ARTICLE:

Digital evidence and digital forensic education

By **Goran Oparnica**

Introduction by editor: I invited Goran to write about the need for education in digital evidence from his perspective: that is, somebody that moved into digital forensics in Croatia some years ago because of a need by his then employers. Goran is well aware of some of the excellent books on digital forensics, as well as the books written by lawyers on the topic. This is a polemic and a personal view from a person providing a digital forensics service in a country that does not have the luxury of resources that other, better off, countries have.

What is the current situation in Europe regarding education in the field of digital evidence? Do we understand the need to explain to lawyers and investigators what digital evidence is, and how do we need to deal with it? The situation differs across Europe. The developed part of Europe has a long tradition in the education and formal training of both lawyers and police investigators. For example, there are a number of universities in the UK, Germany and France offering master degree in digital forensics.

But the position in Eastern Europe is different. For example, it is very common for Croatian law students to get their diploma without even mentioning digital evidence during a course that takes five years.[1] Similarly, the police academy will not even mention to future criminalists that at this very moment there is no organized crime without digital evidence. And only few information and communication technology (ICT) engineers will attend an optional class that will cover information security, including, in part, digital evidence and digital forensics. But it is not just about Croatia, because many of the states that make up the Eastern European countries need to understand that a fundamental change has occurred, which means digital data and the misuse of modern ICT technologies by criminals must be covered by a core curriculum.

This article has been written in an attempt to convince the people responsible for the curricula that it is not possible to respond against organized crime without a substantial shift in approach towards digital evidence.

[1] Editor's note: it is the same in the UK.

Technology is developing at rapid speed. This rate of development poses great challenges not only for non-IT people, but also for computer professionals. There is one fact not to be forgotten: with every change of technology, the nature of digital evidence also changes. Some changes are so revolutionary that we need a new approach during the investigation phase. One of the main questions is: how can police investigators and prosecutors, who do not have an IT background, keep up with those changes?

Introduction

One might get the impression that the importance of digital evidence itself is overestimated and that digital evidence is just another type of evidence that police investigators, prosecutors, defence lawyers and judges have to deal with. Nothing special about it, why so much noise? But is it really so? Is digital evidence just another type of evidence that does not require any special attention?

I have strong belief that it is not. Digital evidence is substantially different than any other type of evidence that the courts and police are used to dealing with. There are few reasons for this statement.

First, digital evidence is dependent on information and communication technology (ICT). If we look back not that many years into the past, maybe just 15-20 years, we have witnessed the enormous advance of ICT technology and the penetration of it into everyday life. Every technological advancement means a little bit of different digital evidence. Slowly but surely, digital evidence has evolved bit by bit, and today the complexities are completely different from the 1990s. Unlike traditional evidence (finger prints, DNA, spirals on the bullet), the nature of digital evidence is constantly changing, and every new version of an operating system brings slightly different forms of digital evidence.

The next point is the fact that not all digital evidence is the same. The family of digital evidence is enormously huge. The digital forensics of mobile telephones requires a different approach than digital forensics of computers or networks or the Internet. Even if we focus only on mobile telephone forensics,

every operating system requires different approaches. More recently, the encryption of mobile devices brings completely new challenges into the equation.

Besides this, we have to take care of malware analysis, RAM memory forensics, cloud forensics, Internet and network forensics. And at this moment we cannot even imagine what challenges will bring with the advancement of the Internet of (every)thing, when almost every little box around us will start to communicate IP language and become connected.

This article does not offer a universal solution, and I will not offer any comprehensive solution. The idea behind this article is just to share my experience in educating the different types of participant in this linked topic of digital evidence. I also offer my views on this very complex and very demanding area – digital evidence and digital forensic education definitely is a very complex and demanding area.

Challenges

How to match speed and time

The digital forensic field is enormously wide. As technology advances, it becomes more and more complex. Understanding what is really going on beneath the surface on the level of bits and bytes is very hard, and with time it will be even harder. Under these circumstances, it is a challenge to decide where and how to start the process of education.

One of the main challenges is the lack of good, comprehensive up-to-date educational programs in the digital forensic field. Imagine that developing one good course takes between 6 months and one year of hard work of a few people who are experts in their field. Why does it take so long? Digital forensics is a hands-on discipline. To develop a course you need to define the syllabus. In accordance with this syllabus, the next step is to write a manual (or recommend a book or number of books) that will provide simple and clear language to explain all the areas covered on the syllabus. The manual should be supported by other relevant materials to reinforce the training of students. In addition, the most important and more complicated part is to develop hands-on training. Digital forensics is a practical discipline, and you need to be able to sit by the computer and do the investigation. You cannot learn it by reading a book, you need to try it and to solve the problems you will encounter that no one can predict in the first place.

To have hands-on training, you have to have an evidence file. An evidence file is a forensic image of real system, for example of a mobile telephone or a PC. But it cannot be just any mobile telephone or PC. The content of the mobile telephone or PC needs to reflect the learning objectives of the course itself. So, there is an option to use real forensic images from a real case, which might not be acceptable from the legal point of view, or you can spend the time and effort to fabricate material. I took part in fabricating images for mobile telephone forensics training for iOS, Android and Windows mobile telephones. It took 3 months of around the clock work of 6 college students to create a 'near-real' image of a mobile telephone.

