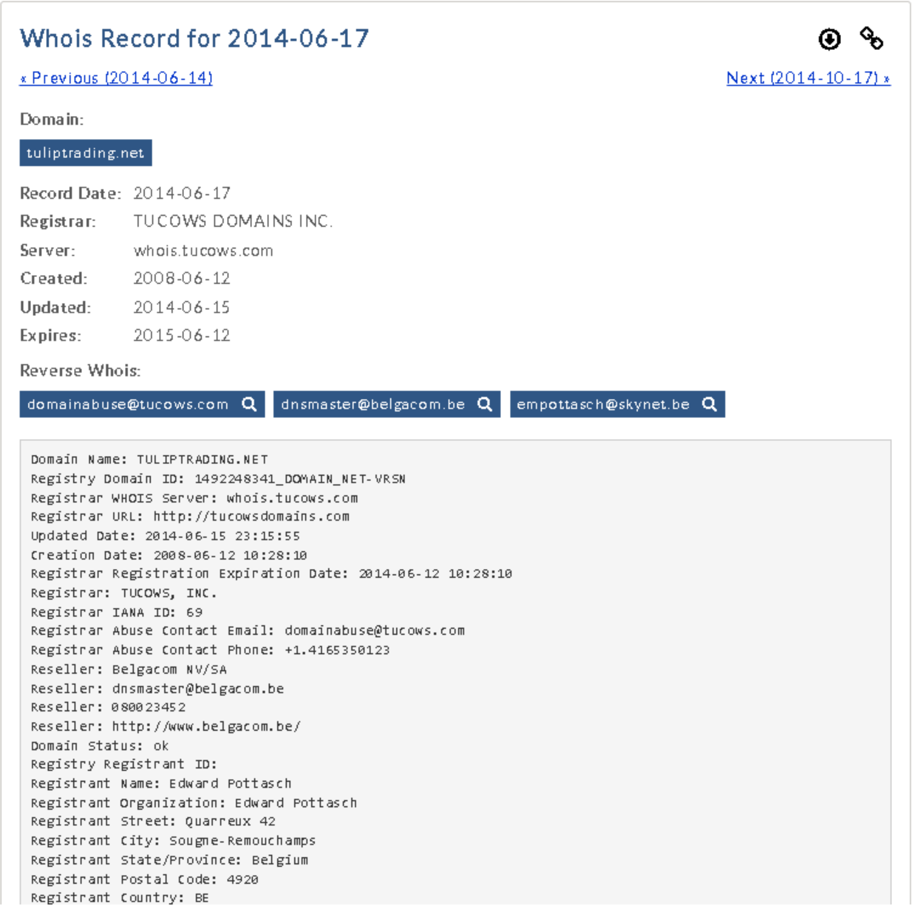
182. The registration information dated 17 October 2014 is the first entry that lists “Craig S Wright” as the registrant. The Registrar history for the domain is listed below. From this, it can be seen that there was a previous registration that pre-dates this registration:



Registrar History

Date	Registrar
2008-06-12	Tucows
2014-10-17	Directl.com

183. Inspecting the two registrations either side of 17 October 2014 indicates the following two sets of information:



Whois Record for 2014-06-17

« Previous (2014-06-14) Next (2014-10-17) »

Domain:

