IN THE HIGH COURT OF JUSTICE **Claim No: IL-2021-000019**

BUSINESS AND PROPERTY COURTS OF ENGLAND & WALES

INTELLECTUAL PROPERTY LIST (ChD)

B E T W E E N :

CRYPTO OPEN PATENT ALLIANCE **Claimant**

-and-

DR CRAIG STEVEN WRIGHT

Defendant

FOURTH EXPERT REPORT

OF MR PATRICK MADDEN

INTRODUCTION AND SUMMARY OF FINDINGS

1. This is my Fourth Report in these proceeding I have approached it in the same way as my previous reports and with the same duties in mind. For the purpose of this report I have been provided with:

    a. The information available to me when I attended the PTR hearing on 15 December 2023 (including the witness statements of Dr Wright, Ms Field, and Mr Sherrell used at that hearing);

    b. A forensic image of the Samsung Drive,

    c. The relevant confidentiality terms and a list of documents in which privilege has been asserted, and

{E/26} d. The Ninth and Tenth Witness Statements of Dr Wright, and

{E/31} e. Copies of letters between Shoosmiths and Bird & Bird dated 10 January 2024 and 15 January 2024.

2. I have been asked to do my best in the short time available to provide my views on the authenticity of the 97 New Reliance Documents, and the BDO Raw Image, taking into account the information available. As with my previous report, Bird & Bird has assisted with the drafting after I reported the results of my analysis and conclusions to them. Bird & Bird has also created the diagrams.

Approach to this report

{G/1} {G/2} {G/5} 3. I have approached my analysis of these new data sources in the same way as my First, Second, and Third Reports. I have done a lot of analysis in a short time, including recovering deleted files and analysing various drive images totalling over 800GB of data. I have worked on it every day since the PTR (including Christmas day and other bank holidays) to conduct my analysis, and to ensure that my findings are accurate.

4. This has involved a great deal of steps, checks, and avenues of investigation. Some of those have provided information which has assisted me to form an opinion, in which case I have repeated the steps at least once (in some cases multiple times) to double check and confirm my findings. Other investigations did not result in any pertinent information, or were done to double check that there were no other surroundings facts that needed to be accounted for. Unlike my earlier reports, it is not possible for me to report on the details of all those avenues. Instead I have focused on the

observations which relate to the question of authenticity of documents, and I have tried to present my observations very directly and to explain how these informed my conclusions. This is different to my earlier reports in which I tried to be much more comprehensive, even including mentioning details of investigative avenues that did not produce meaningful results in the context of authenticity (at least where they might be thought pertinent). However, this is the only way that I have been able to conduct my analysis and produce this report in the limited time provided. Other avenues could be investigated which may potentially provide further indications, though the findings I have made are based on very clear indications that I have found within the new data sources, and I do not consider it necessary or likely to be useful to do so.

Structure of this Report

5. This report is divided into the following sections:

{E/26}
{E/31}
{CSW/7}

{H/278}
{H/289}
{H/304}

a. My Main Report, which addresses the Samsung Drive and BDO Image as a whole and responses to Dr Wright's 9th, 10th, and 12th witness statements,

b. Three Appendices, PM46 to PM48, which contain observations on specific documents,

c. An Annex 1, in which I set out what I believe (to my best ability) to be the true timeline of editing of the BDO Image BDOPC.raw and associated documents, and

d. An Annex 2, in which I summarise findings on the 97 New Reliance Documents in the form of a tick-list.

6. My Main Report and Appendices take things by themes rather than a chronological account of my investigation, as the different parts are so interrelated that it was not possible to do so. Although I attempted to draft it chronologically, it became very difficult to follow because different findings informed each other, and led me to build up an overall picture. The sections are:

a. First, I explain the content of the Samsung Drive in overview.

b. I then move on to discuss observations about the BDO Drive image itself, as a whole.

c. I then explain about another disk image, which is called InfoDef09.raw, and how that relates to BDOPC.raw

d. I then address various New Reliance Documents individually and in groups, to set out some pertinent findings about those.

e. I have also been asked to comment on other recent statements of Dr Wright and do so in the final section of this report.

Understanding the different data sources

7. This report therefore requires looking at files from three or more different sources. They are all contained in the Samsung Drive, but some files within the Samsung Drive are drive images. When those drive images are mounted (opened as if they were drives themselves), more files within them become visible. In some cases, the same file is present in more than one of these locations: in other cases, they are very similar versions of a file (but which are different often in small but important ways) which need to be compared.

8. It is therefore easy to lose track of where each file comes from. As a shorthand to solve this problem, in this report wherever I talk about a file from a drive, there is a suffix to show where it comes from, as follows:

Suffix	Example	Meaning
{SS}	example.txt{SS}	This file would be called example.txt and would be on the Samsung Drive directly (not extracted from within any of the raw image files)
{BDO}	example.txt{BDO}	This would be a file extracted from within the BDO Image, called example.txt

9. Note that since the BDO Image itself is a single file on the Samsung Drive, using this convention the file of the BDO Image is listed as **BDOPC.raw{SS}**

Terminology

10. In this report I refer to the following terms:

    a. "**Image**": I use the term 'image' to refer exclusively to disk images. (I will use other words to refer to e.g. "*pictures*" or "*photographs*" if needed). Just like any other computer file, a disk image is a single file[1], that is stored on a storage medium like a drive in the same way, and can be copied, deleted, or recovered from deletion like any other file. The purpose of a disk image is usually to record the data bytes of another computer disk. Images are usually created by 'imaging' (i.e. copying the data bytes of) an existing drive, but as I explain below this report also covers drive images that have later been edited.

    b. **RAW and Forensic Images:** Just as picture files can be stored in various different formats, so there are different file formats for a drive image file. A forensic image is usually created

[1] Or a collection of files that are used collectively as one.

with metadata recording its collection process, and in a forensic preservation context, it is routinely accompanied by an audit trail documenting the image creation process and including data validation information such as MD5 checksums. On the other hand a "Raw" image usually has the file extension ".raw" and is a much lower metadata format: it just records the data bytes of a drive without anything additional.

c. **Samsung Drive**: The 1TB Samsung USB Drive also denoted as **{SS}**. I have been provided with a forensic image of this drive as follows. I received a hard disk from a KLD consultant on 20 December 2023 at 15:55. The drive was encrypted using Veracrypt. The password was provided to me by Shoosmiths at 16:28 of that day. This hard disk contained a forensic image of the Samsung Drive. This was produced as an E01 evidence container which captures the content of a storage medium in a tamper resistant / tamper evident file structure. It includes some basic audit information regarding its capture, such as the date and time of acquisition (according to the devices used to conduct the capture), and an MD5 hash of the entire captured content. The forensic image is recorded as being captured on 20 September 2023 starting at 10:03 and has an MD5 checksum "`d1e53392c27e6bf5c7ef4b811bde1e79`". I assume this to be a good copy of the Samsung Drive.

d. **BDOPC.raw**: The BDO Raw Image file, that was introduced following the PTR. This is itself a single file contained on the Samsung Drive so it is denoted as **BDOPC.raw{SS}** when helpful in context.

e. **The Original 2007 BDO Image**: As I explain below in my opinion there was a true, original image which was taken of the BDO PC in July 2007, which I refer to as the "Original 2007 BDO Image". However, that is different to BDOPC.raw, which in my opinion is a later-edited version of the Original 2007 BDO Image. I do not have access to the Original 2007 BDO Image, which has not been provided.[2]

f. **The BDO PC:** the 2007 computer, likely a laptop computer whose hard drive was captured to form the Original 2007 BDO Image.

g. **New Reliance Documents**: The 97 additional reliance documents introduced after the PTR.

h. **Note on file sizes / Gigabytes:** The definition of "Gigabytes" varies, with some applications calculating 1GB=1000MB and others as 1GB=1024MB. This difference has not been important for my analysis at all, and so where I list file sizes in this report they are

[2] There is however a similarly-named file which has been deleted from the Samsung Drive. I address this at [ref].

approximate, to give a general view of what each file entails and how they relate to each other. There is only one case where my analysis has been informed by (among other things) comparing file sizes, and in that one case I have given the specific number of bytes so the definition of "Gigabytes" does not matter.

Summary of findings

{G/5} 11. In my Third Report I formed the opinion based on the information which was then available to me that the BDO Image BDOPC.raw content has been manipulated, that data on the Samsung Drive had been deleted in September 2023 and that several of the documents showed signs of backdating with the use of clock manipulation and metadata editing techniques, with several of the 97 New Reliance Documents appearing to date from 2020 onwards.

{G/5} 12. However, as I wrote in my Third Report, the vast majority of the 97 documents could not at that time be properly analysed outside their forensic context. I have now been provided with access to the 97 New Reliance Documents in their forensic context for the Samsung Drive and the BDO Files, and it has allowed me to investigate those files more fully.

13. In summary, I have found as follows:

a. **There are multiple iterations of BDO image files stored on the Samsung drive.** There is not just one version, but multiple different versions that have undergone an editing process.. Some of these have been deleted but I was able to entirely recover two of them (called Image.raw{SS} and InfoDef09.raw{SS}). These two images are previous iterations of the BDOPC.raw{SS} file: The content of them is over 99.5% identical to BDOPC.raw{SS}, but some files have been changed in ways that make them look older than they are.

b. **The file BDOPC.raw{SS} has been manipulated.** The internal content of BDOPC.raw as a whole is not authentic to 2007 and has definitely been manipulated. In addition to the findings in my Third Report, I was able to confirm that the internal timestamps record that its content was edited in September 2023, among other things.

c. **The manipulation was recent, and timestamps in 2007, 2009, 2014, and 2017 are unreliable.** The Samsung Drive shows indications of (genuine) routine use in 2015-2016.There are also a variety of timestamps relating to the Samsung Drive and the image BDOPC.raw which appear to record actions taken in 2007, 2009, 2014, and 2017. However, these are all contradicted by other indications, which show that they must have been recorded at a time after 12 September 2023, and by the presence of software and references which do not match the recorded 2007-2017 dates. This indicates the use of clock manipulation

techniques, and the 2007, 2009, 2014, and 2017 timestamps are not reliable. The manipulation was recent, done in September 2023, and involved backdating.

d. **There is a large encrypted zip file on the drive, InfoDef09.zip{SS}, which is relevant.** It contains 1 file called InfoDef09.raw (within the zip). The passwords have not been provided so the content cannot be inspected directly. However, the metadata of the zip shows that it contains an identical copy of the deleted file InfoDef09.raw{SS} that I have been able to recover (and that in turn is related to BDOPC.raw{SS} as described above).

e. **Hundreds of GB of data were deleted from the Samsung Drive in September 2023.** In addition to the two raw files mentioned above (which are recoverable), large amounts of other data has been deleted but are not recoverable (including compressed archives "Prior PC.rar{SS}" and another version of the file BDOPC.raw{SS} which has the same file name and file size but was deleted).

f. Of the 97 New Reliance Documents:

- **At least 71 are not original to the BDO PC and were entirely added later.** Most of the 97 New Reliance Documents did not exist on the BDO PC in 2007 and have been entirely added much more recently. There are several indicators of this, including that they were added with dates that are after the time that the BDO PC was last used as a computer, and that they were added using a different computer with a different user account.
- For around a quarter of those 97 New Reliance Documents, I was able to directly establish a pattern of editing showing that they were manipulated even after being added to the images, in September 2023. The editing included changes that appear relevant to the case, for example modifying "Bitcoin" to "Timecoin" and altering references to dates mentioning 2009 and 2016 dates.
- **The remaining 26 of the 97 are inconclusive, and I approach them with caution:** After addressing the 71 documents above, there remain 26 out of the 97 for which there is not the same level of evidence of inauthenticity. I can say that at least *some* version of those documents definitely existed on the BDO PC when it was originally imaged, with the same file name and location on the imaged drive. However, these may well have been modified more recently after the Original 2007 BDO Image was created: it is not possible to be sure because the Original 2007 BDO Image has not been provided. I treat the authenticity of these 26 documents with caution, in view of my findings about the data source as a whole.

g. **ChatGPT:** In the deleted copies of some of the 97 New Reliance Documents, there are indications that ChatGPT may have been used to create them. These indications were

removed from the versions disclosed and those contained within BDOPC.raw{SS}, but are present in the earlier revisions that were deleted.

h. **Clock manipulation:** further to the analysis mentioned in my Third Report, there are more indications of clock manipulation used in connection with the 97 New Reliance Documents, BDOPC.raw, and the Samsung Drive as a whole.

14. Although the above summary contains various conclusions for convenience, I did not jump to these conclusions: they were not formed until after completing my analysis.

Timeline Summary

15. Based on my findings which I explain throughout this report, it has been possible to establish a timeline of use of the Samsung Drive, and a resulting pattern of editing documents.

16. The timeline is included at Annex 1 to this report. That timeline represents my best effort to reconstruct the events that I have observed, based on concrete observations about activity that took place in respect of BDOPC.raw and the Samsung Drive on 12 September 2023, 17 September 2023, 18 September 2023 and 19 September 2023 before the drive was forensically imaged on 20 September 2023.

17. In some cases, the order of steps taken may not be possible to establish precisely. However, each step of the timeline is founded on the steps that went before, and it is possible to be confident about the overall order of editing from one image to the next; and the time period for that editing.

18. Since the pattern of editing involved clock manipulation (which is very clearly indicated in a number of independent ways), it is not possible to be entirely precise about the order of editing, and the timeline sometimes gives general periods in which an event took place (e.g. “between 18 and 19 September 2023”).

OVERVIEW OF THE SAMSUNG DRIVE AND ITS FILES

File system

19. The Samsung Drive is a USB connected SSD (Solid state drive) with 1 terabyte of capacity. It is formatted with an ExFAT file system. The ExFAT file system is a standard type of file system and is typical for such a drive, though it is not the filing system most commonly associated with Windows.

20. However, this file system is relatively basic in terms of the metadata recorded for the files stored on it (compared to some other file systems such as NTFS, which records additional details about

the user accounts and much more metadata for each file, such as UUIDs in relation to the user deleting files). By contrast, the internal content of BDOPC.raw is formatted with NTFS.

Manufacture of Samsung Drive

21. The Samsung Drive is a portable SSD T1. That model was first manufactured and released in 2015, as is shown by the following press release on the Samsung website dated 5 January 2015, which announces the release of the Samsung T1 drive https://news.samsung.com/us/samsung-electronics-new-portable-ssd-t1-brings-exceptional-speed-style-and-durability-for-todays-on-the-go-lifestyle/[3] and states: "Available in 250 gigabyte (GB), 500GB and 1 terabyte (TB) storage capacities, the Portable SSD T1 will launch globally in 15 countries across the United States, European and Asian markets later this month"

22. I have also confirmed this against a number of reviews from that month (January 2015), such as the following review dated 6 January 2015 at the following web page, which describes the model T1 as "Samsung's first portable SSD": https://newatlas.com/samsung-first-portable-ssd/35465/[4].

