Van: https://www.helpnetsecurity.com/2013/05/31/becoming-a-computer-forensic-examiner/

# Becoming a computer forensic examiner



Since the advent of affordable personal computers, digital devices, and later the Internet, these technologies have been used for both legal and illegal purposes, and in order to collect evidence to help prosecute some of the people engaged in the latter, a new science had to be born: digital forensics.

One of the branches of digital forensic science is computer forensics, which deals with legal evidence that can be extracted from computers and digital storage media.

Evidence secured by practicing it has begun to be used in criminal law in the mid-1980s, and since then, the need for computer forensics and specialists that practice it has risen in concordance with the exponential escalation of computer and computer related crime.

But as **Gary Kessler** – president of Gary Kessler Associates, a consultancy that among other things offers services related to computer, network, and mobile device forensics – tells me, breaking into the field is surprising hard considering the need for this specialty.

“One key is that someone who wants to enter the field has to be prepared to move. While there are a ton of information security jobs and they’re all over the place, computer forensics companies large enough to hire entry-level people or give internships tend to be clustered in the larger population centers,” he points out, adding that the U.S. government can also provide great training, and that the DoD and DHS are currently hiring.

“I would recommend you get at least a bachelor’s degree in computer science so you have a good background. Get experience in a corporate IT department and then you can work for a law enforcement agency or cyber security firm,

among others," advises **Dr. Hans Henseler**, founder of the Forensic Computer Investigation Department at the Netherlands Forensic Institute, and managing partner of the Forensics Business Unit at Fox IT, the Dutch security audit firm that investigated the DigiNotar breach.

"Starting in law enforcement helps to obtain important experience and after five years you can go to a commercial company and be very valuable," he says, and points out that while many law enforcement agencies require one to be a law enforcement officer, some will hire civilians or outsource their work to commercial companies.

In the U.S. that could mean any number of federal, state, and local agencies, including the FBI, secret service, IRS, SEC, Department of Justice, and so on. In the Netherlands there are perhaps twenty different government bodies involved in computer forensic investigations.

Kessler's advice on being prepared to move might even mean moving around the world. According to Henseler, there is a big need for people in Asia, including China and Singapore.

"If you take advantage of these opportunities you can grow your career quite fast," he says, adding that being able to speak several foreign languages as well as to communicate well with non-technical staff such as lawyers and accountants is a big plus.

**Maqsood Ahmed**, Principal Security Consultant (EMEA & APAC) at Guidance Software got his start in the British Police Force, in 2002, with one of United Kingdom's biggest ever computer crime investigation. "I've always been interested in IT and so Operation Ore, coupled with my IT skills, was a right fit."

"I enjoy the digital analysis and the development of technology, various processes, procedures, and so on. I don't necessarily consider it a difficult job – more of a hobby," he adds, then points out that a good computer forensic investigator has to be inquisitive, analytical, detailed and have an advanced level of interest in technology.

“I think the recipe for success is a mix of higher education and professional certificates, coupled with common sense, as well as professional certificates that can demonstrate your interest in, and ability to understand the security field, technology, processes, and so on.”

If you’re wondering where to get the needed education, Henseler offers some pointers: “We are starting to see Bachelor and Master programs in Computer Forensics offered. For example, the University College in Dublin offers a masters degree in computer forensics. There are commercial training programs such as those offered by the SANS Institute. They provide pretty good training in all parts of the world. And there are digital forensics product certifications that are also important. The two main companies whose products you will use are Guidance Software, and AccessData. Finally, computer forensic investigators need to understand how computers work so companies such as Microsoft and Oracle have certifications that can also be useful.”

Kessler considers problem solving, the ability to manipulate symbols and numbers, tenacity, and technical astuteness as traits essential for any good specialist in this field.

“Educational background should be something that supports those traits; ideally – but not necessarily – math, engineering, or computer science but also criminal justice. What people need is the methodical approach to the problem and a well educated person of any stripe can be trained to the level they need, particularly as it relates to conducting investigations,” he says, adding that good certifications that are generic and useful include the Certified Computer Examiner (CCE), Certified Forensic Computer Examiner (CFCE), those from SANS, as well as product-specific certs.

“In my career I have hired a lot of people, and there are three general types that I see be successful,” says Henseler:

- People with a computer science background who have also worked in a corporate IT department, as they know how companies manage their IT systems. Still, they also need to add the necessary forensics requirements.
- Students who have their masters in forensics investigations but not necessarily in forensic IT. They know how to generate reports but are

usually not technical enough. But they need to have a forensic mindset and an avid interest in computers and IT, and to be trained to use the appropriate tools.
- Smart people that have a masters in computer science and who can pick up the forensic tools or can make their own tools. They can become great computer forensic experts, but also good project managers and can help with client communications.

Finally, I wanted to know what are the biggest challenges of the job, and do they consider it to be a hard?

“It is hard job because it is highly technical but you have to also be very precise in your communications,” says Hensler.

“There have been big changes over the years. Data starting growing ten years ago and while law enforcement agencies have hired more experts there are not enough experts to go through all the data. The challenge is to enable non-technical people to help investigate so the experts can focus on the most challenging and technical aspects of the investigation,” he points out, and to that end he developed Tracks Inspector, a product designed for criminal investigations that enables non-technical investigators to examine evidence themselves.

Kessler thinks that one of the hardest parts about it is the effort needed for staying current. “Many of the criminal cases are also very trying on an emotional level, particularly those involving child sexual exploitation. But, again, it is very rewarding, too,” he says. “I enjoy working with law enforcement because the work is important and they need the help. I don’t do criminal defense work but I do engage in civil forensics work.”

When asked how he approaches testifying at trials, he says that he talks to judges, juries, and lawyers the way he talks to his students (he’s currently on the faculty of the Homeland Security program at Embry-Riddle Aeronautical University, where he is developing a minor in cybersecurity) or his mother: he tries to explain things as simply and accurately as possible, providing no more detail than necessary to illustrate rather than confuse the issues. “In that regard, I view myself as an educator as much as anything else,” he shared.

He also says that the prosecution of cybercriminals is handled pretty well in most cases but could certainly be improved by better preparation of prosecutors and investigators. “We can’t control the jury pool and most judges are looking to the attorneys – and their experts – for appropriate explanations.”