

## X-Ways Forensics 교육 과정 안내

### 1. 교육 개요

본 교육 과정은 X-Ways Forensics 컴퓨터 포렌식 소프트웨어를 이용하여 컴퓨터 저장매체에 대한 시스템적이고, 효율적인 분석 방법에 중점을 두고 있습니다. WinHex와 X-Ways Forensics 소프트웨어의 모든 컴퓨터 포렌식 기능에 대한 교육을 수행하며, 실무적인 예제를 이용한 실습과 컴퓨터 포렌식 절차의 모든 측면을 수행해 볼 수 있습니다.

교육 참석자들은 강사에게 전수 받은 지식을 통해서 샘플 증거 파일을 이용하여 즉각적인 포렌식 관련 시야를 높이게 됩니다.

본 교육 과정의 목표는 저장매체에 저장되어 있는 데이터와 메타데이터 또는 삭제된 정보 등에서 확실적인 결과를 도출하도록 하는데 있습니다. 이를 통해 법정에서 증거로서의 증거 능력과 증명력이 인정되기 위함입니다.

본 교육 과정은 세계적인 포렌식 소프트웨어 개발사인 독일 X-Ways 사<sup>1</sup>의 정규 교육 과정을 국내 환경에 맞춰 일부 수정 및 추가하여 제공하며, 교육 참석자들에게는 해외에서도 인정받는 교육 수료증, 교재 및 기타 기술 자료가 제공됩니다. 또한, 레드아이포렌식스 기술 커뮤니티 사이트를 이용할 수 있게 됩니다.

### 2. 교육 내용

본 교육을 통해 아래의 예와 같은 다양한 주제 들에 대한 실무 능력을 이론적인 기반 지식

과 함께 교육 참석자들에게 전수합니다.

- ✓ .e01 파일은 내부적으로 어떻게 운영되나?
- ✓ hash 데이터베이스의 내부적인 구조는 무엇인가?
- ✓ 삭제된 파티션이 어떻게 자동으로 복구되는가 ?
- ✓ X-Ways Forensics 소프트웨어가 삭제된 파일을 복구하는 방법은 무엇인가?

또한, 포렌식한 디스크 이미징(imaging) 및 클로닝(cloning), 데이터 복구, 검색 기능, 동적인 필터링, 보고서 생성 등에 대한 실습과 지식을 제공합니다.

교육 참석자 들은 컴퓨터 저장매체 내에 존재하는 또는 삭제된 파일의 완전한 전체적 상황을 얻을 수 있는 방법, 불법적 이미지를 찾는 가장 효과적인 방법, 일반적인 데이터 카빙(carving) 기술로는 복구 불가능한 NTFS 압축형태의 삭제된 파일을 수작업으로 복구하는 방법 등을 배울 수 있습니다.

4일 간 교육 되어지는 세부 내용은 아래와 같습니다.

- ✓ 프로그램 설치 방법
- ✓ 프로그램 사용자 인터페이스 컴포넌트 학습
- ✓ 데이터 변환기(data interpreter) 이해
- ✓ 저장매체 클로닝을 위한 준비
- ✓ 저장매체 클로닝과 사본(Image) 생성
- ✓ Case 생성 및 증거물 추가하기
- ✓ Hash 생성 및 검증

- ✓ 갤러리 뷰를 이용 방법과 효과적인 스킨 컬러 검증 방법
- ✓ 카렌다 뷰 사용법(타임라인 분석)
- ✓ 파일 내용 미리보기
- ✓ 체계적인 드라이브 목록 테이블 생성하기
- ✓ Hash set 생성 및 Hash set 비교 방법
- ✓ ADS(alternate data stream), HPA(host-protected area), 잘못된 확장자(misnamed file)를 가진 파일 등과 같은 데이터 은닉 기술을 감지하는 방법
- ✓ 주석 및 북마크 추가하기
- ✓ 리포트 생성
- ✓ 디렉토리 브라우저(directory browser) 이용
- ✓ 디렉토리 브라우저와 디렉토리 트리(directory tree)를 완벽한 조사 업무를 맞게 동기화 하는 방법
- ✓ Access 버튼 메뉴를 이용하는 방법
- ✓ 다양한 파일 복구 기법
- ✓ 파일 시그니처 기능 추가 방법
- ✓ free space, slack space 등에서 데이터 추출 및 분석하는 방법
- ✓ 삭제된 파티션을 찾고, 분석하는 방법
- ✓ 효과적으로 검색 및 인덱스 기능을 사용하는 방법
- ✓ 파일 시스템 데이터 구조에 대한 효과적인 조사
- ✓ 데이터 프로파일링
- ✓ Base64, Uuencode 등 디코딩 방법
- ✓ RAM 내용 보기
- ✓ RAID 정보 조합

- ✓ 삭제된 NTFS 압축형태의 파일을 수작업으로 복구
- ✓ 국내 환경에서 포렌식 분석 기법 및 보고서 작성 방법
- ✓ 템플릿 및 스크립트 프로그래밍과 같은 토픽 들(Optional)

### 3. 교육 일정 및 비용<sup>ii</sup>

#### 1) 일시

- 9월7일 ~ 9월10일

2) 장소 : 서울시 강남구 역삼동 소재 (주)레드아이포렌식스 교육장

3) 비용 : 1인당 198만원 (VAT포함)

### 4. 교육 참가 신청 및 문의

- ✓ (주)레드아이포렌식스 교육담당자
- ✓ TEL : 02-566-2310
- ✓ EMAIL : redeye@redeyeforensics.com

---

<sup>i</sup> <http://www.x-ways.net/>

<sup>ii</sup> 기타 사정으로 변경 되어 질 수 있습니다.