Appendix 2: The searches at the Iraq Historical Allegations Team (IHAT)

SOFTWARE – Access Data Lab & ECA Viewer

1. The software used by the IHAT was supplied by 'Access Data', a software company specialising in computer forensics. 'Access Data Lab' forensically processes the data onto the FDHC. The software used by the Inquiry to view the processed data was initially AD LAB and later an interface to 'LAB' known as 'Early Case Assessment Viewer' or 'ECA'.

2. AD LAB provides various methods of searching a Case each with its own benefits. One such method is in 'Explorer mode'. AD LAB displays the directory structure of the Case as a hierarchical file system (that is, one in which files and directories are organized in a manner that resembles a tree). A directory contained inside another directory is called a subdirectory. In this way a file can be manually found, its location within the directory structure established and all surrounding documents reviewed.

3. Another method provided by the AD LAB interface is to examine documents by type via the 'Overview mode'. This renders it possible to differentiate files by specific file extensions allowing a review of for instance, just Word documents or spreadsheets. Email mode separates all emails allowing them to be reviewed by dates, if the embedded metadata has been recovered by AD LAB during the processing phase, including an overview of how many emails were sent (or received, if applicable) by day, month and year.

4. AD LAB also allows the review of all images as thumbnails in 'Graphic mode'. This mode excludes any document that does not meet the necessary requirements to be an image. Therefore files with the extension of jpg, gif, etc would be included while Word and Excel files would not. The main operating system files would not be included but the small icon files contained within an operating system would be. Adobe pdf documents are recognized as images. The list of what would be included and what excluded is vast and not for this report. Where a full size image was available the thumbnail image could be opened up to full size if required.

5. Utilising 'Email Mode' allows files to be examined by sub mode as categorised by AD LAB.

    a. 'Email' which was then categorised down via various sub type of message or action i.e. appointment, contact or distribution list etc.

    b. 'Email Status' identified emails by being sent, received replied or forwarded or whether attachments were included.

    c. 'Email Archives' identified any pst (personal storage table) files or pab (personal address book) type files. These files are in effect storage areas normally found on a local machine as opposed to a server used to archive messages and calendar events as created by a user operating Microsoft Exchange programs.

    d. 'Email Address' provided details of senders and recipients email addresses, domains and display names.

    e. 'Email by Date' enabled the searching of emails by a specific sent or received date.

6. The most useful method of searching in AD LAB is via an Indexed search whereby a complex search string can be constructed with the addition of Boolean operators (AND, OR, NOT and NEAR) having the effect of limiting, widening or in other ways defining the parameters of the search. The results are displayed and can be sorted by type, size, date etc and then reviewed individually for relevance. Once the documents have been reviewed they can be labelled so any subsequent search will identify files already examined.

7. In some instances the result of searches provided very high numbers of documents and files being returned. When this occurred additional filtering was employed to eliminate irrelevant documents while ensuring a thorough search was still conducted. To this end the following was employed.

a. An additional filter was applied restricting the returned documents to have a modified date found within the documents embedded 'metadata', to be within a defined range. The date range applied was designed to encompass the period prior to the incident on 14 May 2004 and the release of the detainees from the DTDF to the Iraqi penal system, accordingly the date range applied was 01 May 2004 to 01 October 2004.

b. The filter was created utilising the modified date of a document which captures the last date and time a document was saved. The action of copying and moving documents between computers can have the effect of generating creation dates for documents and files that post date the modified date. As such utilising the creation date for a filter can provide misleading results.

c. As multiple filters could be applied simultaneously an additional filter was applied to ensure a search included in the results any document where no date was recorded within the metadata. An additional filter was also applied that eliminated any document where the 'logical size' recorded by AD LAB was empty indicating no actual data was available for inspection. All files have a physical and logical size, often the physical size is larger than the logical size due to the way data is stored on a hard drive. The logical size is the actual size of the data while the physical size is the space required on a hard drive to store the data.

d. The documents returned by the search were then reviewed by reference to aspects of those documents to form an initial view on potential relevance. The document title in many instances could provide sufficient indications as to what was contained within the body of the document. An example of this effect was while searching for emails where the name 'Curry' was included resulted in substantial returns regarding a 'curry club'. The document title if referencing operational documents such as Assessreps and Sincreps enabled the identification of duplicates which did not require examination.

e. Once a document was identified as requiring further examination it could be opened using various views. Natural view allowed the close scrutiny of a document's content in its native format i.e. as a complete word document. In text view the document could be examined without any formatting. This was often the main view utilised when a document was incomplete. Finally it was possible to examine the contents of a file or document in hexadecimal view providing sight into the raw data that constituted the file. This was necessary when a file was so badly corrupted or overwritten that natural or text view failed to show the files content.

8. AD LAB provides full audit capability creating a report during the download process providing details of the exhibits used to create the case along with the location of documents found within the reconstructed hard drives that made the RAID. It is also possible to create an event

log in Excel spreadsheet format, which captures all activity undertaken by the Inquiry staff during the search

Explanation of a RAID

9. The term RAID was first used by David Patterson, Garth A. Gibson, and Randy Katz at the University of California, Berkeley in 1987, standing for a redundant array of inexpensive disks. Industry RAID manufacturers interpreted the acronym as standing for a redundant array of independent disks. The term RAID is now used as a simple term to describe computer data storage schemes that divide and replicate data among multiple physical hard drives allowing the operating system to access the contained data as one single drive.

10. There are various types of RAID schemes. These are identified by the word RAID followed by a number for example RAID 0, RAID 1 etc. In 2004 the most cost effective and efficient system was RAID 5 which required a minimum of three separate hard drives to construct the RAID. Taking a RAID 5 as an example, if only a single drive from the RAID was now available, any data recovered would be incomplete; if two or more drives were available the data could be recovered intact.

