A framework for a syllabus on electronic evidence

It is anticipated that no university at present will be able to cover the areas of knowledge noted below in detail. However, as a compromise, a high-level approach will enable the ground to be covered in 4.5 hours. Ideally, newly qualified lawyers should be required to undertake post-qualification courses on the topic. Ideally, this requirement should also apply to all lawyers currently in practice.

The syllabus and materials: copyright

1. The syllabus, the three vignettes (The abacus; The 'forged' document and The 'competent' witness) and the questions posed in the Julie Amero exercises (collectively, 'the materials') are by Stephen Mason (the author), and copyright is duly vested in the author, and the author has asserted his rights under the Copyright, Designs and Patents Act 1988 to be identified as the author of these works.

2. The author grants not-for-profit universities (as defined by local legislation) a non-exclusive licence to use any of these materials for no fee as part of a course on evidence and as exam questions, providing that (i) where a vignette is used, it is clearly identified as being written by the author, and (ii) where the syllabus is adopted wholly or in part, the author is acknowledged, and (iii) the university agrees not to derive profit in any way from the use of these materials (for the avoidance of doubt, this refers to courses that are accredited by the recognised accreditation mechanisms, but does not preclude the university from offering commercial courses under the provisions of paragraph 3 below).

3. With the exceptions noted above, no part of these materials may be used for commercial purposes, reproduced, stored in a retrieval system or transmitted in any form or by any means, digital, mechanical, photocopying, recording or otherwise, without obtaining the prior permission of the author in writing.

4. For the avoidance of doubt, the author makes no claim to the excerpts from the transcript of the trial of Julie Amero.

Introduction: 1 hour

The sources and characteristics noted below only need to be highlighted – what is necessary is to identify one or two that are implicated in case law in order to draw out why it is necessary to be aware of each for the purposes of substantive and procedural law. It is not essential to cover each in depth – merely to highlight the need to be aware of the issues that might arise.

The nature, definition and sources of electronic evidence

Physical devices: computers; mobile telephones; smartphones; PDAs; tablets; etc.

The components: hardware; the processor; storage; software (system software; application software); the clock; time stamps; storage media and memory; data formats; powering up and powering down

Networks: e.g. internet; corporate intranets; wireless networking; cellular networks; dial-up; etc.

Applications: e.g. e-mail; instant messaging; computer to computer; social networking; etc.

The characteristics of electronic evidence

The dependency on machinery and software

The mediation of technology

Speed of change

Volume and replication

Metadata

Storage media

Illicitly obtaining confidential data

Anti-forensics and interpretation of evidence: destruction of data; falsifying data; hiding data; attacks against computer forensics; trail obfuscation

Exercise: discussion of 'The abacus' (given to students in advance)

Substantive law: 2 hours

In this part, the emphasis needs to be on ensuring that it is understood that digital data is controlled by software written by human beings – this is a crucial element to

grasp, because mistakes have been made regarding the nature of electronic evidence, and an astute lawyer needs to be aware of the nuances, otherwise some judges will continue to misunderstand the nature of digital data. Furthermore, there is a misplaced presumption about the 'reliability' of electronic evidence that must be addressed, even if it is covered slightly – the main points must be put over if the law is to concentrate on its core function of being fair to both parties and in the search for the truth.

NOTE: ideally, the following list of topics should also be included, but given the limitation on time, they can be identified for self study (fitting in time for the exercise: discussion of 'The abacus' will be beneficial – possibly in a tutorial): direct and indirect evidence; real evidence; best evidence; primary and secondary evidence; admissibility; definitions: document; book or paper; writing; record; instrument; video-recorded and tape-recorded evidence, and computer generated animations and simulations.

Hearsay

Three categories of electronic evidence:

Category 1

The records of activities that contain content written by one or more people.

e.g.: e-mail messages; word processing files; instant messages

As evidence it may be necessary to demonstrate that the content of the document is a reliable record of the human statement that can be trusted.

Category 2

Records generated by a computer that have not had any input from a human.

e.g.: data logs; connections made by telephones; ATM transactions

As evidence to demonstrate that the computer program that generated the record was functioning consistently at the material time.

