

**IN THE HIGH COURT OF JUSTICE**  
**BUSINESS AND PROPERTY COURTS OF ENGLAND & WALES**  
**INTELLECTUAL PROPERTY LIST (ChD)**

**Claim No: IL-2021-000019**

B E T W E E N :

CRYPTO OPEN PATENT ALLIANCE

**Claimant**

-and-

DR CRAIG STEVEN WRIGHT

**Defendant**

---

THIRD EXPERT REPORT  
OF MR PATRICK MADDEN

---



<b>SECTION 1: INTRODUCTION AND SUMMARY OF FINDINGS.....</b>	<b>4</b>
SUMMARY OF FINDINGS.....	4
DETERMINING FULL EXTENT OF MANIPULATION WOULD REQUIRE ACCESS TO COMPUTING EQUIPMENT.....	6
<i>Possible loss of information in the time since September 2023 .....</i>	<i>7</i>
<i>Some artefacts expected to persist unless major action taken .....</i>	<i>7</i>
<b>SECTION 2: THE 97 DOCUMENTS.....</b>	<b>8</b>
OVERVIEW OF THE 97 DOCUMENTS AND THE BDO DRIVE .....	8
<i>File types .....</i>	<i>8</i>
<i>Lack of metadata in many of the 97 documents.....</i>	<i>8</i>
<i>Need for review in context .....</i>	<i>9</i>
<i>Review of each file type within the drive .....</i>	<i>10</i>
LATEX DOCUMENTS.....	10
<i>LaTeX documents in general .....</i>	<i>10</i>
<i>Packages used in Latex documents .....</i>	<i>13</i>
<i>Conclusions on ID_004687 and ID_004648.....</i>	<i>18</i>
<i>Further note on ID_004687 and ID_004648.....</i>	<i>18</i>
PLAIN TEXT DOCUMENTS.....	19
HTM DOCUMENT .....	19
BMP IMAGES.....	20
PNG IMAGE (AND RELATED LATEX DOCUMENTS) .....	20
<i>Metadata inconsistencies.....</i>	<i>21</i>
<i>Relation of ID_004686.png to ID_004736.tex and ID_004735.tex.....</i>	<i>21</i>
<i>Direct metadata editing software .....</i>	<i>24</i>
<i>Why should I change the file attributes and date stamp? .....</i>	<i>25</i>
<i>Features of AttributeMagic (Standard edition) .....</i>	<i>25</i>
Change file date and time (Created, Modified, Accessed).....	25
Change attributes of files and folders .....	25
Rename files and folders.....	25
<i>Application to current findings.....</i>	<i>27</i>
<i>Note on inadequate previous timestamps .....</i>	<i>28</i>
<i>Conclusion on ID_004735, ID_004736 and ID_004686.....</i>	<i>28</i>
<i>ID_004735 - image.....</i>	<i>28</i>
OUTLOOK EXPORTS.....	32
DRA FILES .....	33
RTF FILES .....	33
<i>Overview of RTF files.....</i>	<i>33</i>

<i>Very little useful metadata in RTF files</i> .....	35
<i>Dating Riched20 10.0.19041</i> .....	36
DOC FILES .....	37
<b>SECTION 3: THE BDO IMAGE AND REPLY TO STROZ FRIEDBERG REPORT</b> .....	<b>40</b>
INTRODUCTION TO BDO IMAGE .....	40
INITIAL CONCLUSIONS BASED ON REVIEW OF DOCUMENTS FROM THE BDO IMAGE .....	41
<i>Access to computing equipment</i> .....	41
REPLY TO THE STROZ FRIEDBERG REPORT .....	41
RECYCLE BIN - INFORMATION DELETED.....	42
<i>Behaviour of Recycle Bin</i> .....	42
<i>The 20GB RAR file</i> .....	43
<i>The ESDT PDF</i> .....	45
METADATA DATES ON THE RECYCLE BIN AND BDO IMAGE .....	46
<i>User ID for Recycle Bin deletion</i> .....	46
<i>Metadata on ESDT.PDF</i> .....	46
<i>Metadata on 20GB RAR File</i> .....	47
<i>Date of deletion of the 20GB RAR File</i> .....	48
<i>Date of creation of the BDO Image</i> .....	49
TRANSACTIONAL LOGS WITHIN THE BDO IMAGE .....	49
<i>Meaning of transactional logs</i> .....	49
<i>First Transactional log segment: Likely creation date of BDO Image</i> .....	50
<i>Second log segment within BDO Image: 17 September 2023 dates</i> .....	51
<i>Fourth log segment within BDO Image: time-travelling dates</i> .....	51
<i>Fifth log segment within BDO Image: time-travelling dates</i> .....	51
<i>Transactional logs inside BDO Image: Conclusion</i> .....	52
DR WRIGHT’S INTERACTION WITH THE SAMSUNG DRIVE .....	52
<i>Behaviour of software listed by Dr Wright</i> .....	53
<b>SECTION 4: LATEX, OPENOFFICE, AND BITCOIN WHITE PAPER</b> .....	<b>56</b>
<i>Bitcoin White Paper created with OpenOffice version 2.4</i> .....	56
<i>Checking OpenOffice.org 2.4 functionality</i> .....	57
<i>Text check – first page of Bitcoin White Paper</i> .....	58
<i>Flowcharts and images within OO2.4</i> .....	63
<i>Comparative output from a different editor</i> .....	67
<i>Conclusion on method of creation of Bitcoin White Paper</i> .....	68

## SECTION 1: INTRODUCTION AND SUMMARY OF FINDINGS

1. This is my third expert report in these proceedings. I have approached it in the same way as my first and second reports. For the purpose of this report I have been provided with:
  - a. The Fifth Witness Statement of Dr Craig Wright and its exhibits (including a report from Stroz Friedberg, the “**SF Report**”),
  - b. The First Witness Statement of Ms Hannah Field and its exhibits (including a schedule of The 97 Documents (the ‘**97 Documents Schedule**’), and at pages 45-51 a chain of custody document for 93 out of 97 of those documents (the ‘**93 CoC Table**’).
  - c. The documents comprising disclosure volumes VOL008 and VOL012, which includes documents that I understand have been extracted from the Samsung Drive and the BDO image stored there-on.
2. I have been instructed that:
  - a. Dr Wright wishes to rely on the 97 documents 97 Document Schedule (the “**97 New Documents**”), and
  - b. The 93 documents listed in the 93 CoC Table are sourced from the BDO Image referred to in those statements (The “**BDO Image**”), and
  - c. A question has arisen about whether the Bitcoin White Paper was created using LaTeX or not.
3. I have been asked to do my best in the short time available to provide my views on the authenticity of the 97 New Documents, and the BDO Raw Image, taking into account the information available including the SF Report, and the question about the Bitcoin White Paper.

### Summary of findings

4. In summary, for the reasons in this report my view about the BDO Drive and 97 Documents is as follows.
  - a. **BDO Image content has been manipulated.** My view (without access to the BDO Image itself, but based on the information Dr Wright and Stroz Friedberg have provided) is that the internal content of the BDO Image as a whole is not authentic to 2007 and has definitely been manipulated, as internal timestamps record that its content was edited in September 2023. On

the information available, the most likely date of its creation is 17 September 2023. It is possible that the BDO Image itself is based on an image that was originally created in or around 31 October 2007, which was then altered, to add content that is inauthentic to the purported 31 October 2007 timestamp (and so creating a new image which has been backdated). The metadata provided is not consistent with an image that was created and remained unaltered. There may be some content within it that is authentic, but the raw image as a whole has been manipulated.

- b. **Drive and BDO Image modified / data deleted in September 2023.** I agree with the SF Report that the Recycle Bin of the Samsung Drive was emptied in September 2023. The information in the SF Report also reveals significant indications which I take into account in drawing my conclusion at a. above, particularly that the BDO Image itself and the Samsung Drive on which it resided were manipulated on 16 to 19 September 2023, including the deletion of data from the drive (first to the Recycle Bin, and then permanent deletion by emptying the Recycle Bin thereafter as I have stated above). Of the two documents deleted, it is very likely that one (ESDT.PDF) was a PDF export of one of the 97 New Documents. It is at least possible, and quite probable (though impossible to be certain), that another deleted document (20GB RAR file) was a compressed copy of the BDO Image itself. It is likely that either of those would have provided valuable sources of data for forensic examination.
- c. **Clock manipulation and metadata editing appears to have been used in relation to the drive.** The information in the SF Report also reveals impossible metadata records (for example files being deleted 'before' they were created), indicating the use of clock manipulation techniques to interact with the BDO Image and the Samsung Drive on which it resided. There are also indications that timestamps of files in the drive may have been edited directly.
- d. **Low-metadata documents not suitable for analysis outside their forensic context.** The vast majority of the 97 documents are in formats with little or no metadata for forensic analysis. 8 of the documents are in a proprietary format that I am unable to analyse. These files cannot be properly analysed outside their forensic context.
- e. **Documents in BDO Drive date from 2020 or afterwards.** Of the minority of files that do provide information that can be analysed forensically, I found several bear strong indications of metadata tampering and backdating:
  - i. **8 were created since 2020** - I have established that 8 of the 97 documents (all from within the BDO Image) were created at some point in the period 2020-2023.

- ii. **One Lynn Wright document with inconsistent metadata** - There is also one Lynn Wright document within the BDO Image which purports to have been Created and Last Modified in June 2007, using a version of MS Word which was not released until September 2007. It cannot therefore be authentic to its purported timestamps.
- iii. **LaTeX documents containing software references that post-date the creation of the BDO drive** - I analysed two LaTeX documents and found that they use software packages that were not consistent with 2007, and which were released several years later.
- iv. **One PNG Image and two related LaTeX files** are all related to each other and to the ESDT.PDF that was deleted from the Recycle Bin. All have identical timestamps (precise to the second), but one of them (the one that was inside the BDO Image) is different by precisely 1 year, which is an indication of the use of direct metadata editing tools to alter metadata timestamp.

**Determining full extent of manipulation would require access to computing equipment.**

5. Based on the information available, I have formed firm conclusions as to the presence of manipulation in the BDO Image and Samsung Drive. If it were necessary to determine the full extent of manipulation of the BDO Image, I would require access to the forensic image of the drive from which the BDO Image was taken, as well as access to the computing equipment used to interact with it, and the computing equipment used to interact with the Samsung hard drive in September 2023.
6. I have also addressed the benefits of inspection of the computing equipment itself in both my First and Second Reports. Dr Placks has also addressed this in his report, and we have agreed that this is important.
7. The computers will be expected to contain a number of logs, audit trails, and other forensically valuable artefacts that can be analysed for interaction with the content of the BDO Image and Samsung Drive. This may help to establish the nature of any automatic or user-initiated processes that took place which may have affected the integrity of the data on the drives and if so, in what way.
8. Assuming system logs and journals have been preserved and access to all relevant equipment was provided, I would expect that access to allow more information about the extent and possibly the time of manipulation.

Possible loss of information in the time since September 2023

9. However, I note that it has been several weeks since the BDO Image was discovered and interacted with. Logs and information can expire, be overwritten or deleted. Other artefacts may also suffer degradation.
10. Typically, it is strongly advisable that a system be preserved for inspection as soon as possible, to avoid degradation. If the system logs and journals or other artefacts have been degraded by user activity, or interfered with by editing or deletion, or the system altered, it may not be possible to determine the extent of manipulation. However, other forensically useful artefacts can be expected to survive and remain available for analysis.

Some artefacts expected to persist unless major action taken

11. Several artefacts can be expected to remain on the computer(s) indefinitely unless specifically targeted with data elimination software or techniques.
12. The exception to this would be if a particularly destructive action was conducted, such as reformatting a hard drive and/or reinstalling the operating system, which could be expected to remove all traces of useful data, or if the computing equipment itself was lost or damaged beyond repair.

**SECTION 2: THE 97 DOCUMENTS****Overview of the 97 documents and the BDO Drive**File types

13. The file types of the 97 files are as follows:

COUNT	FILE TYPE	EXTENSIONS	FILES
37	<b>Plain text (Latex Source)</b>	.bib	ID_4702.bib; ID_4648.latex; ID_4687.latex; ID_4645.tex;
		.tex	ID_4653.tex; ID_4654.tex; ID_4655.tex; ID_4656.tex;
		.latex	ID_4657.tex; ID_4658.tex; ID_4659.tex; ID_4698.tex;
		(1x .c++)	ID_4699.tex; ID_4700.tex; ID_4701.tex; ID_4703.tex;
			ID_4704.tex; ID_4706.tex; ID_4710.tex; ID_4714.tex;
			ID_4715.tex; ID_4716.tex; ID_4717.tex; ID_4718.tex;
			ID_4719.tex; ID_4720.tex; ID_4722.tex; ID_4723.tex;
			ID_4724.tex; ID_4725.tex; ID_4735.tex; ID_4736.tex;
			ID_5567.tex; ID_5568.tex; ID_5569.tex; ID_5570.tex;
			ID_4705.C++
10	<b>Plain text (.txt)</b>	.txt	ID_4661.txt; ID_4662.txt; ID_4664.txt; ID_4665.txt; ID_4666.txt; ID_4667.txt; ID_4668.txt; ID_4669.txt; ID_4670.txt; ID_4732.txt
6	<b>Plain text (C++ source)</b>	.c++	ID_4708.c++; ID_4711.c++; ID_4712.c++; ID_4707.C++; ID_4709.C++; ID_4713.C++
1	<b>Plain text (Html source)</b>	.htm	ID_4671.htm
7	<b>Images</b>	.bmp (x6), .png (x1)	ID_4726.bmp; ID_4727.bmp; ID_4728.bmp; ID_4729.bmp; ID_4730.bmp; ID_4731.bmp; ID_4686.png
2	<b>Outlook Journal exports</b>	.msg	ID_4663.msg; ID_4676.msg
8	<b>DragonDictate files (proprietary format)</b>	.dra	ID_4650.dra; ID_4672.dra; ID_4674.dra; ID_4675.dra; ID_4684.dra; ID_4689.dra; ID_4691.dra; ID_4693.dra
15	<b>Microsoft Rich Text format document.</b>	.rtf (1x .doc)	ID_4644.rtf; ID_4646.rtf; ID_4647.rtf; ID_4681.rtf; ID_4685.rtf; ID_4688.rtf; ID_4690.rtf; ID_4692.rtf; ID_4694.rtf; ID_4695.rtf; ID_4696.rtf; ID_4697.rtf; ID_4733.rtf; ID_4734.rtf; ID_4721.doc
11	<b>MS Word DOC documents</b>	.doc	ID_4649.doc; ID_4651.doc; ID_4652.doc; ID_4660.doc; ID_4673.doc; ID_4677.doc; ID_4678.doc; ID_4679.doc; ID_4680.doc; ID_4682.doc; ID_4683.doc

Lack of metadata in many of the 97 documents

14. In my First Report at paragraphs 102 to 105, I explained that different technologies have different approaches to metadata, specifically:

- a. Different file types record and store Internal Metadata in different ways.



- b. Even within the same file format, content can be structured and stored differently.
- c. Some formats contain very little metadata at all such as plain text files, some image documents, and documents scanned from hard copies.
- d. I also explained in my First Report that when items are extracted from MS Outlook or converted to MSG format files, it can cause a loss in metadata (e.g. paragraphs 151 to 159); and that MS Word is capable of using other formats than DOC and DOCX, such as RTF, TXT and HTML (paragraph 128.d.),

15. That is relevant to the 97 New Documents as follows:

- a. 54 of the 97 are plain text files of various kinds, so as mentioned in my First Report, have no Internal Metadata that can be analysed for indications of manipulation.
- b. 7 of the 97 are images (including scanned documents) which (as mentioned in my First Report) have no Internal Metadata (or none that is relevant).
- c. 2 of the files are .msg extracts from Outlook, whose metadata is either inauthentic or not reliable. Specifically, they are listed as having been modified on 23 September 2023, which is after the date I understand the BDO Drive was imaged.
- d. 15 of the files are Rich Text Format files (RTF). RTFs contain very little, and sometimes no relevant Internal Metadata for analysis. In the case of these RTFs, some contain no metadata at all; while others I have been able to establish could not have been created before 27 May 2020.

16. I note that almost all of the filetypes in the 97 New Documents were not present in the original Reliance Documents. The original Reliance Documents did not contain any LaTeX, RTF, C++, HTM, TXT, or DRA files and only a small number of images (including images embedded within PDFs).

Need for review in context

17. In view of the overall lack of Internal Metadata across the set,

- a. it is not possible to get a full perspective on the 97 New Documents without access to the forensic environment from which they were taken, i.e. the forensic disk image of the Samsung drive (which itself contains the BDO Image).
- b. It would be important to take account of the full context of the computing environment from

which the 97 New Documents were taken, including establishing a pattern of how that environment was interacted with, inspection of logs, comparative analysis between other documents in the Image, and considering the extent to which the BDO Image itself exhibits signs of tampering.

- c. Since most of the 97 New Documents themselves do not inherently contain traces of that information, considering those documents in isolation from their context would not be informative and would not allow the documents to be dated to any particular date.

18. However, for reasons explained below, I have established that several of the 97 New Documents from within the BDO Drive exhibit indications of manipulation and tampering.

#### Review of each file type within the drive

19. In the following section I explain the documents I have been able to analyse taking each filetype at a time.

#### **LaTeX documents**

##### LaTeX documents in general

20. LaTeX files are typically stored as plain text and PDFs. My familiarity with LaTeX (or just “Latex”) is less than my familiarity with more common file types of the kinds I have addressed elsewhere in my Reports. However, I am sufficiently familiar with the format to provide the following opinion.