So, after whole this procedure, after almost one year of hard work on developing a course, what can happen? If we talk about some extremely fast developing technology such as malware or Internet traffic, in the one year time frame you need to develop the course, you can find yourself in trouble: the knowledge you built into the course or some part of it will already be obsolete.

Lack of digital evidence professionals

Who will do the job? Who will design and develop courses? And who will deliver it? First things first. The design and development of courses needs to be done by digital evidence professionals. In today's world, people with such knowledge are extremely busy with conducting investigations. They can hardly devote themselves to spending time to such an attractive activity like writing material for courses. Even if you persuade someone to make version 1.0 of some course, maintaining the content of the course and keeping it up-to-date will be a struggle. We have seen courses that have simply disappeared as they have become obsolete.

The challenge is about finding experienced instructors to provide the course. The instructor must be a person with personal experience in digital forensic investigations who can solve tiny but crucial every day problems, such as finding the right connector, improvising power supplies, finding workarounds for network segments, VLANs, bridges, etc. Digital forensic investigation is never straight forward outside the conditions of the laboratory. There are always situations where knowledge obtained by experience and that cannot be read from books is crucial. This is

why a person teaching digital forensics needs to be an investigator.

We also need number of professionals to cover the very wide spectrum of subjects that make up digital forensic education. It is very clear that finding a single organization capable of performing this task is not easy.

Who needs educating?

As IT technologies emerge in every aspect of our lives, we become increasingly comfortable with its use due to the 'friendliness' of IT. However, the ways bad guys misuse the same technology becomes more and more innovative. Can you remember 20 years ago when e-mail slowly started to be part of our everyday lives? Did anyone have an idea at that time that e-mail will become a very popular channel for malware distribution? Do we know how IP fridges, microwave ovens and wearables will be misused in the future? No. We need to sit and wait to see what the future will bring. And where possible, to prepare ourselves.

Proportionally, the population of good girls who seek digital forensic education is increasing. The need for forensic knowledge by law enforcement is very easy to understand. They are the ones who will sooner or later find themselves in a position that requires them to investigate digital evidence. Their demand for digital forensic knowledge is self-explanatory.

But when we speak of the law enforcement people, we mainly consider professional digital forensic investigators or analysts. We do not think of first responders – the people who will find themselves first on a crime scene. They surely know what do to, or what not to do with the spots of blood or spent cartridges. But do they know how to protect a mobile telephone found on the crime scene from being remotely erased? Or what (not) to do with live computers? The time is now when some degree of digital forensic knowledge is as important to law enforcement people as the traditional police skills.

After the police finish their job, the case will hopefully reach court. The prosecutor will have to explain the charges as well as the evidence supporting the indictment. The judge will have to understand the evidence. When we refer to 'traditional' evidence, there will surely be no problems, because the prosecutors, judges and defence lawyers know how to interpret this evidence: this is what they have been doing their whole career. But if evidence is digital, do they really have enough knowledge to be able to understand the nature of the digital evidence as well as the process of collecting and interpreting it?

I have the strong opinion that digital evidence will become (or already is) inevitable in more or less all cases in legal proceedings. This is why prosecutors and judges will have to have at least the conceptual knowledge connected to digital evidence as well as the procedures dealing with handling and investigating digital evidence. Without it, the effectiveness and fairness of legal proceedings will be questionable.

There is also one party that we often forget in our considerations about knowledge on digital evidence. This party is the defendant in criminal proceedings. We have seen many cases around the world where best practices and lawful procedures have been disrespected and where digital evidence has been misinterpreted by all those taking part in the proceedings. How can a defendant be sure that their defence lawyer really understands the evidence? Has the defendant chosen the right lawyer? This situation is not much different with any other type of evidence: how can the defendant trust that their lawyer is sufficiently knowledgeable to represent them? If a lawyer does not have any knowledge of digital evidence, are they negligent?

Who provides education?

Many organizations offer digital evidence and digital forensic education. They include law enforcement agencies; academia; the private sector; NGOs; independent consultants. Which one is the best for the task? There is no universal answer on this question, as each of those organizations have their strengths and their weaknesses, depending on the area of education we refer to.

From my experience, one of the main criteria to use when deciding where to educate is the duration of knowledge that will be acquired. Some organizations are by their nature slow in defining educational programmes. For example, universities have procedures they need to follow that will additionally slow down the development of programmes. This is why, arguably, they might not be the first choice for educational programmes whose content changes very fast.

On the other hand, a good digital forensic practitioner cannot avoid getting her hands dirty with bits and bytes and low level digging into content of memory and hard drives. The best place to learn such basic and comprehensive knowledge is definitely academia. Academia can offer the deepest possible basic knowledge how ICT technology works. No matter how technology will change in the future, unless some revolutionary new computing technology will be introduced (such as, for example, quantum computing) this knowledge with enable forensic investigators to solve every challenge they will face in their practise. Good fundamental knowledge works as facilitator for acquiring new knowledge and for solving operational problems. No one can do it better then academia.

