Information Security Now – 10

John Mitchell

The defence lawyers usually ask the wrong question. They usually want to know if I can confirm that certain things the prosecution say that they found on a computer actually do exist. The answer is invariably yes, but what they should be asking is: how did it get there, is it likely that the accused knew it was there and very, very importantly, when did it get there? The importance of accurate time determination is often a crucial part of the forensic computing evidence chain. If it got there before the accused owned the computer then it is unlikely that he knew it was there. If the last accessed date is when the accused did not have access to the computer, then it is unlikely that he accessed the file concerned. But unless the timestamp is accurate all the above are cast into doubt. Most timestamps are produced from the computer's internal clock, or from the clock of another computer that the file may have been transferred from. Many computer clocks are adjusted for the local time zone of the country that the computer usually sits in, but laptops travel the world and we need to know if the time zone adjustment was made. The potential for accidental or deliberate manipulation of the time/stamp is huge, so the best form of comfirmation evidence is from something outside of the target machine. Perhaps a transaction on a credit card issuer's machine, or a PayPal invoice. However, in many cases these are not available so it is back to the tedious task of creating a timeline of the events on the target computer. Emails may provide the appropriate mechanism. After all, the reply to an email can hardly occur before the initial message is sent and the reply will have been generated on a different computer and possibly transferred over the internet. Examination of the headers can prove the hypothesis that the target computer's clock was accurate at the time of the email exchange. But was it always so? The creation of a time-line may be tedious, but it can reveal inconsistencies in timestamp evidence.

One of my cases involved a 'missing seventeen minutes' hypothesis that when proven totally destroyed the other side's case. In another, the prosecution's case that the accused had accessed 31 web sites was jeopardized when a time-line showed the sheer implausibility of a person accessing a web site every six seconds in just the three minutes and eleven seconds that the prosecution's internet history revealed. The prosecution's case had been put forward without a timeline and thus without realizing that they were potentially claiming

that the accused had the fastest fingers and most speedy internet connection in the whole world.

Different systems operating in different time zones also present problems. Trying to show a jury that an ATM receipt produced in a British high street showing a British Summer Time timestamp is the same transaction as recorded in Mountain Standard Time on the credit card's computer in the USA is fraught with difficulty (and some amusement when observing the baffled looks of the twelve good people on the receiving end of the explanation).

The documentation of timestamps created by software, whether it be base or application, is woefully inadequate and the forensic investigator often has to experiment in order to ascertain what is being recorded. This is especially true where timestamps have been recovered from deleted records. In some cases timestamps are recorded differently in what are basically the same files. Take the internet history file for example. Yes, but which one? The internet history file exists as a daily, weekly and full-history file, yet each records the time somewhat differently. When looking in the full history file records are stamped with the time zone setting as the base, whereas the daily file takes daylight saving time (if initiated) as its base point. What other applications do is almost anyone's guess, hence the need for experimentation before offering an opinion.

Many pieces of evidence recovered during a forensic examination of a computer are partial fragments recovered from either a cache, or from the slack space between records. These often contain no time stamp information at all and so answering my originally suggested questions will depend on the existence of circumstantial evidence. This may be in the form of an invoice showing that the machine was purchased new on a certain date and has only been used by a single person, ergo it was 'them that did it'. It is then up to the jury to determine if this is sufficiently beyond reasonable doubt to convict.

We urgently need more information on timestamp formats, how the data is obtained and how it is recorded. This a research project which could be conducted internationally and continuously into the future. Is their a British university out there willing to initiate a project and is the BCS willing to provide the seed capital to get it started? Please let me know.

John is Managing Director of LHS Business Control, a corporate governance consultancy which he founded in 1988. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454