[종합시험 : 윈도우 포렌직]

윈도우 포렌식의 아래 내용을 출제 예정입니다.

- 디지털 포렌식의 5원칙

- 디지털 포렌식 수사절차 5단계

- 실시간 대응(활성 포렌식)의 중요성

- 휘발성 증거와 비휘발성 증거

- 생성증거와 보관 증거의 특징과 증거목록

- 프로세스/사용자/ 파일 관련 증거 수집의 목적

- Hash 알고리즘의 특징

- 윈도우 레지스트리 분석을 하는 이유

- Prefetch 파일 분석을 하는 이유

- Link 파일의 증거로서의가치