디지털 포렌식 전문가

디지털 포렌식 분석 실무 과정

5일 교육과정 커리큘럼

INSEC security

디지털 포렌식 전문가

디지털 포렌식 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
1일차	**디지털 포렌식 기술 동향** – 디지털 포렌식 역사 – 현 디지털 포렌식 주소 – 디지털 포렌식 발전 방향	10:00 ~ 10:50
	디지털 포렌식 절차 – 디지털 증거의 특징 – 디지털 증거 수집 시 주의 사항 – 디지털 증거 수집 방안 – 디지털 증거 수집 도구	11:00 ~ 11:50
	증거수집 절차 – 현장 상황에 따른 디지털 증거 수집 방안 · 데이터 선별 압수에 따른 유효한 도구 · 휘발성 데이터 수집에 따른 유효한 도구 · 온 보드(On-Board) Chip에 따른 유효한 도구 · 수집 Software와 장비에 대한 비교	13:00 ~ 13:50
	저장장치의 종류와 인터페이스 – 저장장치 인터페이스 설명 · 저장 장치 인터페이스 구조 (IDE, SATA, SAS, Firewire, USB(A, C Type), M.2, – 쓰기 방지 장치 설명 · 저장 장치 인터페이스 별 쓰기방지 장치 연결 방안 · 하드웨어 타입 쓰기방지 장치와 소프트웨어 타입 쓰기 방지 장치	14:00 ~ 14:50
	Digital Forensics 제품 소개 – 전문 디지털 포렌식 도구 소개 – 포렌식 도구 장점 소개 – 포렌식 도구 인터페이스 설명	15:00 ~ 15:50
	환경에 따른 증거 데이터 수집 방안 – 데이터 선별 압수에 따른 유효한 도구 – 휘발성 데이터 수집에 따른 유효한 도구 – 온 보드(On-Board) Chip에 따른 유효한 도구 – 수집 Software와 장비에 대한 비교	16:00 ~ 16:50
	증거파일 수집 – 이미지 파일 생성 · Desktop Full Disk 이미징 실습 · L01 또는 Lx01 확장자를 이용한 Logical File 수집 · 포터블을 활용한 데이터 수집 · Agent를 이용한 원격 Disk 수집	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	*** 교육 진행 시 사용 툴** opentext tableau kit, EnCase, FTK, X-Ways, AXIOM, Falcon, Media Imager, MagiCube, Dump it, FastDump Pro, MAGNET Process Capture	

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

상담문의 : 02-851-5687

디지털 포렌식 전문가

디지털 포렌식 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
2일차	**Windows Registry 개요** – Windows Registry 란? – Windows Registry 개요 – Windows Registry 하이브 – Windows Regsitry 구성 요소 – LastWrittern Time	10:00 ~ 10:50
	Windows MRU (1) – MRU 종류 – RunMRU – OpenSavePidlMRU / LastVisitedPidlMRU 동작 방식 – OpenSavePidlMRU / LastVisitedPidlMRU 구조	11:00 ~ 11:50
	Windows MRU (2) – RecentDocs 개요 – RecentDocs 동작 방식 – RecentDoc 구조	13:00 ~ 13:50
	이벤트 로그 분석 – 윈도우 이벤트 로그 분석 방법 – 이벤트 ID별 유형 분류 – 원격 접속 및 침해사고 관련 이벤트 로그 분석	14:00 ~ 14:50
	윈도우 아티팩트 분석 – ShellBag – ShellBag 아티팩트 특징 – ShellBag 구조 분석 – 전문 도구를 활용한 ShellBag 구조 분석 실습	15:00 ~ 15:50
	윈도우 아티팩트 분석 – 링크파일(Lnk) 분석 – 링크 파일 아티팩트 특징 – 주요 실행 흔적 분석 방법 – 링크 파일 생성 조건 및 분석 시 유의사항 확인	16:00 ~ 16:50
	윈도우 아티팩트 분석 – 점프 파일 분석 – 점프 파일 아티팩트 특징 – 윈도우 7 / 10 / 11 버전 별 차이점 이해 – AutomaticDestination / CustomDestination 차이점 이해	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	*** 교육 진행 시 사용 툴** EnCase, FTK, X-Ways, AXIOM, Hex Editor, Jumplist Parsor, lnk Parsor, Event Log View	

