# MAKING SENSE OF ELECTRONIC EVIDENCE (AVOIDING THE COMMON MISTAKES)

Authors – Andrew Smith & Ghaff Khan

June 2019

Even after 20 years I can still vividly remember what it was like as a new police officer having to stand up in court and give evidence as a witness for the first time. It was one of the most nerve-wracking experiences I had ever been through. Having gone through that experience and learnt from my mistakes helped prepare me for my role as a digital forensic investigator. I soon learnt to document everything and not to overlook even the tiniest details.

I have been based in Bangkok now for the past 7 years and, with the push for a digital economy, Thailand 4.0 has meant that the issue of cyber-security has been pushed to the forefront. Each year we continue to see a growth in demand for forensic awareness training and for forensic examinations. However, there is still a general lack of understanding about digital forensics and we continue to see companies making the same mistakes over and over again.

Electronic data is fragile, if there is any chance it may be used as evidence in legal proceedings, then it must be handled in a certain way so it is possible to demonstrate to the court that the integrity and authenticity of the evidence has been maintained. If mishandled, then the evidence may be called into question when presented at court.

The majority of our investigations involve the theft of company data by rogue employees. Management will naturally turn to their IT staff to begin an investigation and collect potential evidence. However, consider the following points:

- Usually the IT staff have not been trained in how to conduct a methodical investigation
- They are often unaware of the need to maintain a complete chain of custody from the collection of data stage through to producing a report
- They are unaware of all the potential sources of evidence
- They lack the specialist tools required to conduct a forensic investigation
- They lack experience in correctly interpreting the findings of the investigation
- They lack experience in preparing evidence and professional reports for court
- They are inexperienced at presenting digital evidence at court as an expert witness

Companies often assume that as long as the person conducting the investigation holds some type of IT qualification then this will be sufficient. Digital forensics is a highly specialized field and, as demonstrated by the points above, requires a forensic investigator with the qualifications and experience to conduct the forensic investigation.

Another important issue to consider is the experience of your legal team. Do they have experience of dealing with cyber-crime cases and do they have the technical understanding of digital evidence? Due to the potential complexity of cyber-crime cases the legal team will often have to work closely with the forensic investigator to ensure the best possible outcome in any legal proceedings.

Without doubt the number of legal cases using electronic evidence will continue to grow. Also, as the number of forensic specialists in Thailand increases, we can expect to see electronic evidence that has not been handled correctly being more robustly challenged in the courts. If you are involved in legal proceedings where the other side is presenting digital evidence, you should consider hiring your own forensic expert to examine the validity of their evidence. In order to give yourself the best chance of success in any legal proceedings, make sure you use suitably trained forensic investigators and lawyers with the experience of dealing with electronic evidence.

My colleague Andrew was keen to get my perspective as a lawyer. Here it is.

As a young criminal defence lawyer a senior colleague advised me that the only way to succeed, whether you are prosecuting or defending, is to put all your energy into preparing your case for trial and most importantly, to "know and understand the subject matter". Back then it was reasonably straight forward to understand the subject matter of the criminal charges before you. Today it's a very different story indeed.

Technology has developed at an exponential rate in the last decade or so and has given rise to a far more sophisticated medium for the dishonest perpetrator to cause damage to the unsuspecting victim, be that an employer, a business, a bank, the Authorities or even another individual.

The motive of the crime can be to damage the reputation of the victim, unlawfully obtain the victim's confidential information or fraudulently acquire cash or other assets belonging to the victim.

As a lawyer prosecuting or defending such a case the task of knowing and understanding the subject matter of your cybercrime case is an extremely difficult one. After all you are a lawyer and not a trained scientist. This is where you need to work alongside an expert with digital forensics training and experience.

As Andrew mentions above, lawyers and other prosecuting Authorities will often rely on persons who have some level of IT training to try and make sense of the data. This is where mistakes can occur.

As lawyers we have a duty to our clients to get it right from the outset. There is no point in taking a case to trial with little prospect of success because you cannot properly explain highly technical evidence to a judge in such a way as to convince him of the perpetrators guilt, beyond reasonable doubt. Equally, the accused has a right to a fair trial and that means we have to be able to challenge technical evidence which clearly does not support the charges faced by the accused.