IN THE COURT OF..

Queen's Bench Division of The High Court

BETWEEN:

(1) MR JOHN CHRISTOPHER
DEPP II

<div align="right">Claimants</div>

<div align="center">-and-</div>

(1) NGN

(2) Dan Wootton

<div align="right">Defendant</div>

<div align="center">

REPORT OF TIMOTHY JAMES LATULIPPE, MSc

Expertise: Computer & Digital Forensics

On the instruction of: Simons Muirhead & Burton LLP

19th July 2020

</div>

Table of Contents

Introduction

On 18th July 2020 iDiscovery Solutions ("iDS") were instructed by Simons Muirhead & Burton LLP (Defendant's Counsel) via formal letter in an e-mail transmission. The instruction relates to providing forensic analysis and opinion on issues relating to the integrity of select audio and graphic image files (photos).

Central to the claim are several graphic image files dating from May 2016, December 2015 as well as an audio file recording referred to as "the Boston plane audio recording".

Issues Addressed and Statement of Instruction

I was instructed by counsel to address issues relating to the veracity of certain graphic image files and one audio file recording: May 2016 Images, December 2015 Images and Boston Plane Audio Recording, respectively.

As regards point (2) in my initial draft report memorandum and correlating to point (2) in counsel's initial letter of instruction dated 16th July 2020, I was interpreting the request as stated. Specifically, I was instructed to assess whether *metadata* were edited, modified or otherwise manipulated, rather than a question of the photos themselves showing evidence of edits, enhancements or manipulation.

As it relates to a photograph from 21st March 2013 titled, "13.03.21 AH.jpg" disclosed Friday, 10th July, this shows a time of 06:31 AM. A copy showing the same photograph dated 21st March 2013 at 11:31 PM can be explained as a time zone discrepancy.

May 2016 Images
- (a) I was asked to address the ways in which any photo could be edited, enhanced or otherwise manipulated in the native environment of a device, particularly an iPhone handset that would have been in use May 2016.

- (b) I was asked to address —generally speaking —how it would be possible to detect such enhancements, edits or manipulation through data forensic examination.

- (c) I was asked to address —generally speaking —whether images can be edited, enhanced or manipulated in such a way as to later avoid detection through forensic examination, and if so, how?

- (d) I was asked to address with specific reference to the metadata for the May 2016 images, what the probability that those images have been subject to editing, enhancement or manipulation.

- (e) I was asked to address the nature of basis on which any editing, enhancement or manipulation of the above may have occurred.

(f) I was asked to address the basis on which I reached conclusions on both (d) and (e).

December 2015 Images

(g) I was asked to address based on available metadata, the date and times each picture was taken.

(h) I was asked to address with reference to the metadata for the December 2015[1] images, what the probability that those images have been subject to editing, enhancement or manipulation?

(i) I was asked to address the nature of any editing, enhancements or manipulation which have or may have occurred in relation to the December 2015 images.

(j) I was asked to address the basis on which I reached conclusions to (g), (h) and (i) above.

Boston Plane Audio Recording

(k) I was asked to address based on the available metadata, on what date and time was the audio recording made?

(l) I was asked to address my opinion of the probability that this audio recording had been subject to editing, enhancement or manipulation.

(m) I was asked to address the nature of any editing, enhancement or manipulation which has or may have occurred.

(n) I was asked to address the basis on which I reached conclusions to (k), (l) and (m) above.

My Investigation of the Facts

A. Edits, enhancements, or manipulations as regards <u>May 2016 Images</u>

In May 2016, there were three methods by which photos could be edited, enhanced, or manipulated on a device, particularly an Apple iPhone handset.

- One method would use the features that are built into the device operating system. In May 2016, that operating system would have been the Apple iOS version 9.[2] Examples of built in Apple iOS photo editing functionality in version 9 include, but is not limited to, cropping, rotating, red eye reduction, and enhancing (e.g. light enhancement).

---

[1] Note that the 18th July letter of instruction made a reference to December 2016 when in fact December 2015 is the correct period.
[2] Released on 16 September 2015. https://support.apple.com/en-us/HT209441

- Another method would use a third-party application that could be purchased and downloaded to the device from Apple's application store ("App Store")[3]. These applications are submitted to Apple by third-parties and, once vetted by Apple as an approved application, are available for purchase and download. Often, the developers of these applications provide additional photo editing features that are not built into the Apple iOS operating system.

