

Teil VI

Fortgeschrittene Analyse



Ein Intrusion Detection-System ist in der Lage, einen Einbruch oder einen versuchten Einbruch zu melden. Dieser Teil beschäftigt sich nun mit der forensischen Analyse eines Rechners nach einem Einbruch. Es erklärt Ihnen den Unterschied zwischen flüchtigen und nicht-flüchtigen Daten. Anschließend lernen Sie die verschiedenen Methoden und Open-Source-Werkzeuge für die Anfertigung eines forensischen Duplikates des kompromittierten Rechners kennen. Den Abschluss bildet eine kurze Einführung in die forensische Analyse und die Anwendung der Werkzeuge.