21. Latex is a markup language allowing documents to be typed in plain text with formatting instructions. The plain text files can then be converted into PDFs. An example of a Latex file taken from the 97 New Documents (chosen because it is short) is ID\_004645 the beginning of which presents as follows:

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Document Owner: Ridges Estate / BDO
% Author: Craig Wright
% Copyright: 2005 -
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

\documentclass[12pt]{article}
\usepackage{url}
\usepackage{hyperref}

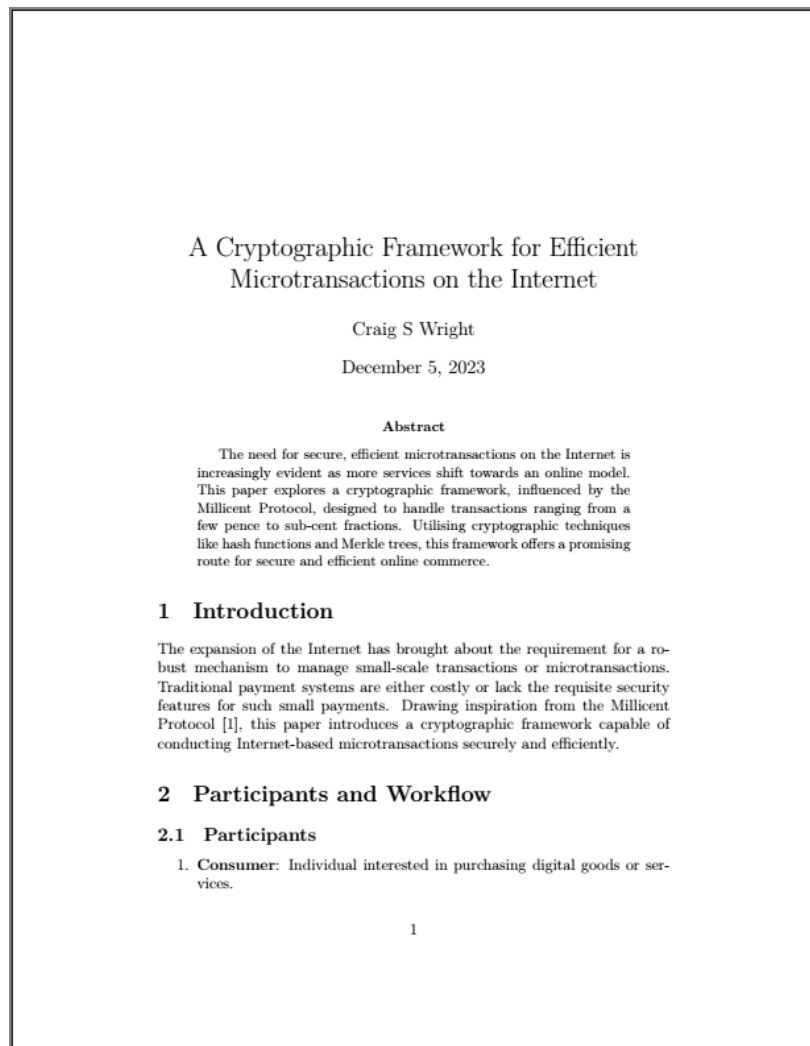
\begin{document}

\title{A Cryptographic Framework for Efficient Microtransactions on the Internet}
\author{Craig S Wright}
\date{\today}
\maketitle

\begin{abstract}
The need for secure, efficient microtransactions on the Internet is increasingly
evident as more services shift towards an online model. This paper explores a
cryptographic framework, influenced by the Millicent Protocol, designed to handle
transactions ranging from a few pence to sub-cent fractions. Utilising cryptographic
techniques like hash functions and Merkle trees, this framework offers a promising
route for secure and efficient online commerce.
\end{abstract}

```

22. When a PDF is built from that source the first page it presents as follows (noting that the date is given by the clock on the computer that produces it due to the “\date{\today}” line shown above, and so displays the date of writing this report):



2. **Intermediary:** Facilitates the transaction between the consumer and service provider, often by supplying digital tokens or "scrip."
3. **Service Provider:** Offers the actual product or service.

## 2.2 Workflow

1. **Initial Connection:** A secure connection is established between the consumer and the intermediary to procure intermediary scrip.
2. **Vendor-Specific Scrip:** If absent, the consumer obtains vendor-specific scrip from the intermediary.
3. **Intermediary-Service Provider Interaction:** The intermediary secures vendor-specific scrip.
4. **Transaction Completion:** Scrip is transferred from the intermediary to the consumer.
5. **Service or Product Exchange:** The consumer uses the scrip for the actual transaction with the service provider.

## 3 Cryptographic Techniques Employed

1. **Hash Functions:** Utilised for data integrity and verification.
2. **Hash Chains:** Employed for added layers of security during a series of transactions.
3. **Merkle Trees:** Implemented to validate the content of data blocks securely and efficiently.

## 4 Practical Applications

Potential areas of application include, but are not limited to:

1. **Network Security:** Used in firewall services resembling Kerberos-like authentication suites.
2. **World Wide Web Services:** Utilised through a pseudo-proxy that manipulates HTTP headers for transactional security.

2

## 5 Performance Indicators

Early tests show that the system is highly efficient, capable of validating approximately 1000 microtransaction requests per second on legacy hardware.

## 6 Conclusion

The cryptographic framework discussed offers a viable option for the secure and efficient handling of online microtransactions. By incorporating cryptographic elements such as hash functions, hash chains, and Merkle trees, it manages to ensure both transactional security and efficiency.

## 7 Future Directions

1. **Service Extension:** As demand for usage-based online services increases, the framework could be adapted for wider application.
2. **Performance Optimisation:** Additional gains in efficiency could be achieved through focused optimisation efforts.

## References

- [1] Millicent Protocol for Microtransactions. *Publication Name*, Year. URL

3

23. The format<sup>1</sup> is a typical presentation of a Latex “article” document:
- a. The source specifies to use the `\documentclass` template called `article`. Latex is instructed to generate a PDF according to that predefined Latex template. Features such as the margin spacing, font, and overall structure is generated according to that template.
  - b. The `\title{}`, `\author{}` and `\date{}` commands specify the information placed and formatted into the title block;
  - c. The plain text `{abstract}` section shown in the code extract above is formatted in a block with an “**Abstract**” heading above it.
  - d. Sections and subsections specified as `\section{Participants and Workflow}` and `\subsection{Participants}` are formatted with default headings and subheadings formatting and numbered.
  - e. The References section is automatically applied in the typical format.
24. Latex is therefore normally written in a plaintext form, and exported to PDF (or other formats) for publishing. However,
- a. No output files have been provided. PDF files for example contain significantly more metadata which might allow for a deeper forensic analysis of the output. However, there are no PDF documents in the 97 New Documents.
  - b. The Latex source files themselves are plain text and carry no internal metadata timestamps.
25. There exist a number of conversion tools which convert documents between formats including conversion into Latex format from other filetypes.

#### Packages used in Latex documents

26. As part of my review I was able to spend a relatively short amount of time checking which packages are used by some of the Latex documents.
27. In the code extract above it can be seen that ID\_004545 uses two external software packages by specifying the packages named “url” and “hyperref”: `“\usepackage{url}”` and `“\usepackage{hyperref}”`. Packages are add-ons to the default Latex functionality which add

---

<sup>1</sup> Bird & Bird has created an exhibit of the same PDF export at **Exhibit PM-R3.1**.

extra functions. While ID\_004545 only uses two packages, some of the other Latex documents use many more.

28. As I did not have much time available, I chose to look at ID\_004687, because it uses a significant number of packages (around 15) with some distinctive names. The beginning of ID\_004687 presents as follows:

```
% Options for packages loaded elsewhere
\PassOptionsToPackage{unicode}{hyperref}
\PassOptionsToPackage{hyphens}{url}
%
\documentclass[
]{article}
\usepackage{amsmath,amssymb}
\usepackage{lmodern}
\usepackage{iftex}
\ifPDFTeX
  \usepackage[T1]{fontenc}
  \usepackage{utf8}{inputenc}
  \usepackage{textcomp} % provide euro and other symbols
\else % if luatex or xetex
  \usepackage{unicode-math}
  \defaultfontfeatures{Scale=MatchLowercase}
  \defaultfontfeatures[\rmfamily]{Ligatures=TeX,Scale=1}
\fi
% Use upquote if available, for straight quotes in verbatim environments
\IfFileExists{upquote.sty}{\usepackage{upquote}}{}
\IfFileExists{microtype.sty}{% use microtype if available
  \usepackage[]{microtype}
  \UseMicrotypeSet[protrusion]{basicmath} % disable protrusion for tt fonts
}{}
\makeatletter
\@ifundefined{KOMAClassName}{% if non-KOMA class
  \IfFileExists{parskip.sty}{%
    \usepackage{parskip}
  }{% else
    \setlength{\parindent}{0pt}
    \setlength{\parskip}{6pt plus 2pt minus 1pt}}
}{% if KOMA class
  \KOMAOptions{parskip=half}}
\makeatother
\usepackage{xcolor}
\setlength{\emergencystretch}{3em} % prevent overfull lines
\providecommand{\tightlist}{%
  \setlength{\itemsep}{0pt}\setlength{\parskip}{0pt}}
\setcounter{secnumdepth}{-1} % remove section numbering
\ifLuaTeX
  \usepackage{selnolig} % disable illegal ligatures
\fi
\IfFileExists{bookmark.sty}{\usepackage{bookmark}}{\usepackage{hyperref}}
\IfFileExists{xurl.sty}{\usepackage{xurl}}{} % add URL line breaks if available
\urlstyle{same} % disable monospaced font for URLs
\hypersetup{
  hidelinks,
  pdfcreator={LaTeX via pandoc}}

\author{}
\date{}
\begin{document}

\textbf{360° Security Summit}

Dr Craig S Wright DTh

15 June 2006.

BDO NSW

\textbf{Abstract:} In an era increasingly dominated by cyber threats and
vulnerabilities, we must reassess our approach to risk and security.
```

Reactive responses to risks can lead to disillusionment and financial wastage. This presentation paper offers insights into implementing adequate risk-based controls within an organisation. Specifically, it discusses the nuances between qualitative and quantitative risk, methods to add value to a risk engagement process, and strategies to look at risk non-emotionally. Additionally, it explores the utility of hazard survival models and hash chains in building a robust risk management system.

RISK: Implementing Effective Risk-Based Controls

Dr. Craig S. Wright, DTh

cwright@bdosyd.com.au

\textbf{Abstract}

In an era increasingly dominated by cyber threats and vulnerabilities, we must reassess our approach to risk and security. Reactive responses to risks can lead to disillusionment and financial wastage. This paper offers insights into implementing adequate risk-based controls within an organisation. Specifically, it discusses the nuances between qualitative and quantitative risk, methods to add value to a risk engagement process, and strategies to look at risk non-emotionally. Additionally, it explores the utility of hazard survival models and hash chains in building a robust risk management system.

29. I investigated the dates of packages referred to here by searching online and by searching records on the website <https://ctan.org/>, which contains an archive of packages and details of when they were released and announced.

**CTAN**  
Comprehensive TeX Archive Network

Location: CTAN Comprehensive TeX Archive Network

## The Comprehensive TeX Archive Network

The Comprehensive TeX Archive Network (CTAN) is the central place for all kinds of material around TeX. CTAN has currently [6521 packages](#). [2957 contributors](#) have contributed to it. Most of the packages are free and can be downloaded and used immediately.

### Announcements on CTAN-announce

You can see what's new and even get informed about new or updated packages on CTAN.

- [2023-12-04 CTAN update: tkz-elements](#)
- [2023-12-04 CTAN update: Scrabble](#)
- [2023-12-04 CTAN update: pwebmac](#)
- [2023-12-04 CTAN update: cweb](#)

[more](#)

### Activity on CTAN

An active TeX community takes care that CTAN is updated and extended regularly. CTAN receives usually more than 100 uploads per month.

### Search on CTAN

The contents of CTAN can be searched with full-text search. This search considers the description, the documentation, and the contributors.

If you want to have finer control on the parameters of the search you can use the [advanced search form](#) instead.

### Did you know?

The topic [Thai Font](#) in the TeX Catalogue has 5 packages for font for typesetting Thai script. [more](#)

### TeX

TeX is a typesetting program designed for high-quality composition of material that contains a lot of mathematical and technical expressions. It has been adopted by many authors and publishers who generate technical books and papers. It was created by Professor [Donald E. Knuth](#) of Stanford University, originally for preparation of his book series "[The Art of Computer Programming](#)". TeX has been made freely available by Knuth.

From these origins a whole eco-system of distributions, macro packages, and supporting programs has arisen. [more](#)

30. I found as follows:

- a. One of the packages, “selnolig”, did not appear to be released in 2007. Specifically,
  - i. the record at <https://ctan.org/pkg/selnolig> (**Exhibit PM-R3.2**) stated that using SelNoLig “requires use of a recent LuaLaTeX format (for example those from TeX Live 2012 or 2013, or MiKTeX 2.9).”
  - ii. CTAN contained a record of its release announcement at <https://ctan.org/ctan-ann/id/mailman.427.1369694287.5851.ctan-ann@dante.de> (**Exhibit PM-R3.3**) which is dated to “May 28, 2013 12:38:04AM CEST” and which contains the same reference to “recent” software from 2012-2013.
  - iii. I also found a post at <https://tex.stackexchange.com/questions/28437/can-one-more-or-less-automatically-suppress-ligatures-for-certain-words> (**Exhibit PM-R3.4**) which is dated to 12 years, 2 months ago (and hovering the mouse pointer over that date gives a timestamp of 2011-09-14 at 16:56:26Z). That contains a long question about using ligatures in LaTeX and states that “**This question led to a new package: selnolig**”:



Home  
Questions  
Tags  
Users  
Companies  
Unanswered  
AMS  
Stack Overflow for

TEX  $2Na + Cl_2 \xrightarrow{\text{oxidation}} 2Na^+ + 2Cl^- \xrightarrow{\text{reduction}}$   $\oint_{\partial S} \mathbf{E} \cdot d\mathbf{l} = -\frac{\partial \Phi_{B,S}}{\partial t}$

## Can one (more or less) automatically suppress ligatures for certain words?

Ask Question

Asked 12 years, 2 months ago Modified 5 years, 3 months ago Viewed 3k times

2011-09-14 16:56:26Z

**51**

**This question led to a new package:**  
`selnolig`

One of the major attractions -- for me at least -- of typesetting my papers in  $(L^a)TeX$  is its automated and fully-transparent use of

- b. Similarly the package “xurl” also appears to date from after the purported date of the BDO image in 2007:
- i. I found a similar post at <https://tex.stackexchange.com/questions/3033/forcing-linebreaks-in-url> (Exhibit PM-R3.5) to the one above, dated to 13 years, 2 month ago (timestamp 2010-09-13 at 03:55:59Z) which contained a similar note that “**This question led to a new package: xurl**”:

Home  
Questions  
Tags  
Users  
Companies  
Unanswered  
AMS  
Stack Overflow for

TEX  $2Na + Cl_2 \xrightarrow{\text{oxidation}} 2Na^+ + 2Cl^- \xrightarrow{\text{reduction}}$   $\oint_{\partial S} \mathbf{E} \cdot d\mathbf{l} = -\frac{\partial \Phi_{B,S}}{\partial t}$

## Forcing linebreaks in `\url`

Ask Question

Asked 13 years, 2 months ago Modified 9 months ago Viewed 342k times

2010-09-13 03:55:59Z

**349**

**This question led to a new package:**  
`xurl`

I wish to typeset some relatively long URLs in a piece of text, and when I use `\url{...}`, the resulting text does not respect the margin boundaries that govern the main text body, instead going all the way to the edge of the paper before wrapping around.

```
\documentclass{article}
\usepackage{hyperref}
```

- ii. The CTAN record for the xurl package is at Exhibit PM-R3.6 and the announcement

record is at **Exhibit PM-R3.7**. The date of the announcement is “December 21, 2017 9:30:47PM CET” with the version number 0.2 2017-12-20:

**New on CTAN: xurl**

Date: December 21, 2017 9:30:47 PM CET

Herbert Voß submitted the

xurl

package.

Version number: 0.02 2017-12-20  
License type: lpl1.3

Conclusions on ID\_004687 and ID\_004648

31. At this point I had checked around half of the packages mentioned in ID\_004687 and stopped checking more, since I had formed the opinion that ID\_004687 is not authentic to its purported date and likely could not have been created before 2017.
32. Searching the 97 New Documents, I found the same packages selnolig and xurl were also referred to in ID\_004648 and formed the view that ID\_004648 is not authentic to its purported date and likely could not have been created before 2017.
33. I have not been able to conduct a further analysis of the other Latex documents in the time available, other than two which I refer to below in the context of another document. However, the method of investigating the software referred to in the Latex documents depends on the specifics of each document and does not permit a wider contextual review. As I mentioned, I chose the file ID\_004687 because it appeared to have had many packages specified.

Further note on ID\_004687 and ID\_004648

34. At this point after the section of my report was drafted, Bird & Bird provided me with a copy of the First Witness Statement of Dr Mico Loretan and asked me to review it, and to consider whether it affected my opinion.
35. I was not aware of this before, but it did not affect my opinion. Mico Loretan is the name of the person who asked the ligatures question at Stack Exchange and made the announcement of selnolig both referred to above. The witness statement seems to confirm my own opinion which I had established independently.

**Plain text documents**

36. The plain text documents are categorised according to their content in the table above.
37. The documents that are pure plain .txt files have little or no information for forensic analysis. Similarly, the C++ source code files are plain text files with computer code written in them. Their content is outside my expertise, and I cannot comment on them.
38. In my opinion the authenticity of these documents cannot be established outside their forensic context.

**HTM document**

39. ID\_004671 is the only document which is an html source document (having the extension .htm). It specifies the HTML source for a web page. The beginning of the source presents as follows:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from
url=(0072)http://www.kentlaw.edu/classes/rwarner/D&A/definition_elect_contract
.htm -->
<HTML><HEAD><TITLE>ELECTRONIC CONTRACTING</TITLE>
<META http-equiv=Content-Type content="text/html; charset=windows-1252">
<META content="MSHTML 6.00.2900.2963" name=GENERATOR>
<META content=FrontPage.Editor.Document name=ProgId>
<META content="ricepapr 011, default" name="Microsoft Theme"></HEAD>
<BODY text=#000000 vLink=#333366 aLink=#990000 link=#666633 bgColor=#ffffff
background="ELECTRONIC CONTRACTING_files/ricebk.jpg"><!--mstheme--><FONT
face="Times New Roman, Times"><!--msthemeseparator-->
<P align=center><IMG height=10 src="ELECTRONIC CONTRACTING_files/aricerul.gif"
width=600></P>
<P align=center><FONT face=Eurostile size=6>DEFINITION OF AN ELECTRONIC
CONTRACT</FONT></P><!--msthemeseparator-->
<P align=center><IMG height=10 src="ELECTRONIC CONTRACTING_files/aricerul.gif"
width=600></P>
<P class=MsoNormal
style="MARGIN-TOP: 30px; MARGIN-BOTTOM: 30px; WORD-SPACING: 0px; LINE-HEIGHT:
150%; mso-margin-bottom-alt: auto"
align=justify><SPAN lang=EN-US style="mso-ansi-language: EN-US"><FONT
face=Tahoma size=2>Ukrainian legislator defines a contract as an "agreement by
and between two or more persons with respect to establishing, modifying or
terminating the civil rights and obligations."<A title=""
style="mso-footnote-id: ftn1"
href="http://www.kentlaw.edu/classes/rwarner/D&A/definition_elect_contract
.htm#_ftn1"
```

40. Although it is saved in a human-readable plaintext format the document can be viewed in a browser to interpret that code, and the beginning of the file presents as follows:

## DEFINITION OF AN ELECTRONIC CONTRACT

Ukrainian legislator defines a contract as an 'agreement by and between two or more persons with respect to establishing, modifying or terminating the civil rights and obligations.'<sup>[1]</sup> But it is only one of facets of phenomenon of a contract. As far back as in ancient Rome, a contract has been considered in threefold manner:<sup>[2]</sup> as a 1) 'ground for arising of legal obligations, 2) these obligations themselves and, at last, 3) document, where all parties' obligations are contained.'<sup>[3]</sup> Because of the topic of this research only contract in the meaning of a document will be considered in this paragraph.

