

(주)인섹시큐리티 공인 교육센터

디지털 포렌식 / 자격증 과정

AX300 자격증 과정

4일



2023.06

INSEC
security

✓ AX300 자격증 과정

교육일정	교육내용	교육시간
1일차	MODULE 1 - AX300 진행 절차 안내 - 모바일 (Mobile) 증거 처리 프로세스	10:00 ~ 10:50
	MODULE 2 – 아이폰 (iOS) 시스템 개요 - iOS 파일 시스템 구성 - 아이폰(iOS) 보안 - 애플 아이디 (Apple ID) 개요 - 아이디바이스 (iDevice) 개요	11:00 ~ 11:50
	MODULE 2 – 아이폰 (iOS) 증거 데이터 추출 - 아이폰 (iOS) 증거데이터 추출 방안 - 환경 설정 (최신 iTunes 설치) - 엑시움 프로세스 (AXIOM Process)를 활용한 아이폰 정보 추출	13:00 ~ 13:50
	MODULE 2 – 아이폰 (iOS) 증거 데이터 추출 - 아이폰 로지컬 (Logical) 데이터 추출 방안 - iTunes 백업 방식을 통한 데이터 추출 방안 (일반 백업 / 암호화 백업) - iCloud를 활용한 데이터 추출 방안	14:00 ~ 14:50
	MODULE 3 – iOS 추출 데이터 분석 - 기기 정보 분석 (Apple Device) - 사용자 정보 분석 (Account) - 애플 스토어 (Apple Store) 정보 분석	15:00 ~ 15:50
	MODULE 3 – iOS 추출 데이터 분석 - 기기 사용정보 분석 (KnowledgeC) - 생활 패턴 분석 (Biomes, Powerlog)	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	* 교육 진행 시 사용 툴 MAGNET AXIOM, iTunes	

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

✓ AX300 자격증 과정

교육일정	교육내용	교육시간
2일차	MODULE 4 – iOS 애플리케이션 분석 (Application) <ul style="list-style-type: none"> - 설치된 애플리케이션 (App 설치일, Package Name) - 애플리케이션 권한 분석 - 애플리케이션 프로파일 구축 	10:00 ~ 10:50
	MODULE 4 – iOS 애플리케이션 분석 (Application) <ul style="list-style-type: none"> - iOS 애플리케이션 데이터 저장 방법 - 파일시스템 탐색기 (Filesystem Explorer)를 통한SQLDB 분석 - 오픈소스를 이용한 SQLDB 분석 	11:00 ~ 11:50
	MODULE 4 – iOS 애플리케이션 분석 (Application) <ul style="list-style-type: none"> - 기기에 설치된 애플리케이션 분류 - 과거 설치된 애플리케이션 정보 분석 - iCloud에 저장된 애플리케이션 정보 추적 	13:00 ~ 13:50
	MODULE 4 – iOS 애플리케이션 분석 (Application) <ul style="list-style-type: none"> - Discord, WhatsApp, Snapchat 애플리케이션 분석 - KakaoTalk, Telegram 대화방 분석 - 대화 보기 형식을 통한 메시지 기록 분석 	14:00 ~ 14:50
	MODULE 5 – 인터넷 브라우저 분석 (safari) <ul style="list-style-type: none"> - 사파리 (safari)를 통한 인터넷 사용 기록 분석 - 즐겨찾기, 활성화된 브라우저 분리 - 기본 인터넷 서칭엔진 분석 - 다운로드 기록 분석 	15:00 ~ 15:50
	MODULE 5 – 인터넷 브라우저 분석 (Chrome) <ul style="list-style-type: none"> - 크롬 (Chrome)을 통한 인터넷 사용기록 분석 - 즐겨찾기, 탑사이트 (Top Site), 로그인 정보 (Login) 분석 - 크롬 다운로드 기록 분석 - 인터넷 검색어 분석 	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	* 교육 진행 시 사용 툴 MAGNET AXIOM, DB Browser for SQLite	