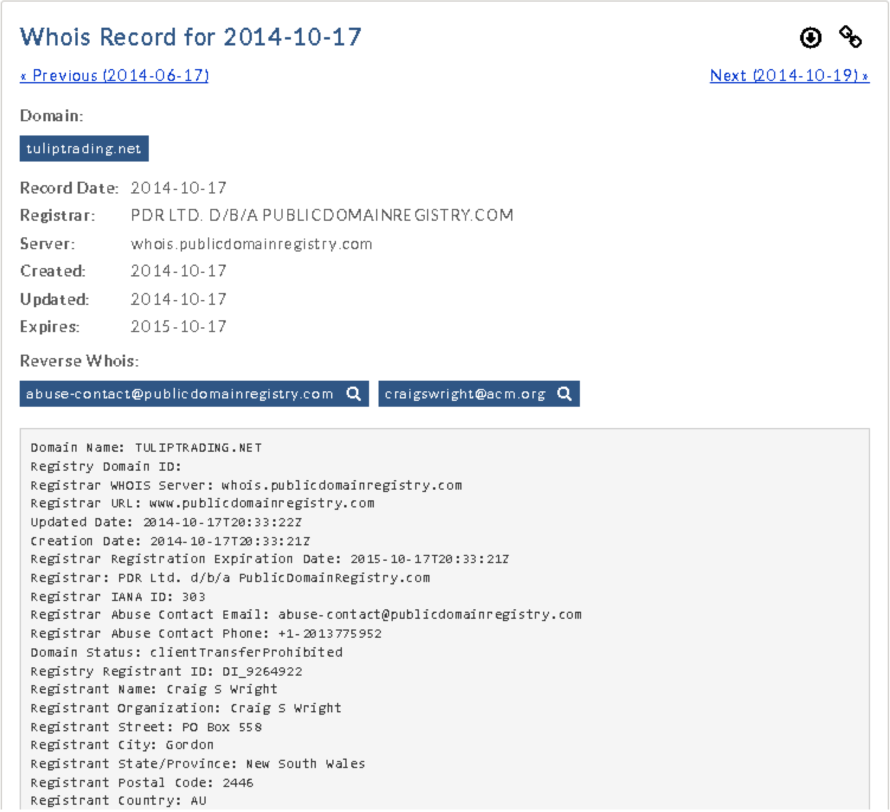
tuliptrading.net

Record Date: 2014-06-17
Registrar: TUCOWS DOMAINS INC.
Server: whois.tucows.com
Created: 2008-06-12
Updated: 2014-06-15
Expires: 2015-06-12

Reverse Whois:

domainabuse@tucows.com dnsmaster@belgacom.be empottasch@skynet.be

```
Domain Name: TULIPTRADING.NET
Registry Domain ID: 1492248341_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2014-06-15 23:15:55
Creation Date: 2008-06-12 10:28:10
Registrar Registration Expiration Date: 2014-06-12 10:28:10
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Reseller: Belgacom NV/SA
Reseller: dnsmaster@belgacom.be
Reseller: 080023452
Reseller: http://www.belgacom.be/
Domain Status: ok
Registry Registrant ID:
Registrant Name: Edward Pottasch
Registrant Organization: Edward Pottasch
Registrant Street: Quarreux 42
Registrant City: Sougne-Remouchamps
Registrant State/Province: Belgium
Registrant Postal Code: 4920
Registrant Country: BE
```



Whois Record for 2014-10-17

Domain:

tuliptrading.net

Record Date: 2014-10-17
Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Server: whois.publicdomainregistry.com
Created: 2014-10-17
Updated: 2014-10-17
Expires: 2015-10-17

Reverse Whois:

abuse-contact@publicdomainregistry.com
craigswright@acm.org

```
Domain Name: TULIPTRADING.NET
Registry Domain ID:
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2014-10-17T20:33:22Z
Creation Date: 2014-10-17T20:33:21Z
Registrar Registration Expiration Date: 2015-10-17T20:33:21Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1-2013775952
Domain Status: clientTransferProhibited
Registry Registrant ID: DI_9264922
Registrant Name: Craig S Wright
Registrant Organization: Craig S Wright
Registrant Street: PO Box 558
Registrant City: Gordon
Registrant State/Province: New South Wales
Registrant Postal Code: 2446
Registrant Country: AU
```

184. These indicate that prior to 17 October 2014, the domain tuliptrading.net was registered to a Belgian national named Edward Pottasch, and after that the owner changed to Craig S Wright.