A contract as a document was originally invented as an evidential tool, which allow locking parties' contract obligations in and proving their existence and content in the future. Historically, the very materials used in creation of a document were paper and ink. That is why a piece of paper with written or typed text on it is the first association with the word 'document.' Such perception of a document significantly influenced contract law and stipulated strong believe that a contract, concluding 'in writing' must be only in paper form. This was true for centuries, before new mediums of information were invented. Telegraph, telex, fax, and invention of second part of 20 century – EDI and Internet electronic messaging shook the 'paper documents' dogma and demanded to 'create novel law to fit the situation.'<sup>[4]</sup>

It is obvious that 'EDI and the Internet do not alter the substance of business contracts, they alters the process of agreement'<sup>[5]</sup> by creating the possibility

41. The code above includes a comment that it is "saved from url"  
[http://www.kentlaw.edu/classes/rwarner/D&A/definition\\_elect\\_contract.htm](http://www.kentlaw.edu/classes/rwarner/D&A/definition_elect_contract.htm) . That page is not currently live and has not been archived by the WayBack Machine. I note that the name of the link (definition\_elect\_contract) matches the title of the page (DEFINITION OF AN ELECTRONIC CONTRACT).
42. In the content of ID\_004671 it contains references to a number of cited sources by URL which state that they were "accessed Apr. 9, 2002".
43. I have no reason to doubt that the content of ID\_004671 is authentic to its stated date of Apr. 9 2002 or that it was saved from the [www.kentlaw.edu/classes/rwarner](http://www.kentlaw.edu/classes/rwarner) website at the URL stated above. However, the file itself does not contain any Internal Metadata that would allow its authenticity to be established beyond checking the validity of the URLs and sources referred to.

### **BMP Images**

44. There are 6 BMP images in the 97 New Documents which present as scans or conversions of individual pages of handwriting.
45. As I mentioned in my First Report and referred to above, image files and scans often do not contain any suitable metadata for analysis. The BMP (bitmap) format is an example of a file type which contains little or no Internal Metadata. As with the plain text files, it is not possible to conduct a proper examination without the forensic context.

### **PNG Image (and related Latex documents)**

46. There is one PNG image, ID\_004686, in the 97 New Documents which presents as follows (with a border added within this Report):



47. As with the BMP files mentioned above, there is no relevant Internal Metadata for analysis. However, although the content of the document (a BDO logo) matches the context of the BDO image (which is a drive image described as originating from BDO), the metadata indicates that it dates from later than 2007:

	ID_004686
File Created:	19/09/2017 11:17:16
File Last accessed:	13/08/2007 02:02:36
File Last modified:	13/08/2007 02:02:36
File name:	BDO.png

Metadata inconsistencies

48. The metadata above indicates that the file was created in 2017, which is over a decade after the date recorded for Last Accessed and Last Modified. That is anomalous:

- a. It is consistent with the use of clock manipulation (or, as I explain below, metadata editing) while creating and interacting with this file, and
- b. is also consistent with the use of clock manipulation while interacting with the BDO Image itself, having the image mounted (opened on a computer as if it was a real drive) and being accessed and modified at a time likely to be after 2017, but with the computer clock set back to 2007.

Relation of ID\_004686.png to ID\_004736.tex and ID\_004735.tex

49. I also observed that the Latex document ID\_004736.tex has similar timestamps. It refers to a file called "BDO.png" as follows:

```
% Title Section
\title{\huge\bfseries Ensuring Secure Data Transfer and Data
```

```

Sharing}
\author{\Large\itshape Dr Craig S Wright GSE-c \\ \large From:
BDO Kendalls (NSW)}
\date{\large Date: 01/11/2007}

\begin{document}

\maketitle

\begin{figure}[h]
\centering
\includegraphics[width=0.6\textwidth]{BDO.png}
\caption{BDO - Data Sharing and Analysis}
\end{figure}

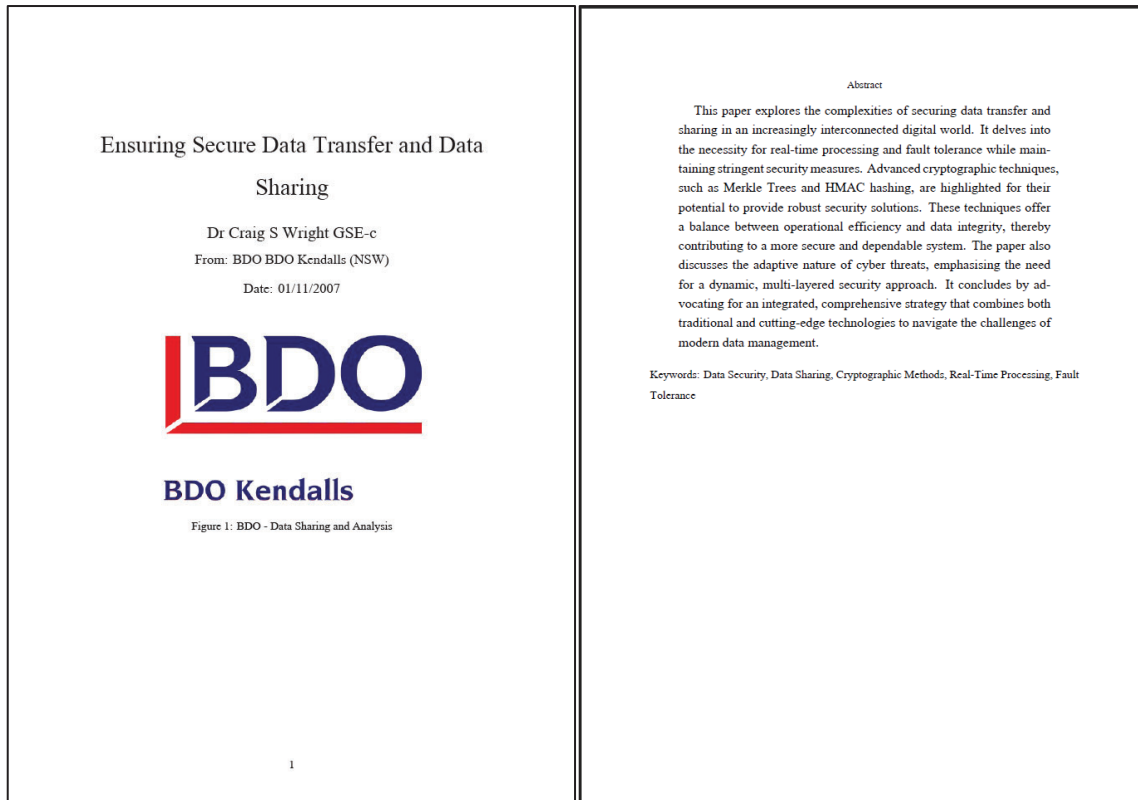
\newpage

```

50. That Latex document also refers to another file, “*image.tex*”, later in its code. The metadata load file indicates that “*image.tex*” is ID\_004735.tex. Adding the load file metadata for ID\_004736.tex and ID\_004735.tex alongside ID\_004686:

	ID_004686	ID_004736	ID_004735
File Created:	19/09/17 11:17:16	19/09/17 11:17:16	19/09/17 11:17:16
File Last accessed:	13/08/07 02:02:36	13/08/08 02:02:36	13/08/08 02:02:36
File Last modified:	13/08/07 02:02:36	13/08/08 02:02:36	13/08/08 02:02:36
File name:	BDO.png	ESDT.tex	image.text

51. Bird & Bird has also output a PDF of ID\_004736 (ESDT.tex) which is at **Exhibit PM-R3.8**. The first two pages of that present as follows:



52. Although I understood from the list of document sources that ID\_004736 and ID\_004735 were within the BDO Image, Bird & Bird has informed me that Shoosmiths have stated that ID\_004736 and ID\_004735 were not within the BDO Image but were outside it on the Samsung Drive. I have not been provided with access enabling me to verify this.

53. I note as follows:

- a. All three files have an identical "creation" date. This is anomalous because one of them, the image ID\_004686, appears to be from within the BDO Image while the others are outside it. Since there has been a correction about this in respect of ID\_004736 and ID\_004735, I have proceeded on the assumption that the same mistake has been made for ID\_004686 and assumed that this was not within the BDO Image. However, if ID\_004686 actually was within the BDO Image (as listed), that would be a serious indication of tampering with the BDO Image itself.
- b. The Last Accessed and Last Modified day, month, hour, minute, and second for all three files is identical. However, the *Year* is different, listed as 2007 for ID\_004686 but 2008 for the other files.
- c. I do not consider that three connected files could naturally have been accessed at the same time (down to the second), precisely one year apart, when they are interrelated.

Direct metadata editing software

54. In my experience, anomalous timestamps of this kind are more typical of using a dedicated software tool to edit metadata timestamps.
55. In my First Report at paragraph 222, I gave an example of how metadata properties can be edited directly within a Windows operating system (and above that I gave examples of how clock manipulation can be used to generate manipulated timestamps). That is an example of a software tool that allows metadata editing directly. However, there are other such tools which allow more efficient direct editing of metadata including timestamps.
56. One such tool that I am familiar with is known as “AttributeMagic Free” and is available for free at <https://www.elwinsoft.com/attributemagic-free.html> (Exhibit PM-R3.9). That web page allows the file to be downloaded and provides the following screenshot showing how it looks in use:



57. As indicated in the screenshot and Exhibit PM-R3.9, the tool allows timestamps to be freely edited without needing to alter the local system clock.
58. There are also other versions including AttributeMagic - “Standard” and “Pro”. As can be seen at the bottom of the screenshot above, the “Pro” edition allows for timestamps to be changed “en



masse”. The “Standard” version is available at <https://www.elwinsoft.com/attributemagic-standard.html> (Exhibit PM-R3.10). There is further information in the Screenshots page for “Standard” at [https://www.elwinsoft.com/am\\_std/shots.html](https://www.elwinsoft.com/am_std/shots.html) (Exhibit PM-R3.11) and “Pro” at <https://www.elwinsoft.com/amp/shots.html> (Exhibit PM-R3.12).

59. As can be seen from those screenshots, it also allows for processing of files and folders in a batch. The text of the “Standard” web page is also helpful to understand the functionality, and advertises its features as follows:

Why should I change the file attributes and date stamp?

- Mask the time you really created your files
- Hide when you last accessed files
- Fix date/time stamp for files downloaded from Internet
- Version control issues. Stamp file/folder dates and indicate the version number in the file date/time stamp
- CD-ROM operations. Drop "Read Only" flag for files copied from CD with few mouse clicks!
- When creating a CD layout stamp a CD-ROM image with the same time and date before recording it
- Set the "archived" attribute of the files that were backed up

Features of AttributeMagic (Standard edition)

Change file date and time (Created, Modified, Accessed)

- explicitly set new date-time;
- relatively change date-time: increment/decrement, AM to PM and PM to AM;
- date-time masking;
- copy one date-time stamp to another (ex: **Created Date=Modified Date**);
- sequentially modify date-time.

Change attributes of files and folders

Rename files and folders

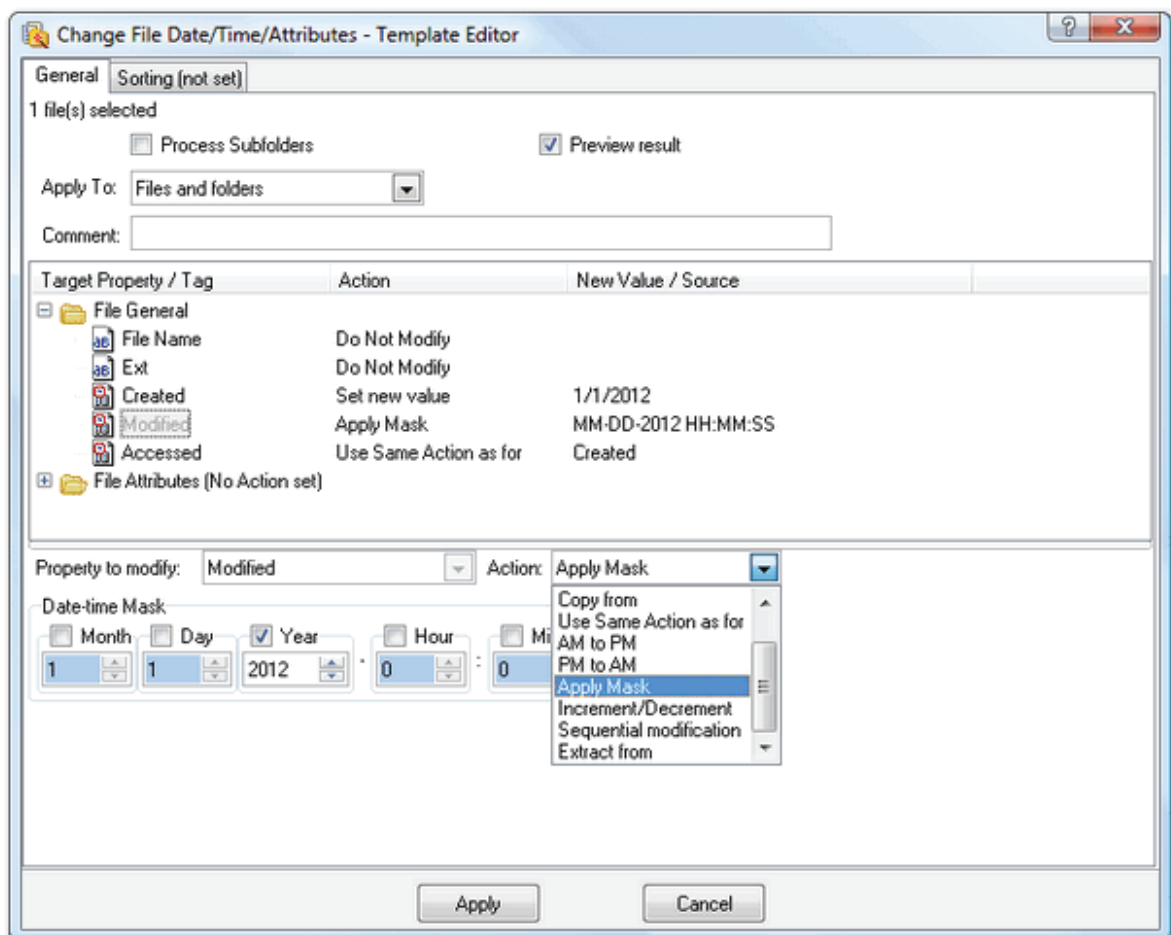
- rename file extension
- add date, time, size, prefix, suffix to the file name
- replace characters or string
- change case of entire file name or only change specified range
- process one file, folder or a group of files, folders, subfolders
- recursive operations: process whole directory tree (or certain branch)
- print folder contents
- powerful custom filters to selectively process certain files or folders
- custom templates
- folder size calculation
- preview result mode, detailed error reporting

60. In my opinion, the presence of the abovementioned timestamps is anomalous and highly unlikely to have occurred naturally. I consider it more plausible that the timestamps were manually reverted

back by exactly one year with the use of a tool such as AttributeMagic to edit timestamps directly, because,

- a. Such tools often allow direct subtraction or addition to a timestamp, or editing only the ‘year’ portion while leaving others unchanged; and
- b. When using clock manipulation by changing the settings on the operating system, the clock is not ‘frozen’ but continues to tick forward from the time that is set. Therefore, it would not explain the second-level accuracy of these timestamps 1 year apart.




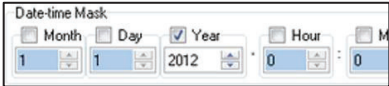
61. To demonstrate this it is possible to see the functionality illustrated in screenshots of the “Pro” version of AttributeMagic as shown below:



62. It can be seen that the functionality of this tool allows files within an entire folder to be selected and:

- a. Changes to metadata can be applied to files and folders:



- b. Subdirectories within a directory tree can be included: 
- c. Timestamps such as Last Modified can be altered: 
- d. An action can be applied as a mask, making a specific change across the whole folder or directory tree: 
- e. The mask applied can be selected so that the day/month and hour/minute/second are not changed, but only the year is: 

### Application to current findings

63. This is relevant to the findings above in respect of ID\_004686, ID\_004736 and ID\_004735, because the presence of second-precise timestamps which differ by year and are otherwise identical is a possible indication of the use of such a tool. Specifically, the findings are consistent with a process whereby:
- ESDT.tex and Image.tex and BDO.png were created (possibly by being copied) when the computer clock was set to 19 September 2017 11:17:16.
  - They were then backdated to 2008, likely by the use of clock manipulation techniques, and were assigned a timestamp of 13 August 2008 02:02:36.
  - A Date-Time metadata editing mask was then applied to edit the year (but not the other timestamps) of a directory of folders and files, changing the directory to appear as if all files within it were Last Modified and Accessed in 2007.
  - That directory *did* include BDO.png (ID\_004686) but *did not* include the other two files ESDT.tex and Image.tex (ID\_004736 and ID\_004735).
  - This would have led to the mask being applied to BDO.png (which was within the BDO Image, and so had its year changed by further backdating to 2007), but not to the other two files (which were outside the BDO Image and therefore in a different directory).
64. While I cannot be sure whether this was done, I would expect that such a process would result in similar anomalies to those which I have observed and explained above. There also exist other software utilities with similar functionality, and AttributeMagic is one example of a tool which I have seen used on previous occasions.

65. It may be possible to be more precise about whether such a tool was used if I was given access to the forensic images of the Samsung Drive, and the computing equipment used to interact with it, to inspect logs and journals such as the Event Log on the computer used to access the drive.

