

(주)인섹시큐리티 공인 교육센터

디지털 포렌식 / 자격증 과정

# AX320 자격증 과정

4일



2023.06

**INSEC**  
security

✓ AX320 자격증 과정

교육일정	교육내용	교육시간
1일차	<b>MODULE 1</b> <ul style="list-style-type: none"> <li>- AX320 진행 절차 안내</li> <li>- 이미지 파일 시나리오 설명</li> <li>- 클라우드 ( Cloud ) 포렌식 조사 방법</li> </ul>	10:00 ~ 10:50
	<b>MODULE 2 – 클라우드 ( Cloud ) 접근 기록 수집</b> <ul style="list-style-type: none"> <li>- 상세결과 ( Refined Results ) 정보 확인</li> <li>- 인터넷 브라우저 ( Edge, Chrome, Firefox 등 ) URL 분석</li> <li>- 원본 아티팩트 분류 및 활용</li> </ul>	11:00 ~ 11:50
	<b>MODULE 2 – 클라우드 ( Cloud ) 접근 기록 수집</b> <ul style="list-style-type: none"> <li>- 설치된 클라우드 어플리케이션 정보 수집 ( Install Software )</li> <li>- 설치된 클라우드 어플리케이션 정보 수집 ( Chche )</li> <li>- 사용자 정보 수집</li> </ul>	13:00 ~ 13:50
	<b>MODULE 3 – 오픈소스 인텔리전스 수집 ( OSINT )</b> <ul style="list-style-type: none"> <li>- 오픈소스 인텔리전스 개요</li> <li>- 인터넷 서칭을 활용한 오픈소스 인텔리전스 정보 수집</li> </ul>	14:00 ~ 14:50
	<b>MODULE 4 – 소셜미디어 정보 수집 개요</b> <ul style="list-style-type: none"> <li>- 소셜미디어 정보 수집 방안</li> <li>- 상세결과 ( Refined Results )를 통해 수집한 계정정보 활용 방안</li> <li>- AXIOM Process를 활용한 클라우드 정보 수집 ( 인터넷 / 오프라인 )</li> </ul>	15:00 ~ 15:50
	<b>MODULE 4 – 소셜미디어 정보 수집 개요</b> <ul style="list-style-type: none"> <li>- 트위터 데이터 추출 방법 ( 예제 )</li> <li>- Public 정보를 통한 트위터 정보 수집 방안</li> <li>- 사용자 계정 정보 ( ID / PW )를 이용한 정보 수집 방안</li> </ul>	16:00 ~ 16:50
	<b>질문 &amp; Review</b>	16:50 ~ 17:00
	<b>* 교육 진행 시 사용 툴</b> MAGNET AXIOM	

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

✓ AX320 자격증 과정

교육일정	교육내용	교육시간
2일차	<b>MODULE 5 – 애플 아이클라우드 수집 ( Apple iCloud )</b> <ul style="list-style-type: none"> <li>- 아이클라우드 수집개요</li> <li>- 애플 아이디 ( Apple ID ) 개요</li> <li>- 아이디바이스 ( iDevice ) 개요</li> </ul>	10:00 ~ 10:50
	<b>MODULE 5 – 애플 아이클라우드 수집 ( Apple iCloud )</b> <ul style="list-style-type: none"> <li>- Apple ID를 통한 클라우드 접속</li> <li>- 2단계 인증 (2FA) 인증</li> <li>- 수집 가능 항목 ( iOS 백업, Desktop, Picture 등 )</li> </ul>	11:00 ~ 11:50
	<b>MODULE 6 – 구글 드라이브 수집 ( Google Drive )</b> <ul style="list-style-type: none"> <li>- 구글 드라이브 수집 개요</li> <li>- Google 사용자 기록 목록 ( Email, Calendar, Site, Maps, Photos 등 )</li> <li>- 구글 테이크아웃 ( Takeout )</li> </ul>	13:00 ~ 13:50
	<b>MODULE 6 – 구글 드라이브 수집 ( Google Drive )</b> <ul style="list-style-type: none"> <li>- 인터넷 환경에서 구글 드라이브 정보 수집 방안</li> <li>- 사용자 자격 증명을 통한 구글 드라이브 정보 수집</li> <li>- 외부 브라우저를 활용한 구글 드라이브 정보 수집</li> <li>- 구글 테이크아웃 ( Takeout )을 통한 클라우드 정보 분석</li> </ul>	14:00 ~ 14:50
	<b>MODULE 6 – 구글 드라이브 분석 ( Google Drive )</b> <ul style="list-style-type: none"> <li>- 구글 맵 활용 정보 분석 ( Google Map Query )</li> <li>- 구글 활용 기록 분석 ( 검색어, 유튜브 시청 기록, 확장 프로그램 등 )</li> <li>- 구글 캘린더 기록 분석</li> </ul>	15:00 ~ 15:50
	<b>MODULE 6 – 구글 드라이브 분석 ( Google Drive )</b> <ul style="list-style-type: none"> <li>- 구글 메시지 ( Email ) 정보 분석</li> <li>- 구글 드라이브 사용 기록 분석</li> <li>- 구글 주소록 분석</li> </ul>	16:00 ~ 16:50
	<b>질문 &amp; Review</b>	16:50 ~ 17:00
	<b>* 교육 진행 시 사용 툴</b> MAGNET AXIOM	

