Chapter 4.10
Digital Child Pornography:
Offender or not Offender

Frank Y.W. Law
The University of Hong Kong, China

K.P. Chow
The University of Hong Kong, China

Pierre K.Y. Lai
The University of Hong Kong, China

Hayson K.S. Tse
The University of Hong Kong, China

Kenneth W.H. Tse
The University of Hong Kong, China

ABSTRACT

Child pornography has become a major cyber crime in recent years. One of the challenging problems in child pornography cases is to distinguish if the subject files were downloaded intentionally or by accident without the knowledge of the computer user. The suspect may admit that he is an erotomania, but argue that the child porn materials were downloaded accidentally while surfing the pornographic web sites. In many jurisdictions, possession of child pornography without user knowledge is not a crime, while the burden of proof is on the prosecution. It is therefore important to identify if the child pornography exists by accident or not. In this chapter, the authors first review the technologies which sustain the prevalence of online child pornography and the recent research on child pornography investigation. Then, the authors present a set of practical investigation techniques. Subsequently, they apply the techniques in a case study with an attempt to distinguish if a suspect is a child pornography offender or just a normal erotomania. This is an important distinction to be made, since a person guilty of child pornography offenses is likely to be punished more seriously under most legal jurisdictions.

DOI: 10.4018/978-1-61350-323-2.ch4.10

INTRODUCTION

This Internet era has propelled communication and information exchange to the global stage. With an ever-growing penetration rate, the Internet is no longer confined to just homes and offices and is increasingly available wherever and whenever we want it. Technology is constantly changing and the types of computer equipment evolved as well as the capacity of storage media is increasing day by day. The development of technology increases accessibility and the distribution of materials online. These are done by enhancing the ease of possession and dissemination, and decreasing the cost of production and distribution, especially cross-border activities.

The advent of IT technologies not only facilitates people on communication and business, it also provides avenues for savvy criminals in the commission of cyber crimes. In these days, digital crimes have evolved such that digital evidence is found in traditional types of crime. Although the motivations of criminals rarely change, the methods of crime commission do. Mobile phones, emails, memory cards, thumb drives, etc are equipments commonly used by offenders used for crime commission. Child pornography is one of the most prevalent cyber crimes. According to the estimated Internet pornography statistics (Ropelato, 2006), there were 100,000 websites offering illegal child pornography in 2006. A greater number of offenders are now using information technology to organize, maintain and increase the size of their child pornography collections. Furthermore, encryption, P2P networks, light and small storage devices and free online storage are used by offenders to share the illicit materials with high efficiency. It is obvious that when child pornographic materials reach cyberspace, they would be circulated more readily and rapidly.

To cope with the emerging problem of digital child pornography, investigators need to develop the skills and competence required for conducting investigations in the digital environment. They must follow the judicial procedures laid down in their own countries to ensure evidence is admissible. They should always be aware that their investigation might be contested on technical grounds. They are also required to get familiar with the concept of digital evidence and the way to present it at the court of laws.

Echoing the widespread of digital evidence, forensic computing emerges. Forensic computing refers to the application of computer science techniques to retrieve digital evidence from electronic device for legal proceedings. Similar to ordinary forensic science, the analytical results of forensic computing examinations are expected to be reliable, accurate and scientific. However, with the increase of space on digital storage media as well as the strength of encryption, it is envisaged that the process of analyzing and locating digital evidence would become more tedious and time consuming without the help of special digital investigation technique and tools. Though the investigation moved from the physical environment to the digital world, traditional techniques still stand. For example, criminals may claim that they are innocent since they only visit pornographic websites, whereas the child pornographic materials were accidentally downloaded to their computers. In order to prove the knowledge of criminals, digital investigators need to analyze the retrieved digital evidence and distinguish whether the act of criminals is intentional or accidental.

It is obvious that child pornography investigation has become one of the greatest challenges to law enforcement agencies. On one hand, it requires very specialized knowledge in information technology and computer forensics which are not normally possessed by traditional crime investigators. On the other hand, the global reach of the Internet allows criminals to effect their illegal acts in any place they choose. The investigation therefore requires synergy of various parties from private and public sectors. The speed of investigation also becomes one of the critical factors. This requires the harmonization of competencies borne