185. I note that the registration of the domain name for Tulip Trading in this is consistent in date with my analysis of the invoice documents in the initial disclosure dataset which indicates the purchase of a shelf company at that time.

VMWARE CONFIGURATION FILES

186. Four configuration files that relate to the VMware application have been included in disclosure. The table below lists the limited available information provided in the disclosure load file.

ID number	Master DateTime	Date Created	Time Created	Extension	File Name
ID_006471	31/10/2007 18:56:28	21/09/2006	07:13:46	vmsd	image.raw.vmsd
ID_006472	31/10/2007 18:58:40	21/09/2006	07:13:46	vmx	image.raw.vmx
ID_006492	31/10/2007 18:56:18	21/09/2006	07:12:58	vmdk	image.raw.vmdk
ID_006493	31/10/2007 18:56:26	21/09/2006	07:13:46	vmxf	image.raw.vmxf

187. From the other information available in the Load file, I understand the column “Master Datetime” to correlate to the last modified timestamp for the file, although this is not a heading used in other load files in these proceedings.

188. I understand from the various statements of Dr Wright that he attests that he used VMware products in relation to the BDOPC.RAW {SS} (the disk image stored on the Samsung drive), and that these four configuration files have been disclosed as evidence of how this was configured.

189. I have analysed the content of these files and make several observations regarding their content and properties as follows.

Reminder about images on the Samsung Drive

190. As well as BDOPC.RAW{SS}, I also found a number of other disk images that existed on the Samsung drive, but have since been deleted. I produce below a table of the timestamps and basic properties of these files, which is explained further in my Fourth Report:

Name	Deleted	Logical Size	File Created	Last Written	Last Accessed
BDOPC.raw		39,999,504,384	31/10/2007 23:48:05	31/10/2007 23:48:06	31/10/2007 23:48:06
BDOPC.raw	yes	39,999,504,384	31/10/2007 07:14:42	31/10/2007 07:15:18	31/10/2007 07:15:18
InfoDef09.raw	yes	179,594,199,040	13/09/2009 09:35:22	19/09/2017 11:34:42	13/09/2009 09:35:22
image.raw	yes	522,117,840,896	13/09/2009 09:50:10	13/09/2009 09:47:28	13/09/2009 09:50:10

191. My first and most obvious observation is that the creation timestamps for the VMware configuration files (21 September 2006) predate all of the disk images on the Samsung drive. This is, that the configuration files are listed as being created before the disk images themselves. However, I do not draw a conclusion from this itself as it is possible to manually modify a pre-existing configuration such that it points to a different disk image.

The four configuration files provided

192. It is not possible to fully analyse the VM environment using only the files provided. The four files provided do not amount to a complete VM environment to which these files relate. It is not possible to reconcile the differences between the disk images on the Samsung drive (BDOPC.raw, Image.raw, and InfoDef09.raw) against these configuration files without access to the remaining environment data.

193. The four configuration files themselves are as follows:

a. **ID_006472 - image.raw.vmx.** The VMX file is the main apex configuration file. It sets the VM environment and attached virtual hardware or disk images

b. **ID_006492 - image.raw.vmdk.** The VMDK is a disk descriptor file. It is not the disk image itself, but contains information about the disk image, and how this should be addressed by VMware.

c. **ID_006493 - image.raw.vmxf.** The VMXF file is used to store extended configuration information.

d. **ID_006471 - image.raw.vmsd.** The VMSD file is used to track snapshot files and information.

