수 업 계 획 서

1. 강의개요

학습과정명	사이버포렌식실습	학점	3	교강사명		교강사 전화번호	
강의시간	5시간	강 의 실		수강대상		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 갖춤으로써 증거 수집부터 법정 전문가 증언을 아우르는 사이버 포렌식 전문가로서의 전반적인 실무지식을 학습한다.

3. 교재 및 참고문헌

주교재	디지털포렌식의 세계	저자	이준형, 조정원	출판사	인포더북스	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 2 3 4 5	1] 강의주제: 사이버포렌식 개념 2] 강의목표: 사이버포렌식의 이해 3] 수업방법: 강의 및 토론 4] 세부내용: ① 포렌식의 정의 ② 관련 법규 및 사례 ③ Chain of Custody ④ E-Discovery, 준비도, 포렌식 동향	교재: p16 ~ p55 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 2 주	1 2 3 4 5	1] 강의주제: 실시간 증거 획득 2] 강의목표: Live Response & Memory 분석 3] 수업방법: 강의 및 실습 4] 세부내용: ① Live Response 정의 및 수집 방법 ② 메모리 획득 방법 및 분석	교재: p56 ~ p94 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 3 주	1 2 3 4 5	1] 강의주제: 증거 이미지 획득 2] 강의목표: 파일시스템의 이해와 증거 획득 3] 수업방법: 강의 및 실습 4] 세부내용: ① 저장장치의 이해 ② 데이터 획득 방법 및 실습 ③ 볼륨과 파티션	교재: p128 ~ p165 **평가: 수시 #1** 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 4 주	1 2 3 4 5	1] 강의주제: FAT 파일시스템 2] 강의목표: FAT 파일시스템과 복구의 이해 3] 수업방법: 강의 및 실습 4] 세부내용: ① FAT 파일시스템 구조 ② FAT 파일 복구	교재: p166 ~ p188 **과제: FAT32형 USB 메모리 분석** 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 5 주	1 2 3	1] 강의주제: NTFS 파일시스템 2] 강의목표: NTFS 파일시스템과 복구의 이해 3] 수업방법: 강의 및 실습	교재: p189 ~ p229 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드

	4 5	4] 세부내용: ① NTFS 파일시스템 구조 ② NTFS 파일 복구	
제 6 주	1 2 3 4 5	1] 강의주제: 포렌식과 안티포렌식 2] 강의목표: 포렌식 도구 및 안티포렌식의 이해 3] 수업방법: 강의 및 실습 4] 세부내용: ① 포렌식과 안티포렌식 ② PE(Portable Executable) 구조 ③ 포렌식 도구	교재: p314 ~ p359 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 7 주	1 2 3 4 5	1] 강의주제: 윈도우 아티팩트 분석 I 2] 강의목표: 레지스트리 분석 기법 습득 3] 수업방법: 강의 및 실습 4] 세부내용: ① 레지스트리 용어 ② Hive 구조 ③ 주요 레지스트리 아티팩트 분석	교재: p291 ~ p313 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 8 주	1 2 3 4 5	중간고사	
제 9 주	1 2 3 4 5	1] 강의주제: 윈도우 아티팩트 분석 II 2] 강의목표: 레지스트리 분석 기법 습득 3] 수업방법: 강의 및 실습 4] 세부내용: ① MRU의 이해 및 분석 ② USB 사용 기록 분석 ③ 기타 시스템관련 정보 분석	교재: p291 ~ p313, p366 ~ p388 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 10 주	1 2 3 4 5	1] 강의주제: 윈도우 아티팩트 분석 – 파일사용 흔적 2] 강의목표: 사용자 작성 파일 사용 흔적 분석 3] 수업방법: 강의 및 실습 4] 세부내용: ① 윈도우 링크파일, Jump list 분석 ② 레지스트리 분석 ③ 윈도우 휴지통 분석 등	교재: p366 ~ p415 **과제: Windows 10 아티팩트 수집** 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 11 주	1 2 3 4 5	1] 강의주제: 윈도우 아티팩트 분석 – 인터넷 사용 2] 강의목표: 인터넷 사용 흔적 분석 3] 수업방법: 강의 및 실습 4] 세부내용: ① 웹 브라우저의 이해 ② Cache, History, Cookie 분석	교재: p433 ~ p446 **평가: 수시 #2** 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 12 주	1 2 3 4 5	1] 강의주제: 윈도우 아티팩트 분석 – 기타 2] 강의목표: 아티팩트 분석 기술 향상 3] 수업방법: 강의 및 실습 4] 세부내용: ① Event Log, Prefetch 분석 ② 프린터 스풀러 분석	교재: p430 ~ p432, p447 ~ p453 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 13 주	1	1] 강의주제: 증거 이미지 분석 2] 강의목표: 증거 이미지 분석 기초 지식 습득	교재: p461 ~ p489 기자재: 실습용PC, 빔 프로젝터

	2 3 4 5	3] 수업방법: 강의 및 실습 4] 세부내용: ① 이미지 획득 ② 이미지 분석 기술 및 관련 도구	스크린, 화이트보드
제 14 주	1 2 3 4 5	1] 강의주제: Sleuth kit 2] 강의목표: Sleuth kit 사용법 습득 3] 수업방법: 강의 및 실습 4] 세부내용: ① 설치 및 도구 사용법 ② 이미지 분석	교재: p532 ~ p581 기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드
제 15 주	1 2 3 4 5	기말고사	

5. 성적평가 방법

중간고사	기말고사	과 제 물	출 결	기 타	합 계	비 고
30 %	30 %	20 %	20 %	0 %	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)