Note on inadequate previous timestamps

66. I note that this has been possible to establish as an avenue for investigation only because the metadata of the present files has been provided with second-level precision. The metadata provided in relation to earlier disclosure was rounded to the nearest minute, masking the more precise information. It is therefore possible that similar indications exist in relation to other documents in disclosure. However, the provision of less precise metadata would have masked that, if present.

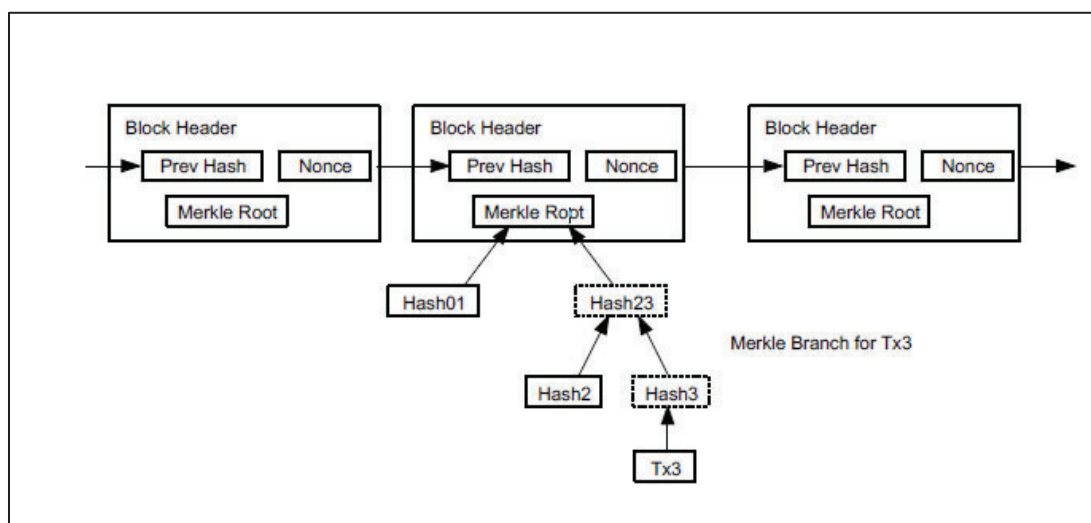
67. While on the topic of the Metadata Load Files provided, while some of the data has been provided with this useful information, I note that many of the entries do not provide any timestamps for the files that they relate to.

Conclusion on ID\_004735, ID\_004736 and ID\_004686

68. Taking the above into account, I do not consider that ID\_004735, ID\_004736 or ID\_004686 are authentic to their purported 2007 dates. The timestamps provided are more consistent with later editing using a dedicated metadata editing tool, in 2017 or afterwards.

ID\_004735 - image

69. I note that there is a flowchart within the PDF Exhibit PM-R3.8 on page 21 which appears as follows, similar to a diagram from the Bitcoin White Paper:



70. That diagram is created when converting ID\_004736 (“ESDT.tex”), which embeds the code from

ID\_004735 (“image .tex”). That file appears to contain code for drawing lines and adding text.

71. The file is 786 lines long. The beginning of the file is as follows:

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Document Owner: Ridges Estate / BDO
% Author: Craig Wright
% Copyright: 2007 -
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% experimenting with relative offsets in the image.
% need to learn how to use the graphics package without reliance on OpenOffice

\definecolor{color_black}{rgb}{0,0,0}
\definecolor{color_white}{rgb}{1,1,1}
\definecolor{color_gray}{rgb}{0.298039,0.298039,0.298039}

\begin{tikzpicture}[overlay]\path(0pt,0pt);\end{tikzpicture}

```

72. An extract of the code relating to image drawing is as follows:

```

\begin{tikzpicture}[overlay]
\path(0pt,0pt);
\begin{scope}
\clip
(103.5pt, -334pt) -- (478.9pt, -334pt)
-- (478.9pt, -334pt)
-- (478.9pt, -174.7pt)
-- (478.9pt, -174.7pt)
-- (103.5pt, -174.7pt) -- cycle
;
\filldraw[color_white][even odd rule]
(251.3pt, -271.3pt) -- (234.2pt, -271.3pt)
-- (234.2pt, -271.3pt)
-- (234.2pt, -259.9pt)
-- (234.2pt, -259.9pt)
-- (268.3pt, -259.9pt)
-- (268.3pt, -259.9pt)
-- (268.3pt, -271.3pt)
-- (268.3pt, -271.3pt)
-- (251.3pt, -271.3pt) -- cycle
;
\draw[color_black,line width=1pt,line join=round]
(251.3pt, -271.3pt) -- (234.2pt, -271.3pt)
-- (234.2pt, -271.3pt)
-- (234.2pt, -259.9pt)
-- (234.2pt, -259.9pt)
-- (268.3pt, -259.9pt)
-- (268.3pt, -259.9pt)
-- (268.3pt, -271.3pt)
-- (268.3pt, -271.3pt)
-- (251.3pt, -271.3pt) -- cycle
;
\end{scope}

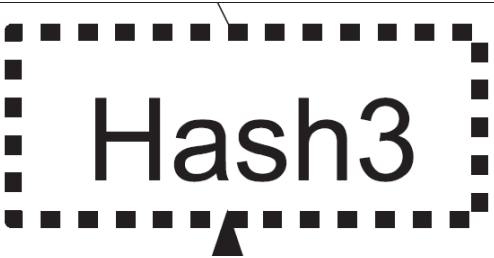
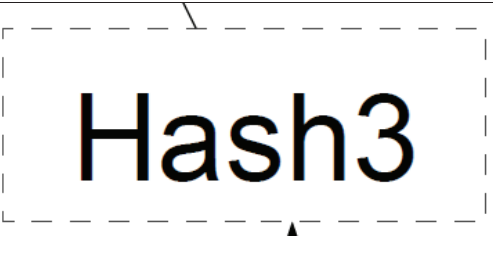
```





```

\end{tikzpicture}
\begin{picture}(-5,0)(2.5,0)
\put(239.1,-
268.6){\arialmt\fontsize{7}{1}\selectfont\color{color_black}Hash01}
\end{picture}
\begin{tikzpicture}[overlay]
\path(0pt,0pt);
\begin{scope}
\clip
(103.5pt,-334pt) -- (478.9pt,-334pt)
-- (478.9pt,-334pt)
-- (478.9pt,-174.7pt)
-- (478.9pt,-174.7pt)
-- (103.5pt,-174.7pt) -- cycle
;
\filldraw[color_white][even odd rule]
(299.6pt,-305.4pt) -- (285.4pt,-305.4pt)
-- (285.4pt,-305.4pt)
-- (285.4pt,-294pt)
-- (285.4pt,-294pt)
-- (313.8pt,-294pt)
-- (313.8pt,-294pt)
-- (313.8pt,-305.4pt)
-- (313.8pt,-305.4pt)
-- (299.6pt,-305.4pt) -- cycle
;
\draw[color_black,line width=1pt,line join=round]
(299.6pt,-305.4pt) -- (285.4pt,-305.4pt)
-- (285.4pt,-305.4pt)
-- (285.4pt,-294pt)
-- (285.4pt,-294pt)
-- (313.8pt,-294pt)
-- (313.8pt,-294pt)
-- (313.8pt,-305.4pt)
-- (313.8pt,-305.4pt)
-- (299.6pt,-305.4pt) -- cycle
;
\end{scope}
\end{tikzpicture}

```

73. I observe that the resulting image, though superficially similar to the figure on page 5 of the Bitcoin White Paper, is significantly different, including the alignment of the boxes to each other, as well as the thickness of the lines, style of dashed lines, and whether or not the arrows align with the boxes. As shown below, the lines in Exhibit PM-R3.8 (ID\_004735 image) are overall thicker, and the arrows only align approximately to the borders they are pointing to:

ID_004735 (Exhibit PM-R3.8):	Bitcoin White Paper:
	

ID_004735 (Exhibit PM-R3.8):	Bitcoin White Paper:
	
	

74. While it is possible that the line thickness could vary with the tools used to create the PDF, the difference shown is very significant and that explanation is unlikely to account for such a big difference. I note that the line thickness and style of dashed line seen in the Bitcoin White Paper are consistent with the default options in OpenOffice 2.4. The way that the dashed line wraps around the corner of the box in an L shape is also the default option in Openoffice 2.4, as seen here:



75. I observe that the code in the (786-line long) ID\_004735 file is long and complex, and specifies very detailed lengths to tenths of a point size (such as “478.9pt”). This appears to be a cumbersome way of creating a graphic compared to using the default settings in OpenOffice which allows graphics to be drawn. I observe that there do exist online conversion tools which offer conversion between PDF and Latex “tikzpicture” format including “Aspose” at <https://products.aspose.app/tex/conversion/pdf-to-latex>, however, I have not used them and cannot comment other to say that it is possible to create such a document automatically from a PDF.

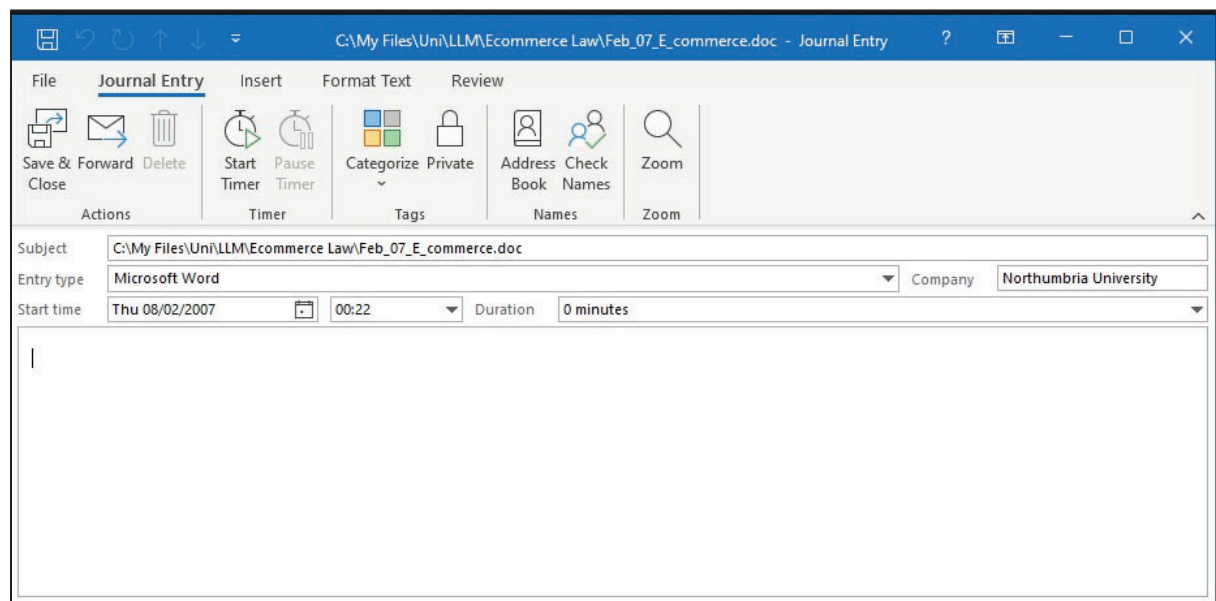
76. In view of the date listed for creation of ID\_004735 (discussed above), the anomalies with its metadata and apparent indications of using a direct metadata editing tool on those files, it is my opinion that:

- a. The diagram in the Bitcoin White Paper did not originate from ID\_004735, and is not similar in several details. It is however possible that the diagram in ID\_004735 originated from a conversion of the Bitcoin White Paper.

- b. The image in ID\_004735 in fact post-dates the Bitcoin White Paper, rather than the other way around.

### Outlook exports

77. Two files, ID\_4663.msg; ID\_4676.msg, are “msg” files exported from Outlook. These are similar to emails but are not emails. They are exports from Microsoft Outlook’s “journal” function. Viewed within MS Outlook, they present as follows, and as shown Outlook presents a menu bar titled “Journal Entry” specific to this type of record:



78. These two files both contain metadata entries indicating that they were originally created in February 2007:
- Both contain references to external files: Feb\_07\_E\_commerce.doc and Assign 1.doc. However, the files are not attached, and merely record the filenames of files they refer to. It is not therefore possible to inspect the files in context, and it is not possible to establish whether the files they refer to have or have not been changed since these journal records were created.
  - Both contain metadata entries indicating that they were created as standalone files on 26 September 2023. This probably indicates that they were exported from an Outlook PST or OST archive after the Samsung drive was imaged, in the course of the disclosure process.
79. In the circumstances these did not have any relevant data allowing analysis of the files to which they refer, or allowing analysis of whether the files referred to may or may not have changed since the Journal entries were created.



**DRA files**

80. Of the remaining files, 8 have a “.dra” extension. I am not familiar with this file format. As I understand it based on research and technical documentation online, these are associated with the program “Nuance Dragon Dictate”, which is a speech-to-text dictation software.

81. I note that the presence of Dragon Dictate files is consistent with my analysis of the wider disclosure dataset. Specifically, I have observed the presence of metadata tags within MS Word .DOC files apparently indicating that they were interacted with by Dragon Dictate, in the form of tags named “dgnword” as shown in the example below. Within DOC files<sup>2</sup> I have found these tags within ID\_000525, ID\_00550, and their duplicates (which were attached to the “CD Files” email ID\_003927). The example given below is taken from ID\_00550:

```
<w:docVar w:name="dgnword-docGUID" w:val="{608F8654-B883-4C34-9FD9-362F384B2564}"/>
```

82. DRA files are a proprietary format requiring specific software to read. Since they are not standardised files, and I do not have the necessary software (or the necessary version of the right software), I am not able to investigate them in the time available, or without access to the software used to create them.

**RTF files***Overview of RTF files*

83. RTF files are a Microsoft WYSIWYG file format which can be created and edited in a similar way to MS Word .DOC or DOCX files. However, they are a much simpler format, which allows for more basic formatting compared to DOC and DOCX files.

84. RTF files can also be viewed in plain text, and have a relatively simple formatting syntax somewhat like Latex. The following shows the beginning of ID\_004681.rtf when viewed in plain text:

```
{\rtf1\ansi\ansicpg1252\deff0\nouicompat\deflang2057{\fonttbl{\f0\fnil\fcharse
t0 Times New Roman;}{\f1\froman\fprq2\fcharset0 Times New
Roman;}{\f2\fnil\fcharset0 Calibri;}}
{\colortbl ;\red0\green0\blue0;}
{\stylesheet{ Normal;}{\s1 heading 1;}{\s2 heading 2;}}
{*generator Riched20 10.0.19041}\viewkind4\uc1
\pard\cf1\f0\fs24\lang9\par

\pard\s200\s1276\slmult1\cf0 \b\fs87 360\'b0 Security Summit\fs28\par
```

<sup>2</sup> .DOCX files being more difficult to search, I have not checked those in the time available to prepare this report.

\pard\sa200\sl276\slmult1\qc\b0\fs24 Dr Craig S Wright DTh\par  
15 June 2006.\par

\pard\sa200\sl276\slmult1\tab\tab\tab\tab\tab BDO NSW\par  
\par

\pard\widctlpar\sa160\sl480\slmult1\qj\b\f1\lang3081 Abstract: \b0 In an era increasingly dominated by cyber threats and vulnerabilities, we must reassess our approach to risk and security. Reactive responses to risks can lead to disillusionment and financial wastage. This presentation paper offers insights into implementing adequate risk-based controls within an organisation. Specifically, it discusses the nuances between qualitative and quantitative risk, methods to add value to a risk engagement process, and strategies to look at risk non-emotionally. Additionally, it explores the utility of hazard survival models and hash chains in building a robust risk management system.\par  
\par

\pard\widctlpar\sa160\sl480\slmult1\qc RISK: Implementing Effective Risk-Based Controls\par  
Dr. Craig S. Wright, DTh\par  
cwright@bdosyd.com.au\par

\pard\widctlpar\sa160\sl480\slmult1\qj\par  
\b Abstract\b0\par  
In an era increasingly dominated by cyber threats and vulnerabilities, we must reassess our approach to risk and security. Reactive responses to risks can lead to disillusionment and financial wastage. This paper offers insights into implementing adequate risk-based controls within an organisation. Specifically, it discusses the nuances between qualitative and quantitative risk, methods to add value to a risk engagement process, and strategies to look at risk non-emotionally. Additionally, it explores the utility of hazard survival models and hash chains in building a robust risk management system.\par  
\par

\pard\keep\keepn\widctlpar\sl\sb240\sl480\slmult1\qj\fs28 Introduction\par

85. Viewed within an editor, the beginning of the same file presents as follows, corresponding to the text above (I note that the presence of two “Abstract” sections is as seen in the original document):

# 360° Security Summit

Dr Craig S Wright DTh  
15 June 2006.  
BDO NSW

**Abstract:** In an era increasingly dominated by cyber threats and vulnerabilities, we must reassess our approach to risk and security. Reactive responses to risks can lead to disillusionment and financial wastage. This presentation paper offers insights into implementing adequate risk-based controls within an organisation. Specifically, it discusses the nuances between qualitative and quantitative risk, methods to add value to a risk engagement process, and strategies to look at risk non-emotionally. Additionally, it explores the utility of hazard survival models and hash chains in building a robust risk management system.

**RISK: Implementing Effective Risk-Based Controls**

Dr. Craig S. Wright, DTh  
cwright@bdosyd.com.au

**Abstract**

In an era increasingly dominated by cyber threats and vulnerabilities, we must reassess our approach to risk and security. Reactive responses to risks can lead to disillusionment and financial wastage. This paper offers insights into implementing adequate risk-based controls

### Very little useful metadata in RTF files

86. The simple syntax and lightweight format mean that RTF files contain very little Internal Metadata, similarly to the Latex and other files. However, some files do contain some optional metadata which can indicate which software was used to create them. Specifically, the files can contain a “generator” tag indicating the software that was used to generate them. The generator tag cannot help to establish the exact date of a file, but can provide useful information.

87. Of the 15 RTF files in the 97 New Documents, the generator tags and metadata dates from the Load File are as follows:

	GENERATOR TAG	DateTime Created	DateTime Last Modified	DateTime Last Accessed
ID 004644.rtf	Msftedit 5.41.15.1507	10/09/05 07:23	10/09/05 06:06	15/10/07 02:59:25
ID 004646.rtf	Msftedit 5.41.15.1507	24/09/05 06:54	25/09/05 10:58	15/10/07 02:59:25
ID 004647.rtf	Msftedit 5.41.15.1507	30/09/05 09:04	25/11/05 07:03	15/10/07 02:59:25
ID 004681.rtf	Riched20 10.0.19041	18/09/06 07:42	10/05/07 06:58	15/10/07 02:59:25
ID 004685.rtf	n/a	31/10/07 03:04	05/07/07 06:14	31/10/07 03:07:02
ID 004688.rtf	n/a	08/09/07 12:02	06/10/07 08:23	31/10/07 03:04:38
ID 004690.rtf	n/a	08/09/07 12:04	08/10/07 05:49	31/10/07 03:04:38

ID 004692.rtf	n/a	08/09/07 12:05	08/10/07 05:52	31/10/07 03:04:38
ID 004694.rtf	Riched20 10.0.19041	01/09/07 05:15	15/10/07 02:57	15/10/07 02:59:25
ID 004695.rtf	Riched20 10.0.19041	01/09/07 08:16	15/10/07 02:59	15/10/07 02:59:25
ID 004696.rtf	Riched20 10.0.19041	31/10/07 03:04	31/10/07 03:08	31/10/07 03:14:25
ID 004697.rtf	Riched20 10.0.19041	08/09/07 12:08	31/10/07 03:13	31/10/07 03:13:51
ID 004721.doc	Riched20 10.0.19041	10/05/06 07:44	31/10/07 07:47	31/10/07 07:47:29
ID 004733.rtf	Riched20 10.0.19041	01/05/07 11:00	31/10/07 04:53	15/10/07 02:59:25
ID 004734.rtf	Riched20 10.0.19041	15/06/06 05:45	31/10/07 04:56	15/10/07 02:59:25

88. Of these,

- a. Three were generated with “Msftedit 5.41.15.1507”. This software corresponds to the use of a default Microsoft editor, such as WordPad, and pre-dates the timestamps seen here.
- b. Four do not have any generator tag, and are very simple files akin to plain text files. As an example, the entire content of ID\_004690 is shown below.

