Step 7: Check ISP Logs

ISP logs contain all Internet activity information that Internet service providers save. They are the logs of the users’ visited Web pages. It can be difficult for an investigator to extract information from these logs for the following reasons:

- Some ISPs refuse to show their logs in order to maintain user privacy.
- Even when ISPs release their logs, investigators may find it difficult to extract the required information from the huge amount of log data.

ISP logs can reveal whether any users that the ISP serves have visited a site that police have identified as a child pornography site.

Sources of Digital Evidence

The following are some of the sources of evidence that play an important role during an investigation:

- **Offender’s computer:** The offender’s computer is the main source of evidence during the investigation of child pornography cases. Any pornographic material stored on the offender’s computer is important evidence for the investigation. Log files show detailed information about who logged on to the computer and when. Web browser history shows the online activities of the criminal. E-mail and chat logs constitute an online communication record of the offender.

- **Handheld devices:** Offenders may also use handheld devices for child pornography. They may use devices such as PDAs and mobile phones with digital cameras to record offensive pictures and transmit digital images. Therefore, these devices are also important in an investigation.

- **Servers:** Servers may also play an important role in an investigation. For example, an ISP authentication server records a customer’s information, including the IP address that can be used to identify the user. FTP and Web servers are generally used for uploading and downloading files; these servers record details about what files are uploaded or downloaded, and they also keep track of the IP addresses of users who connect to the servers.

Citizens’ Responsibility in Fighting Against Child Pornography

Citizens have a responsibility to act against child pornography to try to eradicate it completely. The following are some ways that citizens can fight against child pornography:

- Protest against child pornography Web sites.
- Provide information about the impact of pornography on children.
- Take initiatives to cease child pornography on the Web.
- Report to anti-child-pornography organizations about any child pornography sites.
- Block credit card transactions that are requested for child pornography.
- Ask ISPs to block the content or URL of a child pornography site.

Guidelines to Avoid Child Pornography on the Web

There are many child pornography sites on the Web. The following are some guidelines for avoiding child pornography on the Web:

- **Use Internet filters that filter unwanted content on the system:** Internet filters are pieces of software that are installed on a system in order to block unwanted content, such as child pornography sites or gambling sites.

- **Make use of search engines that have built-in filters:** Search engines that have built-in filters help a user search safely, as they filter results. For instance, Google’s Safe Search feature filters out any sexually explicit or otherwise unsafe images.