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

✓ AX320 자격증 과정

교육일정	교육내용	교육시간
3일차	<b>MODULE 7 – 마이크로 소프트 ( Microsoft Account )</b> <ul style="list-style-type: none"> <li>- MS 사용을 및 수집 개요</li> <li>- 사용자 계정 정보를 통한 수집 방법</li> <li>- 외부 브라우저 인증 방식을 통한 수집 방법</li> </ul>	10:00 ~ 10:50
	<b>MODULE 7 – 마이크로 소프트 ( Microsoft Account )</b> <ul style="list-style-type: none"> <li>- 오피스 파일 사용기록 ( Office 365 )</li> <li>- 등록된 Device 장치 정보</li> <li>- 아웃룩 캘린더 정보 ( Outlook Calendars )</li> <li>- 아웃룩 주소록 ( Outlook Contacts )</li> </ul>	11:00 ~ 11:50
	<b>MODULE 7 – 마이크로 소프트 ( Microsoft Account )</b> <ul style="list-style-type: none"> <li>- 아웃룩 이메일 ( Outlook Email ) 기록</li> <li>- 운영체제 정보 ( Operating System )</li> <li>- 클라우드 데이터 ( OneDrive File )</li> </ul>	13:00 ~ 13:50
	<b>MODULE 8 – 트위터 ( Twitter )</b> <ul style="list-style-type: none"> <li>- 트위터 핵심용어 ( Tweet, Thread, Feed, Moment, Follower, DM 등 )</li> <li>- 트위터 포스트 ( Twitter Posts )</li> <li>- 트위터 다이렉트 메시지 ( Twitter DM )</li> <li>- 트위터 사용자 정보 ( Twitter Users )</li> </ul>	14:00 ~ 14:50
	<b>MODULE 8 – 트위터 ( Twitter )</b> <ul style="list-style-type: none"> <li>- 대화 보기를 통한 다이렉트 메시지 분석 ( DM )</li> <li>- 미디어 탐색기 ( Media Explorer )를 활용한 이미지 분석</li> <li>- 빌드 커넥션 ( Build Connections )을 이용한 시각화 분석</li> </ul>	15:00 ~ 15:50
	<b>MODULE 9 – 페이스북 ( Facebook )</b> <ul style="list-style-type: none"> <li>- 페이스북 개요</li> <li>- 페이스북 수집 가능 데이터</li> <li>- 페이스북 데이터 수집 방안</li> </ul>	16:00 ~ 16:50
	<b>질문 &amp; Review</b>	16:50 ~ 17:00
	<b>* 교육 진행 시 사용 툴</b> MAGNET AXIOM	

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

✓ AX320 자격증 과정

교육일정	교육내용	교육시간
4일차	<b>MODULE 9 – 페이스북 ( Facebook )</b> - 사용자 정보를 통한 페이스북 접근 - 페이스북 대화 내역 ( Facebook Messenger Messages ) - 페이스북 사용자 정보 ( Profile info )	10:00 ~ 10:50
	<b>MODULE 9 – 페이스북 ( Facebook )</b> - 페이스북 타임라인 ( Facebook Timeline ) - 친구 목록 ( Facebook Friends ) - 윈도우 타임라인 분석 ( Timeline ) - 윈도우 알림센터 분석 ( Notification Center )	11:00 ~ 11:50
	<b>MODULE 10 – 인스타그램 ( Instagram )</b> - 인스타그램 개요 - 인스타그램 수집 방안	13:00 ~ 13:50
	<b>MODULE 10 – 인스타그램 ( Instagram )</b> - 인스타그램 대화기록 ( Instagram DM ) - 인스타그램 사용자 정보 ( UserAccount )	14:00 ~ 14:50
	<b>MODULE 11 – 드롭박스( Dropbox )</b> - 드롭박스 개요 - 업로드 파일과 공유 중 파일 - 드롭박스 환경 설정	15:00 ~ 15:50
	<b>MODULE 11 – 드롭박스( Dropbox )</b> - 사용자 계정을 활용한 드롭박스 정보 추출 - 드롭박스 드라이버 정보 추출 - 드롭박스 데이터 분석 ( 업로드 시간 / 수정 시간 등 )	16:00 ~ 16:50
	<b>질문 &amp; Review</b>	16:50 ~ 17:00
	<b>* 교육 진행 시 사용 툴</b> MAGNET AXIOM	

\* 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](mailto:insec@insec.co.kr) TEL : 02-851-5687 [www.insec.co.kr](http://www.insec.co.kr)