Category 3

Records comprising a mix of human input and calculations generated and stored by software written by a human.

e.g.: financial spreadsheets that contain human statements (input to the spreadsheet program); computer processing (mathematical calculations performed by the spreadsheet program)

As evidence whether the person inputting the data or the writer of the software created the content of the record, and how much of the content was created by the writer of the software and how much by the person inputting the data.

Evidential foundations and authenticity

By using circumstantial evidence

The five-point test for electronic evidence from complex systems (for which see *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012) chapter 4)

The presumption of 'reliability' or 'being in order'

Weight

Exercise: discussion of 'The "forged" document' (given to students in advance)

Proof – evidence and forensics: 45 minutes

The case law indicates that when investigating a case, some police investigators will inadvertently or through negligence fail to deal properly with electronic evidence, and might, because of their actions, render the evidence unfit for trial because of their actions. In addition, it was previously rare to find a truly independent, articulate and competent digital evidence specialist that could provide a suitable analysis and report to the court. This is beginning to change now that specialist courses have begun to be devised by universities for the forensic examination and reporting of electronic evidence. This is also an important area that the lawyer should be aware of, because a break in the chain of evidence, a failure to identify all the relevant evidence, and poor analysis and conclusions have caused innocent people to be held in custody when they ought not have been.

It is recommended that in the time allocated to this topic, consideration be given to identifying one or two cases that highlight the issues as examples. Note: because

of the culture of recording cases in the United States of America – especially criminal trials, most of the case law is from the US; this does not mean that blunders have not occurred elsewhere – undoubtedly they have, but they may not have been recorded.

Investigation

Search and seizure

Preservation

Deleted data

Analysis and reporting

Interpretation

Exercise: discussion of 'The "competent" witness' (given to students in advance)

Exercise: 45 minutes

State of Connecticut v Julie Amero (2007) (given to students on the day to work collectively in four groups to cover the five questions in order to discuss and prepare responses to the entire group)

The justification for using the case of Julie Amero is set out in the 'Introduction' to Stephen Mason, editor, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), pp xxxvi – xxxvii:

> 'A serious concern with respect to digital evidence is the failure of everybody involved in justice systems (whether civil or criminal) to fully appreciate that evidence in digital format, now virtually ubiquitous, in that it appears in almost every case in one form or another, is far more complex than those taking part in the proceedings are aware. The lack of any understanding of digital evidence by the lawyers and the judge is usually demonstrated by the way a case is conducted, and the prosecution of Julie Amero by the State of Connecticut serves to illustrate why judges and lawyers must take steps to purge their minds of any ignorance in relation to this topic. This is one of two case studies included in this chapter, both from the United States of America. The second case study, *State of Arizona v Bandy*, illustrates the nature and interpretation of the digital evidence that a prosecutor must consider before deciding to proceed against an individual. Although the cases are from the United States of America, it will be disappointing if lawyers and judges, from whatever jurisdiction they happen to be in, adopt the view that the facts surrounding either case are not relevant to them. The facts of both cases are relevant to every jurisdiction on earth, and to adopt the view that what happens in a court other than the home jurisdiction is irrelevant, is to fail to grasp that digital evidence transcends the boundaries of individual jurisdictions, and it will be increasingly necessary for lawyers to obtain evidence from other jurisdictions, regardless of the nature of the case they are dealing with. If lawyers and judges do not begin to make themselves aware of digital evidence, it is inevitable that the justice system will be the subject of the sort of unwelcome adverse media attention given to the Julie Amero case in particular in due course.'[1]

Materials

The abacus

(First published in *Electronic Evidence: Disclosure, Discovery & Admissibility* (1st edition, LexisNexis Butterworths, 2007))

'Your honour, I seek to exhibit the abacus.'

The judge looked over his spectacles 'Which form of abacus is it?'

The barrister looked perplexed and turned to his solicitor and whispered 'Which form of abacus? How do I know? Are there different types of abacus?'

'Oh yes' whispered the solicitor, 'it's a Chinese abacus.' 'Oh, right. Thanks.' 'It's a Chinese abacus, your honour.'

'Thank you, Mr Puffington. And what is the purpose of exhibiting the abacus?'

