(주)인섹시큐리티 공인 교육센터

디지털 포렌식 / 자격증 과정

AX200
자격증 과정

4일

2023.06

INSEC security

✓ AX200 자격증 과정

교육일정	교육내용	교육시간
1일차	**MODULE 1** – MCFE 진행 절차 안내 – AXIOM Process / Examine 소개	10:00 ~ 10:50
	MODULE 1 – AXIOM Process – AXIOM Process 설정 가이드 – 케이스 생성	11:00 ~ 11:50
	MODULE 1 – 증거 추가 – 증거 데이터 추가 설정 (Computer , Mobile, Cloud) – 운영체제별 증거 데이터 추가 설정 – 증거 데이터 불러오기	13:00 ~ 13:50
	MODULE 1 – 증거 데이터 이미징 – 컴퓨터 증거 이미징 방법 (Raw, E01, File type) – 모바일 증거 이미징 방법 (Quick, Full) – 클라우드 데이터 이미징 방법 (Zip, AFF4)	14:00 ~ 14:50
	MODULE 1 – AXIOM Process 상세 설정 및 데이터 추출 – 상세 설정 (키워드, 모바일 백업 검색, 해시, MAGNET A.I 등) – 아티팩트(Artifacts) 상세 설정 (Computer, Mobile, Cloud) – 데이터 추출	15:00 ~ 15:50
	MODULE 2 – AXIOM Examine – AXIOM Examine 탐색기 인터페이스 설명 (대시보드, 아티팩트, 파일시스템, 미디어, 레지스트리, 커넥션, 타임라인) – 아티팩트 탐색기 인터페이스 설명 (필터, 검색, 네이게이션, 상세 정보 카드 등)	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	*** 교육 진행 시 사용 툴** MAGNET AXIOM	

* 교육시간 및 교육 내용은 강의 내용 / 설명 / 질문에 따라 조금씩 변경 될 수 있습니다.

✓ AX200 자격증 과정

교육일정	교육내용	교육시간
2일차	**MODULE 2 – 상세결과(Refined Results)** – 상세 결과창 데이터 정형화 방식 – 인터넷 검색어 분류 (Google / Other) – 클라우드 서비스(Cloud Service) / 페이스북(Facebook) / 암호 토큰 (Token) – 사용자 정보 분류	10:00 ~ 10:50
	MODULE 3 – 필터 / 주석 / 프로필 – 필터 생성 방법 및 관리 – 필터 적용 및 수정 – 주석 적용 / 필터와 주석의 차이점 – 프로필 생성 및 분류	11:00 ~ 11:50
	MODULE 4 – 운영체제 아티팩트 분석(Operating System Artifacts) – 시스템 정보 수집 (OS Version, Install Date, Owner, Build 등) – 사용자 정보 수집 (SID, RID, Last Login Time, User Name 등) – 타임존 설정 (TimeZone Information)	13:00 ~ 13:50
	MODULE 4 – 운영체제 아티팩트 분석(Operating System Artifacts) – 파일시스템 정보 (Filesystem Name, Total Sector 등) – 네트워크 인터페이스 정보 (Network Interface) – 휴지통 분석 (Recycle.bin)	14:00 ~ 14:50
	MODULE 4 – 운영체제 아티팩트 분석(Operating System Artifacts) – 설치 / 삭제 파일 분석 – 이동식 저장 장치 접근 기록 분석 – 공유 폴더 사용 기록 분석	15:00 ~ 15:50
	MODULE 4 – 운영체제 아티팩트 분석(Operating System Artifacts) – 실행 창을 이용한 검색어 리스트 분석 (RunMRU) – 폴더 실행 기록 분석 (Shellbags) – 문서 실행 기록 분석 (lnk, Jumplist, OpensavedpidMRU, RecenDocs) – 인터넷 기록을 이용한 문서 실행 기록 분석 (Chrome, Edge, Firefox)	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	*** 교육 진행 시 사용 툴** MAGNET AXIOM, Passware Kit Forensics, DB Browser for SQLite	

* 교육시간 및 교육 내용은 강의 내용 / 설명 / 질문에 따라 조금씩 변경 될 수 있습니다.