- A third method would require an export of the image from the Apple iPhone handset to another device (e.g. a laptop computer) where the image can be edited by a third-party application (e.g. Adobe Photoshop). As with mobile device applications from the App Store, often the developers of these applications provide additional photo editing features that are not built into the Apple iOS operating system.

B. Detection of edits, enhancements, or manipulations as regards May 2016 Images

- To detect enhancements and forensically investigate whether an image file has been altered or edited, I would first examine the internal metadata fields that are generated by the device used to create the image file. There are hundreds of internal metadata fields including, but limited to, geolocation metadata, camera make/model/lens metadata, and multiple fields that record date and time metadata. I would then analyse all of the internal metadata fields in totality, looking for patterns of metadata updates, such as date/time fields that are out of alignment (e.g. modified after it was created), and additional fields added by editing software and applications, such as IPTC[4] metadata that would be added by applications post-image creation.

C. Avoiding detection as regards May 2016 Images

Internal metadata that I would rely on for a forensic investigation can be theoretically altered and/or removed in an anti-forensic manner. However, this cannot be performed using built-in functionality on an Apple iPhone handset and would require a high level of user sophistication and deep understanding of cameras, computers, and the hundreds of internal metadata fields that are embedded in an image file.

To avoid detection, an individual would have to first create an extraction of the image file in a manner that maintains all image metadata, then use a photo editing application to alter the image, followed by a metadata editing application that can update and/or remove specific internal metadata fields to obfuscate a forensic analysis that would examine the hundreds of metadata fields in totality. This would all have to be performed in a manner that would not alter, edit, or add any new internal metadata fields in the process. In my experience, the average user of an iPhone, even one who

---

[3] https://www.apple.com/ios/app-store/
[4] https://iptc.org/standards/photo-metadata/#:~:text=The%20IPTC%20Photo%20Metadata%20standard,described%20and%20easily%20acce ssed%20later.

creates and/or edits pictures often, does not possess the level of sophistication needed to perform image manipulation anti-forensics and avoid detection.

D. Probability that May 2016 images have been altered.

To determine whether there is evidence that the May 2016 images have been altered, I examined the internal metadata of each image as follows:

- I analysed the internal metadata related to the device that created the images.

- I analysed all internal metadata fields and looked for inconsistencies in the values that could suggest the images were altered, such as modified date metadata that post-dates created data metadata.

- I analysed all metadata fields and looked for evidence of third-party IPTC metadata fields, such as those that are added by Adobe image editing software when an image is altered or edited.

The chart below details the results of my analysis as it relates to the May 2016 images.

Images - Trial Bundle	Device that Created the image	Metadata Inconsistencies	Third Party Metadata Fields
F894.155.JPG	iPhone 6	No	No
F894.157.JPG	iPhone 6	No	No
F894.159.JPG	iPhone 6	No	No
F894.161.JPG	iPhone 6	No	No
F894.163.JPG	iPhone 6	No	No
F894.165.JPG [5]	iPhone 6	Yes	Yes
F894.167.JPG	iPhone 6	No	No
F894.169.JPG	iPhone 6	No	No
F894.171.JPEG	iPhone 6	No	No
F894.173.JPG [6]	iPhone 6	Yes	Yes
F894.175.JPG	iPhone 6	No	No
F894.177.JPG	iPhone 6	No	No
F894.179.JPEG	iPhone 6	No	No
F894.181.JPEG	iPhone 6	No	No
F894.183.JPEG	iPhone 6	No	No
F894.187.JPEG	iPhone 6	No	No
F894.189.JPEG	iPhone 6	No	No
F894.191.JPG	iPhone 6	Yes	Yes
F894.193.JPG	iPhone 6	No	No

[5] This appears to visually be duplicative with no 167.
[6] This appears to visually be duplicative with no 175.

