그분들 말씀 - 포렌식편

현업에 계신 분들의 ''솔직한'' 이야기

INDEX

1

''포렌식 공부?''

잠깐, 디지털 포렌식 정의!

법적 목적으로 사용을 위한
디지털 증거 분석과 관련된
컴퓨터 기술 및 법적(수사) 절차의 적용

1 포렌식 공부?

''포렌식 공부 어떻게 해요?''

''나때는 포렌식 프루프 밖에 없었지.''

''에이~ 제대로 말씀해주세요!''

''ㅋㅋ 내가 만약 시간을 되돌릴 수 있다면 말야.''

1단계: 프로그래밍 언어, 파일 시스템, 네트워크, 문서 작성, 검색 능력

1단계

1) 프로그래밍 언어
2) 파일 시스템
3) 네트워크
4) 문서 작성
5) 검색 능력

2단계

1) 아티팩트
2) 파일 분석
3) 파일 포맷
4) 문서 작성
5) 검색 능력

3단계 : 물리장비는 4단계: 해킹 검색만으로 숙지, 로그 분석은 샘플 최대한, 다양한 도구 설치 및 숙지

3단계

1) 물리장비
2) 로그 분석
3) 해킹 공격
4) 문서 작성
5) 검색 능력

4단계

1) 스스로 망 구성하여 침해사고 감염 시나리오 만들어보고 분석
2) 지인 동의 얻어 PC 분석해서 보고서 적어 보기

1 포렌식 공부?

- 포렌식 관련 사이트 : https://attack.mitre.org/matrices/enterprise/
(어떻게 유입, 공격, 지속성유지, 들어오고 나가는지, 공격에 모든 것 정리)

- 분석 도구 다 있음 : https://github.com/rshipp/awesome-malware-analysis#online-scanners-and-sandboxes

2

''수사관이 되고 싶어?''

2 수사관이 되고 싶어?

''포렌식은 취업 어디로 해요?''

''다양한 곳으로 할 수 있지!''

''사이버 수사관 어때요??''

''기다리던 질문이 나왔군..ㅎㅎ''

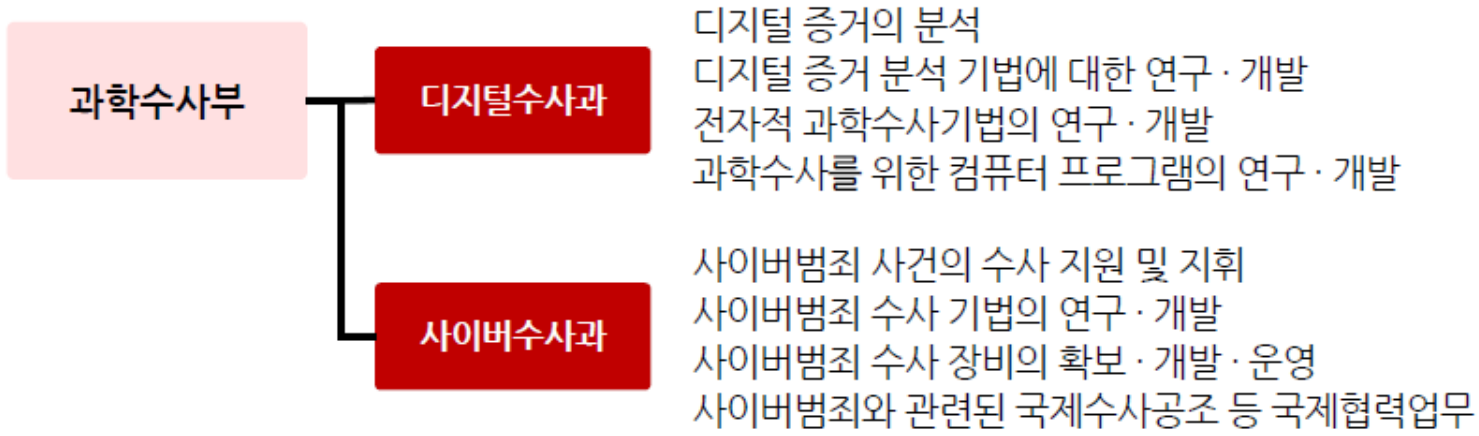
2 수사관이 되고 싶어?

디지털포렌식 전문가 채용 기업 · 기관

- 디지털포렌식은 법정에서 증거능력이 있도록 디지털 증거를 다루는 일이기 때문에 **민 · 형사 소송과 직 · 간접적으로 관련된 분야**에 종사할 수 있음.

검찰의 디지털포렌식

- 검찰의 디지털포렌식은 대검찰청 과학수사부 산하 디지털수사과와 사이버수사과를 중심으로 이루어지고 있음.
- **디지털수사과**의 경우 **일반 사건에서의 디지털 증거 처리를 전담**하고 있으며, 전국 고등검찰청 및 서울중앙지방검찰청, 서울남부지방검찰청, 서울북부지방검찰청에 〈디지털포렌식 센터〉를 구축하고 전국의 디지털 증거 수집 및 분석을 지원하고 있는 지원 부서임.
- **사이버수사과**의 경우 사이버범죄 사건의 수사 지원을 담당하고 있으며, 사이버범죄의 특성 상 디지털 증거와 밀접한 관련이 있기 때문에 **자체 수사 사이버범죄 사건에 대한 디지털포렌식을 수행**하고 있음.



말.말.말

1) 수사관, 공직 시험 봐서 들어가라. 특채 막내 생활 15년 정도 해야 되고 서러운 일 많다.

2) 수사관 일 진짜 많다. > 범죄 접수 한달 10만 건, 사이버 수사관 5000명

3) 간부후보생 추천 > 6급 시작, 대신 다 포기하고 시험, 사이버 경쟁률 18:1(2-3년 준비)

4) 변호사 자격증 따서 로펌, 컨설팅 분야 추천 > 로스쿨 가면 50% 변호사 시험합격(3년 투자), 되면 넘사

3

''포렌식 대회?''

문제 유형?

대세 : 침해사고 분석 문제, 크게 두 부류

FILE : 이미지 -> 압축해제 -> 분석 -> 문제풀이

LIVE : 접속 -> 분석 ->문제풀이

가치있는 대회

국내 > 디지털 포렌식 챌린지 (현재 진행중)

국외 > DFRWS (직접 툴 개발, 난이도 높음)

감사합니다 :)