'Well, your honour, it's the item upon which the calculations were made to perpetrate the alleged fraud.'

'Indeed, but that does not mean the abacus ought to be exhibited. Have you a submission on this matter Miss Jawleyford?'

Miss Jawleyford stood as Mr Puffington sat down.

'Well, your honour, the defence does not seek to argue about an inanimate object.'

1 *A detailed analysis of the case follows to p lxxv.*

'Quite.'

'But what we must look to, in my submission, is the reason for admitting the abacus as an exhibit, your honour.'

'Indeed.'

'We have already had the opportunity of viewing the abacus, and take no point on the object itself. It is admitted that the defendant used the device. As a material object, it can be admitted into evidence. But the question is, what purpose is served in admitting the device. It is my submission that the presence of the abacus serves no purpose, because the device is merely a device. There is no record of what, if any, calculations might have been made on the device.'

Miss Jawleyford sat down. Mr Puffington stood.

'Your honour, in our submission, it's important to exhibit the abacus, because it will serve to make the members of the jury ask themselves why the defendant, a finance director earning over a million pounds salary a year, deliberately used such a device. It is our case that he used the abacus to avoid the creation of records that would implicate him in the alleged fraud. To that end, it's an important exhibit that ought to be admitted into evidence.'

The 'forged' document

(First published in *Electronic Evidence* (2nd edition, LexisNexis Butterworths, 2010))

'The problem with the e-mail submitted by the witness, madam, is that the signature cannot be trusted. For this reason, the evidence cannot be admitted.'

Mr Tulkinghorn sat down. Mr Tangle stood up.

'With the deepest possible respect, madam, my learned friend has let his usual penetrating insight into the analysis of evidence fail him. If this was a letter, for instance, the first question will be "Is the letter genuine?" If the letter is a forgery, then the signature matters not – unless it is genuine and intended to deceive the recipient. If the letter is genuine, *then* the question arises as to whether the signature is a forgery. Thus it must be with the e-mail. If my learned friend claims that the e-mail is a forgery, the status of the signature is irrelevant. Is my learned friend suggesting that the e-mail is a forgery?'

Mr Tangle sat down.

Her Honour Judge Flite QC looked at Mr Tulkinghorn 'Well? It strikes me that this must be correct. Are you suggesting the e-mail is a forgery?'

Mr Tulkinghorn stood up.

'In this instance, my learned friend has indicated an error of logic on my part, which I concede. The point is, anybody can forge an e-mail and write any name as an electronic signature. If we cannot trust the signature, then we cannot trust the e-mail.'

Her Honour Judge Flite QC continued the questioning, 'But the authenticity of the e-mail must come before the verification of the signature? Mr Tangle?'

Mr Tulkinghorn sat down. Mr Tangle stood up.

'Where the authenticity of a document is challenged, a wide range of tests can be made to determine whether it is a forgery. I acknowledge that the contents can help determine whether it is a forgery. But if it was a letter, the paper, ink, and the type face might all be the subject of tests. In the case of an e-mail, the technical information relating to the status of the document is of the utmost relevance. In my submission, determining whether to trust the signature can only follow *after* it has been established whether the e-mail is genuine or a forgery.'

The 'competent' witness

(First published in *Electronic Evidence* (3rd edition, LexisNexis Butterworths, 2012))

'My learned friend for the prosecution has established that you are the sub-manager of the hotel, that you are familiar with the functions of the machine that controls the telephone system, and that you know how it works and what it is supposed to do?'

'Yes.'

'And the print-outs you have brought to court purport to indicate when the telephone was used in room 2820?'

'Yes.'

'For this reason, my learned friend considers your evidence is all that is needed to establish the reliability of the telephone system. Let me ask you this, how does the direct inward system access work?'

'Er, I don't know.'

'You don't know what happens, or you don't know what the direct inward system access is?'

'I don't know what it is.'

'So, by implication, you don't know what the password is?'

'No.'

'By implication, you won't know if thieves have used the password to route telephone calls through the hotel telephone system?'

'No.'

'Can you tell me the purpose of the latest software up-date, whether it included a security fix, and when it was downloaded?'

'Er, no, I don't know any of that.'

'Why do you not know?'

'Well, because the IT people do all of that stuff.'

