# Audit and logs

Forensic analysis of software log files is used to extract user behavior profiles, detect fraud, and check compliance with policies and regulations. Software systems maintain several types of log files for different purposes. For example, a system may maintain logs for debugging, monitoring application performance, and/or tracking user access to system resources. The objective of my research is to develop and validate a minimum set of log file attributes and software security metrics for user nonrepudiation by measuring the degree to which a given audit log file captures the data necessary to allow for meaningful forensic analysis of user behavior within the software system. For a log to enable user nonrepudiation, the log file must record certain data fields, such as a unique user identifier. The log must also record relevant user activity, such as creating, viewing, updating, and deleting system resources, as well as software security events, such as the addition or revocation of user privileges. Using a grounded theory method, I propose a methodology for observing the current state of activity logging mechanisms in healthcare, education, and finance, then I quantify differences between activity logs and logs not specifically intended to capture user activity. I will then propose software security metrics for quantifying the forensic-ability of log files. I will evaluate my work with empirical analysis by comparing the performance of my metrics on several types of log files, including both activity logs and logs not directly intended to record user activity. My research will help software developers strengthen user activity logs for facilitating forensic analysis for user nonrepudiation.