AX350
macOS 포렌식
실무 자격증 과정

• AX350 포렌식 자격증 과정 5일 커리큘럼

INSEC security | MAGNET FORENSICS
공인 총판 / 공인 교육센터

AX350

macOS 포렌식 실무 자격증 과정(5일)

교육일정	교육내용	교육시간
1일차	**MODULE1** - Apple 디바이스(Device) - macOS History 및 버전 정보 - Apple 파일 시스템(File Systems)	10:00 ~ 10:30
	MODULE2 - macOS 디렉토리 구조 - 컨테이너와 샌드박스(Containers and Sandboxes) - Apple ID 개요	10:30 ~ 10:50
	MODULE3 - Apple 프로세서 히스토리 - ARM 모바일 프로세서 - 애플 M1 vs M2 Chip	11:00 ~ 11:50
	MODULE4 - 애플 암호화 칩 [T1 vs T2 Chip] - 파일볼트 [FileVault 1 vs FileVault2] - SIP(System Integrity Protection) – 시스템 무결성 보호	13:00 ~ 13:40
	MODULE5 - EFI(Extensible Firmware Interface) – 확장 펌웨어 인터페이스 - TDM(Target Disk Mode) – 대상 디스크 모드 - USB-C vs Thunderbolt3 vs FireWire	13:40 ~ 14:30
	MODULE6 - 부트캠프(BootCamp) – 듀얼 부팅 - 패러렐즈(Parallels) – 듀얼 부팅 - 타임머신(Time Machine) - Thunderbolt3 vs Thunderbolt4	14:40 ~ 15:50
	MODULE7 - macOS 포렌식 수행 시 고려사항 - macOS 포렌식 분석을 위한 도구 [상용 vs 공개용] - macOS 메모리 분석을 위한 도구 [상용 vs 공개용]	16:00 ~ 16:30
	MODULE6 - macOS 디스크 이미징을 위한 도구 소개 [상용 vs 공개용] - macOS 네트워크 디스크 이미징을 위한 도구 소개 - macOS 이미징 실습	16:30 ~ 17:00

*** 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.**

상담문의 : 02-851-5687

AX350

macOS 포렌식 실무 자격증 과정(5일)

교육일정	교육내용	교육시간
2일차	**MODULE 1** - 강사 소개 - AX350 교육 과정 소개	10:00 ~ 10:50
	MODULE 1 - macOS 개요 - APFS 정보 - macOS 부기 기능 (T2, A1&A2 Chip, Time machine etc) - Apple Keychain	11:00 ~ 11:50
	MODULE 2 - Apple Computer 데이터 채증 - Apple Computer 이미징 - Apple Computer 데이터 선별	13:00 ~ 13:50
	MODULE 3 - macOS Artifacts 분석 - macOS 시스템 정보 (macOS System Information) - macOS 사용자 정보 (macOS User Accounts)	14:00 ~ 14:50
	MODULE 3 - macOS 암호화 - FileVault 개요 - FileVault1 / FileVault2 비교 - FileVault 복호화 방법	15:00 ~ 15:50
	MODULE 3 - macOS Artifacts 분석 - macOS 파인더 (macOS Finder) - macOS 사이드 바 (macOS Sidebar)	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	* 교육 진행 시 사용 툴 MAGNET AXIOM	

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

AX350

macOS 포렌식 실무 자격증 과정(5일)

