



Sometimes it's all about timing

When an incident occurs, the time of events may be critical to the legal case. However, how are these times established? Is it the time when the CCTV system captured the image? When the computer said the person left their home? When the satellite navigation said they arrived? When the mobile was cell sited in the area? Or is it all of the above?

Are witnesses always accurate?

- I know it was 13:05 because I looked at my watch,
- I walked past the newsagents and it was open so it must have occurred after 13:30.

Just like humans, digital devices may not tell the correct time. This means that when analysing events, it is crucial to compare like with like, otherwise the chronology may become scrambled and the evidence contradictory.

Assessing time information in a case

Case information derived from digital systems which regulate their time may assist establishing an accurate chronology of events. Examples include, the date and time of connections in telephone records and the time of bank transactions. However, other evidence may not be so certain. It may sound obvious, however, how many witness statements contain "at 14:45 a file was created on the desktop computer", "at 14:47 the CCTV captured the defendant" or "the evidence is consistent with the telephone being located in Little Street at 14:55 but not at 14:46". What does this all mean?

In my experience, when time evidence is collaborated, it may cause confusion and prove difficult to present a coherent case because the time accuracies of each of the events are unknown. Hence, it is important to clarify such time statements, particularly with regard to significant events. This will hopefully result in an unambiguous timeline to clearly demonstrate the chronology of a case.

Establishing an accurate time for telephone and computer evidence

The date and time of mobile handsets and computers are generally set by a user. Hence, the stored date and time when events happen on the device, may not reflect the actual time when they occurred.

Thorough analysis of the digital evidence may assist you in determining accurate times for the digital events in your case. For example, you may have a case where an alleged event occurred, such as a person accused of driving whilst using a telephone. If this analysis is only based on the information present on the handset, it may not accurately reflect when the telephone was in use.

Sam Raincock Consultancy has been instructed in telecommunications cases where using information in the connection records and data stored on telephones, it has been possible to provide an indication of the accurate date and time of when events occurred such as when a video was captured or a call missed.

In a past computer case, determining who may have used a laptop to perform searches related to the death of a male was vital to the case. The evaluation performed was able to determine the accurate time and consistent location of the usage of the laptop to be able to rule out its use by a certain person.

CCTV – when was the incident captured?

CCTV is frequently assumed to be utilising an accurate date and time, especially when the system is monitored by police, councils or large businesses. However, the stamped date and time present on the footage is not always correct. This means that it is important to determine the date and time accuracy so that the actual time of a captured incident can be derived. Similarly the frame rates of CCTV is often used to determine how long a section of footage occurred. However, if the rate has changed (even slightly) the calculations will be incorrect and your 60mph car could be stated as travelling at 120mph!

It's time to evaluate

When dealing with time, assume nothing and ask everything – compile your case questioning every last time!

© All Rights Reserved. Sam Raincock Consultancy Limited accepts no liability for the content or use of this article.

About the Author:

Eur Ing Samantha Raincock BSc (Hons), MSc, CISSP, CCE, MBCS, CEng MIET is principal scientist for Sam Raincock Consultancy providing digital forensics and information security consultancy and expert witness services. She has produced over 300 reports/statements and opinions in a large range of digital forensics cases including computer forensics, software functionality testing, CCTV systems, IT security, telephone examinations, connection record charting and cell site analysis. She frequently takes instructions in 'odd ball' digital cases where she is required to formulate bespoke solutions.



<http://www.raincock.co.uk>

Telephone: 01429 820131 Fax: 01429 450001