F894.195.JPG	iPhone 6	No	No
F894.216.JPG	iPhone 6	Yes	Yes
F894.218.JPG	iPhone 6	Yes	Yes
F894.222.JPG	iPhone 6	No	No

E. Nature or basis of editing as regards <u>May 2016 Images</u>

The metadata for five of the images I analysed (F894.165JPG, F894.173JPG, F894.191JPG, F894.216JPG, and F894.218JPG) indicate one or more of the following inconsistencies:
- Missing geolocation metadata. Often, editing software can strip Geolocation metadata during the image editing process.

- Incorrect software metadata that does not conform to Apple iOS version 9.

- Addition of third-party metadata fields.

F. How did I reach my conclusion regarding the <u>May 2016 Images</u>

There are eighteen images from May 2016 that do not appear to be altered. This is based on my examination of the internal metadata and the analyses I have detailed in the sections above. Specifically:
- The internal metadata confirms that the images were taken with an iPhone 6 using the Apple iOS version 9 (specifically version 9.3.1)

- The internal metadata confirms that there are no inconsistencies between the date/time metadata fields

- The internal metadata does not include any built-in or third-party editing metadata fields.

There are five images from May 2016 that appear to be altered. To identify whether unedited versions of these five images exist, I examined the following sources of evidence:
- A forensic image of an Apple iPad Pro 10.5" belonging to Ms Amber Heard

- A forensic image of an Apple iPhone X belonging to Ms Amber Heard

From the above two sources, I have extracted unedited copies of four of these five images and include them as annexes to my report. The chart below identifies the unedited copy for each image.[78]

Images - Trial Bundle	Unedited version	Source	Metadata Inconsistencies	Third Party Metadata Fields
F894.165.JPG	8935109A-40CB-4924-90F6-74F823F4E7DD.jpeg	iPhone X NO for both	No	No
F894.173.JPG	24368DF7-9FFD-45AB-BAAE-5EBDD07DE9E2.JPG	iPhone X	No	No
F894.191.JPG	3EDD699D-BD5C-4396-933C-B2AA97F69ED5.jpeg	iPhone X	No	No
F894.218.JPG	E5DE0259-23F3-4005-8981-01CD446A9EB7.JPG	iPad Pro 10.5"	No	No

G. Dates and times for each of the December 2015 Images based on available metadata.

For the December 2015 images, I performed the following analyses to confirm that they were created between 16th December 2015, and 18th December 2015:
- Extracted the internal metadata of the images using two different extraction programmes.
- Reviewed the values for all available internal date/time metadata fields to confirm they match.
- Reviewed the values for all available internal date/time metadata fields to confirm that they have values that indicate the pictures were created on the 16th December 2015, 17th December 2015, or 18th December 2015 and were not modified after they were created.
- For each picture I reviewed the values of all available internal metadata fields to determine if there was any evidence of internal metadata manipulation.

Below is a table listing the images for which I have been able to analyse the internal metadata:

---

[7] Photos from the iPhone X were created on the on or after 20th July 2018. As such, any editing of the trial bundle versions would have been on or after 20th July 2018.
[8] Photos from the iPad Pro 10,5" were created on or after 6th October 2018. As such, any editing of the trial bundle versions would have been on or after 6th October 2018.

December 2015 Image - Filename	ExifIFD:DateTimeOriginal
F894.095 - ALH_00001586.JPEG	2015:12:16 10:41:03
F894.097 - ALH_00000505.JPEG	2015:12:16 10:58:58
F894.099 - ALH_00000509.JPEG	2015:12:16 10:57:10
F894.101 - ALH_00000517.JPEG	2015:12:16 10:41:26
F894.103 - AHA_00000002.JPEG	2015:12:16 14:39:48
F894.105 - AHA_00000003.JPEG	2015:12:16 14:39:56
F894.107 - AHA_00000004.JPEG	2015:12:16 14:40:40
F894.109 - AHA_00000005.JPEG	2015:12:16 14:40:44
F894.112 - AHA_00000006.JPEG	2015:12:16 14:40:54
F894.114 - AHA_00000008.JPEG	2015:12:16 14:41:18
F894.118 - ALH_00000515.JPEG	2015:12:16 11:44:13
F894.120 - AHA_00000028.JPEG	2015:12:16 11:44:00
F894.122 - AHA_00000027.JPEG	2015:12:16 10:56:58
F894.124 - ALH_00000511.JPEG	2015:12:16 14:41:02
F894.132 - AHA_00000010.JPEG	2015:12:17 00:46:09
F894.134 - AHA_00000011.JPEG	2015:12:17 00:46:16
F894.136 - AHA_00000012.JPEG	2015:12:17 00:46:17
F894.139 - AHA_00000013.JPEG	2015:12:17 00:46:26
F894.141 - AHA_00000014.JPEG	2015:12:17 10:19:46
F894.143 - AHA_00000015.JPEG	2015:12:17 10:19:52
F894.145 - AHA_00000016.JPEG	2015:12:17 10:20:41
F894.147 - AHA_00000007.JPEG	2015:12:18 14:40:55