교육일정	교육내용	교육시간
3일차	**MODULE 3** - macOS Artifacts 분석 - macOS 최근 실행 파일 (macOS MRU) - macOS 치근 실행 파일 (macOS Documents)	10:00 ~ 10:50
	MODULE 3 - macOS Artifacts 분석 - macOS 최근 실행 파일 분석 (DS_Store) - macOS 독 아이템 분석 (macOS Dock items)	11:00 ~ 11:50
	MODULE 3 - Apple Device 개요 - Apple iCloud 개요	13:00 ~ 13:50
	MODULE 3 - Apple iCloud 계정 공유 분석 - Apple iCloud 키체인 (KeyChain) 수집 - Apple iCloud 키체인 정보를 통한 로그인 계정 정보 수집 - Apple iCloud를 통한 애플 노트(Apple Note) 분석	14:00 ~ 14:50
	MODULE 3 - macOS 검색어 (스포트라이트 – Spotlight) 개요 - 스포트라이트 데이터 베이스 (Spotlight Database) 수집 - 스포트 라이트 분석	15:00 ~ 15:50
	MODULE 3 - macOS Filesystem Event 분석 개요 - macOS Filesystem Event 수집 방안 - macOS Filesystem Event 분석 - 주요 정보 필터링	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	* 교육 진행 시 사용 툴 MAGNET AXIOM	

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

AX350

macOS 포렌식 실무 자격증 과정(5일)

교육일정	교육내용	교육시간
4일차	**MODULE 4** - 인터넷 아티팩트 분석 - Safari 데이터 수집 - Safari 데이터 베이스 테이블 분류 - Safari URL 히스토리 분석 - Safari 검색어 수집	10:00 ~ 10:50
	MODULE 4 - 인터넷 아티팩트 분석 - Chrome 데이터 수집 - Chrome 데이터 베이스 테이블 분류 - Chrome URL 히스토리 분석 - Chrome 검색어 수집	11:00 ~ 11:50
	MODULE 4 - 인터넷 아티팩트 분석 - Firefox 데이터 수집 - Firefox 데이터 베이스 테이블 분류 - Firefox URL 히스토리 분석 - Firefox 검색어 수집	13:00 ~ 13:50
	MODULE 5 - Email 분석 개요 - 기본 메일 응용프로그램 (Mail.App) 데이터 수집 - 메일 응용프로그램 내부 정보 파싱 및 첨부파일 확인 - 메일 분석	14:00 ~ 14:50
	MODULE 6 - 데이터 공유 분석 - 공유 폴더 접속 흔적 추적 - AirDrop 사용 흔적 추적	15:00 ~ 15:50
	MODULE 6 - 데이터 공유 분석 - Bluetooth 사용 흔적 추적	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	* 교육 진행 시 사용 툴 MAGNET AXIOM	

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

AX350

macOS 포렌식 실무 자격증 과정(5일)

교육일정	교육내용	교육시간
5일차	**MODULE 7** - USB 디바이스 접근 기록 조사 - USB 디바이스 사용 흔적 조사	10:00 ~ 10:50
	MODULE 8 - 응용 프로그램 인스톨 기록 분석 - 어플리케이션 사용 기록 분석	11:00 ~ 11:50
	MODULE 9 - macOS 휴지통 분석 개요 - macOS 휴지통 분석 - DS_Store와 휴지통 분석 연동	13:00 ~ 13:50
	MODULE 10 - TimeMachine 백업 개요 - TimeMachine / Snapshot 생성 - TimeMachine을 이용한 데이터 복구 및 증거데이터 수집	14:00 ~ 14:50
	MODULE 11 - KnowledgeC 데이터베이스 구조 - KnowledgeC 아티팩트 분석 방법	15:00 ~ 15:50
	MODULE 11 - KnowledgeC 분석 - Log 파일 분석 - 통합 로그, 파일/폴더 권한, 일일 로그 등 주요 로깅 아티팩트 분석	16:00 ~ 16:50
	질문 & Review	16:50 ~ 17:00
	*** 교육 진행 시 사용 툴** MAGNET AXIOM	

*** 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.**

상담문의 : 02-851-5687

INSEC Security

제품문의	02.863.5687
교육문의	02.851.5687
본사	서울특별시 금천구 가산디지털 1로 19 대륭테크노타운 18차 406호
서울 독산 교육센터	서울특별시 금천구 가산디지털 1로 19 대륭테크노타운 18차 409호
제주 함덕 교육센터	제주특별자치도 제주시 조천읍 함덕3길 17
홈페이지	www.insec.co.kr

INSEC security | MAGNET FORENSICS
공인 총판 / 공인 교육센터