Technical Background Topics

Foremost is a scalping program used in linux to help recover information and files from a storage media. It does this by analyzing the structure of files and looking for certain traits called file signatures that file may have, such as a hex value at the beginning or end of the file. Each type of file has it's own file signature that makes it unique, so a scalping tool will use these signatures to find a file among raw data from a storage media. In some cases, individuals may use this reading of file signature by operating system to manipulate it's existence. A common example is looking in directory entries for a 00 HEX that has been manually changed so the operating system would ignore it's existence and an individual could hide data this way.