Liverpool Case

11. Research identified the following hard drives that had constituted the Liverpool Server as used in Camp Abu Naji in 2004. Five were compiled as a RAID system acting as the 'exchange server' and was named 'Liverpool 1'. The remaining five hard drives were compiled as a separate RAID system acting as the 'file & print server'. This server was named 'Liverpool 2'. Each server had its own 'Internet Protocol' address (IP) indicating they were both connected to a network. By the time the Liverpool server was removed from Camp Abu Naji in June 2006 Liverpool 1 and 2 had increased in size to six drives comprising each RAID.

12. It was possible to identify and track each of the hard drives that constituted the Liverpool server through documentation found within the FDHC. These documents, while of value as research tools, have not been disclosed as part of the Inquiry process. In 2004 each of the hard drives that comprised Liverpool 1 and 2 were referenced on spreadsheets by individual unique reference numbers. Details were included of the role or purpose for each server providing support to the camp as storage or as the email, calendar and contact client for the military INET system.

13. By 2006, a separate spreadsheet highlighting computer assets at Camp Abu Naji identified the reference numbers had changed and were then classed as asset numbers. By April 2009 the asset numbers were listed alongside manufacturers hard drive reference numbers.

Liverpool 1 Drive 1 (IHAT JRY-68-C)

14. The first hard drive that constituted part of the RAID named as Liverpool 1 in 2004 was identified by a serial number (*****3/081). The drive was traced through documentation to being allocated an asset number in 2006 (****6079) to a manufacturers reference number in 2009 (*****2F9M). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-68-C.

Liverpool 1 Drive 2 (IHAT JRY-68-A)

15. The next hard drive that constituted part of the RAID named as Liverpool 1 in 2004 was identified by a serial number (*****3/082). The drive was traced through documentation to being allocated an asset number in 2006 (****6024) to a manufacturers reference number in 2009 (*****1J2M). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-68-A.

Liverpool 1 Drive 3 (IHAT JRY-68-F)

16. The next hard drive that constituted part of the RAID named as Liverpool 1 in 2004 was identified by a serial number (*****3/083). The drive was traced through documentation to being allocated an asset number in 2006 (****6062) to a manufacturers reference number in 2009 (*****11SM). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-68-F.

Liverpool 1 Drive 4 (IHAT JRY-68-E)

17. The next hard drive that constituted part of the RAID named as Liverpool 1 in 2004 was identified by a serial number (*****3/084). The drive was traced through documentation to being allocated an asset number in 2006 (****6031) to a manufacturers reference number in 2009 (*****2FQM). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-68-E.

Liverpool 1 Drive 5 (IHAT JRY-68-B)

18. The last hard drive that constituted part of the RAID named as Liverpool 1 in 2004 was identified by a serial number (*****3/085). The drive was traced through documentation to being allocated an asset number in 2006 (****6055) to a manufacturers reference number in 2009 (*****0X3M). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-68-B.

Liverpool 2 Drive 1 (IHAT JRY-69-E)

19. The first hard drive that constituted part of the RAID named as Liverpool 2 in 2004 was identified by a serial number (*****3/086). The drive was traced through documentation to being allocated an asset number in 2006 (****6130) to a manufacturers reference number in 2009 (*****N1RM). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-69-E.

Liverpool 2 Drive 2 (IHAT JRY-69-C)

20. The next hard drive that constituted part of the RAID named as Liverpool 2 in 2004 was identified by a serial number (*****3/087). The drive was traced through documentation to being allocated an asset number in 2006 (****6123) to a manufacturers reference number in 2009 (*****1WYM). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-69-C.

Liverpool 2 Drive 3 (IHAT JRY-69-B)

21. The next hard drive that constituted part of the RAID named as Liverpool 2 in 2004 was identified by a serial number (*****3/088). The drive was traced through documentation to being allocated an asset number in 2006 (****6109) to a manufacturers reference number in 2009 (*****265M). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-69-B.

Liverpool 2 Drive 4 (IHAT JRY-69-F)

22. The next hard drive that constituted part of the RAID named as Liverpool 2 in 2004 was identified by a serial number (*****3/089). The drive was traced through documentation to being allocated an asset number in 2006 (****6116) to a manufacturers reference number in 2009 (*****2NKM). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-69-F.

Liverpool 2 Drive 5 (IHAT JRY-69-D)

23. The last hard drive that constituted part of the RAID named as Liverpool 2 in 2004 was identified by a serial number (*****3/090). The drive was traced through documentation to being allocated an asset number in 2006 (****6093) to a manufacturers reference number in 2009 (*****5A24). Research identified the hard drive seized by IHAT was 36.4GB in size, was part of a RAID 5 and was referenced as exhibit JRY-69-D.

24. Examination of the Liverpool Case using Overview Mode[5210] identified that the case contained 180,000 word type documents, 9,000 spreadsheets, 8,000 databases, 56,000 emails, 220,000 images and nearly 300,000 unallocated items sat within 'slack/free space' indicating they had been previously been deleted and were occupying hard drive space that the filing system could utilise to store new documents, in effect overwrite. The remaining items consisted of 15,000 archive files from which the above files had been extracted, operating system files and folders and 560,000 items that AD Lab had been unable to categorise.

25. Searching for specific documents using an indexed search[5211] resulted in locating a place holder for a deleted file (created by AD LAB) whereby only a footprint was left within the 'Master File Table' (MFT). This record indicated that the file had once existed along with its last location in the directory tree. Often no actual text or metadata (date/time etc) was recoverable. Occasionally a search would lead to a deleted file, where the MFT located the document title, but the remaining readable data was for a completely different document. It was therefore necessary to adjust the methodology whereby a combination of approaches was adopted.

26. This new approach entailed a mixture of Indexed and Explorer[5212] searching. The Index search would take the ASI investigator to an area of the file directory which would then enable any other readable documents or place holders in the location to be examined. While not as focused as pure Index searching, the combination of these techniques ensured that potentially relevant file locations and their contents were reviewed for relevance. One such directory found within an Archive directory labelled 'PWRR File List' was examined in its entirety.

