Digital forensics electronic evidence

Digital Forensics/Electronic Evidence

Digital forensics/ electronic evidence Digital forensic involves the concept of retrieving information from computer media. Advancement in technology has made it possible for digital forensic to develop and investigators have found an easier way to capture computer criminals. Digital forensic ensures accuracy is observed and criminals are brought to justice (Daniel, 2012). The three types of crimes covered under digital forensic include; child pornography which is the most diverse type of digital crime. Child pornography destroys the minds of children and at times, it bullies them. Therefore, curbing the problem in time will assist to end this type of computer crime. Theft of personal information is another form of digital crime covered under digital forensic (Johnson, 2006). Majority of internet and computer users have complained about the increased rate of digital crime where money and other crucial information stolen. Damage of intellectual property is also another type of digital crime. In the scene of crime things like those that encrypted files will be retrieved, deletion of significant files and at times tools can also be retrieved at the crime scene.

Improper handlings of electronic evidence can jeopardize with a criminal case adversely. Digital evidence is a new piece of evidence in the court system. Therefore, measures have to be taken to ensure evidence collected through electronic means is well handled and not interfered with to ensure the criminal is proven guilty (Daniel, 2012). Investigators involved in collecting evidence of digital nature ought to have permission to undertake the investigation process. Computers are considered personal therefore; the right procedure should be followed in order to retrieve any form of evidence.

In addition, the investigators need to be conversant with computer and electronic operations this will ensure the criminals do not outshine them (Johnson, 2006). Policies with regard to digital evidence should be adhered to prevent interference with the evidence. Digital evidence also recommends that honesty and validity are observed to prevent evidence interference.

References

Daniel, L. (2012). Digital forensics for legal professionals: Understanding digital evidence from the warrant to the courtroom. Waltham, MA: Syngress/Elsevier.

Johnson, T. A. (2006). Forensic computer crime investigation. Boca Raton: CRC Press.