H. Edits, enhancements, or manipulations as regards December 2015 Images

The three methods by which photos could be edited, enhanced, or manipulated on a device, particularly an Apple iPhone handset, in May 2016 are the same three methods by which photos could be edited, enhanced, or manipulated in December 2015. This is because the same operating system would have been in use - the Apple iOS version 9.[9] As such, I follow the same analyses for the December 2015 images.

To determine whether there is evidence that the December 2015 images have been altered, I examined the internal metadata of each image as follows:

- I analysed the internal metadata related to the device that created the images.

- I analysed all internal metadata fields and looked for inconsistencies in the values that could suggest the images were altered, such as modified date metadata that post-dates created data metadata.

---

[9] Released on 16 September 2015. https://support.apple.com/en-us/HT209441

- I analysed all metadata fields and looked for evidence of third-party IPTC metadata fields, such as those that are added by Adobe image editing software when an image is altered or edited.

The chart below details the results of my analysis as it relates to the December 2015 images.

December 2015 Image - Filename	Device that Created the image	Metadata Inconsistencies	Third Party Metadata Fields
F894.095 - ALH_00001586.JPEG	iPhone 6	Yes	Yes
F894.097 - ALH_00000505.JPEG	iPhone 6	Yes	Yes
F894.099 - ALH_00000509.JPEG	iPhone 6	Yes	Yes
F894.101 - ALH_00000517.JPEG	iPhone 6	Yes	Yes
F894.103 - AHA_00000002.JPEG	iPhone 6	Yes	Yes
F894.105 - AHA_00000003.JPEG	iPhone 6	Yes	Yes
F894.107 - AHA_00000004.JPEG	iPhone 6	Yes	Yes
F894.109 - AHA_00000005.JPEG	iPhone 6	Yes	Yes
F894.112 - AHA_00000006.JPEG	iPhone 6	No	No
F894.114 - AHA_00000008.JPEG	iPhone 6	No	No
F894.118 - ALH_00000515.JPEG	iPhone 6	Yes	Yes
F894.120 - AHA_00000028.JPEG	iPhone 6	Yes	Yes
F894.122 - AHA_00000027.JPEG	iPhone 6	Yes	Yes
F894.124 - ALH_00000511.JPEG	iPhone 6	Yes	Yes
F894.132 - AHA_00000010.JPEG	iPhone 6	Yes	Yes
F894.134 - AHA_00000011.JPEG	iPhone 6	Yes	Yes
F894.136 - AHA_00000012.JPEG	iPhone 6	Yes	Yes
F894.139 - AHA_00000013.JPEG	iPhone 6	Yes	Yes
F894.141 - AHA_00000014.JPEG	iPhone 6	Yes	Yes
F894.143 - AHA_00000015.JPEG	iPhone 6	Yes	Yes
F894.145 - AHA_00000016.JPEG	iPhone 6	Yes	Yes
F894.147 - AHA_00000007.JPEG	iPhone 6	Yes	Yes

I. Nature of any edits, enhancements or manipulation that may or has occurred in relation to the December 2015 images

The metadata for 20 of the December 2015 images I analysed indicates one or more of the following inconsistencies:
- Missing geolocation metadata. Often, editing software can strip Geolocation metadata during the image editing process.

- Incorrect software metadata that does not conform to Apple iOS version 9.

- Addition of third-party metadata fields.