'So you are asserting, by bringing along the print-outs of the telephone calls, that these telephone calls were actually made, and they were made from room 2820.'

'Well, yes, if you say so.'

'I do not say so, you do. You also claim that because none of your customers have ever complained about their bills, it follows that the telephone system is reliable and therefore trustworthy?'

'Well, I wouldn't put it quite like that.'

'Thank you, Mr Prunsquallor.'

Judge Sepulchrave turned to prosecuting counsel, 'Unless you have any questions in re-examination Mrs Groan?'

Mrs Groan stood up. 'You honour, no,' and sat down.

'Very well, you may leave the witness stand, Mr Prunsquallor. Yes, Mr Rottcodd?'

'Thank you, your honour. My learned friend for the prosecution would have us believe that because the information printed on the piece of paper apparently looks sensible, it therefore follows that the contents must not only be reliable, but represent the truth. My learned friend also suggests that because Mr Prunsquallor uses the hotel's telephone system in the performance of his duties, this is a sufficient foundation as a qualification as a competent witness. With your honour's leave, I will address the latter point first ...'

Exercises: *State of Connecticut v Julie Amero* (2007)

Citation

State of Connecticut v Julie Amero Docket number CR-04-93292; Superior Court, New London Judicial District at Norwich, GA 21. The trial took place on 3, 4 and 5 January 2007, before the Honorable Hillary B. Strackbein, Judge, with a jury of six. Prosecuting attorney David Smith, Office of the State Attorney. Defending attorney John F. Cocheo, 111 Huntington Street, New London. Transcription of the stenographic notes made by Gail C. Schor, a registered professional reporter.

Outline of the facts

Mr Matthew Napp taught children in the age range 12 – 13 years at Kelly Middle School, Connecticut in the United States of America. On 19 October 2004, Mr Napp went into his classroom and logged in to the teacher's computer under his own username and password before permitting the temporary teacher to use it. Ms Amero took his class because he was on a course for the day. Mr Napp left the classroom at around 8.15 am. Ms Amero went to the ladies cloakroom, and when she returned, her evidence was that Mr Napp was no longer in the room, and she found two children on the teacher's computer. There was a web site showing hair styles displayed on the monitor. Ms Amero told the children to leave the computer.

Ms Amero returned to the teacher's desk and the computer after giving the class their assignment. When she returned to the teacher's desk, she found images popping up on the computer screen, which she described

as images 'that were not for children to see'. During the course of the day, various images in the form of pop-ups appeared on the screen of the computer, and Ms Amero gave evidence that the images did not stop: 'The pop-ups never went away. It was one after another. They were continuous. Every time I clicked the box in the corner, the red box, the red X, more were generated.' It appears that six male children saw pornographic images on the teacher's screen during the course of the morning.

The indictment: The charges read out to Ms Amero that she entered a plea to were phrased as follows:

> Connecticut General Statute Section 53-21(a) (1) and charges that on or about October 19th, 2004, in the City of Norwich, the defendant did willfully and unlawfully cause a child under the age of sixteen years to be placed in such a situation that the morals of said child were likely to be impaired.

Exercise for every group: Qualifications of the experts

Instructions

Please read the extracts from the transcript of the trial (below), and consider the following points for discussion:

1. One report has suggested that the police officer 'completed two two-week FBI training seminars on computer security and other continuing education programs. He is also a certified user of the computer monitoring software ComputerCOP Pro.' (Apparently the ComputerCOP Pro course is a one hour discussion over the telephone). Consider whether this police officer had the appropriate qualifications.

2. Consider whether the defense expert had the appropriate qualifications.

Exercise for everyone – excerpts from the transcript of the trial

The police officer

To establish the qualifications of Mark Lounsbury, the prosecution lawyer asked the following questions of the police officer:

Q How long have you been a police officer?

A Almost eighteen years now.

Q How long have you been involved in the investigation of computer crimes?

A Approximately seven years.

Q And do you have any training and experience specifically in investigating computer crimes?

A Yes, I do.

The defense expert

Mr Wilson H. Horner gave a long employment history and later set out the actions he took after being approached by the defense:

Q Mr. Horner, can you tell us what actions you took concerning this case.