Storage on the Samsung Drive

23. The Samsung Drive has about 143GB of used space and about 787GB of free space:

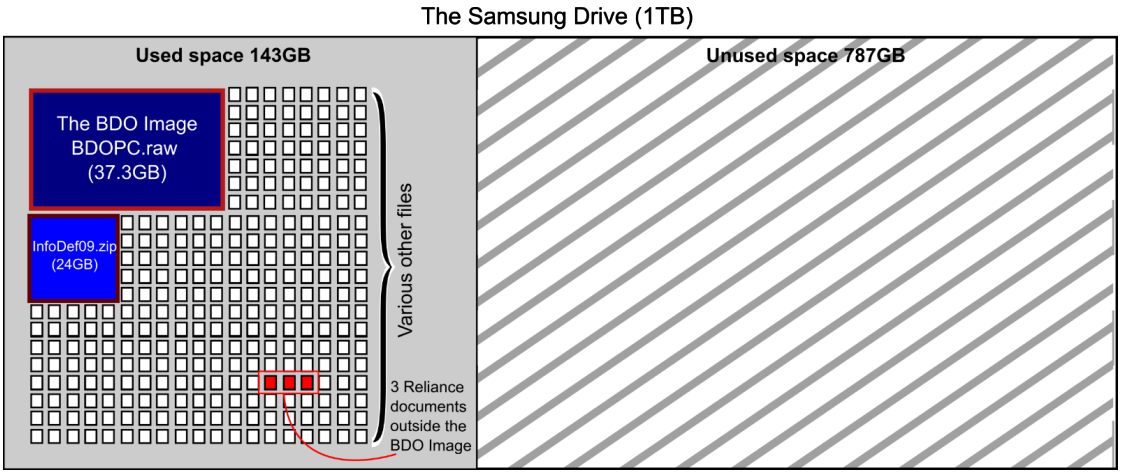


Figure 1: Overview of the Samsung Drive

{H/305}
{H/306}

[3] A capture of this page is available at **Exhibit PM-R 4.1**
[4] A capture of this website is available at **Exhibit PM-R 4.2**

24. As illustrated above (with red highlights), there are 5 main extant files on the Samsung drive that are relevant for this report. They are:

    a. **BDOPC.raw{SS} (37.3GB)**. This is the image that was discussed at the PTR and which I analyse in detail below.

    b. **InfoDef09.zip{SS}**, a 24GB encrypted zip file. Since it is encrypted, I cannot directly access the content,

{ID_004686}
{ID_004735}
{ID_004736}

    c. **Copies of three of the 97 New Reliance Documents:** ID_004686{SS}, ID_004735{SS}, and ID_004736{SS}. I note that this is different to the information that was provided in relation to these files before my Third Report. At that time two out of these three were listed (in the list provided by Shoosmiths) as being within the Samsung Drive alone, and one within BDOPC.raw. I have established that all three are present within BDOPC.raw, and copies of all three are also present in the Samsung Drive.

25. There are also various other files on the drive, which are generically shown as white boxes at Figure 1 above (while I touch on some of these files later in my report, they are not as central to my analysis).

Samsung Drive use as a backup device

26. The Samsung Drive contains 49,786 files overall. Their external metadata gives some indications of how the Samsung Drive was used in the past:

    a. 99.73% of those files (counting by number not filesize: 49,652 out of 49,786) were added to the drive in the period 6 July 2015 to 10 June 2016. These were contained in a small number of root directories, most prominently directories named “FileHistory” and “Recover”. The “FileHistory” folder contains subdirectories mimicking a normal file structure of a Windows operating system, and is consistent with the Samsung Drive being used to create a back up. I did not observe anything unusual about how those files were created.

    b. None of those 49,652 files include any of the 97 New Reliance Documents or any surviving drive images: they are the files illustrated in white above.

    c. After 10 June 2016, there is a long period of inactivity with no files on the drive being Created, Modified or Accessed.

    d. The next sequential file activity on the drive appears to have taken place in 12 September 2023.

27. I will explain below (and note here for completeness) that there are some other timestamps (relating to the remaining 0.27% of files), which do not appear to be reliable:

    a. While there is metadata relating to some files with timestamps dating to 19 September 2017 and 31 October 2017, those timestamps are contradicted by other factors (which I will explain below) and I do not consider them to be reliable for those reasons.

There are some timestamps on the Samsung Drive which record interaction dated before 2015. However, as I have explained above, the Samsung Drive had not yet been manufactured at that time, so those timestamps could not record valid times.

THE ENCRYPTED ZIP FILE INFODEF09.ZIP{SS}

28. One of the two large files identified in Figure 1 above is a zip file called InfoDef09.zip.

Figure 2: representation of InfoDef09.zip{SS}

29. It is 24GB in size after compression. The external metadata of the file is shown below:

Name	Is Deleted	File Created	Last Written	Last Accessed
InfoDef09.zip{SS}	No	13/09/2009 09:46:01	13/09/2009 10:50:48	13/09/2009 10:50:48

30. The file is encrypted (password protected) such that the content cannot be extracted and read.

31. Although encrypting a zip file stops the content being extracted and viewed, it is often still possible to view the names and types of the files and their metadata. In the case of InfoDef09.zip**{SS}**, this is possible, and opening the file in the program 7Zip presents as follows:

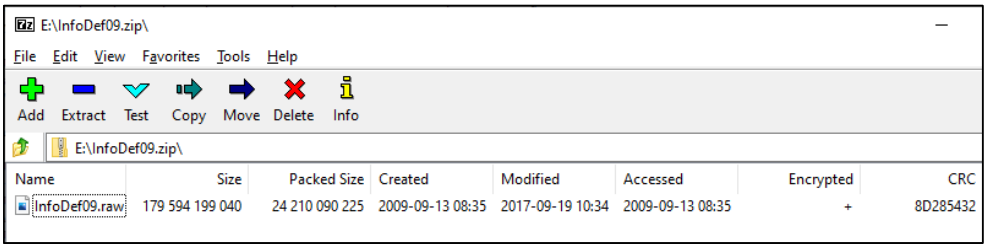


Figure 3: Details of InfoDef09.zip internal content

32. This indicates that:

a. InfoDef09.zip{SS} contains 1 file, which is called InfoDef09.raw.

b. InfoDef09.raw is 179GB (179,594,199,040 bytes) in size before compression.

c. The zip file is encrypted (the + symbol in that column).

d. Given the file size and the extension ".raw", this implies it is likely to be a disk image though that is not certain on the basis of the zip file alone (however I was later able to confirm this by other means explained below).

e. The zip file contains a record of the CRC hash[5] for InfoDef09.raw, allowing the integrity of its contents to be checked. In this case, the CRC hash is 8D285432.

f. The file records that it was created and last accessed in 2009-09-13 (13 September 2009), but that it was modified on 19 September 2017.

33. Comparing the external metadata (of the zip file itself, shown in the table above) to the timestamps recorded within it (shown in the picture above):

	InfoDef09.zip{SS} External file metadata	InfoDef09.raw listed metadata (the file inside the zip)
File Created	13/09/2009 09:46:01	13/09/2009 08:35
Last Written	13/09/2009 10:50:48	19/09/2017 10:34
Last Accessed	13/09/2009 10:50:48	13/09/2009 08:35

34. These timestamps are inconsistent:

a. Logically, the expected sequence of events is that the raw file was first created and modified, and only zipped and encrypted afterwards. The internal timestamps of the zip file (relating to the .raw file) would therefore be expected to date before the creation of the zip file.

b. However, in this case, the zip file records that it was created on 13 September 2009, but the file placed within it records that it was modified on 19 September 2017, which is more than 8 years afterwards.

c. I considered whether the inconsistent timestamps could have arisen other than through clock manipulation, but could not identify any other explanation. In theory, even if the file inside the zip was modified within the zip file directly, that would require the password to be known and the file to be decrypted, and would have led to the 'Last Modified' time of the zip file

[5] The CRC-32 or "Cyclic Redundancy Check-32 bit" is a hash algorithm similar to MD5 or SHA256 which I have discussed in previous reports. Although the CRC is a somewhat weaker hashing algorithm than MD5, the chance of collision in a small dataset is still extremely small, even without taking account of the other factors.

also being updated. That therefore would not explain the timestamps seen here, where the Last Modified of the zip file pre-dates the last modified of the contents within it.

d. This behaviour should not differ between operating systems and does not depend on whether it is NTFS or ExFAT formatted.

e. This indicates that InfoDef09.zip{SS} was created with the clock set to 2009, at a time after the clock had previously been set to 2017.

f. I later confirmed this finding and more relevant information, in a number of other ways explained below.

35. I also note that there are indications that a file InfoDef09.rar was deleted from the Samsung Drive. As with the deleted BDOPC.raw{SS}, it is likely that InfoDef09.rar was an abortive process (in this case, of creating a rar archive) which was aborted before it completed, leading to the file being deleted automatically (and I have expanded on this in my timeline Annex).

DELETED FILES WITHIN THE SAMSUNG DRIVE

36. Above, I have described some extant files on the Samsung Drive. In addition, it is necessary to describe some files that previously existed on that drive but were deleted.

Recoverable data

37. As I explained in my Third Report, I agree with Stroz Friedman that the Recycle Bin of the Samsung Drive was emptied in September 2023, at some point between 16 September 2023 (when one of the deleted files was last written, before being deleted) and 20 September 2023 (when the drive was imaged).

38. However, that deletion did not totally erase all the data concerned. When a file is deleted from the Recycle Bin, it becomes deleted as far as the file system is concerned. At that point, the locations of the disk where files were saved becomes “unused” and is available to be overwritten.

39. When files are deleted in this way the actual data bytes of the files often remain stored on the disk in the same location, at least until they happen to be overwritten later. This means it is often possible to recover files from a deleted drive, even after they have been deleted, by using specialist data recovery tools to examine the unused space and establishing the beginning and end of files. Sometimes, files are partly overwritten and can be partly recovered; sometimes they are irrecoverable; and other times they are wholly recoverable.

Overview of deleted files on Samsung drive

40. Using a combination of Encase forensic, X-ways Forensic, and R-Studio, I have examined the unused space of the Samsung Drive and established the presence of a large amount of data, corresponding to files which used to be extant on the drive but have been deleted. Overlaying these on the same diagram above:

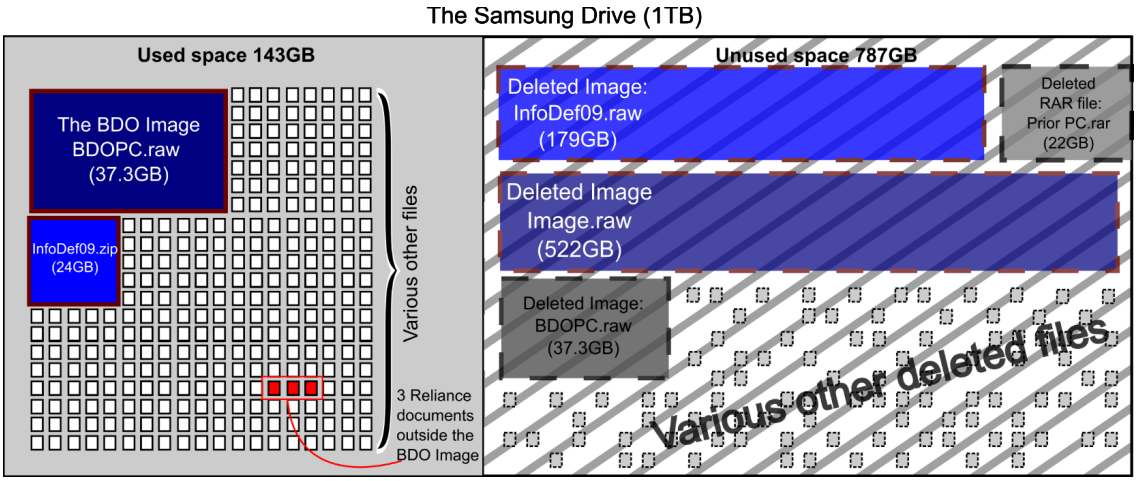


Figure 4: Overview of Samsung Drive including deleted files

41. I have detected 99 deleted files in total on the Samsung Drive:

    a. Deleted files are shown with a dashed-line border in Figure 4.

    b. Of the 99 deleted files, the diagram highlights four large files in particular, ranging from 22GB to 522GB in size: **Prior PC.rar{SS}** and **BDOPC.raw{SS}** (not recoverable, shown in grey) and **InfoDef09.raw{SS}** and **Image.raw{SS}** (recoverable, shown in blue/red).

    c. The diagram is illustrative only and does not focus on other files, however there are some other files that I will address in the course of my analysis below.

42. I note that this is not a complete analysis of deleted files on the Samsung Drive. There are several different ways (and extents) to which files can be recovered depending on the circumstances of the drive and how it was deleted. Some are more time consuming than others and, in this case, I have mainly focused on files and partial files that are easily recoverable, and so I do not go into the technical detail of the other types of recovery. With more time, it may be possible to recover and analyse further deleted files. These may provide further evidence. However, I have been able to reach some pertinent conclusions on the basis of the information available.

43. The metadata for the four large deleted files is set out below alongside BDOPC.raw{SS}:

Name	Is Deleted	File Created	Last Written	Last Accessed	Logical Size
BDOPC.raw{SS}	No	31/10/2007 23:48:05	31/10/2007 23:48:06	31/10/2007 23:48:06	39,999,504,384
BDOPC.raw{SS}	Yes (not recoverable)	31/10/2007 07:14:42	31/10/2007 07:15:18	31/10/2007 07:15:18	39,999,504,384
InfoDef09.raw{SS}	Yes (recoverable)	13/09/2009 09:35:22	19/09/2017 11:34:42	13/09/2009 09:35:22	179,594,199,040
image.raw{SS}	Yes (recoverable)	13/09/2009 09:50:10	13/09/2009 09:47:28	13/09/2009 09:50:10	522,117,840,896
Prior PC.rar	Yes (not recoverable)	31/10/2017 18:48:21	31/10/2017 18:47:56	31/10/2017 18:48:20	22,143,612,981

44. I observe that the timestamps on the deleted BDOPC.raw file may indicate it to be an abortive attempt to export the image (the process being stopped after 36 seconds, and the file deleted at that point before the extant BDOPC.raw was then created). I have recorded this in more detail in my timeline Annex.

45. I will address each of these in turn in later sections of this report.

Recycle Bin on the Samsung Drive.

46. I was able to further analyse the Recycle Bin on the Samsung Drive, following the analysis of my Third Report (which was based partly on the limited information in Stroz Friedberg's memo). The Stroz Friedberg memorandum (SF Memo) dated 30 November 2023 made reference to a Deleted .RAR file that had been sent to the Recycle Bin, and subsequently deleted from there. The recycled name for the file and the accompanying Recycle Bin record were "$RFH6M1E.rar"{SS} and "$IFH6M1E.rar"{SS}. The SF Memo indicates that the files were overwritten, and they were unable to determine the original name of the file. We agreed that the Recycle Bin was emptied in September 2023.