```
{\rtf1\ansi\ansicpg1252\deff0\deflang3081{\fonttbl{\f0\fnil\charset0
Arial;}}
\viewkind4\uc1\pard\fs20 Timestamp server\par
\par
I need to discuss the system with Alan again\par
\par
However, for the point of the current medication I will continue\par
\par
The solution proposed requires the implementation of the timestamp system.
This timestamp server extends the hashing and logging system previously
proposed taking a block of items to be timestamp and widely publishing a
hash of each block. This block is a binary or Merkle tree of a series of
other hashes apart. This data can be published in the same way as the
newspaper USENET post used in the reference example to be included.\par
\par
The timestamp proves that each item of data existed at the time that it
was posted or pash would not be able to be included in the block. Each
timestamp includes the previous timestamp on its cash forming a chain of
information where each additional timestamp reinforces the once before at
making it more and more secure in\par
}
```

- c. The remaining eight are generated with the editor Riched20 10.0.19041.

#### Dating Riched20 10.0.19041

89. This correspond to the use of Microsoft Rich Text Editor 20, a dll file which is provided with Windows operating systems. The Riched20 DLL updates with successive versions of Windows and the version number, “10.0.19041” indicates the version of the DLL in use. Version 10.0.19041 of Riched20 corresponds to version 10.0.19041 of the Windows operating system that it formed part of, i.e. it is a version of Windows 10.

90. Specifically, Windows 10 version 10.0.19041 was the May 2020 update of the Windows 10

operating system. It had an internal versioning number “2004” (which is not a date) and an internal codename “20H1” as is recorded in,

- a. The Microsoft release announcement <https://learn.microsoft.com/en-us/windows/uwp/whats-new/windows-10-build-19041> (**Exhibit PM-R3.13**)
- b. The Microsoft Windows 10 Release history list at <https://learn.microsoft.com/en-us/windows/release-health/release-information> (which is a very long list not exhibited, but which lists the first available date of version 19041 as May 2020), and is also corroborated by various third party online resources<sup>3</sup>, and
- c. The Microsoft end of support announcement relating of that specific version of Windows (version 2004) is at <https://learn.microsoft.com/en-us/lifecycle/announcements/windows-10-version-2004-end-of-servicing> (**Exhibit PM-R3.14**)

91. It is therefore my opinion that those eight RTF files could not have been created before **May 2020** and therefore that,

- a. They are not authentic to their purported timestamps (which range between May 2006 and October 2007),
- b. That their metadata characteristics are consistent with the use of clock manipulation or, based on the findings above in respect of other metadata editing, may also be consistent with the use of direct timestamp metadata editing tools, and
- c. Since they were obtained from within the BDO Image, are indicative of the BDO Image itself being accessed and manipulated at a time between May 2020 and its imaging on 20 September 2023, to insert data which was not original to October 2007, but was backdated to appear as if it was.

### **DOC files**

92. Of the 11 MS Word documents in the drive,

- a. ID\_004649 was created with MS Word version 11.6568 with the author “Craig S Wright”, and with Internal Metadata timestamps of 29-30 July 2006.
- b. ID\_004682 is the only Lynn Wright document, and like other “Lynn Wright” documents it has

---

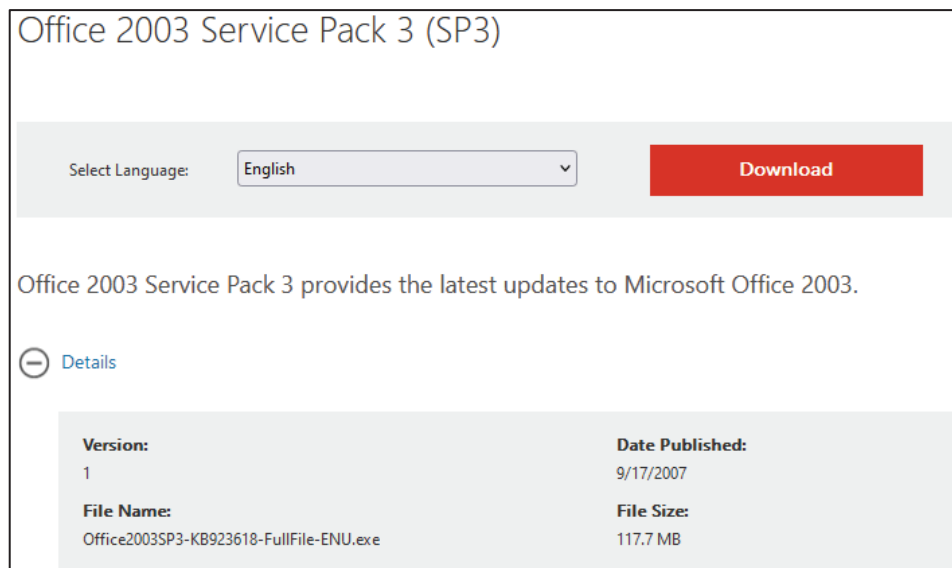
<sup>3</sup> See [https://microsoft.fandom.com/wiki/Windows\\_10\\_version\\_history#Version\\_2004\\_\(May\\_2020\\_Update\)](https://microsoft.fandom.com/wiki/Windows_10_version_history#Version_2004_(May_2020_Update)); <https://www.lifewire.com/windows-version-numbers-2625171>; <https://endoflife.date/windows>

been created with MS Word version 11.9999. It has a Revision Number of 2 and a Total Edit Time of 1 minute, indicating that it is likely to have been created by the use of a “Save As” operation. The Internal Metadata timestamps date to 16 June 2007 (Created and Last Modified).

c. The remaining 7 were created with MS Word version 11.8107.

93. 11.6568, 11.8107, and 11.9999 are all different sub-versions of MS Word 2003 with different release dates:

- a. I believe the first two software versions are contemporaneous to the timestamps provided.
- b. However, MS Word version 11.9999 (MS Word 2003 SP3) was not released until September 2007. This is recorded in the following archived web page of the Microsoft Release announcement<sup>4</sup>, a copy of which is at **Exhibit PM-R3.15**. The screenshot below shows a date-published of 17 September 2007:



94. Since the Internal Created and Last Modified dates of ID\_004682 (and the provided external file metadata in the load file) all predate the release of that software, they cannot be accurate.<sup>5</sup>

95. It is therefore my opinion that:

<sup>4</sup> Available at <https://web.archive.org/web/20170306034822/https://www.microsoft.com/en-us/download/details.aspx?id=8>

<sup>5</sup> I note that this also applies to the documents ID\_000073, ID\_000142, both of which are dated as if last modified before the release of MS Word 11.9999. These documents were both analysed in my Main Report and which I found to be inauthentic for other reasons.

- a. ID\_004682 is not authentic to its purported timestamps, and
- b. Since ID\_004682 was obtained from within the BDO Image, it is also indicative of clock manipulation techniques or metadata editing techniques being used in connection with the BDO Image itself.

### **SECTION 3: THE BDO IMAGE AND REPLY TO STROZ FRIEDBERG REPORT**

96. In this section of this Report I address the BDO Images and provide my views in response to the Stroz Friedberg report, and the information provided about the BDO Image.

#### **Introduction to BDO Image**

97. I understand that the BDO Image is dated to 31 October 2007 and was created as a RAW image.

98. A Raw image is a byte-for-byte copy of the information on a disk. There is typically no additional metadata or file information created in a Raw image, which is in contrast to other types of forensic image (which embed header information such as the date of collection, and a checksum or hash of the content). If the BDO Image was created with a forensic tool or another tool which output logs, it is possible that such information exists, but otherwise it would not.

99. The files within a Raw image cannot be edited or used unless the disk is first “mounted”. “Mounting” an image or disk is the process of connecting it to a filesystem so that it can be used as an ordinary drive.

- a. For hardware drives like USB drives and hard disks, this process is normally invisible on Windows systems – for example, when a USB stick is plugged in, Windows by default would automatically mount it and allow the files to be viewed and interacted with. (On most Linux systems mounting a drive requires a specific instruction, by default).
- b. However, disk images are software files and are not typically mounted automatically in the same way. They require specific configuration or software to enable them to be viewed and interacted with. While many types of software are available allowing this to be done easily, they still require user interaction to cause the raw image to be mounted.

100. Therefore, it is possible for the BDO Image to be interacted with as if it was a normal drive. However, this would have caused the metadata associated with the Image to be altered.

101. Although there is no forensic metadata automatically contained within a raw image about the image itself, there are other sources of metadata in respect of the BDO Image:

- a. It will be a file, (albeit a very large file), and will therefore have file metadata provided with it.
- b. Based on the information provided, the file system of the BDO Image is an NTFS system. The NTFS system contains file transaction journals recording the activity within that filing system. Inspection of those journals by SF has already provided indications that the drive was accessed



and edited in September 2023. However, only a few examples of entries have been provided, and a proper inspection of the transaction journals would be required.

- c. Operating systems, including Windows and Linux, contain various log systems which monitor events and actions that are done with the computer in question. Unless these have been erased or altered, it is likely that the computing system used to connect to the drive will contain logs and other artefacts of its interaction with the BDO Image and the Samsung Drive on which the BDO Image resides.
- d. The BDO Image itself also appears to contain logs of how it was used, based on the information available.

### **Initial conclusions based on review of documents from the BDO Image**

102. It is therefore not possible to authenticate the BDO Image without inspection of the image as a whole, and the forensic image of the Samsung drive from which it was sourced. The current information available does lead me to the view that the authenticity and integrity of the documents sourced from the BDO Image is not reliable, and specifically that it has been manipulated. Overall, based on my analysis above in the first part of this report, there are strong indications that (and it is my opinion that):

- a. The BDO Image was mounted, interacted with, and has been manipulated. Specifically, the content of the BDO Image was edited at a time later than May 2020, and may have been edited on several occasions.
- b. Direct metadata editing and/or clock manipulation techniques were used, so that metadata within the BDO Image was altered.
- c. There is also some indication that metadata was possibly edited “en masse” within the BDO image, potentially using the techniques referred to above.

### **Access to computing equipment**

103. If a fuller picture of the extent of manipulation was required, I have explained above that access to the relevant computing equipment would be required and could be expected to provide further indications.

### **Reply to the Stroz Friedberg Report**

104. I have been provided with a copy of the Stroz Friedberg report exhibited to Dr Wrights’ Fifth

Witness statement and asked to comment and respond to it.

105. In overview, Stroz Friedberg has been provided with forensic images of the Samsung Drive and the BDO Image contained within it.

106. I have not been provided with the same access.

107. In my view, the report only scratches the surface of what might be available for analysis, as for example the findings made require little or no pre-processing. The Stroz Friedberg report covers material that I would also have looked at in the very early stages of my analysis, in around the first day.

108. I assume this is because Stroz Friedberg were only provided with access to the information in the last few days, and so their findings are based on the analysis possible in the time they had.

109. This is consistent with the provided report being described as a memorandum and it being only 4 pages in length.

#### **Recycle Bin - Information deleted**

110. I agree with Stroz Friedberg that their findings indicate that the Recycle Bin in the Samsung Drive was emptied in September 2023.

111. This would have led to a significant amount of information on the drive being irretrievably deleted. Specifically, at least:

- a. A document named "ESDT.PDF" with a file size of 132,747 bytes, and
- b. A RAR archive (similar to a zip archive) with an unknown filename and a file size of 20.6GB, and
- c. Metadata relating to those files.

112. It is also possible that the two files in the Stroz Friedberg findings are not a complete record of the data deleted, but examples.

113. Below, I address the behaviour of the Recycle Bin, and my analysis of each of the two files.

#### **Behaviour of Recycle Bin**

114. The behaviour of the Recycle Bin files described by Stroz Friedberg is consistent with Windows

8 or later desktop operating system being used to interact with the Samsung Drive. When a file is deleted, it creates two files:

- a. The deleted file itself, is renamed with a random string beginning with \$R, and
- b. A record of the metadata including the file path where it was stored, and other external metadata associated with the file. This is named with the same name as the \$R file, except that the prefix is \$I. The time and date on the local computer's clock is assigned to the \$I File, which indicates the date of deletion of the file being deleted (according to the computer's clock). I note that the fact that the \$I files are different sizes in the Stroz Friedberg report indicates a more modern version of Windows (version 8 or later), and that earlier versions of Windows would have had a fixed \$I file size.

115. The information is therefore consistent with a modern computer being used to interact with and delete information from the Samsung Drives.

#### The 20GB RAR file

116. The 20GB RAR file is the first deleted document to be considered.