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

✓ AX300 자격증 과정

교육일정	교육내용	교육시간
3일차	MODULE 6 – 안드로이드 시스템 개요 (AOS) <ul style="list-style-type: none"> - 안드로이드 시스템 개요 - 안드로이드 파일 시스템 - 안드로이드 보안 	10:00 ~ 10:50
	MODULE 6 – 안드로이드 데이터 추출 <ul style="list-style-type: none"> - 안드로이드 데이터 추출 방안 - 로지컬 (Logical) 추출 - ADB 백업 - Samsung Switch 백업 	11:00 ~ 11:50
	MODULE 7 – 안드로이드 아티팩트 분석 (Artifacts 분석) <ul style="list-style-type: none"> - 안드로이드 기기정보 (Device Information) - 사용자 정보 (UserAccount) - 파일시스템 정보 (Filesystem Information) 	13:00 ~ 13:50
	MODULE 7 – 안드로이드 아티팩트 분석 (Artifacts 분석) <ul style="list-style-type: none"> - SMS / LMS 메시지 분석 - 통화 로그 분석 (Call log) - 이메일 (Email) / 달력 (Calendar) 분석 	14:00 ~ 14:50
	MODULE 8 – 안드로이드 애플리케이션 분석 <ul style="list-style-type: none"> - 설치된 애플리케이션 정보 (설치일, 버전 정보 등) - 패키지 이름 및 홈화면 이름 분류 - Google Play Store를 활용한 패키지 이름 확인 	15:00 ~ 15:50
	MODULE 8 – 안드로이드 애플리케이션 분석 <ul style="list-style-type: none"> - 파일시스템 탐색기 (Filesystem Explorer)를 이용한 SQLDB 분석 - 오픈소스를 활용한 SQLDB 분석 	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	* 교육 진행 시 사용 툴 MAGNET AXIOM, Samsung Switch, DB Browser for SQLite	

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

✓ AX300 자격증 과정

교육일정	교육내용	교육시간
4일차	MODULE 8 – 안드로이드 애플리케이션 분석 <ul style="list-style-type: none"> - 채팅 어플리케이션 분석 (Line, Kakao 등) - 대화 형식 보기 방식을 통한 채팅 내역 분석 - 기타 애플리케이션 분석 	10:00 ~ 10:50
	MODULE 9 – 안드로이드 인터넷 브라우저 분석 (Chrome) <ul style="list-style-type: none"> - 크롬 (Chrome)을 통한 인터넷 사용기록 분석 - 즐겨찾기, 탑사이트 (Top Site), 로그인 정보 (Login) 분석 - 크롬 다운로드 기록 분석 - 인터넷 검색어 분석 	11:00 ~ 11:50
	MODULE 9 – 안드로이드 인터넷 브라우저 분석 (네이버 Whale) <ul style="list-style-type: none"> - 웨일 (Whale)을 통한 인터넷 사용기록 분석 - 즐겨찾기, 탑사이트 (Top Site), 로그인 정보 (Login) 분석 - 다운로드 기록 분석 - 인터넷 검색어 분석 	13:00 ~ 13:50
	MODULE 10 – 시스템 사용기록 분석 (iOS / AOS) <ul style="list-style-type: none"> - Wi-fi 사용기록 (SSID, Password, 접속 시간 등) - 블루투스(Bluetooth) 기록 분석 - Apple AirDrop 사용 정보 분석 	14:00 ~ 14:50
	MODULE 12 – 미디어 파일 분석 <ul style="list-style-type: none"> - 동영상 / 사진 데이터 분석 - MAGNET A.I를 통한 카테고리 분류 - 미디어 탐색기 (Media Explorer)를 활용한 동영상 / 사진 분석 - EXIF Data를 이용한 메타데이터 분석 - 이미지 유사도 분석 	15:00 ~ 15:50
	MODULE 13 – 데이터 추출 / 리포트 (Export / Report) <ul style="list-style-type: none"> - 증거 테이블 정보 추출 (Csv, xlsx) - 포터블 케이스 생성 (Potable Case) - 리포트 생성 	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	* 교육 진행 시 사용 툴 MAGNET AXIOM, 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

