FUJ00124313

Comments on *Wylie - further requests for disclosure*

Ref: g:\gij documents\poa\prosecution support\2b27.wylie\wylie - further requests for disclosure.comments.docx
Author: Gareth I Jenkins
Date: 19/02/2013 10:58:00

1. Introduction

I have been asked comment on the document *Report: Disclosure Requests Computer Evidence* provided by the Defence in the case of Regina v Kym Wyllie.

> *There seems to be some discrepancy in how the defendant's name is spelt.*
>
> *Is it Kim Wylie or Kym Wyllie?*

In order to do that I have copied in the Report below in blue font and added in my comments in black font.

In summary, it would appear that the Defence expert is looking for as much information as he can to carry out a detailed analysis. I have no problem in him doing that and am happy to assist in such an analysis (as I have done in the part with other Defence Experts), since the data requested is proprietary to Horizon or Horizon Online and is unlikely to be understood easily without some guidance.

Any such analysis is likely to require a lot of time and effort to analyse and therefore incur considerable cost and elapsed time.

2. Report: Disclosure Requests Computer Evidence

1 Terms of Reference

1.1 Instructions

I was instructed by McKeag & Co Solicitors to the Defendant, to act as an expert witness by letter dated 28 January 2013. My instructions require me to read a bundle of prosecution statements and exhibits (about 100 pages) and to advise on the evidential material that I would require to conduct an independent investigation of the computer evidence relevant to the prosecution case. I have not been instructed to conduct a computer forensic examination of any forensic image copies and have not done so.

1.2 Charges

The Defendant is charged with two counts of Theft relating to cash shortfalls at the Post Office at Winlaton, Tyne and Wear ("Winlaton PO").

1.3 Author's Qualifications

I am Michael John Livingston Turner MA (Cantab) FBCS CITP MAE FEWI of

FUJ00124313

Dulas Mill, Hereford. I am an experienced forensic computer examiner and an established expert witness on computer evidence. I have over forty years of experience of computing and have been in practice as an independent computer consultant since 1977. Please see the CV at Appendix A:

1.4 Statement of Independence

I have previously acted as an expert witness instructed by the Defence in prosecutions brought by the CPS relating to the Post Office Horizon system. I had no prior knowledge of the Defendant in this case. I believe I have complied with my duty to act independently of the parties.

I note that the CV refers to another Horizon Case R v Julia Richards: Winchester Crown Court July 2011. I have no knowledge of that case.

1.5 Expert's Declaration

I have made a Declaration at the end of this report.

2 Introduction to Computer evidence

Virtually all the documentary evidence in the case is ultimately derived from a computer system — Post Office Horizon.

Computer data is highly volatile. Given this characteristic, there is a special duty of care to protect the integrity of the available computer evidence. In practical terms that means the evidence should be secured and/or seized at the earliest possible opportunity and copied using a forensic copying process, so that all investigations may take place on write-protected copies of the computer evidence.

The traditional approach to computer forensics has been to conduct a static post mortem of the persistent data stored on hard disk drives or other non-volatile storage media.

Computing equipment is seized; if the computer is turned on, it is turned off (either by a normal, graceful shutdown or by pulling the power plug). Using a hardware write-blocker, a forensic image is made of the entire storage media and verified, and all subsequent examination is on a copy of the forensic image.

The entire computer forensics process is documented, verifiable and can be recreated by a third-party. That approach forms the basis of the ACPO Guidelines,

My understanding is that the approach that has been taken by the Horizon system for securing evidence was agreed before Horizon was originally developed. However I don't have any specific documents that show this.

I should also point out that at the time of the Audit in September 2010, the system would have been operation Horizon Online and so there would be no useful evidence held on the local terminal.

2.1 ACPO Guidelines

FUJ00124313

> *Good Practice Guide for Computer Based Evidence* is produced by the Association of Chief Police Officers (ACPO). It provides Guidelines for the handling of Computer Evidence. The following quotations are from *Good Practice Guide for Computer Based Evidence, ACPO*, Version 1.0, 25 March 1998.

