Bìa

Mục lục

# LỜI MỞ ĐẦU

Ngày nay, trong thời đại số, tầm quan trọng của an toàn thông tin ngày càng lớn. Hầu hết các nước, các tổ chức đều đề ra quy định, pháp luật để bảo vệ bảo vệ dữ liệu và an toàn thông tin của mình. Với sự gia tăng đáng kể của tội phạm mạng thì vai trò của điều tra số ngày càng lớn. Điều tra số (Digital Forensics) là một nhánh của khoa học điều tra, với mục đích truy tìm và phân tích các tài liệu chứa trong các thiết bị số, thường gọi là “tài liệu số”, để tìm ra các bằng chứng số (Digital Evidence). Rõ ràng, điều tra số liên quan đến tội phạm máy tính (Computer Crime). Điều tra số bao gồm nhiều lĩnh vực như: Computer Forensics, Network Forensics, Data Analytical Forensics, Mobile Device Forensics, .... Trong đó, điều tra mạng (Network Forensics) tập trung vào việc chặn bắt, sao lưu và phân tích lưu lượng mạng nhằm phục vụ điều tra trong công tác phòng chống tội phạm mạng. Thuật ngữ điều tra mạng được đưa ra bởi chuyên gia bảo mật máy tính Marcus Ranum vào đầu những năm 90 thế kỷ XX. Điều tra mạng là một loại hình của điều tra số liên quan đến việc giám sát và phân tích lưu lượng mạng máy tính nhằm phục vụ cho việc thu thập thông tin, chứng cứ pháp lý hay phát hiện các xâm nhập. Không giống các loại hình khác của điều tra số, điều tra mạng xử lý những thông tin dễ thay đổi và biến động, khó dự đoán. Lưu lượng mạng được truyền đi và sau đó bị mất, do đó việc điều tra được diễn ra rất linh hoạt, chủ động. Các điều tra viên chỉ có thể dựa vào thông tin từ các thiết bị an toàn như bộ lọc gói, tường lửa, hệ thống phát hiện xâm nhập đã được triển khai để dự đoán hành vi vi phạm. Các kỹ năng, kỹ thuật cần thiết cho việc điều tra mạng phức tạp và chuyên sâu, sử dụng thông tin được khai thác từ bộ nhớ đệm (cache) của web, proxy hay chặn bắt thụ động lưu lượng truy cập mạng và xác định các hành vi bất thường.