117. Very little information is given about the 20GB RAR file other than its file size and details about the \$R and \$I file. However, the information provided does suggest a possible explanation for the contents of the RAR file, as follows:

118. First, the file size of the file is 22,143,612,981 bytes, or about 22GB. This is comparable to the file size of 39,999,594,384 bytes for the uncompressed BDO Image (which is about 40GB, and Dr Wright notes is a file called "BDOPC.RAW"):

- a. I have a lot of experience imaging hard drives, which often creates large files (the same size as the disk being imaged). However, these often readily compress significantly when put into Zip or RAR archives, especially where the drive image includes coding for significant amounts of unused space on the drive. Most forensic imaging applications will compress the content as standard, and therefore also provide a similar benchmark for comparison.
- b. Dividing the numbers,  $22,143,612,981 \text{ bytes} / 39,999,594,384 \text{ bytes} = \text{around } 55\%$ , indicating a 45% compression ratio. This is within typical parameters for RAR compression, if there was a low to moderate amount of unused space on the drive that was imaged to create the BDO Image.

119. Second, the file size of the \$I file provides a further clue:

- a. A typical \$I file in Windows 10 encodes a standard set of metadata information, including a Header, File Size, timestamp of deletion ('Deleted Timestamp'), and File Name. The structure of an \$I file is set out in the following image<sup>6</sup>:

Windows 10		
Offset	Size	Description
0	8	Header
8	8	File Size
16	8	Deleted Timestamp
24	4	File Name Length
28	var	File Name

**Windows 10 \$I structure**

- b. Within that structure, all the fields are a fixed length except the last one, the File Name (which in fact includes the full file path). The full file path can be as long as it needs to be, with each character taking up 2 bytes.
- c. Therefore, the file size consists of the first 28 bytes (in locations 0 to 27) which include fixed information, followed by the remainder of the file which consists of the file path.
- d. In this case, the \$I file is 60 bytes long according to Stroz Friedberg:

<b>Path</b>	\$RECYCLE.BIN
<b>Full path</b>	\$RECYCLE.BIN\SIFH6M1E.rar
<b>Parent name</b>	\$RECYCLE.BIN
<b>Size</b>	60 B
<b>Created</b>	10/31/2007 06:26:01 +0
<b>Modified</b>	10/31/2007 06:26:02 +0
<b>Accessed</b>	10/31/2007 06:26:02 +0

- e. Accounting for the first 28 bytes of fixed information, this leaves 32 bytes for the Header (60-28=32bytes).
- f. Dividing by 2 (the number of bytes required for each character) indicates that the whole file path and file name together took up 16 characters.
- g. Noting that a typical drive structure takes 3 characters (e.g. "E:\") and an RAR extension takes up 4 characters (".rar"), this leaves a further 9 characters.
- h. "BDOPC.RAW" is 9 characters long.

120. Therefore, taking account of the file size of the deleted file, the length of its filename, the possible

<sup>6</sup> Taken from: <https://df-stream.com/2016/04/fun-with-recycle-bin-i-files-windows-10/>

compression ratio, and the file size of the BDO Image that was located in the same drive,

- a. it seems to me at least possible that the name of the RAR file was “E:\BDOFC.RAW.RAR”, and that it was a RAR-compressed version of the BDO Image itself.

121. It is also possible that the name and content of the RAR file was different, however, no information has been provided as to what it was. I emphasise that this is not a firm opinion, but an observation taking into account the limited information available that the facts provided are consistent with the deleted file being a copy of the BDO Raw Image in compressed RAR form.

122. It may, and often is, possible to recover further information to show more detail about the actual name or content of the deleted file.

### The ESDT PDF

123. The second deleted file is named “ESDT.PDF”. I observe as follows:

- a. There is only one file with a similar name in the disclosure dataset which is “ESDT.tex”, ID\_004736.
- b. I have analysed ID\_004736 (and its associated file ID\_004735 above) and found it to be connected with indications of clock manipulation.
- c. Exhibit PM-R3.8 is a PDF export of ESDT.tex, which would by default usually be called “ESDT.PDF”.
- d. The file size of Exhibit PM-R3.8 is **138,712 bytes**. That is close to the file size of **132,747 bytes** given by Stroz Friedberg for the deleted file ESDT.PDF. The difference of 6,035 bytes is consistent with variations in the environment used, such as minor variations in the version of the PDF software used to generate it.
- e. I also observe that the deleted file “ESDT.PDF” and the three disclosed files ID\_004686, ID\_004735, and ID\_004736 all share a common File Created date of 19 September 2017.
  - i. I observe further that the Deleted “ESDT.PDF” file has a recorded file Last Modified timestamp of 16 September 2023.

124. Taking into account the file name and file sizes and shared creation date, it is in my opinion very likely that the deleted file ESDT.PDF was a copy of the PDF export of one of the 97 New Documents, specifically ID\_004736 (“ESDT.tex”).

125. I note that the \$I file would normally encode the full file path. Taking into account the file size of the \$I file, which according to Stroz Friedberg is 78 bytes, it indicates that the full file path listed in the \$I file is 25 characters long.

126. However, Stroz Friedberg have only provided the last 8 characters (ESDT.PDF).

127. Taking into account the normal file path (e.g. E:\), that indicates that the ESDT.PDF file was located in a subdirectory of the main drive. The name of that subdirectory has not been provided.

### **Metadata Dates on the Recycle Bin and BDO Image**

128. Reviewing the metadata information contained in the Stroz Friedberg report, I have the following observations.

#### User ID for Recycle Bin deletion

129. The Recycle Bin will have recorded a UUID for each user account that has interacted sufficiently with the drive. This UUID is unique to a user account on a specific computer (cloning of computer disks aside) and can be used in effect to identify the computer and user account that was used to send the files and folders to the recycle bin. This has not been provided.

#### Metadata on ESDT.PDF

130. The metadata indicated in relation to the deleted ESDT.PDF file “\$R391BYS.pdf” is consistent with a file having been copied and pasted with a backdated clock. This causes the “Created” And “Last Accessed” timestamps to match each other, but to pre-date the “Last Modified” timestamps given:

<b>Path</b>	\\\$RECYCLE.BIN
<b>Full path</b>	\\\$RECYCLE.BIN\\\$R391BYS.pdf
<b>Parent name</b>	\$RECYCLE.BIN
<b>Size</b>	130 KB (132,747)
<b>Created</b>	09/19/2017 10:15:50 +0
<b>Modified</b>	09/16/2023 13:54:06 +0
<b>Accessed</b>	09/19/2017 10:15:50 +0

<b>Path</b>	\\\$RECYCLE.BIN
<b>Full path</b>	\\\$RECYCLE.BIN\\\$I391BYS.pdf
<b>Parent name</b>	\$RECYCLE.BIN
<b>Size</b>	78 B
<b>Created</b>	09/19/2017 10:17:02 +0
<b>Modified</b>	09/19/2017 10:17:04 +0
<b>Accessed</b>	09/19/2017 10:17:04 +0

131. This may possibly be explained by the file being accessed and edited while deleted within the Recycle Bin in 2023. However, that would require special tools and purposeful action to achieve, and I agree with Stroz Friedberg that these files are not able to be opened from the Recycle Bin directly.

132. Noting that the file was recorded as Last Modified on 16 September 2023,

- a. The deletion operation must have taken place after that.
- b. The deletion date should have been recorded in the \$I timestamps, but those timestamps are listed to 19 September 2017 (rather than 2023). Bearing this in mind it is therefore possible that the actual date of deletion could have been 19 September 2023, but with the clock adjusted back by 6 years. It is also possible that it occurred at any other time between 16 September 2023 and 20 September 2023.
- c. I have considered whether a potential explanation could be that a file called ESDT.PDF was created on 19 September 2017, and then overwritten with a new file on 16 September 2023. I do not think that is the case for two reasons. First, while that might explain the Created date, it would not explain the Last Accessed date being in 2017. In that situation, the Last Accessed date would be expected to update to match the Last Modified date. Second, the \$I file is recorded as being created on 19 September 2017, just two minutes after the Created date of the ESDT.PDF file: that indicates that the file was deleted when the clock was set to 19 September 2017, so it could not later be overwritten with a new file. The file can only have been deleted after it was created and modified, indicating the 2017 timestamps to be manipulated.

133. I further note that ID\_004686, ID\_004735 and ID\_004736 (ESDT.tex and its associated files) share the same 19 September 2017 timestamp (19/09/17 11:17:16, taken from the Load file, which I take to be expressed in BST time (UTC+1) as it was during daylight savings time in the UK). This is therefore just a few seconds apart from the deletion of ESDT.PDF (which is recorded in the Creation of the \$I file. Bearing in mind the relationship of these files together (as originating from the same source and, in effect, being different parts of the same document), I doubt the authenticity of the 19 September 2017 timestamp in relation to all of them, and consider it considerably more likely that the true time of interacting with those files was in 19 September 2023, or at some other point in the period between 16 September 2023 at 13:54:06 and 20 September when the drive was imaged.

#### Metadata on 20GB RAR File

134. The metadata relating to deletion of the 20GB RAR file is inconsistent. Specifically, it indicates

that the \$R file (the deleted file itself) was Last Modified on 10/31/2017 at 18:47:56, Last Accessed 24 seconds later, and then Created a further 1 second after that. While this may be explained if the file was created as a copy (and if the times include a rounding error to the nearest second), it is not consistent with the data of the \$I file (which contains its metadata): that file is recorded as having been Created almost 10 years to the day earlier than the deletion event recorded in its accompanying \$I file.

<b>Path</b>	\\\$RECYCLE.BIN
<b>Full path</b>	\\\$RECYCLE.BIN\\\$RFH6M1E.rar
<b>Parent name</b>	\$RECYCLE.BIN
<b>Size</b>	20.6 GB (22,143,612,981)
<b>Created</b>	10/31/2017 18:48:21 +0
<b>Modified</b>	10/31/2017 18:47:56 +0
<b>Accessed</b>	10/31/2017 18:48:20 +0
<b>Path</b>	\\\$RECYCLE.BIN
<b>Full path</b>	\\\$RECYCLE.BIN\\\$IFH6M1E.rar
<b>Parent name</b>	\$RECYCLE.BIN
<b>Size</b>	60 B
<b>Created</b>	10/31/2007 06:26:01 +0
<b>Modified</b>	10/31/2007 06:26:02 +0
<b>Accessed</b>	10/31/2007 06:26:02 +0

135. Noting the fact that (a) both \$R file and \$I file should be created by the same deletion event and at the same time and (b) the very precise 10-year time gap between their respective timestamps, I can only account for this with the use of clock manipulation techniques.

Date of deletion of the 20GB RAR File

136. As I pointed out above, the behaviour of the Recycle Bin files described by Stroz Friedberg is consistent with more modern versions of Windows which did not yet exist in 2007-2009.

137. However, the date on the \$I file for the deleted RAR file is 31 October 2007. That date ought to record the date that the file was deleted (moved into the Recycle Bin). It is however not possible for that to have been the date, because the Recycle Bin on earlier versions of Windows behaved differently. Therefore,

- a. The RAR file was not deleted on 31 October 2007, but was deleted at a more recent time while the computer clock was set back to the past; and
- b. The presence of that timestamp is consistent with the use of clock manipulation while doing the deletion process.



Date of creation of the BDO Image

138. The metadata of the BDO Image indicates that the file BDOPC.RAW was written to the Samsung Drive at 23:28:05 on 31 October 2007:

<b>Full path</b>	BDOPC.raw
<b>Parent name</b>	\
<b>Size</b>	37.3 GB (39,999,504,384)
<b>Created</b>	10/31/2007 23:48:05 +0
<b>Modified</b>	10/31/2007 23:48:06 +0
<b>Accessed</b>	10/31/2007 23:48:06 +0

139. Significantly, the Samsung Drive was not in existence at that date. Dr Wright indicates that the Samsung Drive was purchased in around 2015-2016. I have also checked its serial number, which encodes the year of manufacture, and found it to be consistent with manufacture around that time.

140. Therefore, the BDO Image file BDOPC.RAW could not have been written to the Samsung Drive in 2007. In my opinion, it is consistent with its timestamps having been edited or the use of clock manipulation to create an image.

- a. I note that this could also be the result of the BDO Image being moved onto Samsung Drive rather than copied, or that it's timestamps were preserved through the use of a compression utility such as a ZIP or RAR application.