I am not familiar with this, as I only claim expertise in the operation of the Horizon system and not the general gathering of Forensic Evidence.

> Two caveats are given on page 2:
>
> > *(This document) is not intended as a guide for Officers dealing with evidence produced by witnesses from third party computer systems.*
> >
> > *Non compliance with this guide should not necessarily be considered as grounds to reject evidence*

I think we need to rely on these caveats.

> Five Principles of Computer Based Evidence are set out with relevant Explanations. The Principles recognise that computer evidence is of a highly volatile nature that risks contamination:
>
> > *Principle 1: No action taken by Police or their agents should change data held on a computer or other media which may subsequently be relied upon in Court.*

I believe that this is true of the evidence provided as part of the Horizon Audit Trail.

> That the processes for securing, preserving copying and examining the evidence in an investigation should be transparent:
>
> > *Principle 3: An audit trail or other record of all processes applied to computer based evidence should be created and preserved. An independent third party should be able to repeat those processes and achieve the same result.*
> >
> > *It is necessary to demonstrate to the Court how evidence has been recovered showing each process through which the evidence was obtained*

I have attempted to outline the process in my Statement. The process is repeatable. The current independent investigation into Horizon Integrity has been attempting to repeat the process.

> That all of the necessary evidence should be secured and copied:
>
> > *In order to comply with the principles of computer based evidence a copy should be made of the entire target device.*

What is preserved is the Data upon which the accounting systems operate. This is not th
 e
same as the entire target device, however I would contend it is sufficient as the processes used to derive the reports upon which discrepancies are based are repeatable on the data.

> That an unbroken chain of custody is to be maintained:

FUJ00124313

It is essential to objectively show to a Court that the continuity and integrity of the evidence has been preserved.

This is what I have tried to describe in my Statement.

That it is essential to observe the highest standards of preservation:

Evidence should be preserved to an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a Court.

I believe that to be the case. It should be noted that I have not been shown any evidence from this case and so have not attempted to repeat the derivation of any results.

I understand that data has been obtained from Horizon covering data archived between 26th June and 17th July 2010, but at this point I have not seen that data.

3 Disclosure Requests

In order to conduct a thorough, independent investigation it would be necessary to apply to the court for disclosure of:

1. Post Office Incident Response procedure documenting the forensic standards to be observed when securing/preserving computer data for use as evidence in criminal proceedings in operation at the material time

This is covered in the standard Witness Statement produced by Fujitsu if requested when transactional evidence is presented at court. My statement also covers this process at a high level though I do not personally have access to the system to carry out the process. I can certainly describe the operation of the process and how it relates to the way the data is stored at the time of the original transactions.

2. Statements and exhibits relating to the forensic processes (seizure/preservation, forensic imaging/processing and subsequent handling) of all evidence relating to the alleged theft from Winlaton PO emanating from Horizon, including transaction records and event logs

I have no knowledge of exactly what evidence has been collected, but am available to assist in the interpretation of any such logs.

3. Statements and exhibits relating to Results of testing the accuracy/synchronicity of the Winlaton PO system clocks:

   - Horizon terminals/system
   - Door alarm
   - CCTV recording system

I can make a statement as to how the Horizon system clock is maintained. Other information is outside my area of expertise.

Application should also be made to the court for disclosure in *electronic, soft copy format made to a forensic standard* of all the following:

FUJ00124313

4. Transactions relating to the Winlaton PO from the date that the last successful audit completed successfully to the date of detection of the alleged second shortfall

Technically this is possible. However I would raise a point of practicality. In previous cases I have found there to be close to 500,000 records per year in these logs and it is thus quite difficult to see the wood for the trees in any such analysis.

