



## PECB 인증 선임 포렌식 조사관

컴퓨터 포렌식 프로세스를 마스터합니다.

### 이 강좌를 수강해야 하는 이유는?

선임 컴퓨터 포렌식 조사관(Lead Computer Forensics Examiner) 강좌의 목표는 완전하고 신뢰할 수 있는 디지털 증거를 습득하기 위한 컴퓨터 포렌식 프로세스를 수행하는 데 필요한 전문성을 개발하는 것입니다. 수강생은 이 강좌를 통해 포렌식 증거 복원 및 분석 테크닉 활용을 위한 우수관행을 기반으로 컴퓨터 포렌식의 기본을 완전히 이해하게 됩니다. 본 강좌는 Windows, Mac OS X, Linux 운영체제와 모바일 기기에서 데이터를 수집 및 분석하기 위해 필요한 주요 기술에 중점을 두고 있습니다.

수강생은 컴퓨터 포렌식 프로세스의 필수 개념을 모두 마스터 후 인증시험에 응시할 수 있으며, PECB의 선임 컴퓨터 포렌식 조사관 인증서를 신청할 수 있습니다. PECB의 선임 컴퓨터 포렌식 조사관 인증서를 통해 첨단 포렌식 조사를 이끌고 포렌식 분석, 보고, 증거 복원 작업을 수행할 수 있는 전문성을 보유하고 있음을 증명할 수 있습니다.



## 이 강좌를 수강해야 할 사람은?

- ▶ 컴퓨터 포렌식 전문가
- ▶ 컴퓨터 포렌식 컨설턴트
- ▶ 사이버보안 전문가
- ▶ 사이버 정보 분석가
- ▶ 전자 데이터 분석가
- ▶ 컴퓨터 증거 복원 전문가
- ▶ 법 집행 당국에 종사 중이거나 관심 있는 전문가
- ▶ 컴퓨터 포렌식 분석에 관한 지식을 향상시키고자 하는 전문가
- ▶ 정보보안 담당 부서원
- ▶ IT 전문 자문역
- ▶ 데이터 추출 및 공개를 위해 미디어 조사를 담당하는 개인
- ▶ IT 전문가

## 강좌 프로그램

길이: 5일

### 1일차 | 사고 대응 및 컴퓨터 포렌식의 개념

- ▶ 강좌의 목표와 구성
- ▶ 표준 및 규제 프레임워크
- ▶ 디지털 포렌식의 역사적 측면
- ▶ ISO 27037의 기본 개념 및 정의
- ▶ ISO 27037 표준 개관
- ▶ 인증 선임 포렌식 조사관의 역할 및 책임
- ▶ 컴퓨터 포렌식 실험실

### 2일차 | 컴퓨터 포렌식 조사 준비 및 지휘

- ▶ 기술적 기초
- ▶ 파일시스템 포렌식
- ▶ 공통 파일시스템
- ▶ 공통 운영체제
- ▶ 포렌식 결과 획득

### 3일차 | 디지털 아티팩트(Artifact) 분석 및 관리

- ▶ 디지털 아티팩트: 식별, 획득, 분석, 커뮤니케이션
- ▶ 오픈소스 포렌식 결과 획득 및 분석 도구 사용
- ▶ ISO/IEC 27037:2012
- ▶ 정규표현식에 의한 고급 키워드 검색

### 4일차 | 사례 발표 및 예제 시뮬레이션

- ▶ 잠재적 디지털 증거의 수집 또는 획득에 관한 의사결정
- ▶ 그 밖의 주요 디지털 포렌식 이슈
- ▶ 인증 선임 포렌식 조사관의 직업윤리
- ▶ 디지털 포렌식 결과 제시하기
- ▶ 조사관의 역량 및 평가
- ▶ 강좌 종료

### 5일차 | 인증시험



## 학습 목표

- ▶ 디지털 포렌식 조사 시 선임 컴퓨터 포렌식 조사관의 역할과 책임을 이해
- ▶ 전자 미디어 조사의 목적과 전자 미디어 조사와 일반적인 표준 및 방법론 간의 관계 이해
- ▶ 컴퓨터 사고 조사 및 디지털 포렌식 작업의 올바른 순서 이해
- ▶ 사고 조사 과정 및 디지털 포렌식 작업 중 사용될 수 있는 일반적인 상업용 툴 및 오픈 소스 툴 이해
- ▶ 컴퓨터 포렌식 작업을 계획 및 수행하고 증거를 보호하기 위한 안전 네트워크 구축 및 유지를 위해 필요한 역량 습득

## 시험

길이: 3시간

'PECB 인증 선임 컴퓨터 포렌식 조사관' 인증시험은 PECB 시험/인증프로그램(Examination and Certification Programme)의 요구조건을 충족합니다. 시험에서는 다음과 같은 역량 영역을 평가합니다.

- 영역 1** | 컴퓨터 포렌식의 기본 원리와 개념
- 영역 2** | 컴퓨터 포렌식 우수관행
- 영역 3** | 디지털 포렌식 실습 요구조건
- 영역 4** | 운영체제 및 파일 시스템 구조
- 영역 5** | 모바일 기기
- 영역 6** | 컴퓨터 범죄 조사 및 포렌식 조사
- 영역 7** | 증거의 연속성 유지

인증시험에 관해 더욱 자세한 사항은 다음을 참조하세요 [시험 규칙 및 정책 보기](#)





## 인증

인증시험에 합격한 후에는 다음 표와 같은 인증을 신청할 수 있습니다. 각 인증명에 따른 요구조건을 모두 충족해야만 인증서가 발급됩니다. 컴퓨터 포렌식 인증과 PECB 인증 프로세스에 관해 더욱 자세한 사항은 다음을 참조하세요.

[인증 규칙 및 정책 보기](#)

인증명	시험	실무경력	CFMS 프로젝트 경력	기타 요구조건
PECB 인증 포렌식 조사관보(Provisional Forensics Examiner)	PECB 인증 선임 포렌식 조사관 시험(또는 이에 상당하는 시험)	없음	없음	PECB 윤리규정 서명
PECB 인증 포렌식 조사관(Forensics Examiner)	PECB 인증 선임 포렌식 조사관 시험(또는 이에 상당하는 시험)	2년: 컴퓨터 포렌식 분야 현장 경험 1년 포함	포렌식 활동 총 200 시간	PECB 윤리규정 서명
PECB 인증 선임 포렌식 조사관(Lead Forensics Examiner)	PECB 인증 선임 포렌식 조사관 시험(또는 이에 상당하는 시험)	5년: 컴퓨터 포렌식 분야 현장 경험 2년 포함	포렌식 활동 총 300 시간	PECB 윤리규정 서명

## 일반 정보

- 인증비용은 시험 응시료에 포함됨
- 정보 및 실용적 사례를 담은 교재 제공(450페이지 이상)
- CPD(Continuing Professional Development) 31 크레딧이 인정되는 수료증 발급
- 시험 불합격시 12개월 이내에 무료 재응시 가능

더 자세한 정보를 원한다면, [marketing@pecb.com](mailto:marketing@pecb.com)로 문의하거나 PECB 웹사이트 [www.pecb.com](http://www.pecb.com)를 방문 해 주세요.