141. This is also consistent with my findings in respect of documents that are contained within the BDO Image, which could not have been created until several years after the recorded timestamps.

142. Therefore it is my view that the BDO Image file BDOPC.RAW on the Samsung Drive is not authentic to its purported timestamps.

143. If the BDO Image was created by extracting it from the deleted RAR file (which I cannot know), then it is likely that the RAR file would encode internal file timestamps relating to its contents.

**Transactional Logs within the BDO Image**Meaning of transactional logs

144. Stroz Friedberg have listed five examples of transactional log files found within the BDO Image itself, including two bearing timestamps on 17 September 2023. Stroz Friedberg indicates that these are just examples.

145. Transactional Log files relate to an integral part of the NTFS file system, the purpose of which is

to record information about changes to files and folders within a drive. The transaction log is not accessible through a normal user interface but requires specialised forensic tools to access. The transaction log works together with another aspect of the file system, called the USN Journal, and together they are a useful point for investigation because they record operations on the drive in a sequential order. Therefore, they can expose the use of clock manipulation or irregular timestamps, if the timeline appears to jump around in sequence. It can also be useful to indicate the scope of clock manipulation.

First Transactional log segment: Likely creation date of BDO Image

146. Of the examples provided, the first example `$Extend$RmMetadta$TxfLog` relates to the root folder in which components of the log itself are stored:

<b>Path</b>	<code>\\$Extend\$RmMetadta</code>
<b>Full path</b>	<code>\\$Extend\$RmMetadta\$TxfLog</code>
<b>Parent name</b>	<code>\$RmMetadta</code>
<b>Size</b>	82.3 MB (4,152)
<b>Created</b>	09/17/2023 13:02:32 +0
<b>Modified</b>	10/19/2007 13:04:01 +0
<b>Accessed</b>	10/19/2007 13:04:01 +0

147. It is irregular that the log has a “Created” date of 17 September 2023. The transactional log is an integral part of the filing system. The date of creation of `$TxfLog` usually matches the date on which the file system it relates to is created.

- a. Therefore, from the limited information made available to me, 17 September 2023 is likely to be the true date on which the file system in the BDO Image was created.
  - i. It would be necessary to inspect the BDO Image itself to investigate this point further.
- b. Subsequent user activity may change the Last Modified and Last Accessed timestamps, but would not alter the Created timestamp of the `$TxfLog` folder.
- c. I note that the Last Modified and Last Accessed timestamps pre-date the Created timestamp by around 16 years (being in 2007 rather than 2023). This should not be possible without the use of clock manipulation.

148. Based on the information available, it is my opinion that the most likely date of creation of the BDO Image itself, `BDOPC.RAW`, was 17 September 2023. It is possible that better access to the Drive, computing equipment, and the Image itself may allow me to refine this opinion, and it is also possible that it may change on review of that equipment.

Second log segment within BDO Image: 17 September 2023 dates

149. The second log example listed has all its Created, Modified, and Accessed dates listed as 17 September 2023 between 13:02:33 (Created) and 13:03:26 (Last Modified and Last Accessed):

<b>Full path</b>	\\\$Extend\SRmMetadata\TxfLog\TxfLogContainer00000000000000000001
<b>Parent name</b>	TxfLog
<b>Size</b>	10.0 MB (10,485,760)
<b>Created</b>	09/17/2023 13:02:33 +0
<b>Modified</b>	09/17/2023 13:03:26 +0
<b>Accessed</b>	09/17/2023 13:03:26 +0

150. This is consistent with ordinary logging procedure and is not suspicious. However, it indicates that the procedure took place on 17 September 2023.

151. The changing of data in the TxfLog file would have led to the updating of the timestamps for the BDO Image itself. However, they instead record the BDO Image file as if it predates the TxfLog entries contained within it and has not been modified. This is therefore a further indication of the use of clock manipulation techniques or direct metadata editing in connection with the BDO Image file itself.

Fourth log segment within BDO Image: time-travelling dates

152. The fourth listed log segment is recorded as being Modified the day before it is created. This is consistent with clock manipulation or direct metadata editing. It is a further indication of manipulation of the BDO Image file itself.

<b>Full path</b>	\\\$Extend\SRmMetadata\TxfLog\TxfLogContainer00000000000000000001
<b>Parent name</b>	TxfLog
<b>Size</b>	10.0 MB (10,485,760)
<b>Created</b>	10/31/2007 16:59:51 +0
<b>Modified</b>	10/30/2007 10:44:18 +0
<b>Accessed</b>	10/30/2007 10:44:18 +0

Fifth log segment within BDO Image: time-travelling dates

153. The fifth listed log segment shares dates and timestamps of 19 October 2007 at 13:04:01-02, i.e. within a second of the timestamps listed for the first log statement (the TxfLog folder discussed above). However, as I have stated above those timestamps could not be accurate for the TxfLog folder, and the second-precise timestamps in the later logs call into question the timestamps on this log also.

<b>Full path</b>	\\\$Extend\SRmMetadata\TxfLog\TxfLogContainer00000000000000000001
<b>Parent name</b>	TxfLog
<b>Size</b>	10.0 MB (10,485,760)
<b>Created</b>	10/19/2007 13:04:01 +0
<b>Modified</b>	10/19/2007 13:04:02 +0
<b>Accessed</b>	10/19/2007 13:04:02 +0

### Transactional logs inside BDO Image: Conclusion

154. In my opinion the examples of transactional logs within the BDO Image strongly indicate the use of clock manipulation to author the Image and while placing it on the Samsung Drive.
155. That is also consistent with my views based on independent characteristics including the problems with documents within the BDO Image itself, and the inconsistency between the file creation timestamp for the Image (which pre-dates the date it was created), and the other serious anomalies that I have explained above, reinforcing my view that the BDO Drive Image as a whole is not authentic.

### Dr Wright's interaction with the Samsung drive

156. In his Fifth Witness Statement Dr Wright acknowledges some of the findings of the Stroz Friedberg report and indicates that he connected the Samsung Drive containing the BDO Image to his computer on one occasion in September 2023. Dr Wright states that:

*30. I believe that these matters may be explained by the software systems and processes that I habitually use. These include VMware, WinUndelete, Storage Sense, SAMBA shares and symbolic links. These may have caused the recycle bin on the Samsung Drive to have been automatically emptied when I plugged the Samsung Drive into my laptop to check that it was working (as explained above). They may also have altered the ordering of files in the recycle bin. It is also possible that one of these systems or processes was configured in such a way as automatically to open the BDO Drive when I checked that the Samsung Drive was working. However, I am sure that I did not myself do anything with either of the Hard Drives, other than to check that they were working, between the time I discovered them and the time they were imaged by KLD.*

157. Bird & Bird has asked me to comment on that passage.
158. I agree that connecting a drive to a computer in this way, when it is intended for forensic imaging, risks contamination of the drive. It is a basic procedure in forensic imaging that drives should not be handled in this way by connecting a drive to computing equipment which might alter it, and it is well known in the field that proper preservation of evidence requires proper care to be taken to avoid data being spoiled, overwritten or deleted.
159. However, I do not consider that the explanation given accounts for the indications in the Stroz

Report, or the other indications of inauthenticity that I have explained above, for the following reasons.

*Behaviour of software listed by Dr Wright*

160. Dr Wright lists five software systems at paragraph 30 of his statement. However, in my opinion those systems would not be expected to interfere with the internal transactional logs of the BDO Image, or the Recycle Bin of the Samsung Drive, or the other factors that I have analysed above.

161. Overall, the explanation is rather vague and does not provide a detailed explanation that enables a response. However, addressing each of the software systems:

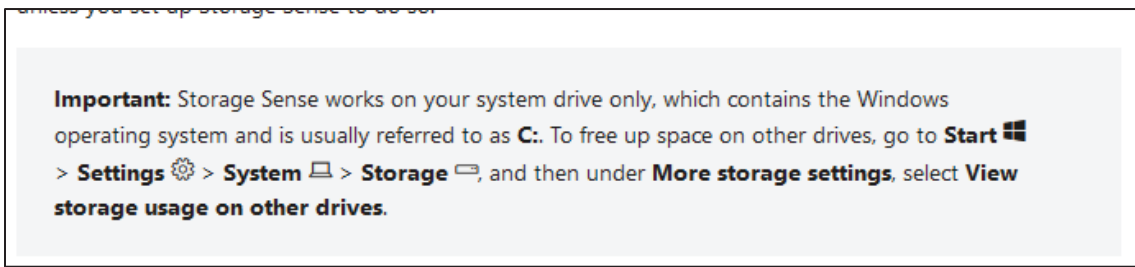
- a. **WinUndelete:** WinUndelete is a file recovery utility which allows recovery of deleted files (although in my experience, I have also seen it used as a tool for checking that files have been securely deleted so that they cannot be recovered). The homepage of the tool is at <https://www.winundelete.com/> (**Exhibit PM-R3.16**). That web page also lists the features of the tool, and specifically states that it does not change or harm the Recycle Bin. Therefore, the software appears to be specifically configured to avoid the activity observed in relation to the Samsung Drive:

- Works safely, stands alone, without changing or harming your Recycle Bin.

- b. **Storage Sense** is a utility that can be enabled on Windows 10 and Windows 11, to automatically deletes temporary files and Recycle Bin items when a computer is running low on disk space. It is a Microsoft Windows Setting found in the System>Storage menu under Windows 10. However, this could not have led to the deletion of the Recycle Bin on the Samsung Drive, because the Samsung Drive is an external USB drive, not the system drive where Windows is installed. The Microsoft Support Page for Storage Sense (<https://support.microsoft.com/en-us/windows/manage-drive-space-with-storage-sense-654f6ada-7bfc-45e5-966b-e24aded96ad5>) (**Exhibit PM-R3.17**) states that Storage Sense does not run on other drives than the system drive on which Windows is installed, as shown below.<sup>7</sup> Therefore, Storage Sense cannot explain the deletion of the Recycle Bin.

---

<sup>7</sup> Further, Storage Sense only runs when a computer is in low disk space mode, and there is no indication that Dr Wright's computer is low on disk space.



- c. **VMWare** is a utility for running virtual machines. I am familiar with VMWare and use it in connection with my forensic investigations. I have never come across any circumstance in which VMWare would cause external files to be deleted without specific user interaction. If it did do so, it would not be suitable for its purpose of running isolated virtual machines.
- d. **SAMBA shares:** Samba is a protocol for sharing file, folder, and printer access across a network between machines. It is a protocol for enabling shared access and not a file management or deletion utility. I am not aware of any circumstances where having a machine using a Samba share would cause the machine to delete files on a removable storage disk, which would be quite unusual and not within the scope of its use at all.
- e. **Symbolic links** are a form of file shortcut, where a file is stored in one location on a computer and a link created in another location, allowing the user to actually interact with the target file by interacting with the symbolic link. However, the presence of a symbolic link would not cause data deletion or changes to metadata information of files in a removable storage drive and it is not associated with the deletion of the Recycle Bin. If a symbolic link was made and then the link was deleted, it would not cause the target file to be deleted, but only the link (unless the user also took specific action to cause the target file to be deleted). Even then, I would not expect it to interact with files in the Recycle Bin.
162. As I have stated above, the BDO Image itself could not be edited without first mounting the image as if it was a physical storage drive. This typically requires active user interaction and I agree with Stroz Friedberg that it is not available with any tools built into windows. Even if the BDO Image was mounted as a disk in addition to the check that Dr Wright states he carried out, I still would not expect the Recycle Bin to be emptied automatically or any other operations to take place that might account for the various anomalies described above.
163. The deleted file “ESDT.PDF” was not only emptied from the Recycle Bin in September 2023, but it must have also been sent to the Recycle Bin after 16 September 2023, this being when a change to the content of the file was last recorded.
164. I also do not consider that any of the software systems discussed would cause transaction logs to

be reordered, or the system clock of the computer to be backdated. Both of these are significant systems within any operating system and in my experience would not be changed without active user interaction to achieve the change.