47. I note that contrary to my expectation at paragraph 129 of my Third Report, the interactions with the Recycle Bin have not caused UUIDs to be recorded identifying each user account that has interacted with the Samsung Drive, because the Samsung Drive is formatted with EXFAT and so does not record that information.

31 October 2007 timestamps using Windows 10 or later

48. I have examined the information available relating to the deleted files and ascertained that some is recoverable. Specifically, the Recycle Bin record $I file is recoverable in the Samsung Drive, which is a record of the metadata associated with the deleted file before it was deleted. That $I

file{SS} indicates that the deleted RAR file was named "Prior PC.rar" and that it is recorded as having been sent to the Recycle Bin on 31 October 2007 at 06:26:01.

49. The Recycle Bin behaviour is a feature of Windows operating systems. As explained in my Third Report, the manner in which the $I Recycle Bin file was created is indicative that the operating system used to send this file to the Recycle Bin was Windows 10. The identifying characteristic is that in Windows 10, Recycle Bin $I records can vary in size, but in previous versions they were all created with the same static file size (which was always 544 bytes). Since the $I file for Prior PC.rar{SS} is not 544 bytes, it must have been created in Windows 10 or later.

50. Windows 10 was released in July 2015[6]. This file could not have been recycled on 31 October 2007, and therefore must have been recycled on a computer with the clock set back to 31 October 2007 when it was sent to the Recycle Bin.

Other deleted files from the Samsung Drive Recycle Bin

51. There are multiple similar $I Recycle Bin records that are recorded on Samsung drive. Some are recoverable, while others are not. The following table lists the basic information available for these Recycle Bin records:

Name	File Created	Logical Size of Recycle Bin file	Internal Timestamp	original Path
$I1X6LZZ{SS}	31/10/2007 06:24:57	46	31/10/2007 06:24:57	E:\Denis
$IFH6M1E.rar{SS}	31/10/2007 06:26:01	60	31/10/2007 06:26:01	E:\Prior PC.rar
$IMKG274{SS}	31/10/2007 18:16:38	48		
$I4CJXQP.pst{SS}	31/10/2014 18:18:04	76		
$I6WGMTP.kdbx{SS}	31/10/2014 18:18:04	70		
$IEBFG72.log{SS}	31/10/2014 18:18:04	48		
$IGK5WF2.txt{SS}	31/10/2014 18:18:04	162		
$IGZH9ZO.kdbx{SS}	31/10/2014 18:18:04	70		
$IUB82DR.txt{SS}	31/10/2014 18:18:04	46		
$IVRBYQL.kdbx{SS}	31/10/2014 18:18:04	70		
$IWRFX6K.zip{SS}	31/10/2014 18:18:04	78		
$IXEA69G.gz{SS}	31/10/2014 18:18:04	84		
$IYYTOFV.kdbx{SS}	31/10/2014 18:18:04	70		
$IZBWGZJ.crd{SS}	31/10/2014 18:18:04	52		
$I0920U8.kdbx{SS}	31/10/2014 18:18:22	70		
$I435UGR.log{SS}	31/10/2014 18:18:22	48		
$I8DRBRP.kdbx{SS}	31/10/2014 18:18:22	70		
$I9WVL9W.gz{SS}	31/10/2014 18:18:22	84		
$IDOOZ0J.txt{SS}	31/10/2014 18:18:22	162		
$IDORYJL.crd{SS}	31/10/2014 18:18:22	52		
$IFW5AAT.txt{SS}	31/10/2014 18:18:22	46		
$IT1J4I2.kdbx{SS}	31/10/2014 18:18:22	70		
$ITQ24VI.zip{SS}	31/10/2014 18:18:22	78		
$IX0D9A0.kdbx{SS}	31/10/2014 18:18:22	70		

[6] https://blogs.windows.com/windowsexperience/2015/06/01/hello-world-windows-10-available-on-july-29/

$I391BYS.pdf{SS}	19/09/2017 12:17:02	78	19/09/2017 12:17:02	F:\Notes - Copy\ESDT.pdf
$IE936WA.rtf{SS}	19/09/2017 12:20:17	86	19/09/2017 12:20:17	F:\Notes - Copy\~$Spyder.rtf
$IJYUAXV.rar{SS}	19/09/2017 12:21:18	66		
$IVXTOIQ.rar{SS}	19/09/2017 12:21:18	64		
$I72FM0K{SS}	31/10/2017 18:46:41	38		

Contradictory timestamps in 2007, 2014, and 2017

52. All but 5 of these recorded timestamps indicate the files being sent to the Recycle Bin on a date before the Windows 10 operating system was available. This would only be possible on a computer with a backdated clock.

53. I note that many timestamps on the Samsung Drive share the same hour, minute, day, and month, but differ in the year. For example, the 31 October date comes up in 2007, 2014, and 2017 (two of which were before Windows 10 existed and before the Samsung Drive was manufactured), and all are in the same hour (6-7pm). Bearing in mind the other contradictory features of these 31 October timestamps (as discussed above and further below), I consider this is indicative of the use of clock manipulation to change the metadata year (but not other fields) while the time continues to tick forward and the date remains the same.

54. I have considered if these now deleted Recycle Bin records could have been migrated from some other storage medium onto the Samsung drive, but I do not think this is plausible to explain the observed behaviour: the Recycle Bin entries, the "$I" files, have been *created* in a manner that is specific to Windows 10, which was not available before July 2015. A migration of data would not have changed the byte size of these files.

The 2017 records

55. The remaining records from 2017 in the Samsung Recycle Bin table are not contradicted by the release date of Windows 10. They are as follows:

    a. $I391BYS.pdf{SS} "ESDT.pdf"{SS}: This is the file which was listed as being Modified on 16 September 2023, which I explained in my Third Report from paragraph 130 onwards. That analysis indicated the use of clock manipulation in relation to the Samsung Drive. I have managed to recover this in its entirety and analysed it in Appendix PM45 in connection with other documents related to it. The deleted file contains metadata relating to 1 November 2007 (which is the day after the 31 October 2007 date discussed above) and 16 January 2008, and contains references to software that was not released until 2019. I therefore do not consider the 19/09/2017 date can be authentic, and consider it was achieved using clock manipulation.

{H/241}

b. $IE936WA.rtf{SS} "~$Spyder.rtf"{SS}: I have managed to recover this file in its entirety. It is a "lock" file, which is a type of temporary file created by Microsoft Word, when another document is being opened for editing (not just read-only opening).

The file being edited (to which this lock file relates) is a blank document named Spyder.rtf{SS}, containing just a header {\rtf1} (which indicates it to be a blank RTF file).[7]

The deleted lock file ~$Spyder.rtf"{SS} includes the name "*Craig S Wright*" as the registered user of the software used to edit Spyder.rtf{SS}.

The deletion activity recorded is dated to 19/09/2017 12:20:17 which is just 3 minutes 15 seconds after the deletion of ESDT.pdf{SS} (referred to above). Since there are indications that the 19/09/2017 date was achieved using clock manipulation, I consider the timestamp also to be unreliable in respect of the $~Spyder.rtf file $IJYUAXV.rar{SS} and $IVXTOIQ.rar{SS}: These files appear to relate to two files named "University.rar"{SS} and "University0.rar"{SS}. I have not been able to recover the content of those files. The following table correlates what information is available about these two files together with the Recycle Bin records, but no further analysis is possible. I note that these files display timestamps dating to 31/10/2017, which I do not consider to be reliable for the reasons explained above.

Name	File Created	Last Written	Last Accessed	Logical Size	Full Path
University.rar{SS}	31/10/2017 18:47:34	31/10/2017 18:56:56	31/10/2017 18:47:34	15,692,610	\University.rar
$RVXTOIQ.rar{SS}	31/10/2017 18:47:34	31/10/2017 18:56:56	31/10/2017 18:47:34	15,692,610	\$RECYCLE.BIN \$RVXTOIQ.rar
$IVXTOIQ.rar{SS}	19/09/2017 11:21:18	19/09/2017 11:21:20	19/09/2017 11:21:20	64	\$RECYCLE.BIN \$IVXTOIQ.rar
University0.rar{SS}	31/10/2017 18:47:34	31/10/2017 18:53:18	31/10/2017 18:54:24	19,696,723	\University0.rar
$RJYUAXV.rar{SS}	31/10/2017 18:47:34	31/10/2017 18:53:18	31/10/2017 18:54:24	19,696,723	\$RECYCLE.BIN \$RJYUAXV.rar
$IJYUAXV.rar{SS}	19/09/2017 11:21:18	19/09/2017 11:21:20	19/09/2017 11:21:20	66	\$RECYCLE.BIN \$IJYUAXV.rar

[7] This is consistent with it being created from the Right Click menu and choosing to create a "New Rich Text format" which would create a blank document named "New Rich Text Document.rtf". I also found a record of a file called "New Rich Text Document.rtf", which is the default name applied to such a document, and that was also blank before being renamed to "Spyder.rtf".

c. Further the Recycle Bin $I files for these two archives are recorded as being created on 19 September 2017, before the files themselves were created.

d. $I72FM0K{SS}: I was not able to find any further information relating to this file.

October 2007 timestamps also in BDOPC

56. I note that other very similar timestamps have come up further in my analysis of other documents below, including 31 October 2007 (which, as detailed in my Timeline Annex, is also connected to an apparent sudden jump in computer clock by ten years, to 30 October 2017). Considering that activity dated to October 2007 is contradicted for several reasons, I do not consider any of the 2017 timestamps in relation to these files to be reliable.

THE BDOPC.RAW IMAGE

57. In this section I explain what I have observed in relation to the BDOPC.raw image file itself.

Metadata of BDOPC.raw{SS} and its deleted equivalent file

58. BDOPC.raw{SS} is a single file stored on the Samsung Drive and recorded with the following external metadata, alongside the similar deleted file: (This is the same information as set out above in relation to the overview of the disk image files on the Samsung Drive, repeated for convenience.)

Name	Is Deleted	File Created	Last Written	Last Accessed	Logical Size
BDOPC.raw{SS}	No	31/10/2007 23:48:05	31/10/2007 23:48:06	31/10/2007 23:48:06	39,999,504,384
BDOPC.raw{SS}	Yes (not recoverable)	31/10/2007 07:14:42	31/10/2007 07:15:18	31/10/2007 07:15:18	39,999,504,384

59. As can be seen above,

a. The deleted BDOPC.raw{SS} shows an identical file size to the extant BDOPC.raw{SS}

b. The external metadata timestamps for both files dates from the same date, 18.5 hours apart.

c. Since it is deleted and not recoverable, it is not possible to analyse the deleted file further.

31 October 2007 timestamps

60. As discussed above in relation to the Recycle Bin{SS}, both BDOPC.raw files are recorded with external metadata dating to 31 October 2007, which I do not consider reliable for the reasons

{H/278} above and further discussed in detail below and in Appendix PM46, and in particular I note that the date is before the existence of the Samsung Drive, which was manufactured in 2015. I made this observation before the other analysis described above (but mention it here as this is not a chronological report), and formed the preliminary view that it was probable that these timestamps did not therefore correlate to the creation and modification timestamps of the disk image file, but have been attributed to the file by some other means or activity. This preliminary view was later informed and became more concrete by reason of the other analysis described in this report.[8]

Overview of the BDOPC.raw Image contents

61. By mounting BDOPC.raw, it is possible to explore the file's data as if it was a hard drive. This allowed me to inspect:

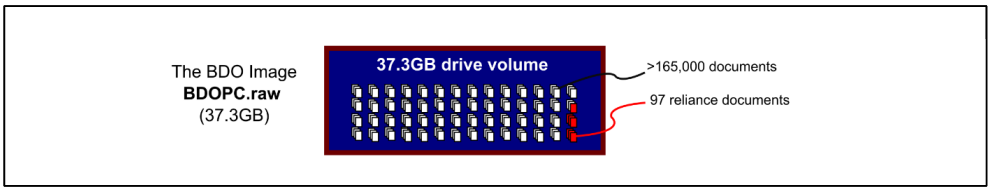
    a. information relating to the image itself and how it came to be created and modified. My observations about the drive itself are set out in this section of my report; and

    b. details of individual files within the drive. My observations about those individual files are separate, in Appendix PM46. {H/278}

Single partition – content of an operating system

62. A computer disk can be 'partitioned' or segmented into different spaces or sectors, which can then be used for different purposes. As well as storage of user files, different partitions can be used for different reasons, e.g. it is common for the first portion of a hard disk to contain information which instructs the computer about where to locate the operating system files in order to initially boot up before the operating system is loaded (referred to as a 'boot sector').

63. As shown below, the BDOPC.raw image is an image of a single partition of a computer hard disk. It does not contain a boot sector:



[8] I have also considered the possibility that these timestamps were inherited when the file was copied from another storage device but have discounted that possibility also because it would not explain the observations I have made in relation to those timestamps, which I explain in further detail throughout this report.

Figure 5: overview diagram of the BDOPC.raw

64. Other format data of the partitioned hard drive is shown below:

Volume Serial Number	E859-F3AF
Full Volume Serial Number	62E85A21E859F3AF
Driver Information	NTFS 3.1 Dirty (301)
File System	NTFS
Total Sectors	78,124,032
Total Capacity	39,999,500,288 Bytes (37.3GB)
Total Clusters	9,765,503
Unallocated	1,676,435,456 Bytes (1.6GB)
Free Clusters	409,286
Allocated	38,323,064,832 Bytes (35.7GB)

BDOPC.raw data partition information

Files on BDOPC.raw

65. Including system files, files associated with installed programs, and user files, there are 165,243{BDO} files within BDOPC.raw, including the 97 New Reliance Documents.

66. Based on my analysis below, the files on BDOPC fall into two groups:

    a. 165,102 appear to be files which were present on the BDO PC at the time the Original BDO PC Image was captured.

    b. 141 files display markedly different characteristics, including being added by a different user at a date after the Original 2007 BDO Image was captured.

    c. Of those, 71 documents are part of the 97 New Reliance Documents.

How BDO PC was used

Activity information on the BDO PC

67. It is possible to establish details about how the BDO PC was used and what its software set up was, as follows:

    a. The image is a clone of the content of the hard disk of a computer that was using a Windows XP operating system with Service Pack 2 installed: The operating system files are included on the drive.

    b. The Windows XP installation date{BDO} is recorded as 18 April 2006.

    c. The computer name is recorded as being "BDO-SYD-NB-439".

d. The configured timezone is "AUS Eastern Standard Time which varies between UTC+10:00 and UTC+11:00.

e. The operating system records that the last time that the BDO PC computer was shut down was 5 July 2007 at 06.31.