J. The basis on which I reached conclusions to (G), (H) and (I) above.

There are two images from December 2015 that do not appear to be altered. This is based on my examination of the internal metadata and the analyses I have detailed in the sections above. Specifically:
- The internal metadata confirms that the images were taken with an iPhone 6 using the Apple iOS version 9 (specifically version 9.2)

- The internal metadata confirms that there are no inconsistencies between the date/time metadata fields

- The internal metadata do not include any built-in or third-party editing metadata fields.

To identify whether unedited versions of the twenty other December 2015 images exist, I examined the following sources of evidence:
- A forensic image of an Apple iPad Pro 10.5" belonging to Ms Amber Heard

From the above source, I have extracted unedited copies[10] of 18 of these twenty images and include them as annexes to my report. The chart below identifies the unedited copy for each image.[11]

December 2015 Image - Filename	Unedited version	Source	Metadata Inconsistencies	Third Party Metadata Fields
F894.095 - ALH_00001586	5D3C8B2B-2446-45C0-A979-5F4D012969CA.JPG	iPad Pro 10.5"	No	No
F894.097 - ALH_00000505	D111845D-08E4-4C61-BA11-AFE5E354B087.JPG	iPad Pro 10.5"	No	No
F894.099 - ALH_00000509	00DFB1C8-A44D-441C-99B9-7CFE312365DA.JPG	iPad Pro 10.5"	No	No
F894.103 - AHA_00000002	IMG_0008.JPG	iPad Pro 10.5"	No	No
F894.107 - AHA_00000004	IMG_0009.JPG	iPad Pro 10.5"	No	No
F894.109 - AHA_00000005	IMG_0147.JPG	iPad Pro 10.5"	No	No

---

[10] Note: a lack of Geolocation specific metadata as a feature is not a pure indication that an image has been altered.

[11] Photos from the iPad Pro 10,5" were created on or after 6th October 2018. As such, any editing of the trial bundle versions would have been on or after 6th October 2018.

F894.116 - AHA_00000009	IMG_0153-2.JPG	iPad Pro 10.5"	No	No
F894.118 - ALH_00000515	1B8B2F6E-FFF1-4B9C-9A4D-C70BA197C72B.JPG	iPad Pro 10.5"	No	No
F894.120 - AHA_00000028	IMG_3322.JPG	iPad Pro 10.5"	No	No
F894.122 - AHA_00000027	D05A6D9A-696D-4BBB-93A7-6733CE1AFBE1.JPG	iPad Pro 10.5"	No	No
F894.124 - ALH_00000511	IMG_0150.JPG	iPad Pro 10.5"	No	No
F894.132 - AHA_00000010	IMG_0173.JPG	iPad Pro 10.5"	No	No
F894.132 - AHA_00000011	5AA0DCA7-645E-4D9C-A5A4-6F504FFC708A.JPG	iPad Pro 10.5"	No	No
F894.132 - AHA_00000012	6D37E3B2-9670-4704-AE7C-05B5BD819DA9.JPG	iPad Pro 10.5"	No	No
F894.139 - AHA_00000013	IMG_0177.JPG	iPad Pro 10.5"	No	No
F894.141 - AHA_00000014	IMG_0180.JPG	iPad Pro 10.5"	No	No
F894.143 - AHA_00000015	IMG_0181.JPG	iPad Pro 10.5"	No	No
F894.145 - AHA_00000016	IMG_0182.JPG	iPad Pro 10.5"	No	No

K. Based on available metadata, on what day and time was the <u>Boston Plane Audio Recording</u> made.

- The audio file was created on 25th May 2014, 02:11[12] UTC (no daylight savings applied internally).

- This consists of the date and time when the audio file commenced recording and when it stopped, and subsequently the actual writing of the audio file, relative to its *duration* (11 minutes, 39 seconds).

    i. The audio track began recording on 24th May 2014 at 21:00:03 Boston time (-05:00 EDT offset).

    ii. If the 05:00 hours are added back in to normalise to UTC, this becomes 25th May 2014 at 02:00:03.

    iii. If you then account for the *duration* of the track (11 minutes, 39 seconds), the overarching date of creation for the audio file comes

---

[12] An e-mail from counsel that references the Boston plane audio as F894.277, *F148j. Boston Plane Freakout Incident Properties* shows the media created as 25th May 2014 at 03:11, precisely 1 hour ahead of the correct date. The reason for this 1-hour discrepancy is that the Windows computer interpreting those metadata are applying a +1 Summertime/daylight savings time bias when it reads that field and reports it.

back to 25th May 2014 at 02:11:42, which is short by 3 seconds. This is explained by the delay on the original iPhone handset stopping the audio track and writing the ultimate audio file (time to compute). This is 21:11:42 on 24th May *Boston Time.*

    iv. Generally speaking, mobile phones that are active in non-connectivity zones (e.g. up in the air), retain their date and time clock settings of their source until the point of next connectivity (e.g. landing in another time zone).