A Basically I - what I had to do is determine as much as I can about this forensic analysis of this particular computer. The first thing we did, my group and my company, we went out and found as much information as we possibly could, either through seminars or through the Internet and libraries on how to conduct this examination. And the reason I did that, even though I had a lot of experience doing that type of thing, I just wanted to make sure that I did not leave anything out. And I wanted to make it as thorough as I possibly could. So what I am showing here are all the references that I used to assist us with this investigation. And I don't know if it is necessary to read them all, but I can. And I also listed up there the authors and either the websites or where they were located.

Exercise for group 1: Analysis of the investigation: The hard drive

Instructions

Please read the extracts from the transcript of the trial (below), and consider the following points for discussion:

1. Did the police officer conduct his examination of the hard drive on the original hard drive or a copy of the hard drive?

2. How important was the tool that was used to take a copy of the hard drive?

3. Should you take more than one copy of the hard drive with different tools?

4. The prosecutor was surprised that there was malicious

software on the computer. Should he have been surprised?

5. The defense hired an expert witness, and the prosecution requested the report to be given to them in advance. It was not. The judge refused to admit the report and permit the defense expert witness to testify what was included in the report. Was this correct?

Exercise for group 1 – excerpts from the transcript of the trial

Copying the hard drive: Evidence of Detective Mark Lounsbury

Q At some point, you had this computer powered up, correct?

A Yes.

Q And you were in the process of conducting a forensic examination of the hard drive, is that correct?

A Yes, sir.

Examination of the hard drive: Evidence of Detective Mark Lounsbury

Q Could you tell the jury what you did in order to begin this investigation.

A I utilized a program known as Computer Cop Pro. It's an examination software. What it does is it examines the hard drive for stuff that I tell it to look for. In this case, I told it to look for things that are associated with the Internet and web pages. So pictures that are commonly used are known as GIFs and JPGs and variations of JPGs. Also, I instructed it to search for certain types of words, and again, in the Internet there is not your words as we know them there, it's HTML, which is a language. HTML, rich text format, TXT's, and I told it to search specifically for them, and then there were specific words that are utilized that give you the most information with that group of words looking for pornographic-type stuff.

Mark Lounsbury was explicitly asked if he had tested the hard drive for viruses and spyware in cross-examination:

Q Did you examine the hard drive for spyware, adware, viruses or parasites?

A No, I didn't.

Malicious software

Evidence of Mr Robert Hartz, the information services manager for the Norwich Public Schools System

Q To your knowledge, was the PC in question, Mr. Napp's PC, to your knowledge at the time infected with any viruses?

A Not to my knowledge.

He confirmed this when cross-examined:

Q Was there any adware, spyware or virus found on the computer?

A I did not find any of that, although I did not look for adware or spyware.

Content filtering

Evidence of Mr Robert Hartz

Q You mentioned in your testimony today that you have content filtering on your computer, your firewall wasn't updated, is that correct?

A That is correct. It had not been updated, I would say, for a few weeks.

Exercise for group 2: Analysis of the presentation of the evidence in court: Colour of links in Temporary Internet Files

Instructions

Please read the extracts from the transcript of the trial (below), and consider the following points for discussion:

1. Is it factually correct that a link changes colour when it is clicked?

2. Can a web designer actually decide what colour a link will be? The police officer asserted that if a web page was in the Temporary Internet File, it proved the user actually clicked on to the web site.

3. Is it factually correct that a web page must be clicked for it to appear in the Temporary Internet Files?

4. Will all the evidence of the web sites visited be included

in the Temporary Internet Files?

Exercise for group 2 – excerpts from the transcript of the trial

The police officer, Mark Lounsbury, was recalled to give further evidence on the third day of the trial. He gave evidence in particular in relation to the change of colour of a link:

Q Are there any specific characteristics that may occur to a web page when you click on specific link?

A Yes. When you click on a link, again, links are Javascripted, you click on a link, it changes color and then you will get sent to that new address, that new page or site.

.....

Q I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?

A The color, it's red.

Q And to your knowledge, based on your forensic examination of this machine, what may that indicate to you?

A That indicates that that link was actively clicked on and you were then sent to that page.