Another very valuable source of knowledge are the law enforcement agencies. Who can teach police better then police itself?! Yes, this is mostly true. Again, problems occur because knowledge changes very fast. Law enforcement agencies do not have digital forensic professionals dedicated just for training. Usually what happens is that they find some enthusiast who will in his free time put together some training material to be used in future training. The challenge appears in the future, when material needs to be updated. Also, enthusiasm has an expiration date. Having training material version 1.0 or even 2.0 is always achievable, but one systematic and persistent approach to education cannot be based on the enthusiasm of a few persons.

Developing the path

Speaking from the perspective of the digital forensic investigator, the main question is what courses to take, when to start, how to proceed. Simply speaking, the question is how to develop the path to knowledge.

Having in mind the technical nature of the digital forensic investigator's job, a technical background is more than welcome, although it does not follow that it is necessary. A degree in computer science will give the candidate the necessary deep and detailed grounds of how ICT technologies work. This is a necessary prelude to understanding the increasingly complex nature of digital forensics.

After having gained a solid knowledge on the basics of ICT technologies, the next step is to learn the basics of digital forensics, like the principles and methodologies of digital forensic investigations, the legal aspects of investigation and possibly the some typical court cases. As the final purpose of every criminal investigation is supposed to be the hearing of the case in the court, every digital forensic investigator ought to understand this legal part of the business.

I have a strong belief in specialization. As digital forensics is a very wide area, covering a lot of different and fast changing technologies, one person cannot simply be a specialist in all areas of digital forensics. That is why it is necessary to choose the area to specialize. From the technical perspective, we can have few areas of specialization. The first one has to be computer forensics, or what is called dead box forensics. It is focused on hard drive investigations and as subspecialisations, such as MS Windows forensics, Linux and Mac forensics, etc.

Memory forensics is connected to computer forensics. Investigations of IT incidents requires a good knowledge of how to acquire data from RAM memory and how each operating system handles memory, as well as a good knowledge of malware. And yes, the bad news here is that things change fast: very, very fast.

The third area for specialization is the investigation of mobile platforms. It is important to understand that mobile platforms do not necessarily mean mobile telephones, but other devices, such as GPS navigation units, cameras, music players, etc. Having in mind the advance of mobile technologies, it is expected that future investigation will involve ever rising number of mobile devices, and over the time, they may prevail above desktop or laptop computers. Again, there are subspecialisations that follow the operating system.

There are some areas of specialization that touch all of those mentioned above. They are based on the investigation of the artefacts on end user devices (mobile telephones, smartphones, computers) but due to the nature of artefact, have a different approach. Those areas are cloud forensics, Internet and network forensics, social media forensics, even open source intelligence can be considered as one special areas of digital forensic investigations.

To certify or not to certify?

Bearing in mind the extremely complex and increasing importance of digital evidence, it is possible to have doubts about how knowledgeable the potential professional can be. The evidence from around the world demonstrates that lawyers, judges and police investigators make mistakes, and they also make mistakes when dealing with digital evidence.

When speaking about this issue with one judge, I got a very interesting opinion from the judge. The judge said that in one case they had an issue with matching the footprint of the defendants shoe in the mud. One expert witness claimed they matched 30 per cent, and another expert claimed they matched 70 per cent. The footprints provided very clear tracks, which meant that we can all understand them. If the difference in interpreting such a clear thing like footprint in the mud can be so significant, how can the lawyers be expected to decide about such a complex and abstract things such as digital evidence? The judge might be right. This is where an independent certification process steps in. The stress here is on the word 'independent'. Obviously, it is not acceptable that the organization that provides education also provides certification at the same time. In such a case, the organization is indirectly certifying itself. This is why certification needs to be conducted by third party.

A more complicated issue is with the certification process for court expert witnesses. Every jurisdiction has its own procedure as to how to become an expert witness, or how to permit a witness to be considered an expert witness. There are few jurisdictions where the procedure does not guarantee anything in regards to digital forensic knowledge. This is something that, for some countries, the provision of suitable education and the reaching of a certain standard will be important.

Conclusion

As described above, education in the area of digital forensics and digital evidence is very complex and there is no one-size-fits-all answer. Digital data, and therefore digital evidence is complex and changing extremely fast. This is why every person who has an interest in digital evidence, no matter whether they are a lawyer, judge or investigator, needs to find the right approach and be educated: for the sake of justice.[2]

Goran Oparnica has a background in information security and digital forensics with more than 15 years of experience. He is the CEO of INsig2, with a portfolio of more than 50 different digital forensic courses designed both for lawyers and digital forensic investigators, they are delivered all around the world.

http://www.insig2.eu

goran.oparnica@insig2.eu

[2] Two authors have already argued for the education of lawyers, for which see Denise H. Wong, 'Educating for the future: teaching evidence in the technological age', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 16 – 24 and Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 23 – 28.