L. Probability that the Boston Plane Audio Recording has been subject to editing, enhancement or manipulation.

- The probability that the audio file was subject to any editing is very low. The maths and pattern of metadata seen above from a source device containing this audio file does not show any anomalous data points. Additionally, there was very little built-in capability to edit audio recordings on an iPhone 4s – limited to audio track length trim functions - and I do not see any third-party editing metadata in this audio recording.

M. The nature of any editing, enhancement or manipulation which has or may have occurred.

- I have not seen any patterns or indications that this audio file was edited, enhanced or in some way manipulated.

N. Basis on which I reached a conclusion on (K), (L) and (M) above.

- I was able to locate an historic copy of the audio recording on a forensic backup copy of an iPhone 4s belonging to Amber van Ree.

- This audio recording file analysed was from the backup copy from its earliest available location.

Statements

Statement of Compliance

I understand my duty as an expert witness is to the court. I have complied with that duty and will continue to comply with it. This report includes all matters relevant to the issues on which my expert evidence is given. I have given details in this report of any matters which might affect the validity of this report. I have addressed this report to the court. I further understand that my duty to the court overrides any obligation to the party from whom I received instructions.

Statement of Conflicts

I confirm that I have no conflict of interest of any kind, other than any which I have already set out in this report. I do not consider that any interest which I have disclosed affects my suitability to give expert evidence on any issue on which I have given evidence and I will advise the party by whom I am instructed if, between the date of this report and the trial, there is any change in circumstances which affects this statement.

Declaration of Awareness

I confirm that I am aware of the requirements of Part 35 and Practice Direction 35, and the Guidance for the Instruction of Experts in Civil Claims 2014.

Signature ....

Date 19th ....

Statement of truth

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.

Signature ...

Date 19th July 2020 ....

My Experience and Qualifications

I am a Director and co-head of the iDS Europe practice. My professional background is that of a data forensic examiner and investigative technologist. I have worked on data forensic matters for thirteen years in both North America and Europe. I hold an advanced degree in Data Forensic Science and Management (MSc) and a university qualification in Computer & Digital Forensics (BSc). I also serve as an expert advisor on leveraging technology in eDisclosure matters in and around litigation, internal compliance and investigations, as well as investigations driven by regulatory authorities.

I have worked on hundreds of matters involving the investigation of electronic information including, but not limited to: theft of intellectual property, trade secret theft and misappropriation, document and e-mail falsification, insider trading, price rigging, OFAC violations, FCPA and employment matters relating to team moves and violations of restrictive covenants.

I have testified in live proceedings in America in Federal, State and Military venues, in addition to taking part in depositions and the filing of affidavits, declarations and expert reports. In England I have provided expert evidence in the form of witness statements and reports.

I am a frequent speaker and author on issues relating to electronic disclosure and investigative technology. I am also a member of several data forensic specific consortia including: The International Society of Forensic Computer Examiners (ISFCE), The High-Tech Crime Consortium (HTCC), The International Association of Computer Investigative Specialists (IACIS) and the Digital Forensic Certification Board (DFCB), of which I am a board member. I hold software specific certifications in Encase Forensic (ENCE) Cellebrite mobile phone forensics (CCPA). I hold non-software specific certifications as a Certified Computer Examiner (CCE #887), as well as certified Mac and iOS Certified Forensic Examiner (MiCFE) from Blackbag Technologies.

Experience and Qualifications of Others Involved in Testing

I was assisted by iDS colleague and data forensic expert, Mr Julian Ackert. Julian is a Managing Director at iDiscovery Solutions ("iDS"), an expert services and consulting firm that provides independent computer forensics, electronic discovery expert testimony and analysis, original authoritative studies, and strategic consulting services to the business and legal community.