194. I consider the content of each of the configuration files in turn below:

ID_006472 – "image.raw.vmx"

195. This is a short file, and the entire content of the file is shown below:

```
 #Static Values
config.version = "8"
virtualHW.version = "3"
floppy0.present = "FALSE"
displayName="image.raw"

#Drive Info
ide0:0.present = "TRUE"
ide0:0.fileName = "image.raw-000001.vmdk"
ide0:0.deviceType = "disk"
ide0:0.mode = "persistent"
ide1:0.present = "TRUE"
ide1:0.fileName = "auto detect"
ide1:0.deviceType = "cdrom-raw"

#User Specified
memsize="512"
rtc.starttime="1193820925"
guestOS = "winxppro"
snapshot.disabled = "TRUE"

extendedConfigFile = "image.raw.vmxf"

ide0:0.redo = ""
uuid.location = "56 4d 52 dc 9d 46 4c 7e-25 b1 16 28 43 36 80 b0"
uuid.bios = "56 4d 52 dc 9d 46 4c 7e-25 b1 16 28 43 36 80 b0"
ide1:0.autodetect = "TRUE"
usb.present = "TRUE"
checkpoint.vmState = "image.raw.vmss"
```

196. Looking at the content of this file:

a. The value of "3" in the line "`virtualHW.version = "3"`" is consistent with older versions of VMware software.

b. The value "`image.raw`" in the line "`displayName="image.raw"`" is a user-customisable name for the virtual machine. It is not specifically indicative of the name of the disk image. The text is set by the user.

c. Under the section "`#Drive Info`", the entry "`ide0:0.fileName =`" indicates the name of the disk image filename as "`image.raw-000001.vmdk`". I understand this to be indicative that the VM is operating with snapshots, and the configuration is pointing to the first snapshot, not directly to the original disk image file itself.

d. The entry “`rtc.starttime="1193820925"`” is used to force the clock within the VM to be set to the specified date and time at system startup. This timestamp would set the clock on the computer to Wednesday, 31 October 2007 08:55:25 as the local time of the VM.

The missing snapshot

197. The relevant Snapshot descriptor vmdk file “image.raw-000001.vmdk” has not been provided.

198. A file with the VMDK descriptor “image.raw.vmdk” has been provided instead, however, that appears to be a different file, as it has a different file name.

No traces of booting BDOPC.raw or other images as a VM

199. I observe that this configuration file makes reference only to one disk as a storage drive, and has a Virtual CD drive attached to it. This means that the VM would attempt to boot from the configured disk image, unless directed to boot from a bootable CD. The disk image “image.raw-000001.vmdk” is configured with the IDE device address “ide0:0” which would be described as Primary Master on a physical computer. This would be the primary boot device if the physical computer was not configured to boot to an alternate device. Put simply, the disk image referred to is the only hard disk configured in this virtual machine.

200. The disk image “image.raw-000001.vmdk” is not configured as secondary storage to this VM configuration.

201. If this VM was started, the computer would attempt to undertake a process of installing drivers and software in the virtual environment to allow the virtual computer to operate in the virtual environment, which would have left traces of such activity on the image itself. However, neither I or Stroz Freidberg found any indications that the disk image BDOPC.raw had been subjected to the installation of such drivers (as we agreed in our joint statement {Q/6/1}).

202. I also found no such traces in any of the other disk images I recovered and analysed in my Fourth Report.

203. This therefore indicates that the image files were not booted up in VMWare. Both Stroz Friedberg and I also agreed that the disk image “BDOPC.raw” was attached to a computer as a secondary storage device (and not as a bootable disk).

204. It is possible that the images might be attached as secondary storage either to a physical computer, or to a computer that was running as a virtual machine. The artefacts of interaction would not differ between those.

ID_006492 - image.raw.vmdk

205. This file image.raw.vmdk is the Virtual Machine Disk Descriptor file. It contains information about the configured disk. As identified above, this descriptor file is not explicitly listed within the .VMX configuration file, which points to a differently-named snapshot file "image.raw-000001.vmdk"

206. I have therefore proceeded on the assumption that this file is intended to be, or be related to, the file that is actually listed, noting however that I am missing information in that the snapshot file actually referred to has not been provided.