[5210] Paragraph 3
[5211] Paragraph 6
[5212] Paragraph 2

27. As AD LAB was able to differentiate files by type, all emails, graphics and multimedia files were manually searched and examined in their entirety. The majority of files identified as relevant were found either within unallocated space (hard drive storage that has been identified by the MFT as available to be written to), within a deleted archive folder for a member of Telic 6 or as pure text buried within large files. These large files were created by AD LAB from recovered data where the software was not able to determine a file type due to the state of the data. When documents etc were found within unallocated space AD LAB allocated the recovered data a title of 'carved' along with a unique reference number. Often the file would retain a file extension appropriate to the type of document e.g. carved [123456].doc.

28. Searching of the 56,000 email items was conducted utilising Email Mode.[5213] Examination of emails sent and received in May 2004 indicated nearly 5,000 items, but closer examination identified most were not actual emails but were in the majority, system generated files indicating either an 'oversized mail box' or the failure to send a message. Of the 35 items found to have been sent or received on the 14 May or the 92 items sent or received on the 15 May only the weather forecast for the day was of any relevance to the inquiry. No email traffic relating to the events subject to the Inquiry's terms of reference were found utilising this method.

29. Of note was the fact that between 14 April 2004 and 21 May 2004 no emails were replied to. Also from 25 April 2004 to 15 September 2004 only 41 emails were forwarded on from one recipient to another. These figures helped emphasise the apparent lack of email traffic on the Liverpool Server.

30. The Inquiry is in possession of both the AD LAB report and event log[5214] following the search of the Liverpool Case. From the event log the indexed search terms were extracted to a separate spreadsheet for later use.

Sensitive Case

31. The Sensitive Case was constructed from 27 separate exhibits seized by IHAT from Military Intelligence Units:

JP-4, JP-1,	MPG-1,	SLJ-29-391,	MPG-2,	SLJ-29-390,	JP-3,
SLJ-29-392,	SLJ-29-394,	SLJ-29-393,	SLJ-29-396,	SLJ-29-395,	SLJ-29-397,
SLJ-29-398,	SLJ-29-399,	SLJ-29-400,	SLJ-29-401,	SLJ-29-393,	SLJ-29-402,
NGT-11,	NGT-4,	NGT-5,	NGT-10,	NGT-8,	
NGT-6,	NGT-7,	NGT-9,			

32. The Sensitive case when examined in Overview mode, identified over 1 million Microsoft Office (Word, Excel, Access etc) type documents. There were over 2 million separate images. Both of these figures could be substantially reduced by the application of filters[5215] built into AD LAB which helped remove any known system files and duplicates from the final results. This reduced the documents down to 566,000 and the images to 424,000 that required some level of searching and subsequent review. Very few email related items were identifiable in Email mode, suggesting that none of the 27 exhibits used to create the case were part of an exchange server, but were used as storage areas. Fourteen of the exhibits were identifiable

[5213] Paragraph 5
[5214] Paragraph 8
[5215] Paragraph 7

by size as hard drives, while the remaining exhibits appeared to be a combination of CDs and DVDs.

33. The same approach was applied to the search and review of the Sensitive Case as for the Liverpool Case. Indexed searching, to first identify the location of potentially relevant material, was followed by searching all files within the directory and any sub directories thereby identified. As the indexed searches continually pointed to the same directories on a few exhibits it was decided that each of the 27 exhibits used to create the Sensitive Case would be examined separately to establish the type of material each contained. It was considered that this was the best method for minimising the risk of anything relevant being missed. All images and multimedia files were reviewed for relevance.

34. Due to software problems encountered during the searching it was not possible to record how many actual items were physically reviewed. However 86% of the documents identified as potentially relevant came from within a specific operational sub directory of exhibit MPG-2.001 while 41% of the identified images were recovered from the recycler directory (deleted area) of exhibit MPG-1(DD).001.

35. The Inquiry is in possession of the AD LAB report and event logs created following the search of the Sensitive Case.

Live Case

36. Examination of the Live Case in 'Email mode' identified 41,000 email related items which could be examined independently. Emails examined by date identified 573 sent in 2004 compared with 1504 in 2005. Closer examination of dates relevant to the Inquiry identified only one email being sent on 13 May 2004, none on 14 and 15 May and five on 16 May 2004. All were not relevant.

37. The transportation of large quantities of high level protectively marked material is strictly controlled. Due to the size of the data set (20GB) that was due to be created when downloading the 2,775 documents along with the accompanying AD LAB report it was established that burning to DVD did not provide sufficient capacity or security. Compliance with regulations required the Inquiry to source a suitably encrypted portable hard drive. This resulted in some delay.

38. The Inquiry is in possession of the AD LAB report and event logs created following the search of the Live Case.

Email Case

39. By this time it was only possible for two members of the Inquiry to utilise the FDHC for searching the Email Case. Also, the method of searching had changed as the tool used to search and review was the web based 'ECA' interface as opposed to AD LAB. This resulted in not being able to utilise Explorer mode but Indexed searching along with the examination of material by type was still available.

40. The approach to the search of the Email Case was to apply each of the terms supplied to IHAT on 7 February 2013 as a separate independent search. The documents returned by each search would then be reviewed and labelled either relevant or irrelevant accordingly. Using the web based interface with the application of in built filters enabled the review of the documents and files returned by a search to be undertaken while excluding any documents or

files already reviewed and labelled as irrelevant as a result of previous searches. Consequently the documents and files returned by each subsequent search diminished in size exponentially as more files were labelled.

41. The Inquiry is in possession of the AD LAB report and event logs created following the search of the Email Case.

42. The Email Address Case consisted of 2.9 million items including 13,000 images in 412GB of data. As with the original Email Case the approach to searching the case was to apply key word (Indexed) searching using each of the terms supplied to IHAT on 3 May 2013 as a separate independent search. The resulting documents returned by each search were then reviewed and labelled independently of the results of other searches. All 13,000 images were viewed.

43. The Inquiry is in possession of the AD LAB report and event logs created following the search of the Email Address Case.