5. Security and Application events relating to the Winlaton PO Horizon system including logons/logoffs for the same period

The application events (such as Log On and Log Off) are normally included in any such date retrieval exercise. Also Critical system events are available for examination (but not normally returned as standard).

6. Horizon NBSC Support Incident/Issue/Call reports from Winlaton PO for the same period

Does he mean HSD or NBSC? HSD Support logs are available on request for Fujitsu. NBSC is Post Office Ltd's responsibility and so outside my scope of expertise.

7. Horizon NBSC Support Incident/Issue/Call reports from all Post Office branches for the same period relating to:

- Branch Trading Procedure
- accounting discrepancies
- balance discrepancies
- stock shortages
- cash shortages
- Known Problems
- Unrecovered sessions
- Balance Problems

Looking at this list, I would say these are all issues that NBSC should be handling rather than HSD.

8. Schedule of Horizon NBSC Support Incident/Issue/Call reports from all PO branches diagnosed as system or software errors for the same period

9. Schedule of Horizon version releases in use at Winlaton PO for the same period

This is not something we normally provide. It may be possible to provide a cost for providing this information.

10. Schedule of Horizon version releases in the 12 months after the date of detection of the second alleged shortfall

As above. However I question the usefulness of this given that the alleged shortfall was on Horizon and the audit was carried out on Horizon Online so fixes to Horizon

FUJ00124313

online are not relevant to issue on Horizon as they are totally different systems as far as the accounting is concerned.

11. Schedule of Resolved Issues in each of Horizon version releases identified in response to the previous request

I don't think this is at all easy to provide. I believe we have been asked this before and have provided a (large) cost to POL for doing this, and it has not been pursued.

12. Horizon System User Guide for Horizon version release in use at Winlaton PO at the date of the alleged shortfalls

This is down to Post Office Ltd. Note with Horizon Online, I believe that this may have been replaced by the online Help System.

13. Horizon Operations Manual for Horizon version release in use at Winlaton PO at the date of the alleged shortfalls

This is down to Post Office Ltd. Note with Horizon Online, I believe that this may have been replaced by the online Help System.

14. POL Technical Evaluation (including in terms of systems performance, reliability, recoverability, auditability) of the consequences of the change from Horizon to HOL system architectures

I'm not sure if such a document exists, but will defer to Post Office Ltd.

15. HOL Branch Database High Level Design

16. HOL XML Message Audit between Counter and BAL/OSR

These are document I refer to in my Statement. I'm not sure what the commercial permission is in making such documents available, but I don't see any problem in doing so. I should point out that I don't think they will be of any real help in carrying out any further analysis.

4 Expert's Declaration

1. I understand that my overriding duty is to the court, both in preparing reports and in giving oral evidence. I have complied and will continue to comply with that duty.
2. I have set out in my report what I understand from those instructing me to be the questions in respect of which my opinion as an expert is required
3. I have done my best, in preparing this report, to be accurate and complete. I have mentioned all matters which I regard as relevant to the opinions I have expressed. All of the matters on which I have expressed an opinion lie within my field of expertise.
4. I have drawn to the attention of the court all matters, of which I am aware, which might adversely affect my opinion.
5. Wherever I have no personal knowledge, I have indicated the source of factual information.
6. I have not included anything in this report which has been suggested to me

FUJ00124313

by anyone, including the lawyers instructing me, without forming my own independent view of the matter.

7. Where, in my view, there is a range of reasonable opinion, I have indicated the extent of that range in the report.

8. At the time of signing the report I consider it to be accurate. I will notify those instructing me if, for any reason, I subsequently consider that the report requires any correction or qualification.

9. I understand that this report will be the evidence that I will give under oath, subject to any correction or qualification I may make before swearing to its veracity.

10. I confirm that insofar as the facts in my report are within my own knowledge I have made clear which they are and I believe them to be true, and the opinions I have expressed represent my true and complete professional opinion.

I would be pleased to provide further explanation of any of the above to the court.

Standard stuff. No comment required.