207. The entire content of "`image.raw.vmdk`" is set out below

```
# Disk Descriptor File
version=1
CID=fffffffe
parentCID=ffffffff
createType="monolithicFlat"

# Extent description
RW 78124095 FLAT "D:\image.raw" 0
RW 16191 ZERO

#DDB - Disk Data Base
ddb.adapterType = "ide"
ddb.geometry.sectors = "63"
ddb.geometry.heads = "254"
ddb.geometry.cylinders = "1023"
ddb.virtualHWVersion = "3"
```

208. This indicates that the base disk image file is the raw disk image "`image.raw`" and that it was stored on the D: drive. I note that:

a. This configuration specifies a sector size of `78124095` (78,124,095) sectors.

b. That number of sectors is equivalent to 39,999,**536,640** bytes.

c. As listed in the table earlier in this report, BDOPC.raw {SS}is only 39,999,**504,384** bytes in capacity and therefore does not match the specified size. BDOPC.raw{SS} is therefore not a candidate for the image which is being referred to.

209. However, I found a deleted raw disk image image.raw{SS} which I analysed in my Fourth Report, which is a better candidate for the image being referred to:

a. The image file name is the same as that referred to in the .vmdk file.

b. Although the image image.raw{SS} was mostly blank space, the last sector with space that was used is the sector at offset 78,124,095.

c. That matches the sector size of the image referred to in the .vmdk file.

210. Therefore, from the available information the booted image may well have been a related ancestor or copy of the recovered (deleted) image.raw{SS}. Since the relevant files have not been fully disclosed, it is not possible to be certain. However, I re-iterate that there is no evidence found on either BDOPC.raw{SS} or image.raw{SS} themselves that would be consistent with them having been modified in the manner consistent with being the files referred to in the VMware configuration files provided.

ID_006471 - image.raw.vmsd

211. The VMSD file includes some information about the snapshot produced. The entire content of the file is shown below:

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "image.raw-Snapshot1.vmsn"
snapshot0.displayName = "Original1193820976484"
snapshot0.createTimeHigh = "277958"
snapshot0.createTimeLow = "465728432"
snapshot0.numDisks = "1"
snapshot0.disk0.fileName = "image.raw.vmdk"
snapshot0.disk0.node = "ide0:0"
```

212. The entry "`snapshot0.displayName =`" relates to the display name of the snapshot. I observe that this display name "`Original1193820976484`" includes an embedded timestamp. This timestamp would be displayed as shown here in VMware, and decodes as Wednesday, 31 October 2007 08:56:16 which is less than a minute after the "`rtc.starttime`" time configured in the VMX file. This corresponds to a forced clock time ascribed to the VM it relates to.

Application to BDOPC.RAW

213. Setting all of these observations aside, in the hypothetical situation of BDOPC being mounted on a VMware virtual machine as attached storage, this still must have been undertaken after 17 September 2023 for the reasons set out in my Fourth Report.