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

상담문의 : 02-851-5687

디지털 포렌식 전문가

디지털 포렌식 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
3일차	**유저 어시스트(UserAssist) 아티팩트 분석** - UserAsssit 아티팩트 이해 및 특징 - 마지막 실행 시간 판별 방법 - ROT-13 디코딩 적용 방법 - 레지스트리 위치 확인	10:00 ~ 10:50
	프리패치(Prefetch) 분석 - Prefetch 아티팩트 이해 및 특징 - 최초 및 마지막 실행 시간 분석 - 아티팩트 저장 경로 확인 - 프리패치 사용 목적 및 침해사고 분석 시 활용 방안 이해	11:00 ~ 11:50
	심캐시(ShimCache) 분석 - ShimCache 아티팩트 분석 및 특징 이해 - 심캐시 아티팩트 저장 경로 설명 - 심캐시가 남는 조건 및 유의사항 이해 - 아티팩트 분석 방법 설명	13:00 ~ 13:50
	앰캐시(AmCache) 분석 - AmCache 아티팩트 분석 및 특징 이해 - 프로그램 설치 / 실행 정보 분류 방법 - 주요 저장장치 연결 기록 분석	14:00 ~ 14:50
	SRUM 분석 - SRUM 개요 및 특징 이해 - 리소스 정보 분석을 통한 응용 프로그램 실행 흔적 조사 방법 - EDB 파일 분석 방법	15:00 ~ 15:50
	Windows Time Line 분석 - TimeLine 분석을 통한 사용자 행위 정보 입증 - Windows 작업보기 히스토리를 통한 타임라인 데이터 수집 - DB 열어보기 및 시간대별 데이터 정형화 - 문서 및 응용프로그램 실행 시간 및 실행 파일 조사 시간대 검증	16:00 ~ 16:50
	휴지통 분석 - 휴지통 분석 개요 - 휴지통 데이터 삭제 프로세스 - $R, $I 파일 개념 및 원본 파일 정보 수집	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	*** 교육 진행 시 사용 툴** EnCase, FTK, X-Ways, AXIOM, Hex Editor, Recover My Files, R-Studio	

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

상담문의 : 02-851-5687

디지털 포렌식 전문가

디지털 포렌식 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
4일차	**디스크 구조** – 하드 디스크의 파일 시스템 구조 · 물리적 하드 디스크 구조 · 플래터 구조 · Sector, Cluster 개념 · Slack Space 개념	10:00 ~ 10:50
	Partition Table 구조 이해 – MBR(Master Boot Record) 이해 · MBR 개념 · MBR의 물리적 위치 · MBR 구조와 특징 · 파티션 생성과 삭제 시 MBR 기록 방식	11:00 ~ 11:50
	Partition Table 구조 이해 #2 – GPT(GUID Partition Table) 이해 · GPT 개념 · GPT의 물리적 위치 · GPT 구조와 특징 · 파티션 생성과 삭제 시 GPT 기록 방식	13:00 ~ 13:50
	파일 시스템 구조 – FAT, exFAT FileSystem 개요 · FAT, exFAT FileSystem 개요 및 활용 · FAT, exFAT 비교	14:00 ~ 14:50
	파일 시스템 구조 #1 – FAT File System 데이터 저장 방식 · 클러스터 할당 · Directory Entry 구조 · 할당 클러스터 위치 추적	15:00 ~ 15:50
	파일 시스템 구조 #2 – NT FileSystem 개요 · NTFS 개요 및 활용 · NTFS 구조 · NTFS $MFT 소개	16:00 ~ 16:50
	파일 시스템 구조 #3 – $MFT 구조 · MFT Entry 구조 · MFT Entry 데이터 기록 방식 · resident / non-resident 속성	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	*** 교육 진행 시 사용 툴** EnCase, FTK, X-Ways, AXIOM, Hex Editor	

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

상담문의 : 02-851-5687

디지털 포렌식 전문가

디지털 포렌식 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
5일차	**Anti Forensic 분석** - 안티포렌식 개요 - 볼륨 암호화 탐지 및 복호화 방법 - 문서 암호화 및 압축 파일 탐지 및 복호화 방법 - 여러 전문 도구를 활용한 암 복호화 실습	10:00 ~ 10:50
	ADS (Alternate Data Stream) 분석 - ADS 영역 이해 - ADS 명령어를 이용한 파일 은닉 실습 - 증거 분석 도구를 활용한 ADS 탐지 방법	11:00 ~ 11:50
	파일 시그니처 분석 - 파일 확장자 별 시그니처 정보 이해 - 시그니처 변조 탐지 방법 이해	13:00 ~ 13:50
	파일 타임스탬프 변조 분석 - 타임스탬프 변조 방법 및 메타데이터 분석 방법 - 타임스탬프 변조 여부 탐지 방법 이해	14:00 ~ 14:50
	웹 아티팩트 분석 기법 - 브라우저 별 아티팩트 저장 경로 확인 - 크롬 브라우저 접속 기록 분석 방법 - 엣지 브라우저 접속 기록 분석 방법 - 브라우저 키워드 검색 및 다운로드 이력 분석 방법	15:00 ~ 16:50
	웹 아티팩트 분석 기법 - 크롬 및 엣지 브라우저 북마크 및 즐겨찾기 정보 분석 - 브라우저 별 데이터베이스 파일 접근 및 분석 방법	17:00 ~ 17:30
	디지털 포렌식 실무 자격증 소개 - MAGNET FORENSIC [MCFE] 자격증 소개 - EXTERRO [ACE] 자격증 소개 - OPENTEXT [EnCE] 자격증 소개 - X-Ways Forensics [X-Pert] 자격증 소개 - EC-Council [CHFI] 자격증 소개 - SANS Technology Institute [GCFE] 자격증 소개	17:30 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	* 교육 진행 시 사용 툴 EnCase, FTK, X-Ways, AXIOM, Hex Editor, Passware Kit Forensic외 제공된 모든 오픈 소스	

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

상담문의 : 02-851-5687

(주)인섹시큐리티 공인 교육센터

교육센터 지점별 안내 [서울 독산 / 제주 함덕] 바로가기

교육일정 안내 바로가기

교육문의 : 02-851-5687

INSEC security