68. That indicates that the last time the BDO PC was used as a computer before the image was taken (i.e. the last time it was turned on and booted up into Windows XP, before being cleanly shut down using a shutdown or hibernate process) was 5 July 2007.

69. The table of data above records that the file system is "NTFS Dirty". This word "Dirty" indicates that there had been an interrupted boot, i.e. the BDO PC computer was turned on partially, but the boot failed or was interrupted before being complete, or that the computer was shutdown unexpectedly, such as a power failure, or system crash, or similar.

70. There are also several sources of information with timestamps relating to system files and events, indicating the last activity performed on the BDO PC before it was shut down, all consistent with the information above:

a. The file "NTUSER.DAT" stored within the folder "\Documents and Settings\220" has a Last Modified timestamp 05/07/2007 06:31:21. The file "NTUSER.DAT.LOG" which relates to the file of similar name above has a Last Modified timestamp 05/07/2007 06:31:18. Collectively these two files are the system registry for the "220" user profile on the computer.

b. The two system event log files "SysEvent.Evt", "and "AppEvent.Evt" have a recorded Last Modified date and time of 05/07/2007 06:31:28. The system log typically records an event in relation to the computer being shutdown as the last entry in the log. The last modification timestamp of this log is usually a good approximate record for when the computer was last shut down.

c. The Internet Explorer most recent browsing record indicates activity at 06:22 on 05 July 2007.

d. When a user accesses documents, Windows computers create LNK shortcut file that records information about the file being accessed. The LNK files file timestamps can be used to indicate when the access occurred. The most recent LNK files on the computer are recorded as being Last Modified on 05 July 2007 at 06:30

e. The interrupted boot is also evident from different sources, including:

i. The last two entries in the Event Log of the computer, which are both dated 05/07/2007, with the penultimate being when the Event Log service was stopped (at 06:31:27, the time of last clean shutdown), and the final entry being timed at 09:19:16, when Event log service was started again during the interrupted boot process.

ii. The file "Pagefile.sys" (a system file which is continually updated as part of the Windows XP operating system), which records a Last Modified timestamp of 05/07/2007 09:19:09.

No further event logs or user activity

71. There are no further event logs nor any other indication that the BDO PC was used or connected to external storage before the image of it was originally captured. Any activity that took place after 05 July 2007 must have been without the operating system in use, and therefore with the computer attached as external storage to a different computer or operating system.

Use as external storage the following day

72. It is then clear that the hard drive of the BDO PC was connected to another computer the following day, 06 July 2007, as secondary storage (as if it was an external drive, and the operating system on the BDO PC's drive was not used). One file and one folder (with content within) were created and written with the word "Backup" in their name:

Name	Description	File Created	Last Written	Last Accessed
Backup 05072007 {BDO}	Folder	06/07/2007 06:43:41	06/07/2007 06:43:41	31/10/2007 13:37:49
cabinet Backup.CBN {BDO}	File, Archive	06/07/2007 06:43:41	06/07/2007 06:45:13	06/07/2007 06:45:13

73. I analysed the file "cabinet Backup.CBN"{BDO}:

a. The file contains the following text "[Cabinet] Name=Backup 05072007 [DB] Path=Backup 05072007\Backup 05072007.mdb Modified=6/07/2007 4:45:13 PM".

b. Comparing those recorded times to the timestamps on the drive shown in the table above, this indicates that the local clock time was 10 hours different to the timestamps for the file and folder above. This appears to relate to backing up certain user files from the computer.

c. The cabinet archive contains 219 user files:

d. None of these files were New Reliance Documents, and none appeared to be related to the New Reliance Documents.

Analysis of documents and dates

74. Taking the above observations, I then inspected the file tables of files within the BDOPC.raw drive image, to ascertain whether any other activity occurred after the activity above. Using the application X-Ways forensic, I have made a list of the files that post-date 6 July 2007 from the BDO.raw drive. That is available at **Exhibit PM-R 4.3**. That schedule lists the timestamps and basic properties for 145 files (excluding folders). The analysis was not limited to extant files but also deleted files and system and log file records. This included the 141 files identified above, and an additional 4.

{H/307}
{H/308}

75. Of the 145 {BDO} files listed in that schedule, it includes:

    a. Extant/deleted: 101 extant {BDO} files and 44 deleted {BDO} files (145 total)

    b. Of the 101 extant {BDO} files added after 6 July 2007:

    c. 86 {BDO} files are user files (user-created documents as opposed to system files), and

    d. 15 {BDO} are Filesystem components/logs

    e. Of the 86 {BDO} user files added to the BDOPC.raw image after 6 July 2007:

    f. 71 are New Reliance Documents.

    g. 11 appear to be files associated with some of the New Reliance Documents, including some fonts referred to in Latex documents. However, I have not analysed the content of these files in much detail, as they are not New Reliance Documents.

    h. The remaining 4 appear to be original to the BDO PC in some form, but have since been modified in some way such that the MFT Records were updated. I have not been able to establish exactly what modification took place.

76. Looking at the dates associated with the 145 {BDO}files dating from after 6 July 2007:

    a. The date “31 October 2007” appears in connection with all the actual user documents (either as their created or modified date or both). I have explained above that this date is not reliable in connection with the Samsung Drive or BDOPC.raw Image, including the fact that it appears in connection with the file metadata associated with BDOPC.raw, as if written to the Samsung Drive in 2007 (which is several years before the Samsung Drive was first manufacturered). There are also extensive further reasons for this conclusion outlined in Appendix PM46, in connection with the individual documents found within the BDO Drive.

    b. 11 entries in the schedule do not have the 31 October 2007 date: they are all system transaction logs ($Txf logs {BDO}). Of those 11 files, 6 are dated to 19 or 30 October 2007; and the remaining 5 are dated to 17 September 2023.

77. This data was sufficient for me to form an initial opinion that these 71 New Reliance Documents stood out from the other files on the BDOPC.raw image, in that the files exhibit timestamps that are consistent with the copying of the data onto BDOPC.raw on a date when the computer clock was set to 31 October 2007, which is consistent with other anomalies I have observed relating to that date.

Folders on BDOPC.raw

78. As well as the files on BDOPC.raw, I also considered the folders inside the image. A schedule of properties for the user folders on BDOPC.raw with timestamps after 6 July 2007 is at

79. As with the files, the vast majority of the folders on the drive are timestamped consistently with a BDO PC that was in use during the period 2006- 5 July 2007, but a few are created with the date set to 31 October 2007.

Folders created with date of 31 October 2007, metadata date later changed

80. Several of the folders that were created with the date set to 31 October 2007 were later altered, so that the date appeared to be from an earlier time. This is clear from the fact that the file system of the BDOPC.raw image, which is NTFS, has retained not only the currently-registered timestamps but also some previous timestamps. Those previous timestamps are indicated by the use of a superscript '^{2}' in the exhibited schedules, such as Created^{2} and Modified^{2}, showing previously existing data which has been changed.

Folder modified in 2023, date later changed to 2007

81. I observe particularly that:

    a. the folder "*My Files*"{BDO} is recorded as having a previous (Modified²) last modified timestamp of 17 September 2023 at 13:18:17,

    b. the existing last-modified timestamp for this folder *"My Files"{BDO}* is recorded as being 31 October 2007 at 19:47:39.

82. I consider this anomalous and a further indicator that the content of BDOPC.raw has been subjected to content and clock manipulation, since the previous modified date (2023) has later been overwritten to 31 October 2007.

Transaction logs show clock manipulation from 2023

{G/5}

83. In my Third Report at paragraph 145 I explained that transaction logs are NTFS file system records that record information about changes to files and folders within a drive, accessible using

forensic tools. In the file schedules exhibited to this report, transaction logs are recorded in the same way as individual files, with names beginning $Txf.

84. There are no transaction logs relating to the use of the BDO PC prior to 7 July 2007. This is to be expected as this transactional logging function was not included with Windows XP, but was introduced with Windows Vista and is available in more recent operating systems including Windows 10.

85. However, such transaction logs do exist, relating only to later activity which took place after the Image was taken, with dates set to 19/10/2007, 30/10/2007, 31/10/2007, and 17/09/2023 comprising the following logs:

Name (all from {BDO})	Existent	Created	Modified	Record changed	Accessed
$Tops	Yes	17/09/2023 13:02:32	17/09/2023 13:02:32	17/09/2023 13:02:32	17/09/2023 13:02:32
$Tops	Yes	19/10/2007 13:04:01	19/10/2007 13:04:01	19/10/2007 13:04:01	19/10/2007 13:04:01
$TxfLog.blf	Yes	17/09/2023 13:02:32	17/09/2023 13:03:26	17/09/2023 13:03:26	17/09/2023 13:03:26
$TxfLog.blf	Yes	31/10/2007 16:59:51	30/10/2007 10:44:18	30/10/2007 10:44:18	30/10/2007 10:44:18
$TxfLog.blf	No	31/10/2007 13:40:37	31/10/2007 13:40:37	31/10/2007 13:40:37	31/10/2007 13:40:37
$TxfLog.blf	Yes	31/10/2007 07:32:50	31/10/2007 07:38:31	31/10/2007 07:38:31	31/10/2007 07:38:31
$TxfLog.blf	Yes	19/10/2007 13:04:01	19/10/2007 13:04:02	19/10/2007 13:04:02	19/10/2007 13:04:02
$TxfLogContainer00000000000000000001	Yes	17/09/2023 13:02:33	17/09/2023 13:03:26	17/09/2023 13:03:26	17/09/2023 13:03:26
$TxfLogContainer00000000000000000001	Yes	31/10/2007 16:59:51	30/10/2007 10:44:18	30/10/2007 10:44:18	30/10/2007 10:44:18
$TxfLogContainer00000000000000000001	No	31/10/2007 13:40:37	31/10/2007 13:40:37	31/10/2007 13:40:37	31/10/2007 13:40:37
$TxfLogContainer00000000000000000001	Yes	31/10/2007 07:32:50	31/10/2007 07:38:31	31/10/2007 07:38:31	31/10/2007 07:38:31
$TxfLogContainer00000000000000000001	Yes	19/10/2007 13:04:01	19/10/2007 13:04:02	19/10/2007 13:04:02	19/10/2007 13:04:02
$TxfLogContainer00000000000000000002	Yes	17/09/2023 13:02:34	17/09/2023 13:02:37	17/09/2023 13:02:37	17/09/2023 13:02:37
$TxfLogContainer00000000000000000002	Yes	31/10/2007 16:59:51	31/10/2007 16:59:51	31/10/2007 16:59:51	31/10/2007 16:59:51
$TxfLogContainer00000000000000000002	No	31/10/2007 13:40:37	31/10/2007 13:40:37	31/10/2007 13:40:37	31/10/2007 13:40:37
$TxfLogContainer00000000000000000002	Yes	31/10/2007 07:32:50	31/10/2007 07:32:50	31/10/2007 07:32:50	31/10/2007 07:32:50
$TxfLogContainer00000000000000000002	Yes	19/10/2007 13:04:01	19/10/2007 13:04:01	19/10/2007 13:04:01	19/10/2007 13:04:01

86. These transaction logs on {BDO} are indicative of manipulation of BDOPC.raw using clock manipulation techniques, including because:

    a. Four of them date to 17 September 2023 (green highlight).

b. Two of them indicate creation dates that post-date their modification dates, which is logically the wrong order (yellow highlights).

Transaction log folders show 17 September 2023 creation

87. Turning to the folders on {BDO} in which the transaction logs{BDO} are stored, there are also anomalies to be observed with the timestamps of the folders that they are stored in. The table below lists the timestamps applied to the various folders that comprise these elements of the NTFS transaction logs. I observe that the folder "$TxfLog"is recorded as being Created on 17 September 2023, but Modified and Accessed on 19 October 2007:

Name	Path	Created	Modified	Record changed	Accessed
$Extend	\	15/12/2004 14:06:59	15/12/2004 14:06:59	15/12/2004 14:06:59	15/12/2004 14:06:59
$Deleted	\$Extend	17/09/2023 13:02:31	17/09/2023 13:02:31	17/09/2023 13:02:31	19/10/2007 12:35:38
$RmMetadata	\$Extend	17/09/2023 13:02:31	17/09/2023 13:02:31	17/09/2023 13:02:31	17/09/2023 13:02:31
$Txf	\$Extend\$RmMetadata	17/09/2023 13:02:32	17/09/2023 13:02:32	17/09/2023 13:02:32	17/09/2023 13:02:32
$TxfLog	\$Extend\$RmMetadata	17/09/2023 13:02:32	19/10/2007 13:04:01	19/10/2007 13:04:01	19/10/2007 13:04:01

User accounts and Serial Identifiers that interacted with the BDOPC.raw image

Main user account on the BDO PC

88. The vast majority of the user files (as opposed to system files) on the BDO PC were created by the user named "220". This is consistent with the user profile name on the BDO image and the user folder "\Documents and Settings\220", which is a folder characteristic of how Windows XP stores user data.

89. From my previous analysis of the VOL001 disclosure dataset, I am aware that "220" was the username associated with Dr Wright's account when he was an employee at BDO.

Security IDs

90. Inside a Windows operating system, user accounts are assigned individual user ID numbers known as "Security Identifiers" or "SIDs". Every account on a network is given an SID when it is first created. User SIDs take the form:

S-1-5-21-0000000000-000000000-0000000000-0000

91. In the SID:

a. The 28 digits in the middle three groups (highlighted yellow) correspond to the 'security authority', usually a computer or domain.

b. The last group of digits (3 or 4 digits) corresponds to the specific user account on that computer or domain, called the Relative ID.

92. It is not possible to relate SIDs to usernames directly without access to the computer on which the accounts were created. It is sometimes possible to relate them by observing the activity on the computer, as when users interact with files, the SID of the user performing that interaction is recorded in an NTFS file system.

SIDs in use on BDOPC.raw

93. In the Recycle Bin folder of the BDO Image there are six different SIDs.

a. **S-1-5-21-1594100890-483875263-1248796406-6100:** This is the SID associated with Dr Wright's account as an employee of BDO (which was actually named "220"). It accounts for the vast majority of user activity on the drive, including all the activity which presents like the normal operation of files on a computer. The central digit groups (159… … …406) will be the ID relating to BDO's computing domain. The last four digits "6100" are Dr Wright's specific account on that domain.

b. There are also three other SIDs which only differ in their last 4 digits **(-3258, -5560, and 9602):** these three SIDs all have the same Domain ID as that referred to above, differing only. They will correspond to other users on the BDO domain who logged onto or interacted with Dr Wright's BDO PC. There are relatively few instances of logs associated with these accounts, and they appear to correspond to users who interacted with the BDO PC very occasionally, for example as might be expected of providing IT services.

c. S-1-5-21-4271588188-547894879-3543215670-500: This corresponds to the built-in administrator account on the computer that was used to create the \Backup 05072007\ folder on {BDO}, and its "cabinet backup" file, with the BDO PC connected as secondary storage. A SID ending in 500 is usually indicative of an Administrator account.

d. S-1-5-21-67634994-2544886514-713616940-1002: This is the SID associated with 88 documents in total including:

i. The 71 New Reliance Documents and other extant documents which were added to the BDOPC.raw image when the clock was set to 31 October 2007,

ii. 6 documents that were added to BDOPC.raw with the clock set to 31 October but which were later deleted.