Search for Hard Drives Fitted To Computers at Camp Abu Naji & Joint Forward Interrogation Team (JFIT) in 2004

44. Examination of documents resulting from the initial searches of the FDHC, identified specific documents that listed by unique reference numbers, 20 computer workstations deployed to Camp Abu Naji in 2004. Along with the reference number, each workstations was allocated a name ranging from 'LIV-0601' through to 'LIV-0620'[5216] Each workstation was deployed to a location within the camp i.e. 'Ops' or 'Briefing Room' etc and had its own Internet Protocol (IP) address indicating they were all connected to a network.

45. Further documents enabled very specific and targeted searching to be conducted across the available FDHC cases, utilising the asset names and various military and manufacturer serial numbers. It was possible to trace computer hard drives to specific points in time when the trail ended with their destruction, loss, storage or re deployment. Initially this task was restricted to the hard drives allocated to 'LIV-0601' to 'LIV-0620' but was later expanded to include additional workstations 'LIV-0622' to 'LIV-0630' as research established hard drives were occasionally moved between workstations.

46. Additional searching of material contained on the FDHC provided a document dated by the embedded metadata to June 2005. This document again listed the computer workstations identified as 'LIV-0601' to 'LIV-0620' but also included an additional seven INET workstations reference 'LIV-0622' to 'LIV-0630'.[5217] The reference 'LIV-0627' was assigned to two separate workstations within the document and may have been entered as such in error. Within this document in most cases the actual hard drive serial number as supplied by the drive manufacturer, is listed instead of the original unique reference number as noted in paragraph 13. The potential error in listing 'LIV-0627' twice is supported by an additional document dated June 2005, which lists the same asset serial number being allocated to different workstations. This type of error in recording equipment did not appear to be restricted to Camp Abu Naji assets, as errors were noted within documents listing equipment at other MND(SE) locations.

[5216] (MOD054151)
[5217] (MOD054147)

LIV-0601 (Destroyed)

47. In June 2004 LIV-0601 was deployed and used within the CAN Operations Room and was referenced by a separate workstation (****1LD7) and hard drive serial number (*****099). By June 2005 the workstation was being used by the Intelligence cell. The same workstation serial number (****1LD7) was applicable but the hard drive reference was replaced by the manufacturers hard drive reference number (****6229). By the end of November 2005 these two reference numbers were being included in documents along with a new asset reference number (*****5324). These three reference numbers were searched across the FDHC whereby it was established the hard drive was destroyed as a result of an operation implemented in 2009 to return all necessary equipment back to the UK from theatre.[5218] The destruction of the hard drive fitted to the workstation LIV-0601 in June 2004, took place outside of the UK in June 2009.

LIV-0602 (Destroyed)

48. In June 2004 LIV-0602 was deployed and used within the 'Comms Ops' and was referenced by separate workstation number (****1LD6) and hard drive serial number (*****097). In May 2005 workstation number (****1LD6) was shown as being LIV-0624 with a manufacturers hard drive serial number (*****21LTG) which was replaced in December 2005 after it failed. By June 2005 workstation LIV-0602 was identified by a serial number (*****1K7W) with a hard drive fitted referenced by the manufacturers serial number (******103771). It was possible through later documents to potentially identify the hard drive fitted to the original workstation number (****1LD6) with a manufacturers reference of (*****103894). Research identified hard drive (*****103894) was destroyed in June 2009 along with the hard drive originally fitted to LIV-0601. Research identified hard drive (******103771) was also destroyed at the same time as (*****103894).

LIV-0603 (Destroyed)

49. In June 2004 LIV-0603 was deployed and used within the G2 office and was referenced by a separate workstation (****40N4) and hard drive serial number (*****102). By June 2005 the workstation was being used by the planning cell. The same workstation serial number (****40N4) was applicable but the hard drive reference was replaced by the manufacturers hard drive reference number (****112352). By the end of November 2005 these two reference numbers were being included in documents along with a new asset reference number (*****5799). These three reference numbers were searched across the FDHC whereby it was established the hard drive was destroyed at the same time as LIV-0601 in June 2009.

LIV-0604 (Destroyed)

50. In June LIV-0604 was deployed and used in the Commanding Officers Adjutant's (CO Adj) office and was referenced by a separate workstation (****1LCG) and hard drive serial number (*****092). By June 2005 the workstation was being listed as used by the Adjutant. The same workstation serial number (****1LCG) was applicable but the hard drive reference was replaced by the manufacturers hard drive reference number (****103087). This hard drive was traced to returning to the UK in June 2009. Enquiries with the MOD identified the hard drive was destroyed.

[5218] (ASI025202) [17] 'Operation Brockdale'

LIV-0605 (Destroyed)

51. In June 2004 LIV-0605 was deployed and used within the Briefing Room and was referenced by a separate workstation (****31LCC) and hard drive serial number (*****107). By June 2005 the workstation was being used by the RAO (Regimental Administration Officer).[5219] The same workstation serial number (****31LCC) was applicable but the hard drive reference was replaced by the manufacturers hard drive reference number (****104948). In early 2006 the hard drive referenced by the manufacturers number (****104948) was recorded along with an asset number of (******609) required re imaging. These four reference numbers were searched across the FDHC whereby it was established the hard drive was destroyed at the same time as LIV-0601 in June 2009.

LIV-0606 (Destroyed)

52. In June 2004 LIV-0606 was deployed and used in the Commanding Officers adjutant (CO Adj) office and was referenced by a separate workstation (****31LC5) and hard drive serial number (*****094). By June 2005 the workstation (****31LC5) had been re identified as LIV-0608 where it was recorded the system was 'unserviceable'. No further details were recorded that enabled any further research. LIV-0606 was by this time recorded as having a workstation reference (*****19Y4) and a manufacturers hard drive reference number (*****266003). This hard drive was traced to returning to the UK in June 2009. Enquiries with the MOD identified the hard drive was destroyed.

LIV-0607 (Lost)

53. In June 2004 LIV-0607 was deployed and used in 'Comms Ops' and was referenced by a separate workstation (****31LC7) and hard drive serial number (*****100). By October 2005 it was established that workstation (****31LC7) was fitted with a hard drive with the manufacturers reference number (****688HR). The computer was deployed in the 2IC Office. No further information could be established regarding LIV-0607 either at IHAT or with the MOD.