214. The provided VMware configuration files and the explanation about use of it as a VM do not account for the anomalies identified with the content of the disk image BDOPC.raw{SS}. They also do not account for the anomalies identified with the content of the deleted disk image file image.raw{SS}.

215. The provision of these VMware configuration files does not, therefore, alter my opinion regarding the BDOPC.raw{SS} and image.raw{SS} disk images.

THE BDO EMAILS AND DEMORGAN APPOINTMENT

216. This section relates to three BDO emails {ID_006473}, {ID_006474}, {ID_006475} and one Demorgan meeting appointment {ID_006477}. I have not undertaken a thorough examination of these emails, but address their face value content as follows.

217. The three BDO email messages are dated 12 June 2008. They appear to discuss the computing equipment that Dr Wright was requesting that BDO provision for him. There is no useful indication regarding what was approved, or what the final deployment was. This discussion post-dates the 2007 dates of the BDOPC.raw image, and does not affect any of my conclusions.

218. The Demorgan Meeting appointment is for a meeting dated 25 September 2014. It describes without much detail a process of deleting or decommissioning un-necessary data/virtual machines on a Dell Blade Server and a Dell VMware server. There is no indication as to what was deleted or retained or what archives, if any, were produced to protect against accidental deletion of important information, other than a suggestion that some were badly configured and ineffective at their intended task. It does not affect any of my conclusions.

219. While both of these sets of information mention Vmware-related virtual machines, there is no indication as to what these were or how they were used, and I have not been provided with access to any virtual machines or information about how they were used. There is insufficient information to for any opinion beyond indicating that Dr Wright discussed VMware services.

220. Overall, the content of these messages does not affect my opinion regarding the BDOPC.raw image in respect of VMware virtualisation or other findings discussed in my reports.

ROBOTS.TXT AND PGP KEY

221. In my Fourth Report, at paragraph 146 {G/6/47}, I addressed a PGP key from the Wayback Machine archive of the domain Bitcoin.org. The key itself contained timestamps relating to October 2008. The Wayback Machine archive was captured in 2011, and the Wayback Machine archives contained headers indicating that it was first uploaded to the bitcoin.org server in October 2008.

222. I understand from Bird & Bird that Dr Wright has stated that the key was not crawled by the Wayback Machine prior to 2011 because it was set to be ignored by ‘robot.txt’.

223. I understand this to be a reference to robots.txt. A robots.txt file is a text file which can be included in a website, which instructs crawlers such as search engines to ignore (i.e. not crawl) certain parts of a website, with a line indicating that it “Disallows” crawling of each line.

224. The robots.txt file of Bitcoin.org was first archived on the Wayback Machine at https://web.archive.org/web/20100813060720/http://www.bitcoin.org/robots.txt on 13 August 2010.

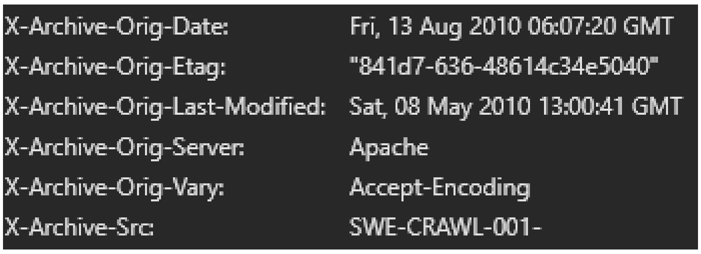
225. The entire content of the robots.txt file is listed below:

```
# $Id: robots.txt,v 1.9.2.1 2008/12/10 20:12:19 goba Exp $
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these “robots” where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /sites/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /contact/
Disallow: /logout/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=contact/
Disallow: /?q=logout/
Disallow: /?q=node/add/
Disallow: /?q=search/
```

```
    Disallow: /?q=user/password/
    Disallow: /?q=user/register/
    Disallow: /?q=user/login/
```

226. Following the same process I undertook for the PGP key itself, the Web Archive has captured a last modified timestamp of 08 May 2010 for the “robots.txt” file as shown below:

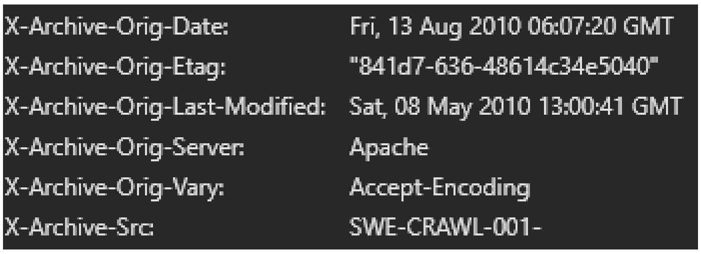


```
X-Archive-Orig-Date:            Fri, 13 Aug 2010 06:07:20 GMT
X-Archive-Orig-Etag:            "841d7-636-48614c34e5040"
X-Archive-Orig-Last-Modified:   Sat, 08 May 2010 13:00:41 GMT
X-Archive-Orig-Server:          Apache
X-Archive-Orig-Vary:            Accept-Encoding
X-Archive-Src:                  SWE-CRAWL-001-
```

227. This demonstrates that a properly-configured robots.txt file was applied to the website prior to 2011, and was first uploaded to the server in that form before Friday 13 August 2010 and possibly as early as Saturday 8 May 2010.

228. However, contrary to Dr Wright’s suggestion, the PGP key that I analysed was at the page /Satoshi_Nakamoto.asc, and that PGP key is not listed in the August 2010 version of the robots.txt file as one of the pages to be ignored.

229. Following the same process I undertook for the PGP key itself, the Web Archive has captured a last modified timestamp of 08 May 2010 for the “robots.txt” file as shown below:



```
X-Archive-Orig-Date:            Fri, 13 Aug 2010 06:07:20 GMT
X-Archive-Orig-Etag:            "841d7-636-48614c34e5040"
X-Archive-Orig-Last-Modified:   Sat, 08 May 2010 13:00:41 GMT
X-Archive-Orig-Server:          Apache
X-Archive-Orig-Vary:            Accept-Encoding
X-Archive-Src:                  SWE-CRAWL-001-
```

230. I have been unable to find an earlier Web Archive snapshot for the file “Satoshi_Nakamoto.asc” or robots.txt. The absence of a capture of the key before 2011 is therefore not due to the configuration of robots.txt on the domain bitcoin.org. It is normal for pages on websites not to be captured for some time, and the absence of a capture snapshot on a specific date does not mean that the page did not exist before then. That conclusion would be unsound, and there is additional evidence that the key did in fact exist (including that it was already linked to on an archive snapshot of the bitcoin.org homepage in 2009, and the fact that the metadata of the PGP key indicates an October 2008 creation).

Declaration

1. I understand that my duty is to help the Court to achieve the overriding objective by giving independent assistance by way of objective, unbiased opinion on matters within my expertise, both in preparing reports and giving oral evidence. I understand that this duty overrides any obligation to the party by whom I am engaged or the person who has paid or is liable to pay me. I confirm that I have complied with and will continue to comply with that duty.
2. I confirm that I have not entered into any arrangement where the amount or payment of my fees is in any way dependent on the outcome of the case.
3. I know of no conflict of interest of any kind, other than any which I have disclosed in my report. I do not consider that any interest affects my suitability as an expert witness on any issues on which I have given evidence.
4. I will advise the party by whom I am instructed if, between the date of my report and the trial, there is any change in circumstances which affects this.
5. I have shown the sources of all information I have used.
6. I have exercised reasonable care and skill in order to be accurate and complete in preparing this report.
7. I have endeavoured to include in my report those matters, of which I have knowledge or of which I have been made aware, that might adversely affect the validity of my opinion. I have clearly stated any qualifications to my opinion.
8. I have not, without forming an independent view, included or excluded anything which has been suggested to me by others including my instructing lawyers.
9. I will notify those instructing me immediately and confirm in writing if for any reason my existing report requires any correction or qualification or my opinion changes.
10. I understand that:

    a. my report will form the evidence to be given under oath or affirmation;

    b. the court may at any stage direct a discussion to take place between experts and has done in this case;

c. the court may direct that, following a discussion between the experts, a statement should be prepared showing those issues which are agreed and those issues which are not agreed;

d. I may be required to attend Court to be cross-examined on my report; and

e. I am likely to be the subject of public adverse criticism by the judge if the Court concludes that I have not taken reasonable care in trying to meet the standards set out above.

11. I have read Part 35 of the Civil Procedure Rules and I have complied with its requirements. I am aware of the requirements of Practice Direction 35 and the Guidance for the Instruction of Experts in Civil Claims 2014.

12. I confirm that I have acted in accordance with the Code of Practice for Experts.

13. I confirm that I have made clear which facts and matters referred to in this report are within my own knowledge and which are not. Those that are within my own knowledge I confirm to be true. The opinions I have expressed represent my true and complete professional opinions on the matters to which they refer.

Signed: Dated: 18 February 2024