94. The SID used to add those 71 New Reliance Documents onto BDOPC.raw is not the user profile assigned to Dr Wright while he was an employee at BDO, but a different SID from a different computer used more recently.

{H/320} {H/322}

95. I produce at **Exhibit PM-R 4.10** the 88 files identified on BDOPC.raw, and at **Exhibit PM-R 4.11**, the 84 identified on InfoDef09.raw that are attributed with this alternate SID.

SIDs in Folders

96. As well as files, the same SID ending in -1002 was used to create 20 folders on the BDOPC.raw drive with timestamps set to 31 October 2007.

97. For example, three folders within the "\My Files\Uni" folder indicate a prior creation timestamp of 31 October 2007 at 14:50:47, but have had these timestamps altered to indicate an alternate date:

Name	Path	Created	Created²	Modified	Owner
2005	\My Files\Uni	30/10/2003 13:56:01	31/10/2007 14:50:47	31/10/2007 15:06:11	S-1-5-21-67634994-2544886514-713616940-1002
2006	\My Files\Uni	03/12/2005 04:58:01	31/10/2007 14:50:47	31/10/2007 16:49:20	S-1-5-21-67634994-2544886514-713616940-1002
2007	\My Files\Uni	14/11/2006 05:33:01	31/10/2007 14:50:47	31/10/2007 14:02:49	S-1-5-21-67634994-2544886514-713616940-1002

98. This appears to indicate that the SID ending in -1002 is the SID associated with the user account on the computer which connected to the Samsung Drive on 17 September 2023 (which I understand from Dr Wright's witness statements was his own computer).

Object IDs in the BDOPC.raw file system

Explanation of ObjIDs

99. Another piece of metadata tracked by NTFS (which is a complex and audit-heavy file system) is an Object Identifier, also known as an "ObjID" for files and folders on the system. These can be used to track files and folders. ObjIDs are specific to NTFS file system and tracks several properties relating to the creation and modification of files and folders. Each ObjID is unique to the file or folder it relates to.

100. ObjIDs are not assigned across every file and folder on a system, but are assigned when required. How they are assigned depends on the method of creating a file, for example in Windows 10:

    a. If a file or folder is created by *copying* a file from one disk to another, an ObjID will not be assigned to the destination copy, however,

b. if a file or folder is created by *moving* from one NTFS volume to another, the ObjID will be migrated with the file, and will be present in the new location.

c. If a file is created without an ObjID and later modified, an ObjID may be created at that time.

Timestamps in ObjIDs

101. The ObjID encodes a significant amount of data, notably encoding a timestamp:

a. The timestamp is known as the "ObjID Boot time",

b. the time it encodes is the time on the computer clock, when the computer concerned was last booted up.

c. If the ObjID is created when a file is modified, it will correspond to the boot time on the computer used to modify it. If the ObjID is created when a file is created and moved, the time it encodes will be the boot time on the computer used to create it in the first instance.

ObjID timestamps in the BDOPC.raw drive

102. Using the application FTE (Filetime Extractor) I have parsed the $OBJID data for BDOPC.raw. I have exported the entries with Boot Timestamps that postdate 06 July 2007. I exhibit these as below. The bold entries in those exhibits indicate the files that differ between the two datasets. These lists include folders as well as files:

a. **Exhibit PM-R 4.5**, OBJID from Infodef09_raw.xlsx

b. **Exhibit PM-R 4.6**, OBJID from BDOPC_raw.xlsx

103. From that list it can be seen that:

a. There are 44 ObjIDs from after 6 July 2007, and in fact the earliest ObjID date after that is 31 October 2007 (relating to 26 files).

b. The remaining ObjIDs all relate to 17, 18, and 19 September 2023.

c. All of the listed files relate to New Reliance Documents (being either Reliance Documents or folders in which New Reliance Documents are stored).

d. All those files are files encoded with the SID ending in -1002 which I have established above is the user account which added documents to the BDOPC.raw image more recently than the Image was created.

104. I note that the ObjID records contain 8 different date and time stamped sessions, including 5 from September 2023:

- 31/10/2007 07:39:16
- 31/10/2007 07:41:38
- 31/10/2007 15:34:39
- 17/09/2023 13:20:48
- 18/09/2023 03:00:12
- 18/09/2023 16:17:30
- 19/09/2023 06:02:20
- 19/09/2023 09:39:41

105. However, as I explain further below, it is possible to establish firmly that the dates in 2007 were recorded after the dates in 2023. This indicates that documents were added to and/or modified on the BDOPC.raw over the course of three days in September 2023, between 17th September and 19th September, but that the clock was set back to 2007. Since the ObjID Boot time is updated only when a computer is rebooted, it indicates that the computer which was used to add the documents and/or modify them within BDOPC.raw was restarted eight times between those dates, and that the files were created/added to the BDOPC.raw over the course of those eight sessions.

Connection between -1002 SID and September 2023 user activity

106. I also note that all of the files that have ObjIDs from 2023 are files that are recorded as being created by the apparently more recent user account with the SID ending -1002. This appears to indicate that the SID ending in -1002 (and which is recorded as being the creator of 71 New Reliance Documents) is an account in use in September 2023, consistent with the rest of my analysis.

VOL001 documents in BDOPC.raw

107. From BDOPC.raw, there are 13 files (9 unique files, plus 4 duplicates) which are identical by MD5 in content to files provided in the original Vol001 disclosure dataset.

ID	Full path
{ID_000195} ID_000195	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Sent Items\Benfords.eml\Project - Benford's Law.doc
{ID_000184} ID_000184	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Sent Items\E-commerce Law Assignment .eml\Assignment_ECL_LLM.doc
{ID_0000095} ID_000095	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Sent Items\Paper.eml\Assignment_FCL_LLM.Alt.doc
{ID_000071} ID_000071	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Sent Items\Papers.eml\papers.zip\G7799.pdf

{ID_000071}	ID_000071	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Sent Items\Papers.eml\papers.zip\G7799.pdf
{ID_000128}	ID_000128	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Sent Items\RE: RUXCON 2006 Call for Papers.eml\Project Proposal.doc
	ID_000128	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\outlook.ost\Inbox\Publishing Stuff\RE: RUXCON 2006 Call for Papers.eml\Project Proposal.doc
{ID_000050}	ID_000050	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\outlook.ost\Inbox\Uni\09 PhD\FW: PhD Proposal for study.eml\SAD - 11th Oct - Pending Approval.doc
{ID_000051}	ID_000051	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\outlook.ost\Inbox\Uni\09 PhD\FW: PhD Proposal for study.eml\Vlans and security.doc
{ID_000071}	ID_000071	\Documents and Settings\220\Local Settings\Application Data\Microsoft\Outlook\outlook.ost\Sent Items\some papers.eml\G7799.pdf
{ID_000386}	ID_000071	\My Files\Papers\papers.zip\G7799.pdf
{ID_000529}	ID_000386	\My Files\Uni\LLM\Foundations of commercial Law\Paper_E_Contracts.doc
	ID_000529	\My Files\Uni\MSTAT\2006\Old STAT 6730 - 3030 - General Linear Models\books\include.pdf

108. These files do not show any indications of manipulation within the BDO Drive, but I have not specifically analysed them for the purpose of this report.

109. I note that none of those files are Reliance Documents or New Reliance Documents.

Deleted files within the BDOPC.raw e

110. It has been possible to recover certain individual deleted files within the BDOPC.raw.

111. One in particular stood out as being relevant, as it was a document I had previously analysed, being "LLM_ProposalA.doc"{BDO} with disclosure number ID_003935. I have addressed this in my First and Second reports, and summarise briefly for ease of reference: {ID_003935}

    a. This document has a Grammarly timestamp of 132105930506145185 which decodes to "Sun 18 August 2019 09:10:50.614 UTC".

    b. It was created with MS Word version 11.9999, which is MS Word 2003 Service Pack 3, a software version that was released on 17 September 2007 (which is before the 31 October 2007 date, but after the BDO PC was last booted up).

112. That file used to be present within the imaged drive, but was deleted before the content of BDOPC.raw was output to the image file (which I consider was on 19 September 2023, based on the findings above). I have been able to recover that deleted file LLM_ProposalA.doc{BDO} in its entirety from within the deleted data of BDOPC.raw. I have confirmed that it is identical by MD5 hash to ID_003935, including the Grammarly timestamp and other indica of tampering that I have reported on previously. {ID_003935}

113. I note that Grammarly was not yet released in 2007 but appears to have begun in 2009-2010 as a web-based application (See my First Report, Main Report at paragraph 62).

114. In my opinion, neither the Grammarly timestamp nor the recorded version of MS Word could have existed on the BDO PC in 2007. The embedded Grammarly timestamp (18 August 2019) is however consistent with my other findings, which indicate that the file BDOPC.raw was created more recently in 2023.

BDOPC.raw: Overall Conclusions

115. A revised diagram of the BDO Image, taking account of the findings above, is below at Figure 6.

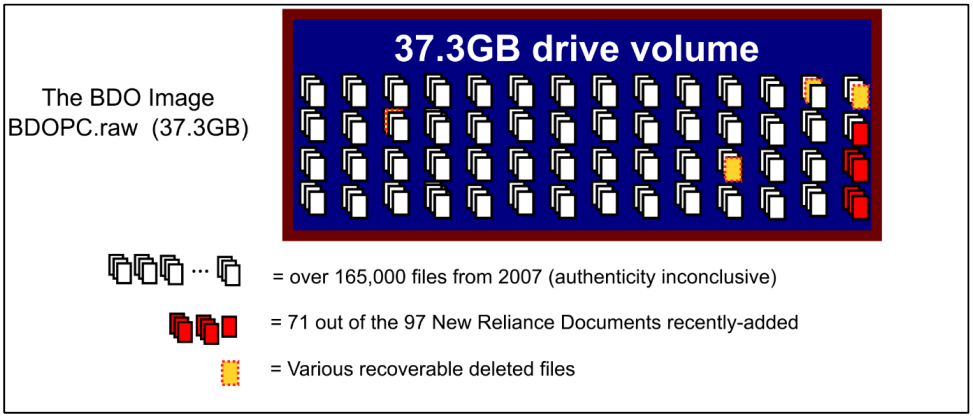


Figure 6: Diagram of BDO Image including deleted files

116. Considering the various interrelated points, my opinion of the BDO Drive is as follows:

a. In my opinion the BDO Drive has been modified. The metadata recorded dating it to 2007 is false, and not contemporary to the actual time of creation. The file was created on or after 19 September 2023.

b. There was an original image from which BDOPC.raw was created, but it has not been provided.

c. In my opinion, that pre-existing original image was edited over the course of three days in 17 to 19 September 2023, using a user account (with SID ending -1002) that was not original to the BDO PC from which the Image was taken. The user added files to the BDOPC.raw image and modified files within it. This took place alongside the modification of the Samsung drive which I have described above, and which displays evidence of clock manipulation using the same manipulated clock times as are found within BDOPC.raw. I consider it very likely that it was done using the same user account.

d. The file BDOPC.raw itself could not have been created until 19 September 2023.

e. The modified files from 17-19 September 2023 include the majority (71 out of 97) of the New Reliance Documents.

f. That user was connected via a computer whose clock was manipulated back and forth between various dates in 2007, but only after it had already read 17 September 2023.

g. The BDOPC.raw image was not connected to that computer only once in September 2023. It was manipulated over the course of at least three days, during at least eight editing sessions of up to several hours each, with the relevant computer being rebooted in between them. The editing is not consistent with automatic or unsupervised software processes, but with a process of editing by a user over the whole course of that time.

h. As well as recording the 2023 timestamps and user SID activity, this also led to the wider presence of timestamps relating to New Reliance Documents which do not match the apparent usage history of the BDO PC from which the Original 2007 BDO Image was captured, including many dates relating to 31 October 2007. However, the BDO PC from which the Original 2007 BDO Image was taken was not booted up between 5 July 2007 and the date of capture of that image, as established by multiple independent indications from within the operating system files on that drive.

i. I also take into account the presence of a copy of LLM_ProprosalA.doc{BDO} which is identical to ID_003935 (and which contains data that in my opinion could not have existed in 2007), as well as the fact that LLM_ProposalA.doc{BDO} was deleted, which is indicative of manipulation.

{ID_003935}

j. In relation to the remaining 26 out of 97 New Reliance Documents, they may have been modified, but it is not possible to be certain:

   i. 3 of them are present on the BDOPC.raw image as well as on the Samsung Drive.

   ii. 26 are present on the BDOPC.raw image. It is possible to say that at least some form of those files was present on the original BDO PC. As a result, the SIDs do correspond to the original user account of the BDO PC and also do not carry ObjIDs (which are not expected to be present on every file, even if modified).

   iii. It is not possible to establish whether or not they have been modified in addition to the other changes recorded above. If the Original 2007 BDO Image was available, it would be simple to establish whether those 26 files were authentic to that Original 2007 BDO Image (by examining to see whether they are present on the unaltered image).

iv. However, the Original BDOPC.raw image has not been provided. There is however an indication that a previous file called BDOPC.raw was present on the Samsung Drive, and has been deleted (and is not recoverable), though this may not be the Original BDO Image.

While I can say with confidence that some form of these files existed on the original BDO drive, the fact that they are taken from within the manipulated BDOPC.raw image (and the indications of deletion of other images in September 2023) leads me to approach the authenticity of the content of those documents with serious caution. It is not currently possible for me to establish whether they are genuine, even though a method of doing so would recently have existed, had the Original BDOPC.raw image been disclosed.

INFODEF09.RAW AND IMAGE.RAW

117. This section of the report addresses two additional drive images that I have managed to recover from the free space on the Samsung Drive, as shown in Figure 4 above.

118. This analysis has supported my conclusions on the image BDOPC.raw{SS}, and in part, I conducted the analysis of all three drive images together.

119. Since my conclusions on BDOPC.raw{SS} are set out quite fully above, this section is much briefer, and I will set only the most relevant investigations and findings as briefly as possible.

