

수업 계획서

결	전공주임	교학부장
재		

< 2018학년도 3월 12일 ~ 6월 24일 >

1. 강의개요							
학습과정명	사이버포렌식 식실습	학점	3	교강사명	교강사 전화번호		
강의시간	5시간	강 의 실		수강대상	정보보호	E-mail	
2. 교육과정 수업목표							
- 사이버 포렌식의 개념, 절차에 대한 지식을 학습하고, - 윈도우즈 시스템의 이해를 기반으로 하여 포렌식 도구의 사용 방법, 증거의 수집, 분석, 보존, 분석서 작성 등에 대한 기술 능력을 습득하며, 이를 활용한 사이버 범죄 해결 능력을 배양한다. - 이러한 포렌식 지식과 사이버 범죄 해결 능력을 갖추으로써 증거 수집부터 법정 전문가 증언을 아우르는 사이버 포렌식 전문가로서의 전반적인 실무지식을 학습한다.							
3. 교재 및 참고문헌							
주교재	디지털포렌식의 세계	저자	이준형, 조정원	출판사	인포더박스	출판년도	2014
부교재(참고문헌)		저자		출판사		출판년도	
4. 주차별 강의(실습·실기·실험) 내용							
주별	차시	강의(실습·실기·실험) 내용			과제 및 기타 참고사항		
제 1 주	1	1] 강의주제: 사이버포렌식 개념			교재: p16 ~ p55 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드		
	2	2] 강의목표: 사이버포렌식의 이해					
	3	3] 세부내용:					
	4	① 포렌식의 정의					
	5	② 관련 법규 및 사례					
제 2 주	1	1] 강의주제: 실시간 증거 획득			교재: p56 ~ p94 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드		
	2	2] 강의목표: Live Response & Memory 분석					
	3	3] 세부내용:					
	4	① Live Response 정의 및 수집 방법					
	5	② 메모리 획득 방법 및 분석					
제 3 주	1	1] 강의주제: 증거 이미지 획득			교재: p128 ~ p165 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 평가: 수시 #1: 사이버포렌식 개념, 증거 획득에 대한 객관식 14문 항 출제(각 0.5점, 소수점 이하 반올림)		
	2	2] 강의목표: 파일시스템의 이해와 증거 획득					
	3	3] 세부내용:					
	4	① 저장장치의 이해					
	5	② 데이터 획득 방법 및 실습					
제 4 주	1	1] 강의주제: FAT 파일시스템			교재: p166 ~ p188 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드		
	2	2] 강의목표: FAT 파일시스템과 복구의 이해					
	3	3] 세부내용:					
	4	① FAT 파일시스템 구조					
	5	② FAT 파일 복구					
제 5 주	1	1] 강의주제: NTFS 파일시스템			교재: p189 ~ p229		

	2	2] 강의목표: NTFS 파일시스템과 복구의 이해	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
	3	3] 세부내용:	
	4	① NTFS 파일시스템 구조	
	5	② NTFS 파일 복구	
		4] 수업방법: 강의 및 실습	
제 6 주	1	1] 강의주제: 포렌식과 안티포렌식	교재: p314 ~ p359 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
	2	2] 강의목표: 포렌식 도구 및 안티포렌식의 이해	
	3	3] 세부내용:	
	4	① 포렌식과 안티포렌식	
	5	② PE(Portable Executable) 구조 ③ 포렌식 도구	
	4] 수업방법: 강의 및 실습		
제 7 주	1	1] 강의주제: 윈도우 아티팩트 분석 I	교재: p291 ~ p313 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
	2	2] 강의목표: 레지스트리 분석 기법 습득	
	3	3] 세부내용:	
	4	① 레지스트리 용어	
	5	② Hive 구조 ③ 주요 레지스트리 아티팩트 분석	
	4] 수업방법: 강의 및 실습		
제 8 주	1	중간고사	
	2		
	3		
	4		
	5		
제 9 주	1	1] 강의주제: 윈도우 아티팩트 분석 II	교재: p291 ~ p313, p366 ~ p388 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
	2	2] 강의목표: 레지스트리 분석 기법 습득	
	3	3] 세부내용:	
	4	① MRU의 이해 및 분석	
	5	② USB 사용 기록 분석 ③ 기타 시스템관련 정보 분석	
	4] 수업방법: 강의 및 실습		
제 10 주	1	1] 강의주제: 윈도우 아티팩트 분석 - 파일사용 흔적	교재: p366 ~ p415 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
	2	2] 강의목표: 사용자 작성 파일 사용 흔적 분석	
	3	3] 세부내용:	
	4	① 윈도우 링크파일, Jump list 분석	
	5	② 레지스트리 분석 ③ 윈도우 휴지통 분석 등	
	4] 수업방법: 강의 및 실습		
제 11 주	1	1] 강의주제: 윈도우 아티팩트 분석 - 인터넷 사용	교재: p433 ~ p446 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 평가: 수시 #2: 중간고사 범위 및 10주차까지 범위 출제 (객관식 16문항, 각 0.5점, 소수점 이하 반올림)
	2	2] 강의목표: 인터넷 사용 흔적 분석	
	3	3] 세부내용:	
	4	① 웹 브라우저의 이해	
	5	② Cache, History, Cookie 분석	
	4] 수업방법: 강의 및 실습		
제 12 주	1	1] 강의주제: 윈도우 아티팩트 분석 - 기타	교재: p430 ~ p432, p447 ~ p453 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
	2	2] 강의목표: 아티팩트 분석 기술 향상	
	3	3] 세부내용:	
	4	① Event Log, Prefetch 분석	
	5	② 프린터 스펠러 분석	

제 13 주	1	4] 수업방법: 강의 및 실습	교재: p461 ~ p489 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드			
	2	1] 강의주제: 증거 이미지 분석				
	3	2] 강의목표: 증거 이미지 분석 기초 지식 습득				
	4	3] 세부내용: ① 이미지 획득				
	5	② 이미지 분석 기술 및 관련 도구				
제 14 주	1	4] 수업방법: 강의 및 실습	교재: p532 ~ p581 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드			
	2	1] 강의주제: Sleuth kit				
	3	2] 강의목표: Sleuth kit 사용법 습득				
	4	3] 세부내용: ① 설치 및 도구 사용법				
	5	② 이미지 분석				
제 15 주	1	기말고사				
	2					
	3					
	4					
	5					
5. 성적평가 방법						
중간고사	기말고사	수 시	출 결	기 타	합 계	비 고
30 %	30 %	15 %	20 %	5 %	100 %	
6. 수업 방법(강의, 토론, 실습 등)						
강의, 토론, 실습 (개별 및 그룹 실습)						
7. 수업에 특별히 참고하여야 할 사항						
8. 문제해결 방법(실험·실습 등의 학습과정의 경우에 작성)						