LIV-0608 (Lost)

54. In June 2004 LIV-0608 was identified as 'Base station and HDD awaiting shipping for repair. The hard drive had a separate reference number of (******096). In June 2005 LIV-0608 was replaced by LIV-0606. No further information could be established regarding LIV-0608 either at IHAT or with the MOD.

LIV-0609 (Destroyed)

55. In June 2004 LIV-0609 was deployed and used in the 'Post Room' and was referenced by a separate workstation (****31LC9) and hard drive serial number (*****093). By June 2005 the location was identified as 'G9 Office' and the hard drive was now referenced by the manufacturers number (*******3103515). This hard drive was traced to returning to the UK in June 2009. Enquiries with the MOD identified the hard drive was destroyed.

[5219] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/227048/acronyms_and_abbreviations_dec08.pdf

LIV-0610 (Destroyed)

56. In June 2004 LIV-0610 was deployed and used in the 'G2' office and was referenced by a separate workstation (****31LL3) and hard drive serial number (*****108). By June 2005 the location was identified as 'Plans' and the hard drive was now referenced by the manufacturers number (*******3103464). These three reference numbers were searched across the FDHC whereby it was established the hard drive was destroyed at the same time as LIV-0601 in June 2009.

LIV-0611 (IHAT JRY-39-A)

57. In June 2004 LIV-0611 was deployed and used in the 'Ops' office and was referenced by a separate workstation (****31LVW) and hard drive serial number (*****103). By June 2005 the location was identified as 'Ops Room' and the hard drive was now referenced by the manufacturers number (*******3106379). This hard drive was traced to returning to the UK in June 2009. Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-39-A. On 13 May 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

LIV-0612 (Destroyed)

58. In June 2004 LIV-0612 was deployed and used in the 'Ops' office and was referenced by a separate workstation (****31LRR) and hard drive serial number (*****106). By June 2005 the location was identified as 'INET Suite' and the hard drive was now referenced by the manufacturers number (*******46068). This hard drive was traced to returning to the UK in June 2009. Enquiries with the MOD identified the hard drive was destroyed.

LIV-0613 (Destroyed)

59. In June 2004 LIV-0613 was deployed and used in the 'RAO' office and was referenced by a separate workstation (****31LTB) and hard drive serial number (*****095). By June 2005 the location was identified as 'AJT' and the hard drive was now referenced by the manufacturers number (*******105326). The last available reference to this hard drive was dated September 2005 as an asset deployed to Camp Abu Naji. Enquiries with the MOD identified the hard drive was recorded as destroyed by 30 April 2007.

LIV-0614 (Destroyed)

60. In June 2004 LIV-0614 was deployed and used in the 'Ops' office and was referenced by a separate workstation (****31LTH) and hard drive serial number (*****105). By June 2005 the location was identified as the 'Int Cell' and the hard drive was now referenced by the manufacturers number (*******112449). This hard drive was traced to returning to the UK in June 2009. Enquiries with the MOD identified the hard drive was destroyed.

LIV-0615 (Destroyed)

61. In June 2004 LIV-0615 was deployed and used within the 'Ops' office and was referenced by a separate workstation (****31LCB) and hard drive serial number (*****109). By June 2005 the workstation was being used by the RAO. The same workstation serial number (****31LCB)

was applicable but the hard drive reference was replaced by the manufacturers hard drive reference number (****106509). These three reference numbers were searched across the FDHC whereby it was established the hard drive was destroyed at the same time as LIV-0601 in June 2009.

LIV-0616 (Destroyed)

62. In June 2004 LIV-0616 was deployed and used within the 'Ops' office and was referenced by a separate workstation (****31LT8) and hard drive serial number (*****104). By November 2005 (****31LT8) was associated to a hard drive referenced as (****5522) which in turn was associated to a manufacturers reference number (*******971987) by August 2006. All these reference numbers were searched across the FDHC whereby it was established the hard drive (*******971987) was destroyed at the same time as LIV-0601 in June 2009.

LIV-0617 (Lost)

63. In June 2004 LIV-0617 was deployed and used in the 'Air Ops' office and was referenced by a separate workstation (****31LTG) and hard drive serial number (*****101). By June 2005 the location had not changed although the hard drive serial number was different (****109). This number had been used in 2004 to identify LIV-0615. The last available reference to this hard drive was dated October 2005 as an asset deployed to Camp Abu Naji. Enquiries with the MOD identified the hard drive (****109) was re deployed to a system in Basra in October 2007. No further trace could be established after this date for either (*****101) or (*****109).

LIV-0618 (Destroyed)

64. In June 2004 LIV-0618 was deployed and used within the 'CO' office and was referenced by a separate workstation (****31LT5) and hard drive serial number (*****098). By December 2005 (****31LT5) was associated to a hard drive referenced as (****5552) which in turn was associated to a manufacturers reference number (*******105436). All these reference numbers were searched across the FDHC whereby it was established the hard drive (*******105436) was destroyed at the same time as LIV-0601 in June 2009.

LIV-0619 (Destroyed)

65. In June 2004 LIV-0619 was deployed and used in the 'CSM' office and was referenced by a separate workstation (****31LT6) and hard drive serial number (*****091). By June 2005 the location remained the same and the hard drive was then referenced by the manufacturers number (*******103706). This hard drive was traced to returning to the UK in June 2009. Enquiries with the MOD identified the hard drive was destroyed.

LIV-0620 (Destroyed)

66. In June 2004 LIV-0620 was deployed and used within the 'Ops' office and was referenced by a separate workstation (****31LT3) and hard drive serial number (*****110). By June 2005 (****31LT3) was referenced to a manufacturers reference number (*******103535). All these reference numbers were searched across the FDHC whereby it was established the hard drive (*******103535) was destroyed at the same time as LIV-0601 in June 2009.