165. Finally I note that the metadata in the Stroz Friedberg report, and my analysis above, indicates that the interactions with the Samsung drive and the BDO Drive took place over a number of days in September 2023, and could not therefore be associated with only one event. Specifically:

- a. On 16 September 2023: ESDT.PDF (the deleted file from the Samsung Drive) was modified,
- b. On 17 September 2023: The BDO Image \$Txflog was created (likely the date of creation of the BDO Image itself),
- c. On 17 September 2023: Further transaction records were made within the BDO Image,
- d. At some point between 17 September 2023 and 20 September 2023 – the file ESDT.PDF was deleted to the Recycle Bin, at a time when the computer clock was backdated, and
- e. At some point between 17 September 2023 and 20 September 2023, the Recycle Bin of the Samsung Drive was emptied.

**SECTION 4: LATEX, OPENOFFICE, AND BITCOIN WHITE PAPER**

166. Bird & Bird have explained that Dr Wright wishes to rely on documents that are claimed to be drafts of the Bitcoin White Paper written in Latex, and asked me to comment.

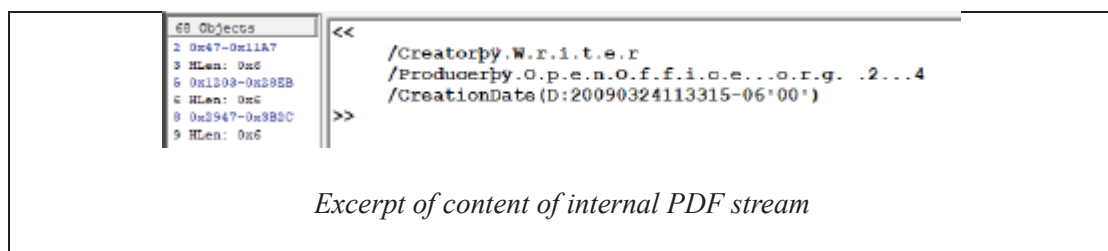
Bitcoin White Paper created with OpenOffice version 2.4

167. I analysed the Bitcoin White Paper in my First Report at Appendix PM3. From paragraphs 16 to 40 of Appendix PM3 I scrutinised and established corroborating validity for two control copies of the Bitcoin White Paper dating to October 2008 and March 2009. (I also analysed a further document, BWP-NB1, between paragraphs 41 and 73, another version of the Bitcoin White Paper which I consider to be very likely to be an authentic intermediate draft between those two versions, but do not take account of that here.)

168. In those parts of Appendix PM3, I explained that the BWP Control Copies contain metadata indicating that,

- a. They were created with the Writer application from OpenOffice.org 2.4,
- b. They did not include indications of editing or tampering after their creation, and
- c. They did not record an internal 'Modified' timestamp, indicating that they were not modified after creation.

169. Some screenshots from Appendix PM3 below summarise part of the information.





Created: 24/03/2009 18:33:15

Modified:

Application: Writer

---

Advanced

PDF Producer: OpenOffice.org 2.4

PDF Version: 1.4 (Acrobat 5.x)

Location:

File Size: 179.97 KB (184,292 Bytes)

Page Size: 8.50 x 11.00 in                    N

Tagged PDF: No

*Screenshot of properties as viewed within Adobe Acrobat software*

	Created date	Modified date	Creator Tool	PDF Producer	PDF Version
ID_000226	3 October 2008 at 13:49:58 UTC-0700	n/a	Writer	OpenOffice.org 2.4	1.4 (Acrobat 5.x)
ID_000865	24 March 2009 at 11:33:15 UTC-0600	n/a	Writer	OpenOffice.org 2.4	1.4 (Acrobat 5.x)

*My summary of metadata characteristics of the BWP Control copies*

170. It is therefore my view, as explained in my First Report, that the metadata properties of the Bitcoin White Paper indicate that it was created directly from the OpenOffice version 2.4 Writer application.

171. It is also my view that the document is not typical of Latex output and displays marked differences to the output of a typical Latex “Article” template, though I cannot say whether or not that is possible, and it may be possible to use Latex in such a way as to produce a similar document.

#### Checking OpenOffice.org 2.4 functionality

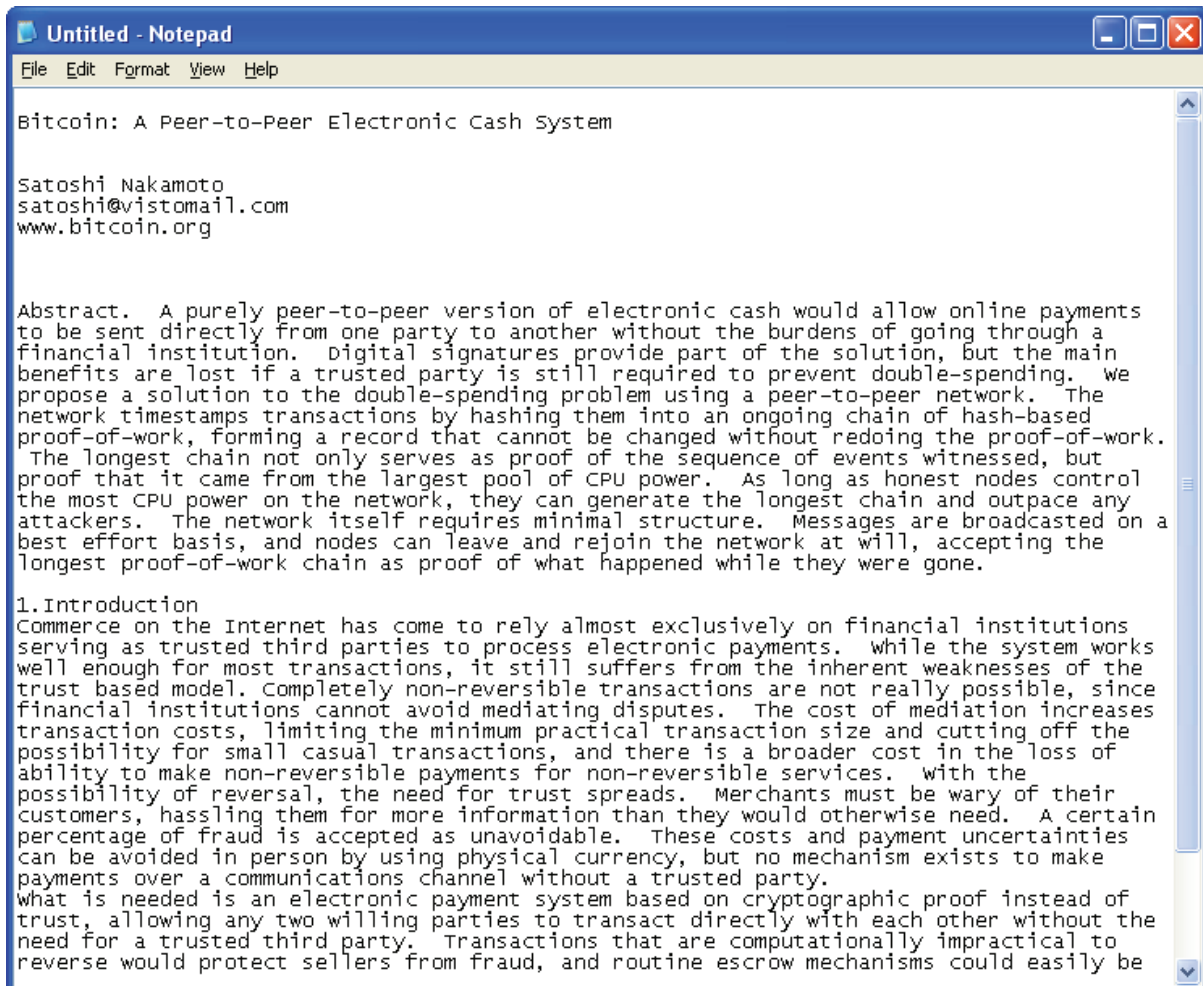
172. I have checked whether the functionality of OpenOffice is consistent with the content of the Bitcoin White Paper. I have found that it is. Specifically, I have checked:

173. How OpenOffice.org 2.4 Writer (“OO2.4”) presents text, when the appropriate margins, font, and paragraph spacing are applied (i.e. the settings used by Satoshi Nakamoto), and

174. Whether the basic diagram options in OpenOffice.org 2.4 create output matching the diagrams in the paper.

Text check – first page of Bitcoin White Paper

175. To check the text layout of OO2.4, I opened OO2.4 in a Windows XP virtual machine consistent with an operating system contemporaneous to 2008-2009, using the same installation of the software described in Appendix PM23 to my first report (obtained via <http://ftp5.gwdg.de/pub/openoffice/archive/stable/2.4.0/>).
176. The text was obtained by taking the plain text content from control version ID\_000226, and correcting the formatting errors that were caused by e.g. hyphenation when doing this. These are the same errors that were observed in Appendix PM2 to my First Report and are typical of conversion from PDF. The result of this being that I had the plain text content of the first page of the Bitcoin White Paper without any of the formatting from the PDF file:



177. I next copied and pasted this into a blank new OpenOffice Writer document and applied the same settings that were observed in the Bitcoin White Paper control to:

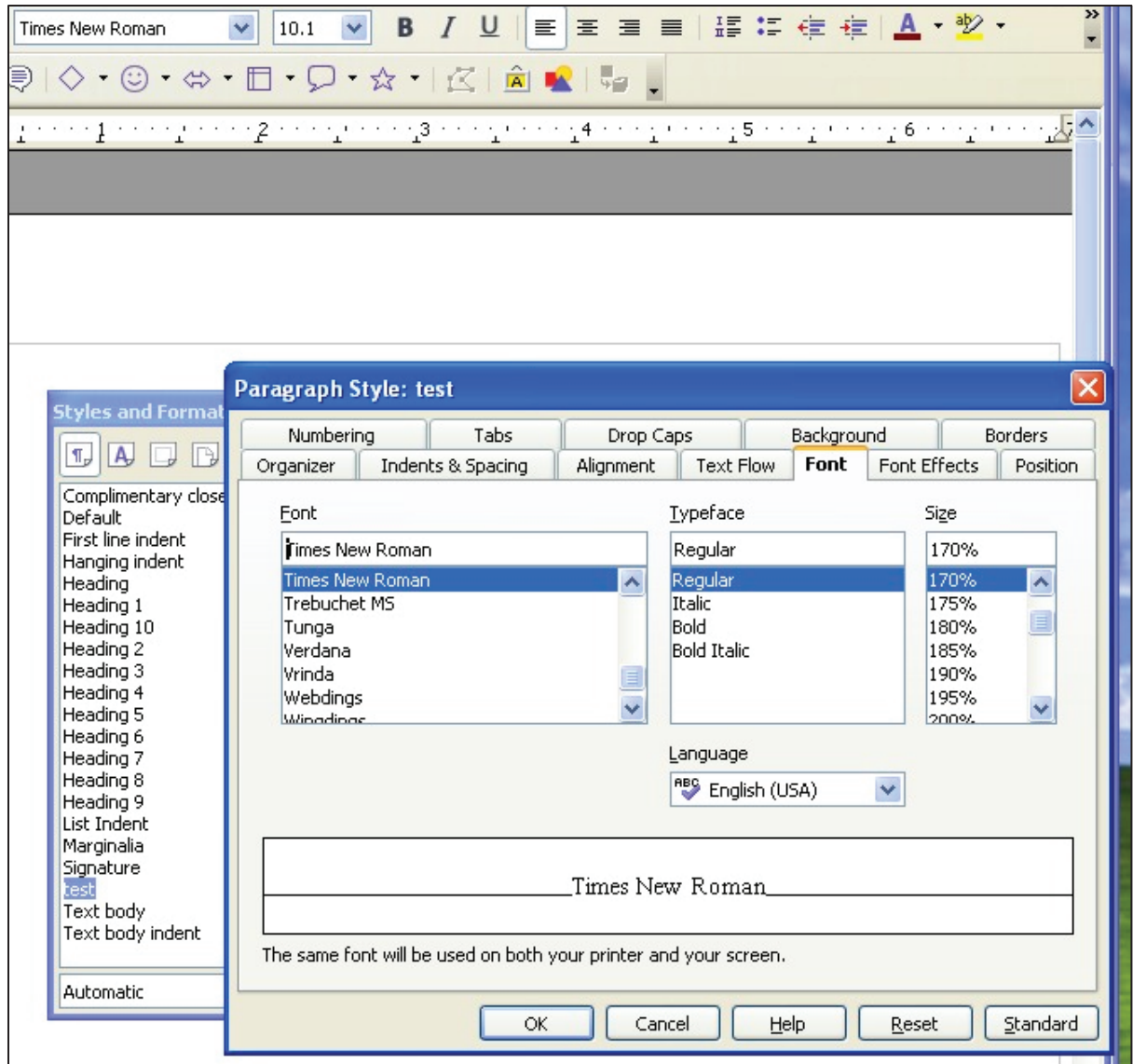
- a. Document fonts, using sizes selected to match the Bitcoin White Paper

- b. Margin sizes
- c. Paragraph settings and line spacing.

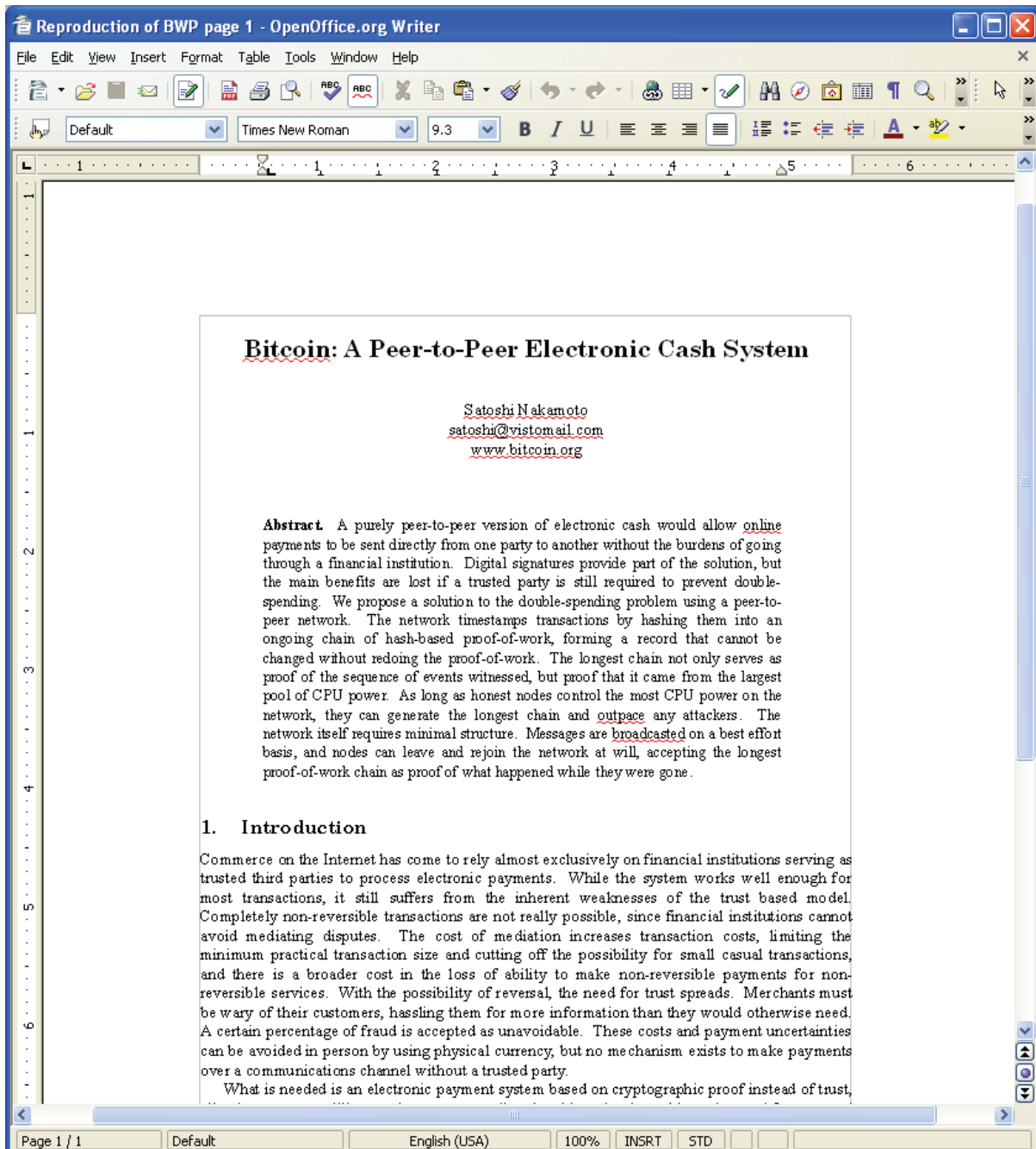
178. I found it easy to set all the settings using OO2.4 standard settings options and dialogs. In some cases, it was time consuming to measure what the correct sizes used by Satoshi Nakamoto were (e.g. the margin sizes and indents selected), but actually setting them was simple.

179. I observed that the font sizes present in the Bitcoin White Paper appear to be 10.1pt for the body text and 9.3pt for the Abstract paragraph:

- a. This initially appeared to be quite unusual as fonts are more normally selectable in whole-number sizes.
- b. However, I found it was consistent with the way that OO2.4 allows fonts styles to be set proportionately by percentage scaling of different sizes.
- c. Using 6pt as the size of the paragraph style named “Default” (which is the smallest reference size that OO2.4 supports), font sizes can be selected as scaled percentages in 5% increments from a normal selection menu, as seen in the screenshot below. Selecting the user-selectable 155% for the abstract paragraph results in a font size matching 9.3pt, and the user-selectable option 170% for the main text results in a font size of 10.1pt (as can also be seen in the screenshot below).



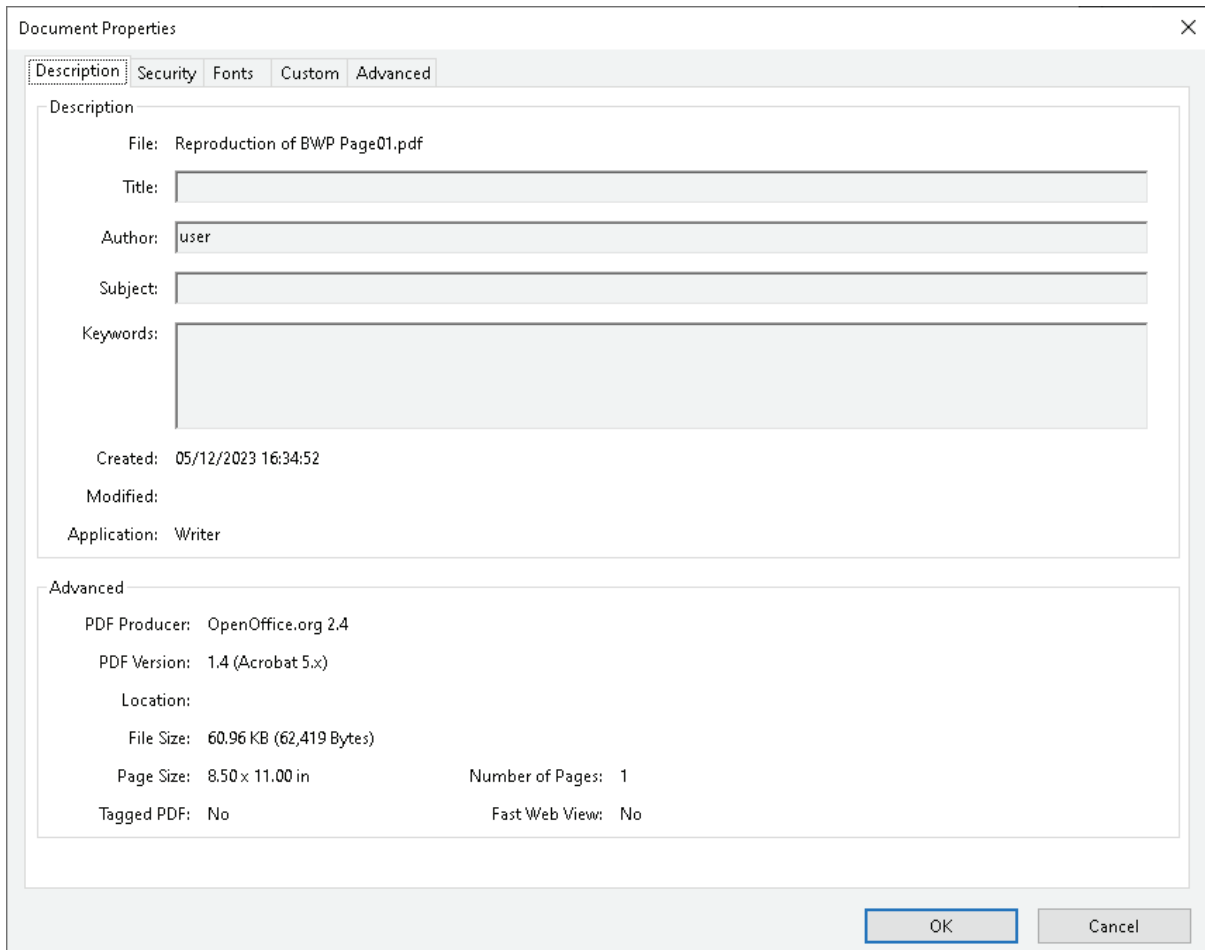
180. This resulted in a document that was almost identical to the first page of the Bitcoin White Paper:



181. OO2.4 Writer has a built-in Export to PDF function that can simply be selected by pressing a button, to create a PDF document.

182. Selecting that resulted in a PDF which I have exhibited that as **Exhibit PM-R3.18** and the ODT is at **Exhibit PM-R3.19**.

183. The Adobe reader properties for the document are consistent with that of the Bitcoin White Paper as seen below, recording an Application of "Writer", and PDF Producer of "OpenOffice 2.4" and a PDF Version of "1.4 (Acrobat 5.x)":



184. The following screenshots compare the output side by side:

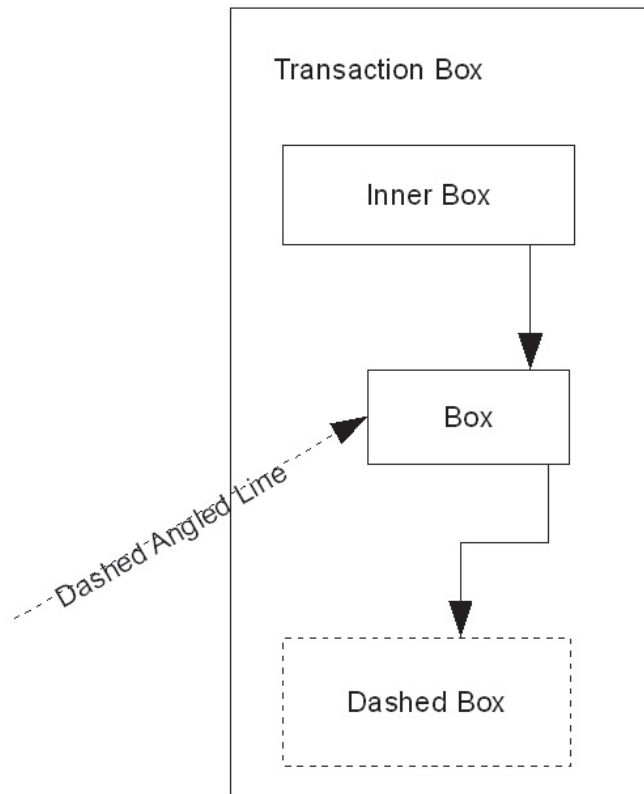
BWP (ID 000226)	Test document
<p data-bbox="268 271 711 293" style="text-align: center;"><b>Bitcoin: A Peer-to-Peer Electronic Cash System</b></p> <p data-bbox="427 320 552 367" style="text-align: center;">Satoshi Nakamoto satoshi@vistomail.com www.bitcoin.org</p> <p data-bbox="280 412 692 618"><b>Abstract.</b> A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.</p> <p data-bbox="233 645 363 663"><b>1. Introduction</b></p> <p data-bbox="233 672 746 851">Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.</p> <p data-bbox="233 853 746 972">What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.</p> <p data-bbox="491 1059 501 1077" style="text-align: center;">1</p>	<p data-bbox="871 259 1315 282" style="text-align: center;"><b>Bitcoin: A Peer-to-Peer Electronic Cash System</b></p> <p data-bbox="1031 309 1155 356" style="text-align: center;">Satoshi Nakamoto satoshi@vistomail.com www.bitcoin.org</p> <p data-bbox="884 400 1295 607"><b>Abstract.</b> A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.</p> <p data-bbox="836 633 967 651"><b>1. Introduction</b></p> <p data-bbox="836 660 1350 840">Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.</p> <p data-bbox="836 842 1350 965">What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.</p> <p data-bbox="1094 1059 1104 1077" style="text-align: center;">1</p>

185. I therefore confirmed that the text and formatting and metadata output of the Bitcoin White Paper was consistent with the ordinary operation of OpenOffice 2.4 Writer, matching the content of the Bitcoin White Paper as well as its metadata.

#### Flowcharts and images within OO2.4

186. Having checked the text output by reference to the first page, I also checked the default functionality of OO2.4's default flowchart diagram drawing.

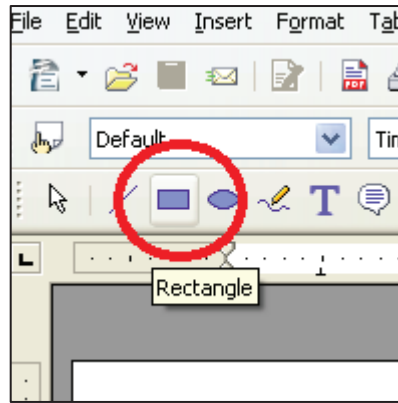
187. OO2.4 Writer provides a standard flowchart-drawing menu allowing users to place shapes, lines, arrows with standard mouse input (and to place typed text labels). I observed that the components created by OO2.4 Writer exactly matched the style and content of the diagrams in the Bitcoin White Paper. I created the below chart to demonstrate some of the default behaviour of that tool:



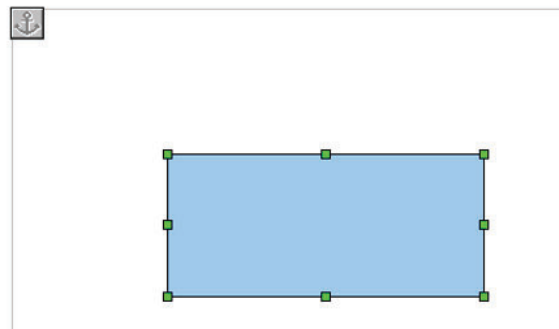
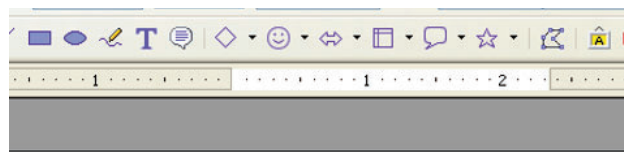
188. I observed that it produced the following in identical styles:

- a. The square boxes with fine borders,
  - b. The arrows at the end of the lines,
  - c. The manner in which the dash lined box behaved in relation to corners, and
  - d. The dashed line at an angle with superimposed text.
- a. These did not require any particular configuration and used the default settings. The following screenshots show the available controls for flowchart objects, which are fairly simple. The program includes a "Draw" toolbar with buttons to select the relevant shapes:





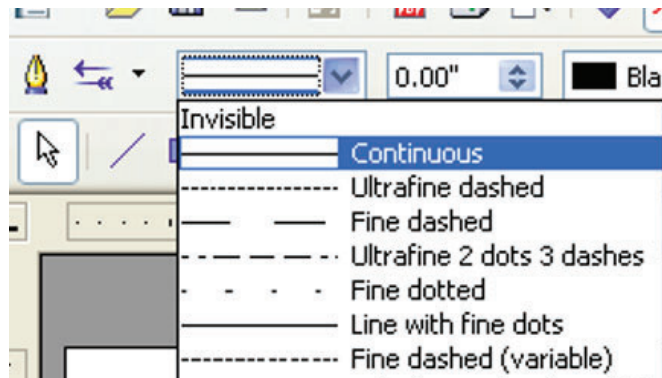
b. Using the button circled above, a rectangle box can be created, then resized or moved around:



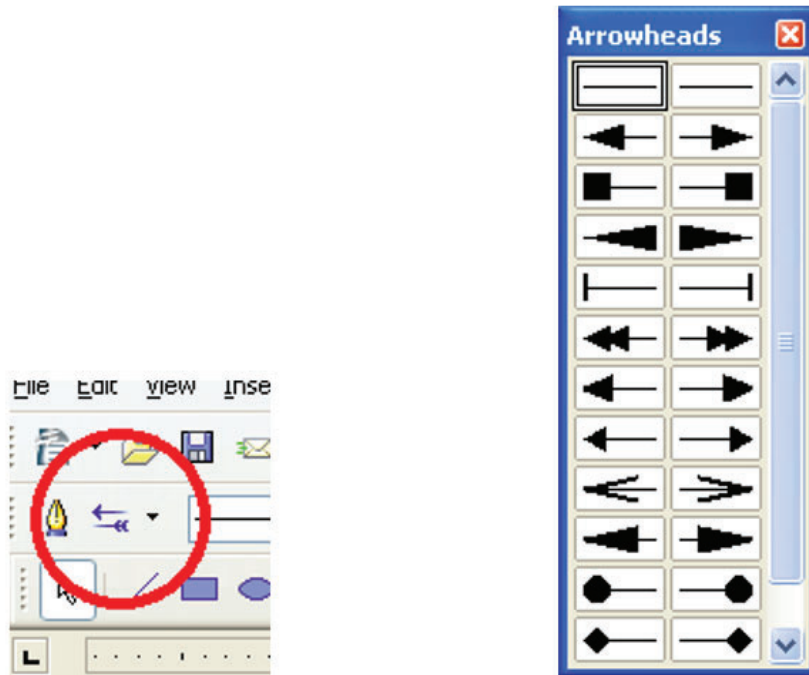
c. The colour can be selected:



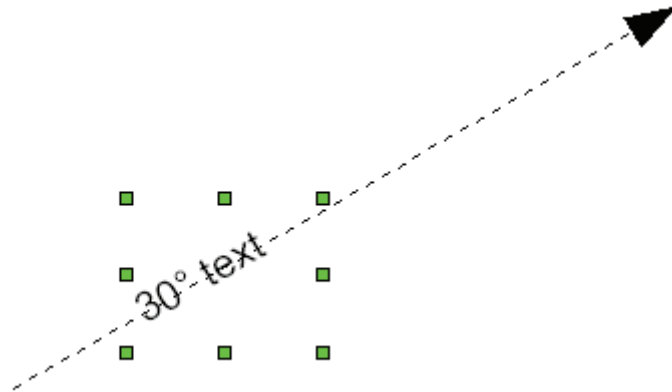
d. The line thickness and colour can also be selected, and using a menu it can be set to dashed:



- e. Arrows can be created with various arrowhead options:

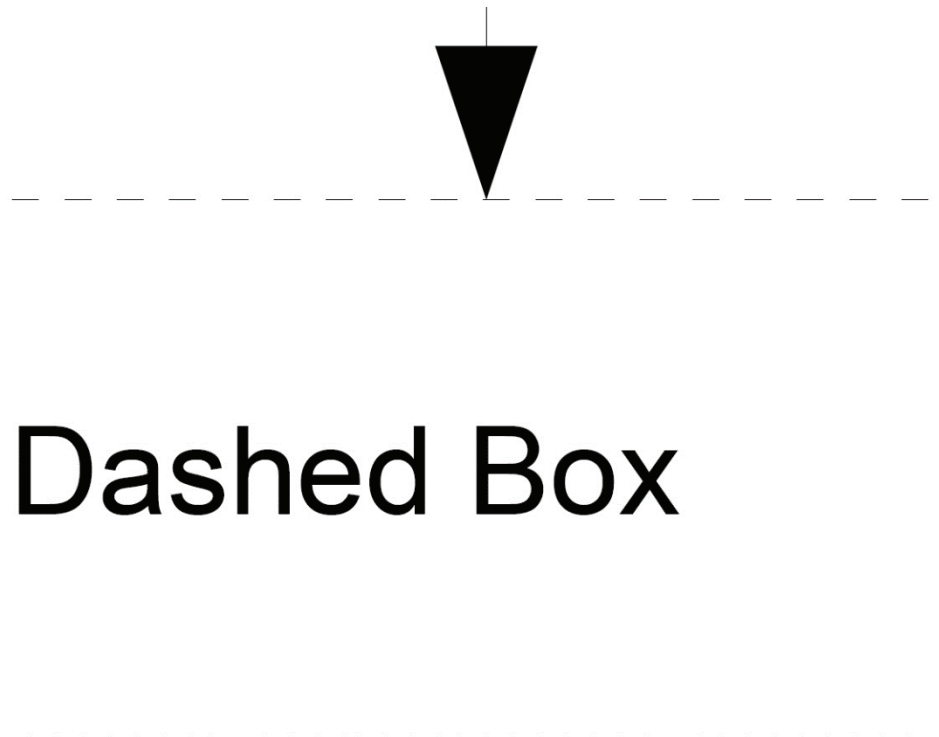


189. I Found the first pair of arrowheads to be a good match for those in the BWP. Arrows can be set to dashed lines in the same way as for boxes and text boxes can easily be added at an angle to overlap them:



190. This is to say that the standard functions built into the OpenOffice version 2.4 Writer application produces the boxes and flow charts that match in character and editing artefacts those found in the BWP.
191. Specifically I observe that when applying a high level of zoom when exported to PDF, the box borders in my diagram behaved in the same way as seen in the Bitcoin White Paper, this being that the border lines remained fine despite the level of zoom applied, and the dashed lines also

wrapped around the corner of boxes in an L shape:



192. A similar sample from the BWP is shown below that shows similar behaviour:



193. I did not try to recreate the diagrams of the Bitcoin White Paper itself because of the very short time available to me to produce this report. I also did not have time to investigate how equations are placed into OO2.4.

Comparative output from a different editor

194. To illustrate how different editors can make subtle differences in output, I also did the same check in Microsoft Word, which I used to open the ODT file. I used Word 2016 and Word 2021 as earlier

versions would not open my ODT file. I then output to a PDF from both versions. The result is at **Exhibit PM-R3.20**. As can be seen, the output is similar but importantly quite different in many technical respects such as:

- a. The font size in the Abstract section, which was adjusted to a whole-integer font size of 9pt
- b. The font size in the Introduction section was adjusted to a whole-integer font size of 10pt.
- c. The font resizing resulted in significant changes to the arrangement of words on the page and locations of line breaks.
- d. The gap between “1.” And “Introduction” was increased
- e. The page number position changed relative to the text on the page.

Conclusion on method of creation of Bitcoin White Paper

195. From the analysis I have conducted,

- a. I conclude that the content of the BWP is consistent with a document authored using the OpenOffice version 2.4 Writer application.
- b. I take into account that “OpenOffice 2.4” and “Writer” are stated on both Control versions, and I have no reason to doubt it is accurate.
- c. Even if there was, I have also confirmed that the PDF output of those versions is consistent with the PDF output of OpenOffice 2.4 Writer.
- d. I have also confirmed that the text output of OpenOffice 2.4 is consistent with the first page of the Bitcoin White Paper, configured using readily-available user settings.
- e. I have also confirmed that the diagrams of the Bitcoin White Paper and their labels are consistent with the default flowchart styles output by OpenOffice 2.4 Writer.

**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: 7/12/2023