Interview with Dr. Ray GENOE

Dr. Ray Genoe is a researcher and lecturer who is currently working for the Centre for Cybersecurity and Cybercrime Investigations at University College Dublin. His primary role involves providing education, training and operational solutions to the global law enforcement community in the field of cybercrime investigations.

Dr. Genoe has been working in the field of cybersecurity and cybercrime investigations for over 5 years, since completing his PhD in 2010. He has a broad experience in numerous fields, which include digital forensics, network security, privacy and data security, and legislation.

1. You are a lecturer in UCD Centre for Cybersecurity and Cybercrime Investigations. Can you tell us about the role of this Centre in education in the field of cybersecurity and cybercrime?

Certainly. UCD-CCI is dedicated to enhancing the capabilities of the law enforcement community, government departments and our industry partners in the fields of cybercrime investigations and cybersecurity. In addition to providing bespoke training courses to these stakeholders, we also contribute to the MSc. in Forensic Computing and Cybercrime Investigations at University College Dublin. This unique Masters is a distance-learning program that is exclusively for law enforcement investigators.

2. How important is the activity of training the investigators?

Training is absolutely vital, in my opinion, particularly when you consider the demands placed on modern-day cybercrime investigators. These professionals must maintain a deep knowledge of all state-of-the-art technological advancements, in order to understand how cybercrime is conducted. Criminals are constantly evolving their practices to evade detection and discover new exploits in IT infrastructures. Not only should the cybercrime investigator attempt to stay one step ahead of the criminals but they should also seek out new methods to carry out their investigations. This is why training is so important and, unlike other fields, professional training should never be complete due to the constant evolution of technology.

3. The variety of applications available on Internet makes the process of extracting evidential data from digital devices a little bit difficult. What does a forensic examiner need to do to face new challenges?

While most examiners will have a standard "tool-belt" of forensic techniques and software applications that they use, these are often found wanting when new applications are encountered in an investigation. Even commercial software vendors find it difficult to keep up with the volume of new applications developed, and their software is often unable to locate and extract evidential data. Two of the key qualities that make a good forensic examiner are flexibility and invention. The ability to create innovative solutions when faced with new challenges is vital for success, in the ever-changing playing field of digital investigations. Since Internet artifacts and data are usually stored in various types of databases, a strong knowledge of database management systems and programming can help examiners. Armed with these skills, the examiner can create new solutions to extract evidential data.

4. Cyber criminals are taking advantage of the evolution of technology and they can create more complex and powerful tools. How difficult it will be to stop them in the future?

I don’t believe that cybercriminals can ever be stopped from conducting crimes, since there will always be some weakness that can be exploited in IT infrastructures, software and hardware. I think the main thing to worry about is how difficult it will be to catch cybercriminals in the future. Encryption technologies are increasingly being used by default, both to secure communications over the Internet and to protect the data stored on devices. The algorithms used for encryption have become much more robust in recent years, making it very difficult to intercept communications and forensically examine storage devices.

5. Nowadays, almost anyone can become a cyber-criminal. Are you concerned with the evolution of cybercrime in Europe?

I find it a little concerning that children are becoming increasingly adept in their technical expertise. With enough interest and a few selected YouTube videos, a 10 year-old child can quickly become a hacker. This will most likely be a huge issue for the next generation of cybersecurity professionals and cybercrime investigators.

6. Lately, the number and the complexity of cyber-attacks have increased in Internet. How do you think these attacks will evolve next years?

I believe that the evolution of the “Internet-of-Things” will raise many issues in the future, with regards to cyber-attacks. These devices will either be the tools or the targets of cyber-attacks. For example kitchen appliances could potentially be hijacked to be participants in a denial-of-service attack, or the safety controls on a smart-car or gas boiler could be remotely disabled.

7. What is your opinion about open source solutions? How good are these solutions for forensic examination?

I would say that, much like commercial software, the quality open source solutions can vary from product to product. Open source software is often frowned upon, particularly by staunch users of commercial software. There are many reasons for this but one of the most prevalent is the historical acceptance of commercial software in courtroom environments. Validation and verification of these tools is often conducted at some point in this history, leading to future software releases to being accepted without question. This is something that I would have issues with personally but these commercial solutions are still being accepted in court without recent validation. Good open source solutions often have to increase the detail of the reports they produce in order to support their findings and compete with their commercial counterparts. To use one example, the excellent file-carving tool “Photorec” produces a report that specifies exactly where each of the files it recovered can be found on a disk image. A skilled forensic examiner can use this information to manually carve the file and prove that the process was correct. This process would probably even be necessary when cross-examined in court, since to my knowledge “Photorec” has not been scientifically validated. This may seem like a strange requirement, since it is highly unlikely that a forensic tool could fabricate a photograph or movie that was recovered as evidence! This is another reason why open source solutions are often frowned upon. In reality, the user must be more knowledgeable in the field, since they may be asked to prove their findings.

Due to the budgetary restrictions of most digital investigation units, I am increasingly being asked to discuss open source solutions in the training that I provide. In fact we now do not possess any commercial forensic software licenses in UCD-CCI, which we would use for consultancy work or training courses. The main focus of our training is now to use Linux as a forensic tool, since this operating system and the forensic tools available for it are completely free of charge. Aside from mobile phone forensics, everything that commercial forensic solutions are capable of producing can be replicated, and often bettered, by these open source solutions. While saying this, the field of open source solutions for mobile phone forensics is growing rapidly and it is only a matter of time before a great solution is developed and maintained in this field also.

I am also involved in developing open source software solutions under the FREETOOL project, which is an EU-funded project that is managed by UCD-CCI. The aim of this project is to develop and disseminate, free reliable tools for the law enforcement community. The project has been hugely successful and, along with our software developers from the law enforcement community, we hope to extend the project for another few years.

8. You have a course about VoIP and Wireless Investigations in UCD. Can you tell us some of the risks of using a free wireless network?

Open wireless networks, such as those found at airports and coffee shops, are a great utility when killing time waiting for a flight or enjoying a coffee. I would not want to put anyone off using them to do some simple tasks like checking flight information or reading the news. However you should always be aware that your information is being broadcasted through the air for anyone with a little knowledge to intercept. You should always consider what you are doing when on these free/open networks. A useful way to think about what you are doing on these type of networks, is to imagine yourself reading aloud on a train that is packed full of people. You might read out the latest news stories but would you read out your bank details? Would you announce your username and password for your email account to other passengers? If the answer is no then you should never do it on an open wireless network!

9. Many people have a home wireless network. Can you give us some advice on how to set up a secure wireless network?

The short answer is to use WPA2 encryption. You should pick a good long password, using a combination of uppercase, lowercase letters, digits and other characters. As someone cleverer than me once stated, you should always treat your password like a toothbrush; change it regularly and never share it with anyone! If you follow these instructions, it will be very difficult for anyone to gain access to your network or listen to your network traffic.

If your wireless router is over 8 years old then it may not be capable of WPA2 encryption; offering only WEP encryption. If this is the case then get rid of it. WEP encryption can be cracked in minutes due to a weakness in the algorithm used. I would also advise readers to have a look at their wireless settings and check if WPS is enabled. I would recommend that you completely disable WPS if possible. There is a known weakness in the authentication process for this feature also and some wireless routers are vulnerable to attack.

Other security features such as hiding the network name or using MAC address filtering offer an apparent layer of security that is simply not sufficient. You can use these but, like using WEP encryption, a determined hacker can bypass these features in a matter of minutes.

Interview made by Ioan-Cosmin MIHAI
Vice President of RAISA