67. Research identified the increase of storage on the Liverpool server by March 2006 with the addition of six extra hard drives identified by the name 'Top Rack'.[5220] Server spares with identifiable hard drives were also recorded within the documentation. Each identifiable asset serial number was searched through the FDHC in the attempt to locate the hard drives. Where the search provided a potential exhibit traced to IHAT as the final result, an explanation is provided. Hard drives which could not be traced through the available documentation will not be listed, although an additional 8 hard drives were identified and traced from Camp Abu Naji to returning to the UK following the closure of Operation Telic. Communication between the Inquiry and the MOD identified that all but 1 of the drives could be accounted for as being destroyed. The whereabouts of the remaining hard drive is not known.

Top Rack Drive 1 (IHAT JRY-119-J)

68. The first 'Top Rack' drive was identifiable by a unique asset number (*****6000). This drive was traced through a 2009 spreadsheet, which identified the above asset number being assigned to a 146GB INET hard drive loaded into bay 1 of the Liverpool MSA30 (HP Modular Smart Array 30) Server. This drive had a manufactures serial number (******65HK). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-119-J. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

Top Rack Drive 2 (IHAT JRY-119-F)

69. Top Rack drive 2 was identifiable by a unique asset number (*****5966). This drive was traced through a 2009 spreadsheet, which identified the above asset number being assigned to a 146GB INET hard drive loaded into bay 2 of the Liverpool MSA30 (HP Modular Smart Array 30) Server. This drive had a manufactures serial number (******5L1K). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-119-F. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

Top Rack Drive 3 (IHAT JRY-119-G)

70. Top Rack drive 3 was identifiable by a unique asset number (*****5959). This drive was traced through a 2009 spreadsheet, which identified the above asset number being assigned to a 146GB INET hard drive loaded into bay 3 of the Liverpool MSA30 (HP Modular Smart Array 30) Server. This drive had a manufactures serial number (******621C). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-119-G. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

Top Rack Drive 4 (IHAT JRY-119-H)

71. Top Rack drive 4 was identifiable by a unique asset number (*****5942). This drive was traced through a 2009 spreadsheet, which identified the above asset number being assigned to a 146GB INET hard drive loaded into bay 4 of the Liverpool MSA30 (HP Modular Smart Array 30) Server. This drive had a manufactures serial number (******61KM). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-119-H. On 07 June

[5220] (MOD054152)

2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

Top Rack Drive 5 (Possibly IHAT JRY-42-C)

72. Top Rack drive 5 was identifiable by a unique asset number (*****6770). This drive was traced through a 2009 spreadsheet, which identified the above asset number being assigned to a 146GB INET hard drive loaded into bay 5 of the Liverpool MSA30 (HP Modular Smart Array 30) Server. This drive had a manufactures serial number (******7YV3). This drive was last recorded within documents found on the FDHC as booked into PJHQ on 8 May 2009. The manufacturers serial number (******7YV3) is not recorded at IHAT but a similar reference number matching the same drive specification is recorded at IHAT as exhibit JRY-42-C. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

Top Rack Drive 6 (IHAT JRY-42-D)

73. Top Rack drive 6 was identifiable by a unique asset number (*****5928). This drive was traced through a 2009 spreadsheet, which identified the above asset number being assigned to a 146GB INET hard drive loaded into bay 6 of the Liverpool MSA30 (HP Modular Smart Array 30) Server. This drive had a manufactures serial number (******7N34). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-42-D. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

Server Spare 1 (IHAT JRY-76-F)

74. The first 'Server Spare' drive was identifiable by a unique asset number (*****5928). This drive was traced through a 2009 spreadsheet, which identified the hard drive had a manufactures serial number (******BS06). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-76-F. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

Server Spare 2 (IHAT JRY-143-G)

75. The next 'Server Spare' drive was identifiable by a unique asset number (*****7005). This drive was traced through a 2009 spreadsheet, which identified the hard drive had a manufactures serial number (******Q9NQ). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-143-G. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

Server Spare 3 (IHAT JRY-143-I)

76. The last 'Server Spare' drive was identifiable by a unique asset number (*****6763). This drive was traced through a 2009 spreadsheet, which identified the hard drive had a manufactures serial number (******7YGT). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-143-I. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

LIV-0630, Ops Room 4 (IHAT JRY-41-C)

77. The hard drive fitted to a workstation referenced by the title 'Ops Room 4' was identifiable by a unique asset number (*****5812). This drive was traced through a 2009 spreadsheet, which identified the hard drive had a manufactures serial number (******2Z58). This number could be traced back to 2005 to being fitted to workstation LIV-0630 by changing the final 'Z' within the manufactures serial number from ******2Z58 to ******2258. Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-41-C.

78. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry. On 29 July 2013 the Inquiry was informed that JRY-41-C was damaged to the extent that IHAT were unable to extract any data from the drive. At that stage no time scales were available regarding the potential repair of the drive.

RAO Back (IHAT JRY-40-C)

79. The hard drive fitted to a workstation referenced by the title 'RAO Back' was identifiable by a unique asset number (*****5400). This drive was traced through a 2009 spreadsheet, which identified the hard drive had a manufactures serial number (******2934). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-40-C.

80. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry. On 29 July 2013 the Inquiry was informed that JRY-40-C was damaged to the extent that IHAT were unable to extract any data from the drive. At that stage no time scales were available regarding the potential repair of the drive.

81. While conducting the above research an additional network system was identified as being deployed to Iraq and Camp Abu Naji in 2004. This system was recorded as the 'DII' or Defence Information Infrastructure. It was not possible with the available documentation, to establish exactly when the system became live in 2004, but as with the previous research it was felt if the hard drives could be located they should also be searched for any potentially relevant material. Research utilising the FDHC identified four separate hard drives that comprised the DII server. Each hard drive was identifiable by a manufactures serial number and asset number and as a result it was possible to establish that each of the hard drives was held as exhibits by IHAT.