✓ AX200 자격증 과정

교육일정	교육내용	교육시간
3일차	**MODULE 5 – 인터넷 증거 분석** – 구글 크롬 분석 (History, Login Data, Top Site) – 엣지 브라우 분석 (History, Cache) – Firefox (History, Cache)	10:00 ~ 10:50
	MODULE 5 – 인터넷 증거 분석 – 인터넷 검색서 분석 – 로그인 사이트 / 로그인 정보 수집 – 기타 URL 접근 기록 분석	11:00 ~ 11:50
	MODULE 6 – 응용프로그램 실행 증거 수집 – 프리패치 분석 (Prefetch) – 유저 어시스트 분석 (UserAssit) – 레지스트리 탐색기를 통한 원본파일 확인 (Rot13 Encording / Decording)	13:00 ~ 13:50
	MODULE 6 – 응용프로그램 실행 증거 수집 – 캐시 기록 분석 (shim, MUI, Amcache, BAM) – 응용 프로그램 모니터링 (Srum) – 윈도우 타임라인 분석 (Timeline) – 윈도우 알림센터 분석 (Notification Center)	14:00 ~ 14:50
	MODULE 7 – 시각화 분석을 이용한 증거 분석 – 커넥션 빌드 개요 (Connection Build) – 커넥션 빌드를 이용한 소스 (source) 선정 – 데이터 시각화 해석 – 연관 분석	15:00 ~ 15:50
	MODULE 8 – 타임라인 (Timeline) 분석 – 타임라인(Timeline) 분석 개요 – 특정 이벤트 필터링 및 검색	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	*** 교육 진행 시 사용 툴** MAGNET AXIOM, plist viewer, DB Browser for SQLite	

* 교육시간 및 교육 내용은 강의 내용 / 설명 / 질문에 따라 조금씩 변경 될 수 있습니다.

✓ AX200 자격증 과정

교육일정	교육내용	교육시간
4일차	**MODULE 9 – 이메일 (Email) 증거 분석** – 이메일 분석 개요 – 이메일 헤더 분석 – 이메일 첨부파일 추출	10:00 ~ 10:50
	MODULE 10 – 미디어 탐색기 활용 (Media Explorer) – 수집 정보 확인 – 미디어 파일 수정 – 미디어 파일 분류	11:00 ~ 11:50
	MODULE 11 – 미디어 탐색기 활용 (Media Explorer) – 수집 정보 확인 – 미디어 파일 수정 – 미디어 파일 분류	13:00 ~ 13:50
	MODULE 12 – 데이터 추출(Export) – 태그(TAG)를 활용한 데이터 추출방안 – 증거테이블 (Evidence Table) 정보 내보내기 – 탐색기별 (Explorer)별 데이터 내보내기 – 파일 타입별 (Filetype) 데이터 내보내기	14:00 ~ 14:50
	MODULE 12 – 휴대용 케이스 (Potable Case) 생성 – 휴대용 케이스 (Potable Case) 생성 개요 – 휴대용 케이스 (Potable Case) 활용 방안 – 휴대용 케이스 (Potable Case) DB 통합	15:00 ~ 15:50
	MODULE 12 – 리포트 (Report) 생성 – 파일 타입별 리포트 생성 – 리포트 설정 – 리포트 템플릿 수정 – 리포트 확인	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	*** 교육 진행 시 사용 툴** MAGNET AXIOM, plist viewer, DB Browser for SQLite	

* 교육시간 및 교육 내용은 강의 내용 / 설명 / 질문에 따라 조금씩 변경 될 수 있습니다.

감사합니다.

INSEC Security

서울특별시 금천구 가산디지털 1로 19 대륭테크노타운 18차 4층

Email : insec@insec.co.kr TEL : 02-851-5687 www.insec.co.kr