The two deleted Image files

120. The two deleted image files are **Image.raw{SS} and InfoDef09.raw{SS}**. The file metadata of these is as follows:

Name	Is Deleted	File Created	Last Written	Last Accessed	File Size
image.raw{SS}	Yes	13/09/2009 09:50:10	13/09/2009 09:47:28	13/09/2009 09:50:10	522,117,840,896
InfoDef09.raw{SS}	Yes	13/09/2009 09:35:22	19/09/2017 11:34:42	13/09/2009 09:35:22	179,594,199,040

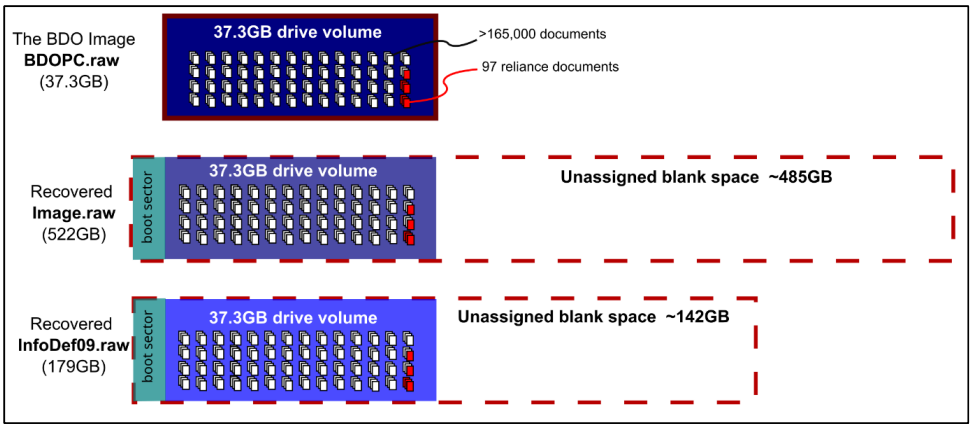


Figure 7: Comparison of three image files showing overlap

121. Comparing these two files to each other and the BDOPC.raw, I make the following observations:

a. **Contain Boot Sectors:** Unlike BDOPC.raw{SS}, both Image.raw{SS} and InfoDef09.raw are not images of just one partition. They include:

   i. A small Boot Sector at the beginning of the images,

   ii. a main data partition which is 37.3GB in size, and

   iii. large tracts of unallocated blank space at the end.

b. **Image.raw and InfoDef09.raw are identical apart from blank space:** The only difference between Image.raw{SS} and InfoDef09.raw{SS} is the size of the blank space at the end: 485GB for Image.raw, and 142GB for InfoDef09.raw{SS}. If that blank space is trimmed off, they are identical (a fact which I have confirmed by MD5 hash comparison).

c. **99.98% similar to BDOPC:** Image.raw{SS} and InfoDef09.raw are both extremely similar in content to BDOPC.raw{SS}. On the data volume of Image.raw{SS}/InfoDef09.raw{SS}, there were a total of 165,241 relevant files.[9] Of these, 165,210 were hash identical to files on BDOPC.raw. This equates to 99.98% of the files compared.

122. Therefore,

[9] This comprised all file items for which it was possible to calculate an MD5 hash value and included items such as system files, OS logs, alternate data streams, and excludes files of 0 bytes in capacity.

a. All three files (BDOPC.raw, Image.raw, InfoDef09.raw) clearly relate to the same Original BDO Drive, but they differ slightly.

b. The only differences between BDOPC.raw and InfoDef09.raw are the presence of the boot sector; the presence of blank white space; and differences in 0.02% of the files on the data volume.

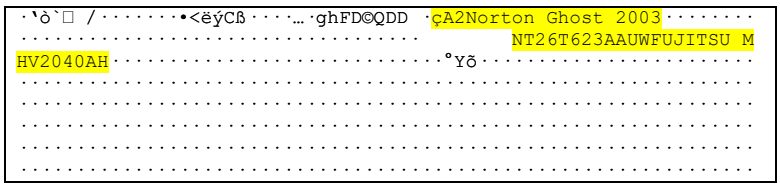
Annotation and terminology

123. I will refer to files and folders in InfoDef09.raw{SS} with the tag {Idf09}.

124. Since Image.raw{SS} and InfoDef09.raw{SS} are effectively identical to each other and differ only in blank space, I will not refer to Image.raw{SS} any further, and will refer only to InfoDef09.raw{SS}.

Boot sector in InfoDef09.raw

125. The Boot Sector of InfoDef09.raw (Boot Sector {Idf09}), which is also adjacent to a partition table for the drive, includes the following content (text highlighted yellow for ease of review):



126. This indicates:

a. The drive was originally populated by a cloning process using Norton Ghost 2003. This is software commonly used to clone computer hard disks and is useful for companies provisioning software onto computers. It is consistent with the image being created from a corporate laptop computer.

b. The Make, model, and serial number of the original hard disk of the BDO PC are recorded:

Make	Fujitsu
Model	MHV2040AH
Serial Number	MNT26T623AAUW

c. As is clear from sales of the device on the internet and other specification sheets also available online,[10] the model MHV2040AH is a Fujitsu model of hard disk dating from 2007 or before, and is a form factor used in laptop computers. The "2040AH" model in particular is 40GB in size:

2.5-Inch, 5,400 RPM Series Hard Disk Drive Specifications						
Model		**MHV2040AH**	**MHV2060AH**	**MHV2080AH**	**MHV2100AH**	**MHV2120AH**
Storage capacity (formatted)[1]		40.0 GB	60.0 GB	80.0 GB	100.0 GB	120.0 GB
Bytes/sector		512				
Seek time	Track to Track	1.5 ms typ.				
	Average	12 ms typ. (Read), 14 ms typ. (Write)				
	Maximum	22 ms typ.				
Average latency		5.56 ms				
Rotational speed		5,400 RPM				

Figure 8 Extract from Fujitsu datasheet

InfoDef09 not the original BDOPC image

127. The observations above suggest that InfoDef09.raw{SS} and Image.raw{SS} are not the Original 2007 BDO Image, since they are much larger than the 40GB hard drive which has been imaged (they are 179GB and 522GB respectively). It would not normally be possible to extract such large images from a 40GB hard disk.

128. These sizes are more consistent with InfoDef09.raw{SS} and Image.raw{SS} being created from a much larger hard drive, onto which the Original BDO Image had been written (and as I establish below, being edited) and then re-imaged, resulting in image files which were larger than the original (and were later deleted).

InfoDef09.raw is the same as InfoDef09.zip

129. Above, under the heading "The Encrypted Zip File InfoDef09.zip{SS}", I explained that there is an extant zip file on the Samsung Drive which is encrypted and cannot be decrypted. It contains only one file, and I explained that the CRC32 hash of that file is shown in the zip archive as being `8D285432`.

130. The following table summarises the known data of the file within InfoDef09.zip{SS}, compared to the data for the recovered, deleted file InfoDef09.raw{SS}:

[10] For example https://www.disctech.com/Fujitsu-MHV2040AH-40GB-7-2K-2-5-IDE-Laptop-Hard-Drive and https://www.fujitsu.com/downloads/COMP/fcpa/hdd/mhv2xxxah_datasheet.pdf from which the table above is taken

	internal content of InfoDef09.zip	Recovered deleted file
Filename	InfoDef09.raw	InfoDef09.raw
Size	179 594 199 040 bytes	179 594 199 040 bytes
Created	13/09/2009 08:35	13/09/2009 09:35:22
Modified	19/09/2017 10:34	19/09/2017 11:34:42
Accessed	13/09/2009 08:35	13/09/2009 09:35:22
CRC32 Hash	8D285432	8D285432

131. As can be seen, they are a perfect match (including hash match), with the only differences being in how the data is presented:

a. a 1-hour time difference (which can be accounted for by the change in daylight saving time as this report is being done during GMT not BST time, or alternatively, if one timestamp is simply recorded in UTC and one in the local time zone BST), and

b. the resolution of the timestamps, with the zip file data being rounded down last minute.

132. It is therefore clear that the deleted file InfoDef09.raw{SS} is the same as the content of the zip file InfoDef09.zip{SS}. I observe that InfoDef09.raw{SS} also shows the same contradictory metadata as I discussed above, in relation to the 2017 and 2009 time stamps.

Comparing BDOPC.raw{SS} and InfoDef09.raw{SS}

133. As I remark above, the data volume partitions between InfoDef09.raw{SS} and BDOPC.raw{SS} are almost identical, but for changes made to 0.02% of the files.

134. I conducted a comparison of hashes to identify which files had changed between the two drives. I observed that,

a. Out of the 97 New Reliance Documents, 17 documents existed on {Idf09} in slightly different versions.

b. Comparison of the documents reveals that the edits made appear to relate to this case and to the provenance of the image, such as changes to dates and wording relating to Bitcoin. I have analysed them in more detail in include a copy of the files that comprise these differences at **Exhibit PM-R 4.7**. I :

{H/316} - {H/317.22}

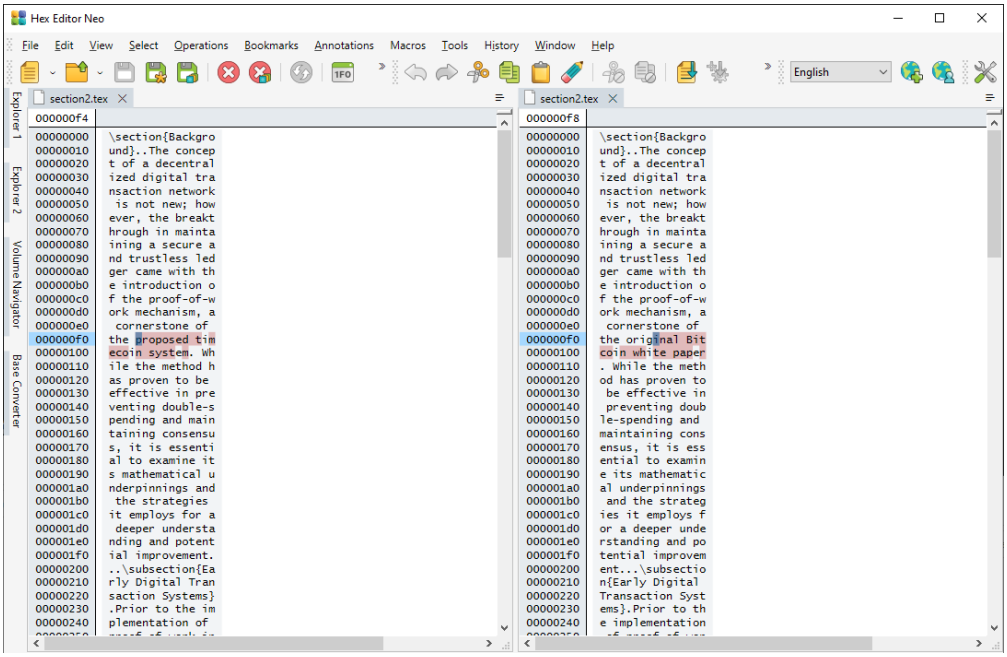


Figure 9: Comparison of ID_004716{BDO} with the equivalent in {Idf09}. ***Note: In this comparison and the comparisons at Appendix PM46, changes are shown from right to left (rather than from left to right) as a result of the order in which the documents were discovered on the drive, the right-hand side documents being deleted versions..***

{ID_004716}
{H/278}

c. I also observed indications that suggest a possibility that ChatGPT may have been used to create content for the documents, which I have explained in Appendix PM46.

{H/278}

135. I therefore formed the preliminary opinion that InfoDef09.raw{SS} was a prior version of the BDOPC.raw{SS} file, which was later edited so as to remove content in the internal documents which would not have seemed authentic to 2007.

<u>Other findings in relation to InfoDef09.raw{SS}</u>

136. I repeated each aspect of my analysis of BDOPC.raw with InfoDef09.raw. Although I went into the same level of detail in my analysis, I summarise the findings as briefly as I can.

a. **Same operating system and volume ID:** the following table lists the equivalent format data of the BDOPC.raw{SS} image alongside the InfoDef09.raw{SS} image. As can be seen, it is a perfect match. In particular, the fact that these both have the same Full Volume Serial Number and Volume Serial Number indicates that one is derived from the other, or they are both derived from a common ancestor:

	BDOPC.raw	InfoDef09.raw
Volume Serial Number	E859-F3AF	E859-F3AF
Full Volume Serial Number	62E85A21E859F3AF	62E85A21E859F3AF
Driver Information	NTFS 3.1 Dirty (301)	NTFS 3.1 Dirty (301)
File System	NTFS	NTFS
Total Sectors	78,124,032	78,124,032
Total Capacity	39,999,500,288 Bytes (37.3GB)	39,999,500,288 Bytes (37.3GB)
Total Clusters	9,765,503	9,765,503
Unallocated	1,676,435,456 Bytes (1.6GB)	1,725,231,104 Bytes (1.6GB)
Free Clusters	409,286	421,199
Allocated	38,323,064,832 Bytes (35.7GB)	38,274,269,184 Bytes (35.6GB)

b. **Same indications of bdopc use:** Both show the same indications about usage of the BDO PC (from which the underlying Original 2007 BDO Image was taken), including shutdown and partial boot times, file system and operating system, and other indications discussed above in relation to BDOPC.

{ID_003935}

c. **LLM_ProposalA.doc:** As I explained above, a copy of ID_003935 was present on BDOPC.raw as a deleted file, which I was able to recover (**LLM_ProposalA.doc{BDO}**). Within InfoDefo09.raw however, the same file was present and extant: **LLM_ProposalA.doc{Idf09}** had not yet been deleted. Further, both LLM_ProposalA.doc{BDO} and LLM_ProposalA.doc{Idf09} were present at exactly the same sector within their respective images. This firmly indicates that BDOPC.raw was derived by editing InfoDef09.raw, with this file being deleted during the editing process (but not overwritten, such that it remained recoverable within BDOPC.raw).

   It also provides a further indication that InfoDef09.raw is not authentic to its purported timestamps, for the same reasons given above in relation to LLM_ProposalA.doc{BDO}.

   i. There are several instances where deleted documents exist on BDOPC.raw, but are extant in the exact same sector location on Infodef09.raw

d. **SIDs**: Similar SID information was present in InfoDef09.raw as compared to BDOPC.raw. In summary, the vast majority of the files inside it were created with SIDs that were authentic to the original time period. 66 New Reliance Documents had been added with the more recent SID ending -1002 which is also associated with September 2023 activity.

e. **ObjIDs**: There were 20 files within {Idf09} that had ObjIDs after 6 July 2007:

   i. This is fewer than within {BDO}, which is again consistent with the direction of editing described above.