82. The DII server for Camp Abu Naji was identified within spreadsheets by a unique asset number (*****PDC02). Research identified four separate hard drives that comprised the DII server. Each hard drive was identifiable by a manufactures serial number and asset number and as a result it was possible to establish that each of the hard drives had been seized by IHAT and are referenced as follows.

DII Server Disk 00 (IHAT JRY-216-C)

83. DII Server asset (*****PDC02) contained hard disk 00 asset (*****Z38H) seized by IHAT and referenced as exhibit JRY-216-C. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

DII Server Disk 01 (IHAT JRY-216-A)

84. DII Server asset (*****PDC02) contained hard disk 01 asset (*****008VP) seized by IHAT and referenced as exhibit JRY-216-A. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

DII Server Disk 02 (IHAT JRY-214-B)

85. DII Server asset (*****PDC02) contained hard disk 02 asset (*****Z1YE) seized by IHAT and referenced as exhibit JRY-214-B. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

DII Server Disk 03 (IHAT JRY-216-E)

86. DII Server asset (*****PDC02) contained hard disk 03 asset (*****YFM7) seized by IHAT and referenced as exhibit JRY-216-E. On 07 June 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

87. Research using the FDHC identified a JFIT stores register from 2004, which included 5 'Panasonic Toughbook' laptops and 6 INET terminals among its assets.[5221] The documentation provided reference numbers for four of the INET computers and their associated hard drives which enabled them to be traced through known FDHC documentation. The remaining two INET drives were recorded with partial reference numbers that did not ultimately provide a conclusion as to their final locations. Research established three of the JFIT INET terminals were destroyed in theatre, two were lost and one, JFIT INET SHB-1235 was traced to IHAT.

JFIT INET SHB-1235 (IHAT JRY-46-B)

88. In May 2004 JFIT INET terminal identified as SHB-1235 was fitted with a hard drive identified with a unique manufacturers reference number (*****94TJV). Research identified the hard drive had been seized by IHAT and was referenced as exhibit JRY-46-B. On 22 May 2013 a request was made via DJEP for the exhibit to be made available for inspection by the Inquiry.

89. On 29 July 2013 the Inquiry was informed that JRY-46-B was damaged to the extent that IHAT were unable to extract any data from the drive. At that stage no time scales were available regarding the potential repair of the drive.

90. The 5 Panasonic Toughbook laptops were recorded within the JFIT stores register with a unique reference number. It was not possible to trace these items beyond December 2004 where they were included in a later copy of the JFIT stores register.

91. While searching for computer systems for the JFIT, research identified two additional computer systems believed to have been deployed to the DTDF main office. Tracing these assets utilising the available reference numbers identified they were both destroyed in June 2009 prior to returning to the UK.

[5221] (MOD050954)

JRY-39-A

92. Exhibit JRY-39-A was identified as LIV-0611.[5222] On examination it was established that the exhibit contained 76GB of data consisting of 77,800 items of which 46,000 were mainly small 'operating system' images. Initial searching identified 1PWRR documents as potentially relevant to the inquiry, but a search of the drive by indexed searching coupled with an examination of all images did not provide any documents that were not already held by the Inquiry.

Service Police Crime Bureau (SPCB)

JDB/1

93. Exhibit JDB/1 was identified to the Inquiry as a hard disk drive seized by IHAT from a military intelligence unit. Following a request by the Inquiry and after obtaining authority from IHAT the hard drive had been repaired by SPCB on to their Forensic Server prior to the examination by the Inquiry. The drive had a visible directory structure that contained over 14 million items. Examination of the directory structure of the hard drive indicated the drive appeared to have been used as a storage area for the military unit. It was not possible to identify if the drive was deployed in theatre or in the UK. The only partition (storage area) was labelled as "Telic". Contained within this area were files ranging in date from 2003 to 2009. There were limited emails and those available appeared to be as a result of saving the email (and attachments where available) or stored within backed up pst files (archived email folders).

94. Key word (Indexed) searching of the hard drive identified directories containing material of potential relevance to the Inquiry. One such directory was labelled 'J2X data'. This directory contained several sub directories one of which was titled 'Danny Boy'. Contained within the Danny Boy directory were nine further sub directories, one for each of the nine DB detainees. Each of the nine sub directories contained intelligence material. Another was labelled 'DIRCS' containing all Divisional Internment Review Committee documents including those relating to the DB Detainees.

95. All 295,000 images contained within the exhibit were opened and viewed.

96. As a result of the search of JDB/1, 212 files were identified as potentially relevant to the Inquiry. A decision was made to delay requesting the identified files until the completion of the search at SPCB when the results of all the searches conducted at SPCB would be requested in one go. Upon receipt of the 212 files a further review was conducted overseen by Counsel for the Inquiry. No new relevant documents were identified during this process emanating from exhibit JDB/1.

97. The Inquiry is in possession of the AD LAB report and Event Logs associated to the search of exhibit JDB/1.

JDB/13

98. Exhibit JDB/13 was identified as a hard disk drive seized by IHAT from a military intelligence unit. It had been repaired and processed by SPCB. The drive had a visible directory structure that contained over 61,000 items.

[5222] Paragraph 36

99. A full examination was conducted comprising of key word (Indexed) searching accompanied by a manual search of directories (Explorer mode). All 10,000 images were opened and viewed. No documents relevant to the Inquiry were found.

100. The Inquiry is in possession of the AD LAB report and Event Logs associated to the search of exhibit JDB/13.

JDB/14

101. Exhibit JDB/14 was identified as a compact disk seized by IHAT from a military intelligence unit. It had been processed by SPCB. The drive had a visible directory structure that contained 729 items including 537 images.

102. A full examination was conducted comprising of key word (Indexed) searching accompanied by a manual search of directories (Explorer mode). All 537 images were opened and viewed. No documents relevant to the Inquiry were found.

103. The Inquiry is in possession of the AD LAB report and Event Logs associated to the search of exhibit JDB/14.

JRY-76-F

104. Exhibit JRY/76F had been identified during the search for hard drives fitted to computer equipment located at CAN in 2004, potentially as a 'Liverpool Server Spare'. The drive did not require repair and was processed by SPCB. Once processed the drive was found to have been part of an unidentified 'RAID' and as such there was no visible directory structure. The exhibit contained over 145,000 items including 28,000 images contained within 52GB of data. It was possible to differentiate file/document types by use of the Overview mode.

