Questions

Countries, United States

Questions Name: Institution: Questions 1. United States federal law provides protection of children from predators, child pornography and prohibits the transfer of pornographic material to minors. It is enabled through the Sexual Predator Act of 1998. Section 203 of the legislation establishes a zero-tolerance outlook on instances of possession of child pornography. As a result, ISPs are required to limit hosting of such content on their servers.

Where necessary, they are required to report such instances to the authorities. Some states provide confidentiality and immunity from prosecution for workers at ISPs who report such cases. Computer technicians, at ISPs, therefore, have a role to play in the fight against child pornography. On the discovery of such content at an ISP, a computer technician has several steps to carry out (O'Donnell & Milner, 2007). First, a computer technician should take preventive action against child pornography traders. The technician may block viewing of such websites and newsgroups.

This is possible through new network configurations, which prevent viewing of such sites by prospective users. In this manner, one ensures that the ISP prevents the spread of child pornography. Secondly, a computer technician should gather maximum information about the instance in question. For instance, the posting dates, URLs and other essential metadata need noting down.

Thirdly, a computer technician should report the incident in question to the appropriate authorities. One may report to federal institutions such as the FBI. Such law-enforcement agencies usually have teams dedicated to

tracking down and arresting perpetrators. After reporting an incident of child pornography, one should determine whether the incident meets the legal specifications of child pornography.

This is done by studying the material in question, with reference to online resources such as the Department of Justice website (The United States Department of Justice, n. d). Finally, one should take measures to exonerate the ISP they work for from legal responsibilities. 2. In this case, the investigator needs to identify the browser used during the incident. This will help to determine the next course of action. To determine whether the story in question is true, first, browser history requires checking.

To determine whether the user in question actually clicked on a pop-up window, the investigations should begin with typed URLs. If ambiguous URLs receive identification, log files on the web server in question need tracing. Servers store log files that indicate IP addresses of computers that are connected to them. The ISP in question should provide subscriber information for the allocated IP address and times of access (Vacca, 2005). Similarly, the IP address, date and time of access need confirmation through the log files. This will prove to the investigator whether the pop-up connected the computer in question to the web server.

Secondly, if the downloaded files are still present, a code analysis needs implementation. To find the files, the download locations need identification. First, the default download locations need immediate checking. Web browser and system caches also need checking for downloaded content, as data may be temporarily stored there. Finally, non-default locations need checking.

This may be the case if the user specified a custom download location for the files, in the web browser settings. When found, the files need comparison with the estimated time of the incident, and the expected filenames. The code analysis will allow the forensics experts to determine whether the code included pop-up functionality for the webpage in question. It will also determine whether the pop-up in question required user interaction or not.

Furthermore, the code analysis will enable the investigators to determine the servers linked to the pop-ups. Finally, investigators should use a virtual machine to confirm whether the suspect’s claims of website functionality were true (Vacca, 2005). References: O’Donnell, I., & Milner, C. (2007). Child pornography: Crime, computers and society. Cullompton, UK: Willan Publishing.

The United States Department of Justice (n. d.). USDOJ: CRM: Child Exploitation and Obscenity Section. Retrieved June 10, 2013, from http://www. justice. gov/criminal/ceos/subjectareas/childporn. html Vacca, J.

R. (2005). Computer forensics: Computer crime scene investigation. Hingham, Mass: Charles River Media.