{H/311}

ii. The ObjIDs also encoded Object Boot Times and are shown in Exhibit PM-R 4.5. Unlike the {BDO}, these fell into just two sessions (instead of eight sessions on BDO):

- One session dated 17/09/2023 13:20:48,
- and another dated 31/10/2007 15:34:39 (the "**First 31 October 2007 session**").

f. The observations about the "First 31 October 2007" session provided much more certainty about the direction and time of editing of both images. The records indicate that:

- First, the computer (not either of the raw images) was booted up while the clock was set to 17 September 2023. I take this to be an accurate date, since it is just a few days before the Samsung Drive was forensically imaged by KLD on 20 September 2023.
- The computer clock was then set back to a past date, likely in September or October 2007, and an image was mounted for editing. However, the computer was not yet rebooted, so the ObjID retained the 17 September 2007 date. Editing began, resulting in 7 ObjID records that are present and identical between {BDO} and {Idf09}, all recording 17 September 2023.
- The computer was then rebooted while the clock was still set to 31 October 2007, resulting in the "First 31 October 2007" session being created timed at 15:34:39. Editing was resumed. After editing 13 more records, InfoDef09.raw was created, resulting in 13 records dated to the boot timed at 31 October 2007 at 15:34:39.
- Editing of the image then continued for a further five sessions on 18 September 2023 and 19 September 2023. This included editing of various New Reliance Documents, deletion of LLM_ProposalA.doc (and at least one other file), and adding further files to the Image.
- The BDOPC Drive image was then created.
- At some point in this process, the encrypted ZIP file InfoDef09.zip was created, and InfoDef09.raw was deleted.

g. **Transaction logs:** Above I explain that the presence of 17 September 2023 metadata within the {BDO}transaction logs indicated editing on that date. Having checked the equivalent logs in detail, the {Idf09}transaction logs are consistent with that analysis and also consistent with the analysis that BDOPC.raw is derived from InfoDef09.raw. Rather than setting out all of the detail, it is possible to explain by reference to the {Idf09}folder metadata, shown below in a

table. This is very similar to the equivalent table for {BDO}, with four differences (shown in highlight):

Name	Path	Created	Modified	Record changed	Accessed
$Extend	\	15/12/2004 14:06:59	15/12/2004 14:06:59	15/12/2004 14:06:59	15/12/2004 14:06:59
$Deleted	\$Extend	17/09/2023 13:02:31	17/09/2023 13:02:31	17/09/2023 13:02:31	31/10/2007 14:49:18
$RmMetadata	\$Extend	17/09/2023 13:02:31	17/09/2023 13:02:31	17/09/2023 13:02:31	17/09/2023 13:02:31
$Txf	\$Extend\$RmMetadata	17/09/2023 13:02:32	17/09/2023 13:02:32	17/09/2023 13:02:32	17/09/2023 13:02:32
$TxfLog	\$Extend\$RmMetadata	17/09/2023 13:02:32	17/09/2023 13:02:34	17/09/2023 13:02:34	17/09/2023 13:02:34

The yellow highlighted dates above indicate where 2023 dates are recorded for {Idf09} which are different in {BDO}. The green highlighted date shows a date of 31/10/2007 in {Idf09} which is different in {BDO}.

In all 4 cases, the timestamp in {BDO} is set to 19 October 2007. This indicates that the editing session with the clock set to 19 October 2007 took place after the "First 31 October 2007" Session (even though the 19 October is an earlier date), and is indicative of clock manipulation being used to adjust the clock backwards and forwards. This is most likely to have taken place on either 18th or 19th September 2023.

137. I did not find any indications within InfoDef09.raw which suggested that my analysis of BDOPC.raw was incorrect. All the findings in InfoDef09.raw appear to support the conclusions that were drawn in relation to BDOPC.raw (and I repeat that the two analyses informed each other and were not conducted entirely separately).

138. An overview diagram of InfoDef09.raw is set out below.

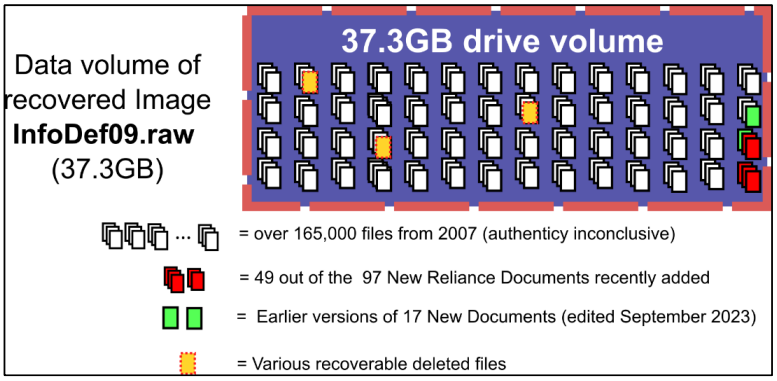


Figure 10. Overview diagram of InfoDef09.raw

Lost Passwords and 2020 Hack

139. I understand from the letters I have been provided that Dr Wright has stated that the passwords to InfoDef09.zip{SS} were lost in a hack which took place in 2020.

140. I do not think that is correct. The content of InfoDef09.raw{SS} (which is the same as the content of InfoDef09.zip{SS}) contains clear indications that it was edited on 17 September 2023. As set out in Appendix PM46, the content of documents within InfoDef09.raw has also been modified in ways that remove content that post-dates 2007 (its purported creation date), including editing of files which are New Reliance Documents. The fact that the hash-identical content was edited in 17 September 2023 indicates that InfoDef09.raw{SS} could not have been zipped up to create the encrypted InfoDef09.zip{SS} in 2020 which is mentioned as the date of the hack.

{H/278}

141. This also indicates that InfoDef09.raw{SS} was deleted after it was created 17 September 2023, so it would have been accessible as an extant file on the Samsung Drive at that point, without encryption (since the raw file is not encrypted, only the zip that was created from it).

142. Also, since the zip file is encrypted, it is not possible to edit the content within the zip file without the password. This limitation stands for user driven activities and automated/background activities.

RESPONSE TO DR WRIGHT'S RECENT EVIDENCE

143. I have been asked to review Dr Wright's 9th, 10th, and 12th Witness Statements and whether they lead me to change my opinions expressed in this Report and previously. They do not.

{E/26}
{E/31}
{CSW/7}

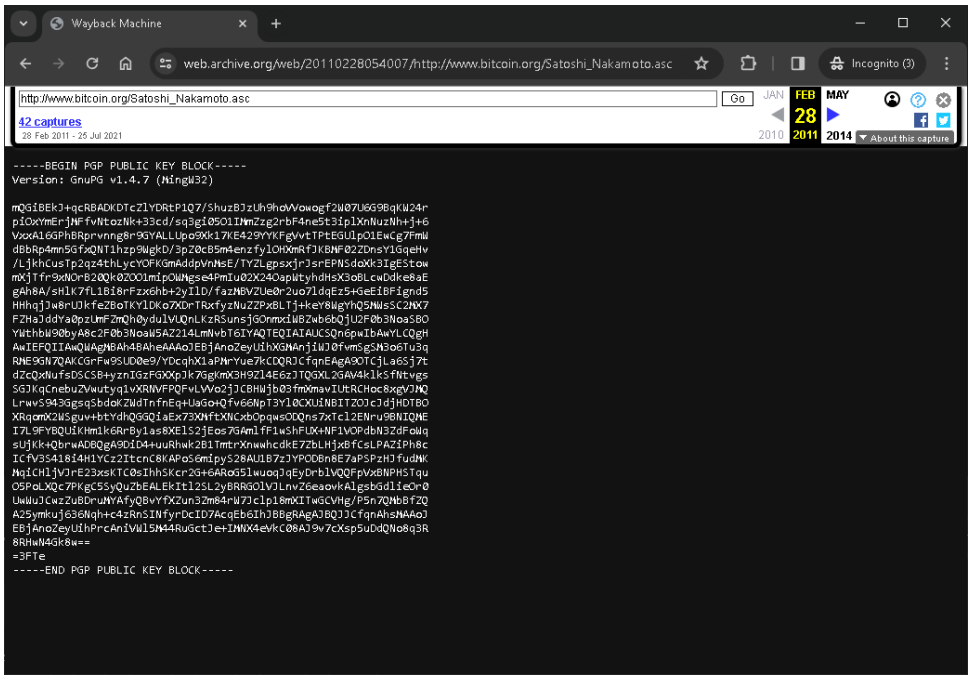
PGP Key

144. I note that in his recent evidence, Dr Wright mentions a PGP key which he says dates from 2011. As part of responding to his evidence, I have been asked to consider whether I can determine a reliable origination date for the file "Satoshi_Nakamoto.asc", a copy of the PGP key that was historically hosted on the website http://www.bitcoin.org/Satoshi_Nakamoto.asc .

145. I have found it is possible to verify the date of the key to October 2008 in two ways.

Wayback Machine capture

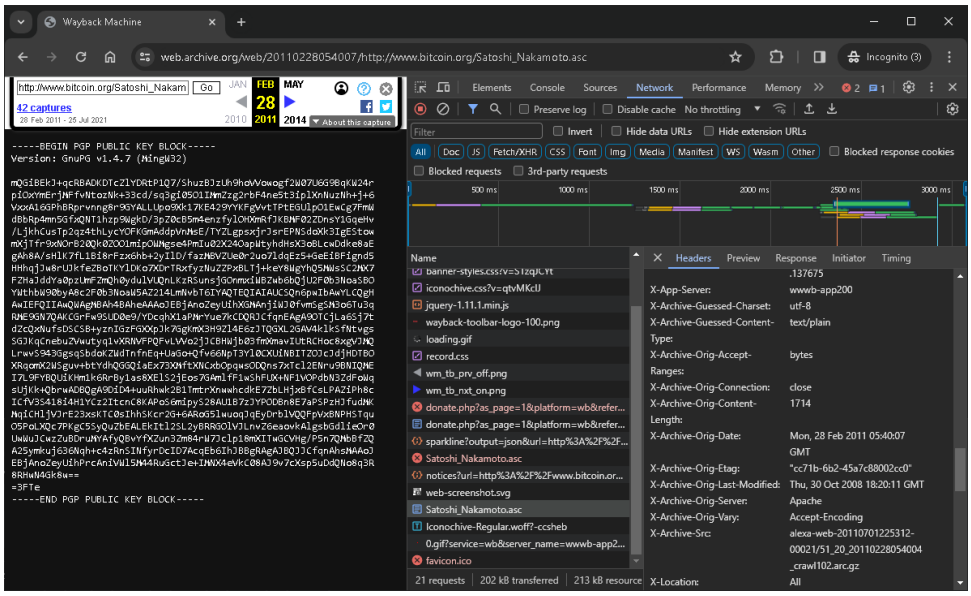
146. The earliest available Web Archive snapshot was produced on 28 February 2011[11]. This is the date on which the snapshot was produced. It does not mean that this is when the file was first uploaded to that URL, but only when the Wayback Machine systems first archived it, meaning that no earlier snapshot was produced. The screen capture for that file is as follows:



147. By invoking the Google Chrome browser, pressing the keyboard combination CTRL-SHIFT-I together to access its advanced tools, and inspecting the header information for the file "Satoshi_Nakamoto.asc", it is possible to inspect the metadata associated with that key, as hosted on the Wayback Machine. There are sections of information relating to the user's own current browsing session, but also a section of information that pertains to the original data present at the time it was crawled and archived, taken from: "http://www.bitcoin.org/Satoshi_Nakamoto.asc". This included the following information attributed to the file "Satoshi_Nakamoto.asc":

[11] https://web.archive.org/web/20110228054007/http://www.bitcoin.org/Satoshi_Nakamoto.asc, a capture of which is available at **Exhibit PM-R 4.7**

{H/316}



148. This shows an array of information about the browsing session, but the most important are the X-Archive-Orig fields, which record the original metadata associated with that file when it was downloaded:

X-Archive-Orig-Date:	Mon, 28 Feb 2011 05:40:07 GMT
X-Archive-Orig-Etag:	"cc71b-6b2-45a7c88002cc0"
X-Archive-Orig-Last-Modified:	Thu, 30 Oct 2008 18:20:11 GMT
X-Archive-Orig-Server:	Apache
X-Archive-Orig-Vary:	Accept-Encoding
X-Archive-Src:	alexa-web-20110701225312-00021/51_20_20110228054004_crawl102.arc.gz

149. This indicates the pgp file was uploaded with a date of 30 October 2008, and retained that upload date as its "x-Orig" last-modified timestamp when archived.

150. It is also possible to verify the same date of the origin for the key in another way, as (although I am not an expert in cryptography) I am aware that PGP keys themselves do encode timestamps which can be extracted simply with a command line program called GPG.

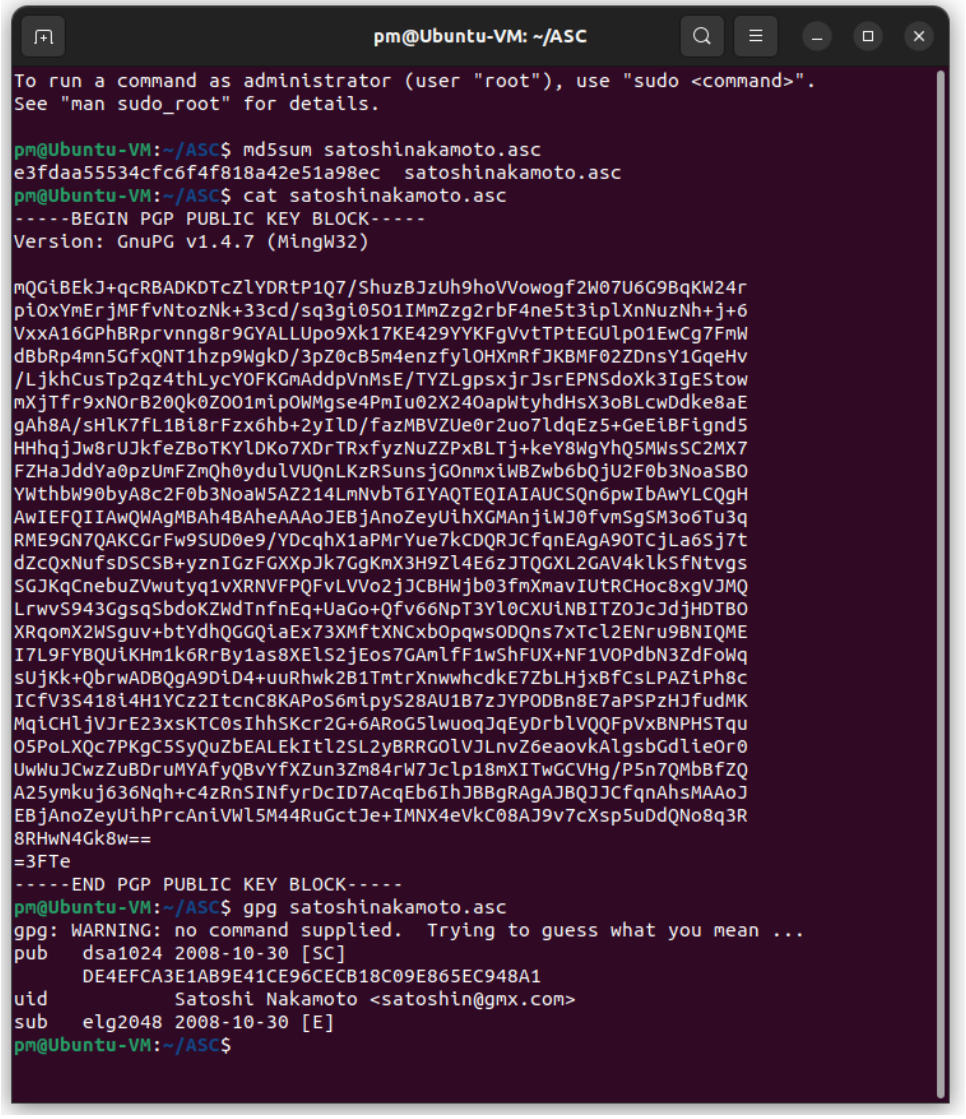
Having checked the MD5 hash and SHA256 hashes set out below and established the file to be an accurate copy, it was then possible to GPG to assess its date.

