# Computer technology and forensic science research paper examples

Law, Evidence

Computer forensics is one of the new and fastest growing fields in forensic science that involves collecting and examining different forms of electronic evidence carefully. this not only to assesses the extent of damage that may have occurred to a computer resulting from an electronic attack, but also recovers all lost information from this system as well in order to take legal action against a criminal. With the increasing importance of computer security and the gravity of cyber crime, it has become very important for all computer professionals to understand fully the technology used in computer forensics. Computer forensics, therefore, involves preserving, identifying, extracting, documenting and interpreting computer data.

## Digital evidence

In today's world, computers are often used for to commit crime, and, all thanks to the growing science that employs digital evidence forensics, it has become possible for law enforcement to put to use computers in fighting crime.

Digital evidence refers to information under storage or/and transmitted in the form of binary codes that could be relied on in a court of law. This evidence can be found on computer hard drives, mobile phones, personal digital assistants (or PDA), CDs, and flash cards in digital cameras, among other places. People often associate it with e-crime or electronic crime, such as credit card fraud and child pornography. Digital evidence, however, can today be used to prosecute other types of crimes, and not just e-crime. For instance, the mobile phone or e-mail files of a suspect may contain critical evidence concerning their intent, or their whereabouts when a crime was committed or their relationship with some other suspects. In the year 2005,

for instance, a floppy disk was the link that led forensic investigators to the BTK serial killer. He had eluded the police since 1974 and in this time period killed at least ten victims.

In their efforts to fight electronic crime and collect digital evidence for every type of crime, law enforcement agencies now incorporate activities such as collecting and analyzing digital evidence into their infrastructure. This is computer forensics. One of the main challenges facing law enforcement agencies is the emerging need to train other officers and have them collect digital evidence while at the same time keeping up with the rapidly evolving technologies, for instance the constantly changing computer operating systems.

In recent years, the use of computers and Internet services has become an essential part of life in the society. Today, computer are used almost everywhere; in the workplace, at home, in schools and even in some public areas, for instance, airports and shopping malls.

According to a report released by the National Telecommunications and Information Administration (NTIA), the growth of the Internet in the United States is currently estimated at about two million new users every month. The negative aspect of this trend of excessive computing is that this has led to an increase in the amount of crimes which are computer-based. According to statistics published and research carried out by the CERT Coordination Center, there has been an increase in the number of incidents related to security every year since the year 1998. From the year 2001 to 2003, these incidences more than doubled.

With the increase in computer crime, there has been an increase in demands

placed on people who specialize on computer security and law enforcement. Although many computer security specialists consider the idea of preventing intrusion to be superior to intrusion detection, it is remains necessary to detect intrusion for as long as these intruders continue to succeed. Additionally, in order to put a stop to similar or repetitive intrusive attacks, it is important to have reliable computer forensics experts so as to help in determining why the attack took place in the first place. Therefore, computer forensics is a very important part of preventing intrusion.

Another main challenge facing computer forensics is the ever changing computer technology. This makes it necessary for forensic scientists in the field of computer forensics to always come up with new ideas and methods so as to keep up with this computer technology. For instance, whenever they come up with a new way of testing for the presence of illegal drugs, fibers, bodily tissues, explosives, etc., other people will come up with other developments through which this test will either be altered to make it better or may be proven defective. However, the real need for this test is not likely to change.

The assessment of data media, which is one of the fundamentals of computer forensics, becomes more complicated because every so often, whole new techniques, methods and forms of data storage are made. This takes place every 5 years or so. For instance, fifteen years ago, floppy disks were used to transfer data and they held 360 KB. These have become obsolete and instead people use CDs, DVDs, and flash cards. Computer forensics is one field where, on one hand, newness is the norm and on the

other, obsolescence. People in this field must constantly change their methods to suit the times.

## References

Clarke, N. (2010). Computer Forensics: A Pocket Guide. Brooklyn: IT Governance Publishing.

Maras, M.-H. (2011). Computer Forensics: Cybercriminals, Laws, and Evidence. New York:

Jones & Bartlett Publishers.

Newman, R. C. (2007). Computer forensics: evidence collection and management. New York:

Auerbach Publications.

Vacca, J. (2005). Computer Forensics. NJ: Cengage Learning.