He has over 20 years of experience in consulting and litigation technologies that focus on electronic discovery and computer forensics. He holds a Bachelor of Science degree in Computer Science from the University of Virginia.

Specifically, he has extensive experience creating and implementing preservation, collection, and production strategies and performing computer forensics and metadata analysis on electronic data.

He has performed preservation, collection, analysis, and production of electronically stored information ("ESI") in hundreds of matters. He has also provided testimony in several cases, some of which are described below:

a) The analysis of document metadata and computer forensic issues in an employee breach of contract case for the financial industry;

b) The analysis of document metadata and computer forensic issues in employee theft-of-trade-secrets case in the healthcare industry; and

c) The analysis of document metadata and computer forensic issues in employee theft-of-trade-secrets case in the transportation industry.

d) The analysis of document metadata and computer forensic issues in employee theft-of-trade-secrets case for the high-technology industry.

Statement of Methodology

I was able to examine the documents discussed herewith by utilising both professionally licenced and open-source, freely available data forensic software and techniques. My methodology for examining the internal metadata available for the files included the use of more than one tool as a means of cross validation.

I was able to review and analyse different copies of the files in question as either duplicates of the images and audio from disclosure, the original source devices housing the files, or later release versions of devices containing data from older devices no longer available.

I was able to perform cause and effect testing on test data not related to this matter that matched the variables of time and type of files being considered.

List Documents or Data I have Examined

May 2016 Images

Images -Trial Bundle
F894.155JPG
F894.157JPG
F894.159JPG
F894.161JPG
F894.163JPG
F894.165JPG
F894.167JPG
F894.169JPG
F894.171JPEG
F894.173JPG
F894.175JPG
F894.177JPG
F894.179JPEG
F894.181JPEG
F894.183JPEG
F894.187JPEG
F894.189JPEG
F894.191JPG
F894.193JPG
F894.195JPG
F894.216JPG
F894.218JPG
F894.222JPG

December 2015 Images

December 2015 Image
F894.095 - ALH_00001586JPEG
F894.097 - ALH_00000505JPEG
F894.099 - ALH_00000509JPEG
F894.101 - ALH_00000517JPEG
F894.103 - AHA_00000002JPEG
F894.105 - AHA_00000003JPEG
F894.107 - AHA_00000004JPEG
F894.109 - AHA_00000005JPEG
F894.112 - AHA_00000006JPEG
F894.114 - AHA_00000008JPEG

F894.118 - ALH_00000515JPEG
F894.120 - AHA_00000028JPEG
F894.122 - AHA_00000027JPEG
F894.124 - ALH_00000511JPEG
F894.132 - AHA_00000010JPEG
F894.134 - AHA_00000011JPEG
F894.136 - AHA_00000012JPEG
F894.139 - AHA_00000013JPEG
F894.141 - AHA_00000014JPEG
F894.143 - AHA_00000015JPEG
F894.145 - AHA_00000016JPEG
F894.147 - AHA_00000007JPEG

Boston Plane Audio Recording

"recordings/file_1/20140524 210003.m4a" (Source: iPhone 4s Backup)

Sources of Evidence

Evidence
Forensic extraction of an Apple iPad Pro 10.5"
Forensic extraction of an Apple iPhone X
Forensic backup of an iPhone 4s

Glossary of Technical Terms

Images: these refer to graphic image files, or "photographs".

Audio recording: refers to an audio recording made electronically by a mobile phone or computing device.

Voice Memo: refers to an audio recording made electronically by a mobile phone or computing device.

Metadata: refers to the "data about data". These are information points within electronic files that store dates, times, authorship, devices used to print or make photos and much more.

EXIF Metadata: refers to a specific type of metadata that is commonly used for audio/visual type electronic files such as audio, video and graphic image files.

IPTC Metadata: Refers to a sub-type of metadata created for use in digital photography and stands for "International Press Telecommunications Council.

Operating System: The basic, baseline software that powers a computer or mobile tablet or handset (e.g. Microsoft Windows, or Apple iOS for iPhones)

Annexes

A. Actual photos for printing by Counsel provided as actual photo files in a ZIP file.