I used the following three commands:

a. Md5sum – to calculate and display the MD5 checksum for the file

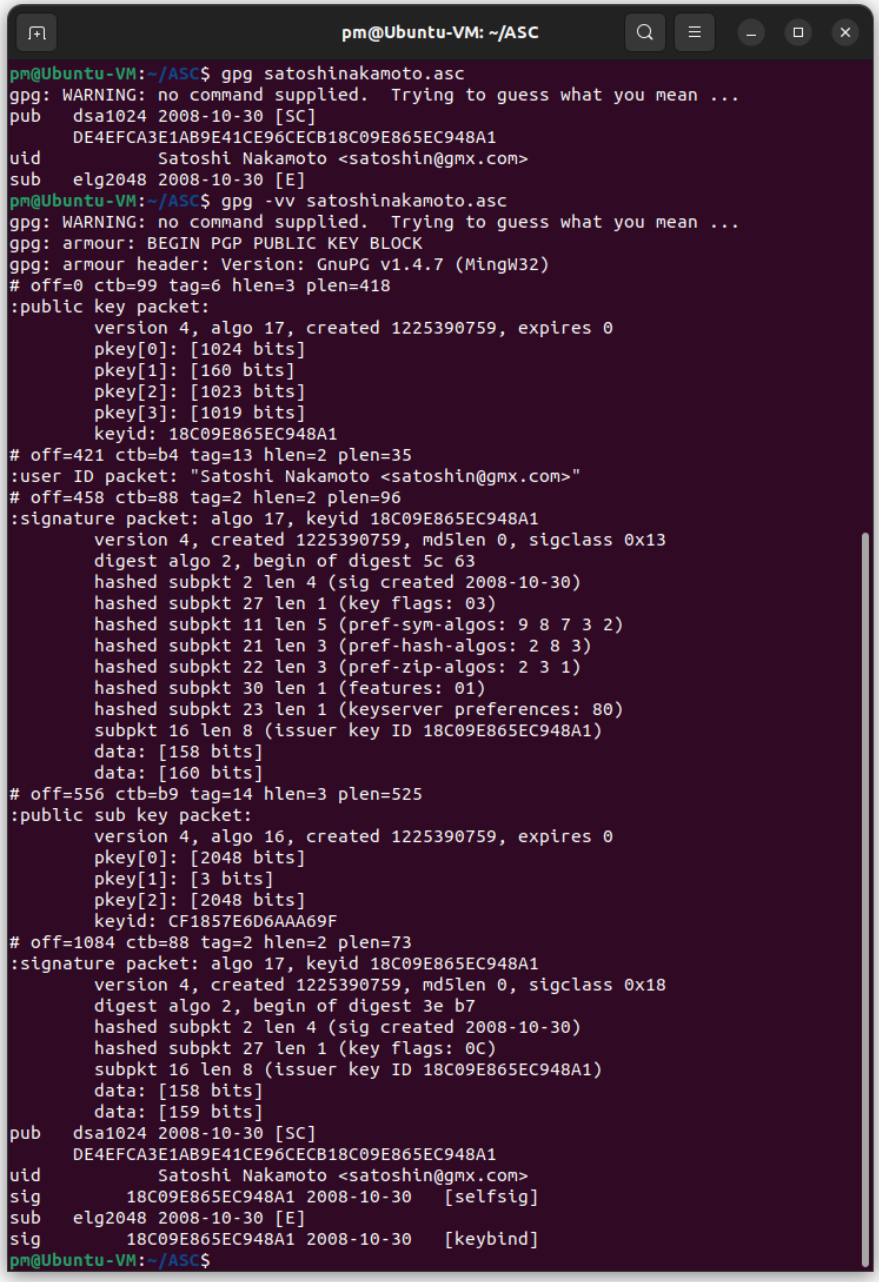
b. Cat - to display the content of the file

c. GPG – to display information pertinent to the file



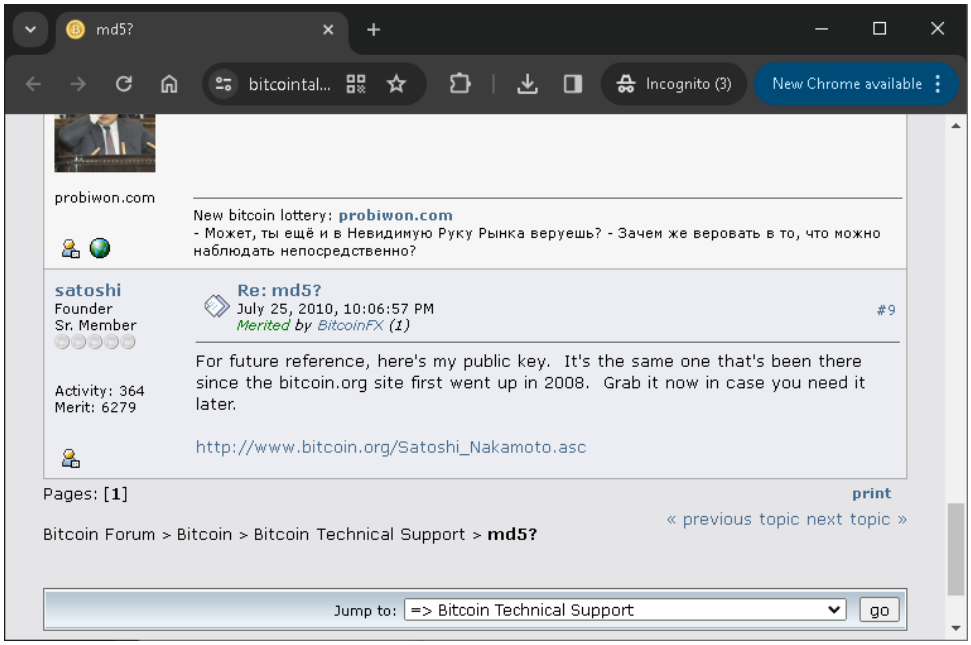
151. As can be seen in the above screenshot, my local file “satoshinakamoto.asc” contains a correct copy of the key, and the same MD5 hash.

152. The output of GPG provides a datestamp for 2008-10-30 (30 October 2008), thus confirming the other analysis conducted. I also used GPG with the option "-vv" which generates a more verbose output as shown below:



153. I observe that this includes a more precise encoded timestamp in UNIX format, "1225390759" which decodes to Thu Oct 30 2008 18:19:19 GMT+0000. This again correlates within 1 minute of the last-modified time captured within the Web Archive snapshot.

154. Finally, I note that other searches for this file led me to the following forum post on Bitcointalk.org[12] which is recorded as being posted by "Satoshi" on 25 July 2010. This date predates the Web Archive snapshot. The post states "*For future reference, here's my public key. It's the same one that's been there since the bitcoin.org site first went up in 2008. Grab it now in case you need it later.*" In my opinion, this is consistent with my findings above.



{E/26}
{E/31}

Response to the technical points in Dr Wright's ninth and Tenth witness statements

155. I have reviewed Dr Wright's Ninth and Tenth witness statements in a great deal of detail. In summary, they did not affect my opinions. My overall view is that the information being provided is rather general in nature, and does not have much or any particular application to the documents that I have analysed. While a great deal of systems and processes mentioned, the statements are rather vague and I do not consider that the explanations given are particularly relevant to my analysis.

---

[12] https://bitcointalk.org/index.php?topic=458.msg5772#msg5772, a capture of which is available at **Exhibit PM-R 4.8**

{H/318}

156. For example, though I observe that Dr Wright talks a great deal about the use of symbolic links, those do not work in a way that would cause the irregularities that I have observed, particularly where I have gone to pains to make sure that my opinions are formed in view of multiple streams of analysis. In the case of symbolic links, they are simply a term for a file or record that acts as a pointer, 'alias', or 'shortcut' to another file. The actual data is contained in the file that is being pointed to, and a symbolic link just contains text that specifies the path to that file, which is often used for convenience. The presence of symbolic links does not affect how the ultimate file is handled by the operating system.

157. I have also addressed many of the points in my previous analysis already and do not repeat them. However, there are two points that I thought it might be helpful to address in more detail as follows.

158. First, the suggestion that documents could be contaminated by changing a Microsoft Word template. This is not consistent with how Microsoft Word operates:

a. It is correct that MS Word allows templates to be set and that Normal.m is the template used for general documents.

b. However, that is a file used by MS Word to build new blank documents from scratch. It does not apply to existing documents, and making a change to a current template would not cause existing or past documents to be modified in the way Dr Wright seems to suggest.

c. Further, the inclusion of elements in templates does not explain the observations made in respect of Dr Wright's documents. For example, adding a Grammarly reference to a Normal template could, in theory, cause future documents (created after that date) to incorporate the same reference. However, in each case the reference would be identical, and would encode the same identical information including the same identical timestamp. That is not what I have observed. I have not observed one Grammarly timestamp being repeated across multiple later-created documents: To the contrary, I have observed many different Grammarly timestamps embedded within documents which would otherwise appear as if they were created in the past, at a time before Grammarly was first created. I have also explained in my First Report that Grammarly does not interact with documents automatically, but only when interacted with by a user's explicit command.

159. Second, the suggestion Dr Wright makes is that due to his file system, files may have become merged together. I do not consider this a plausible explanation for any of the issues I have observed, for the following reasons:

a. The minimum storage unit assignable from a hard disk is 512bytes (for older hard drives) and 4096bytes (for newer hard drives) – called a 'sector'.

b. On a 40GB hard disk, there would be room for over 78 million 512byte sectors.

c. If a storage error led to data from different files being blended together, it would be spliced together in chunks of at least 512bytes.

d. In data terms, 512 bytes is a great deal of information: It would be enough to store 512 text characters (within an MS Word document), or 2048 characters (if stored in hexidecimal).

e. If text data were spliced together, it would be expected to be assigned in large detectable chunks which would stand out from the rest of the document structure very clearly, because it would be out of context.

f. While in theory it is possible for documents to become corrupted if data for a sector or some sectors has been incorrectly drawn from the wrong place on a hard disk, it would result in a "Frankenstein's document". This would not be expected to result in healthy documents that could be interpreted by a reader e.g. MS Word. It would instead be likely to result in a corrupted document.

g. In my view (given the size of storage devices on computing devices) the chances are vanishingly unlikely, that a document would become corrupted in a way that led to a healthy document which did not immediately show signs of corruption – especially taking into account the number of available sectors on a hard drive, which encompasses many different types of document.

h. Going further, it would be something miraculous for such merging of unrelated data from random parts of a disk to result in not only a healthy document, but also a healthy document with sensible, legible text inside a well-defined structure.

{ID_000550}

i. Even in the case of documents such as ID_000550, (which contains extensive content from previous revisions embedded within slack portions of the file), the content in slack portions is human-readable, coherent, text which appears in precisely the same place of the file as would be expected in such circumstances.

j. It reminds me of the idea of drawing 13 cards from a shuffled deck of 52 and expecting the outcome to be a perfectly organised sequence of Clubs: However in this case it is even more unlikely, since given the size of files concerned it is not just drawing a sequence of 13 from a deck of 52, but drawing a sequence of 16-32 (data clusters to make one file) from a deck of

several million – and doing that repeatedly, in each case resulting in hundreds of documents that I have examined.

{CSW/7} *Response to Dr Wright's 12th Witness Statement*

160. Very shortly before the deadline for service of this Report, I have been provided with Dr Wright's 12 Witness Statement. I have read it closely, and though I do not have time to go into detail in my observations or to investigate any of the points raised further, it does not change my overall view. I have the following comments:

a. I do not agree that the file BDOPC.raw{SS} was created with the DD command. That command would typically be expected to capture not just a single data partition, but also the boot sector, and wasted space at the front and end of the physical drive. In my analysis, I have seen that the deleted file {Idf09} does have such information, but BDOPC.raw does not. It is possible that the Original 2007 BDO Image was produced using DD, but that image is not available to me.

b. I note that there is no evidence of Dr Wright using the BDOPC.raw consistently over a period of time, but that activity stopped on 6 July 2007 and jumped to 31 October 2007 (which timestamps were recorded *after* the 2023 timestamps I have observed). There is however evidence of a pattern of editing of creating documents in around 12-16 September 2023, and adding documents to the images and editing within the images between 17 and 19 September 2023.

c. The nature of the $Txflogs folder indicates that the clock was set to 31/10/2007 after being set to 17/09/2023. Further, I note that in 2007, the snapshot would take much longer to create than the time difference listed, and I would estimate it to have taken several hours in some cases to write to disk.

d. The configuration files disclosed by Dr Wright refer to "image.raw". That is the name of a deleted drive image which I have analysed in this report and is consistent with the VMWare machine being used in September 2023.

e. It is also possible to say with certainty that the drive image being discussed in Dr Wright's witness statement is not the same drive image as has been disclosed, because of the extent of the file capacity. In the VMWARE configuration files, these specify the "extent" (amount of

storage space) of the image to which the configuration file applies, specifically as 78124095 is a sector count for 39,999,536,640 bytes.

f. By contrast my own observation is that the extent of BDOPC.raw is 39,999,504,384 bytes, which is smaller. This is therefore a mismatch for the image file to which the VMWare configuration points. It may be that the difference in space is due to excluding the boot sector from BDOPC.raw, but either way it cannot be the same image.

g. BDOPC.raw has not been run as a VM. It has not been booted since 05 July 2007, virtually or physically. If there were snapshot files of the kind Dr Wright refers to in paragraph 14 of his Twelfth statement, these would be expected to be present on the Samsung Drive, but they are not. Further, the content changes that have been made to BDOPC.raw are contained directly within the raw image, not a separate snapshot.

161. Overall, the explanation provided does not explain how the September 2023 documents and timestamps came to exist within the BDOPC image.

162. However, in Dr Wright's statement there is a strong indication of the use of clock manipulation to set the clock date backwards in time while editing an image. I say this because he references an entry in ID_006472 which uses the parameter "RTC.starttime". This parameter can be used to force the clock to an alternate setting, and would not ordinarily be present.

{ID_006472}

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: DocuSigned by: Patrick Madden 5943D537458F4C0... Dated: 18 January 2024