105. A full examination was conducted comprising of key word (Indexed) searching accompanied by a manual search of directories (Explorer mode). All 28,000 images were opened and viewed. 1 document potentially relevant to the Inquiry was found, this being an email chain dating from 2008. Upon receipt of the file a further review was conducted overseen by Counsel where upon the file was deemed irrelevant.

106. The Inquiry is in possession of the AD LAB report and Event Logs associated to the search of exhibit JRY/76F.

JRY-143-G

107. Exhibit JRY/143G had been identified during the search for hard drives fitted to computer equipment located at CAN in 2004, potentially as a 'Liverpool Server Spare'. The drive did not require repair and was processed by SPCB. Once processed the drive was found to have no visible directory structure. The exhibit consisted of 1,400 items totalling 140GB of data where each item was 100MB in size and consisted of either zeros '0' or random text. Overview mode did not supply any file/document types.

108. Key word searches were conducted with no resulting documents being identified. The Inquiry is in possession of the Event Logs associated to the search of exhibit JRY/143G.

JRY-216-C

109. Exhibit JRY/216C had been identified during the search for hard drives fitted to computer equipment located at CAN in 2004, potentially as part of the CAN 'DII Server'. The drive did not require repair and was processed by SPCB. Once processed the exhibit was believed to have possibly been part of an unidentified RAID. While there was no visible directory structure, Overview mode provided details of file/document types. The exhibit consisted of 102,000 items including 63,000 images totalling 75GB of data.

110. Examination of the exhibit using key word (indexed) searches including viewing all 63,000 images identified the drive contained 1 document potentially relevant to the inquiry with the remainder being irrelevant. Upon receipt of the document at the Inquiry a further review overseen by Counsel deemed the document irrelevant. The Inquiry is in possession of the AD LAB report and Event Logs associated to the search of exhibit JRY/216C.

RMP Laptop Exhibit EH-110

111. Once processed EH-110 was examined. It had an identifiable directory structure, as such could be searched in Explorer mode. The types of files/documents could be examined in Overview mode and specific files or documents could be found by applying key word (indexed) searches.

112. The exhibit contained 214,000 items including 40,000 images within 160GB of data. A variety of searches were conducted over EH-110 whereby 7 documents were identified as potentially relevant to the Inquiry. All 40,000 images were viewed. Upon receipt of the documents at the Inquiry a further review overseen by Counsel deemed the documents irrelevant. The Inquiry is in possession of the AD LAB report and Event Logs associated to the search of exhibit EH-110

Damaged Exhibits – Partial Images

113. All 12 drives within the case were searched. The 10 identified by the inquiry processed into the case were JRY-42-C, JRY-42-D, JRY-119-F, JRY-119-G, JRY-119-H, JRY-119-J, JRY-143-I, JRY214-B, JRY-216-A and JRY-216-E. The 2 extra drives were identified as JRY-41-B and JRY-119-I which did not contain any material of relevance to the Inquiry. The total data set for the entire case consisted of 708,000 items including 402,000 images in 1391GB of data.

114. As this case was a compilation of recovered data, no directory tree was available and as such Explorer mode was not utilised to search the drives other than to establish the structure of the case. Document and file types could be established in Overview mode. Key word searches were applied across the entire case with all results being returned from 4 specific drives. These were JRY-119-F, JRY-119-G, JRY-119-H and JRY-119-J. These four drives had been identified during the process identified in paragraph 16 as being part of a system which in 2005 was given the name of 'Liverpool Top Rack'.

115. As a result of searching the Partial Image Case including viewing all 402,000 images 43 items were identified as potentially relevant to the inquiry. Upon receipt of the documents at the Inquiry a further review overseen by Counsel deemed the documents irrelevant. The Inquiry is in possession of the AD LAB report and Event Logs associated to the search of the Partial Image Case.

116. JDB/2, JDB/3, JDB/4 and JDB/6 were processed by SPCB into a single case identified as 'JDB2_3_4_6'. The case comprised 1,250,000 items in 2TB of data. It included 850,000 images. The majority of the recovered documents were from later Afghanistan operation Herrick. Emails were examined by dates which placed them in the date range of 2007 to 2011. Key word searches were conducted which only returned intelligence material already held by the Inquiry. A visual inspection of the images identified imagery from Afghanistan. It was decided that reviewing all 850,000 images was not proportionate considering the documents recovered did not fit the Inquiry's Terms of Reference. The Inquiry is in possession of the AD LAB report and Event Logs associated to the search of the JDB2_3_4_6 Case.

The Forensic Case

117. By late June 2014 the Forensic Case consisted of approximately 42million individual files after processing had filtered all duplicate and system files. This was the most complete data set available at that time. A list of 138 individual search terms used and found productive in previous searches was sent to IHAT in order that a smaller case could be constructed and made available for the Inquiry to search.

118. The list included the names of senior ranking military personnel from Al Amarah, Basra and the DTDF. The reference numbers of the detainees, the RMP investigation and the Phoenix flight from Al Amarah on the 14 May 2004. Role based email addresses were included as were locations and relevant regimental names and their variations.

119. Examination and searching of the case was conducted utilising the web based interface, referenced at paragraph 29, as opposed to AD LAB. No hard drive directory structure was available but files could be searched and then filtered utilising various methods including date, type and size. The case consisted of mainly email related files (295,000), and MS Word type files (256,000). The remainder consisted of presentations, spreadsheets, multimedia, databases and images. There were only 4,000 images contained within the case. These were all examined.

120. As previously each of the search terms used to create the case was applied as an individual search over the new case to extract a list of files to examine. Where high numbers of resultant files were returned, either filtering or the addition of Boolean terms was applied to make the review achievable.

121. The Inquiry is in possession of the event log generated following the search of the Forensic Case.