Q Okay. So a person would actually have to click on the Female Sex Enhancers link to go to another page, correct?

A. Yes.

When examined by the defense attorney, the police officer continued:

Q Detective Lounsbury, you indicated that, I guess, the coloration in the photograph shown to you by Mr. Smith indicates that links were clicked on, is that correct?

A Yes, sir.

Q When you say indicated, you are not saying a hundred percent?

A I've never seen anything other than that.

Q But you're not saying a hundred percent?

A In my mind it is.

Q Are you saying you're positive?

A Based on my knowledge of how it works, yes.

Q What about the science of it also?

A Which is based on my knowledge of the science.

Exercise for group 3: Analysis of the investigation: The physical evidence

Instructions

Please read the extracts from the transcript of the trial (below), and consider the following points for discussion:

1. What items should have been seized?

2. What actions should the police have carried out with the computer?

3. How should the computer have been stored and handled?

5. What information should the police have recorded when seizing the computer?

6. What evidence should the prosecution give to the court before introducing the evidence of the hard drive?

Exercise for group 3 – excerpts from the transcript of the trial

Actions of Mr Napp, the teacher

He went into the classroom on 20 October 2004 after being informed what happened the previous day. From the transcript of the trial:

Q What did you do?

A I turned on the computer and there is a way I can just check basic files that have been placed on the computer within however long you make the time frame, and I just searched for yesterday.

.....

Q Did you see various Internet access sites?

A I saw a bunch of different sites of some pictures that had questionable names.

Q On the Internet site as you say, as an example, what drew your attention to those various sites?

A Some of the names. I clicked on one and I don't remember the name, but it ended up being a discussion board about lesbians.

Mr Napp sent an e-mail to the principle, asking how to proceed. During the afternoon of 20 October, the principle visited the classroom, and Mr Napp showed him the 'log' (probably the temporary cache file).

Actions of Mr Robert Hartz, the information services manager for the Norwich Public Schools System.

He attend the school on 20 October and took the following action (from the transcript):

'I then went to the teacher's computer in that room, his computer, and the first thing I did was I took the IP address, because I was going to need that later, so I recorded the IP address. And then I went into the cookies file. The cookies didn't show me a whole lot. But then I went into the temporary Internet files, and that is a number of files that were dated the previous day, October 19th, with time stamps starting I believe around 8:30, 8:35, and going through the end of the day. And so I looked at these and I saw certain sites that were accessed from this PC.'

Computer taken into custody by the police

The computer was taken into custody by Michael Belair, a sergeant with the Norwich Police Department on or about 27 October 2004. He logged the computer as evidence and placed it in the evidence room.

Mark Loundsbury, a crime prevention officer and the computer crimes officer in the Norwich Police Department, retrieved the computer from the evidence officer on an unknown date some two years later. He gave evidence that the computer was last used on 26 October 2004.

Exercise for group 4: Unfairness of a prejudicial nature

Instructions

Please consider the following points for discussion:

1. Sequence of events

The prosecution did not provide evidence of the sequence of events, the times that the seven children that gave evidence were actually in the classroom, at what time they saw the images, the size of the images they saw, and precisely what images they saw.

Was it necessary to prove the proper sequence of events?

2. The prosecution illustrated a number of images to the members of the jury through a computer and projected on to a screen in the court, but did not indicate whether any of the images shown to the members of the jury had been seen by any of the child witnesses, and also did not indicate which image was related to each of the four charges. It is also uncertain whether any of the images seen by the members of the jury corresponded to the images seen by the children.

Was it necessary to prove which child saw which images?

3. Size of the images shown to the members of the jury

The images that were shown to the members of the jury were viewed many sizes greater than the image that originally appeared on the computer screen. This means that where a pop-up was only a matter of two inches square, for instance, the image would be magnified many times on the screen shown to the members of the jury.

Should the members of the jury have been shown the actual size of the image as it would have appeared on the screen?

Should the court have had a number of computers made available so the images could have been shown on the screen as it would have actually appeared?

4. Advanced notification of the defense expert witness

The judge refused to admit the expert report into evidence, and refused to allow the defense expert to give evidence of what was contained in the report.

Was this a correct response by the judge?