The traditional approach of digital forensics uses pattern-based search algorithms to locate any evidence among a large quantity of data. However, applications can conceal information by embedding some data into other files either intentionally or not. For example, the camera app, embedding text into an image and encryption. The dynamic taint analysis can be used to acquire the information flow and tells what possible information get stored into a file. Our implementation monitors the application under test and generates a table which contains a list of files and their possible content. This allows the investigator focus on files of interest.