**1. 디지털 포렌식 종류를 서술하시오**

네트워크, 디스크, 메모리, 활성테이터, 모바일/임베디드, 시스템, 암호학, 멀티미디어, 인터넷, DB, 이메일, 애프리케이션, 웹, IOT, 소스코드, 안티포렌식, 클라우드, 앱 포렌식이 있다.

**2. 디지털 포렌식 대상물의 특징을 서술하시오**

**데이터 포렌식**

대상물: FAT, NTFS, EXT2, EXT3 등 (디지크 파일시스템 분석 과 디스크 검색, 복구, MAC 분석, 키워드 검색)

**네트워크 포렌식**

대상물: 라우터, 스위치, FW, IDS 등 (네트워크를 통한 데이터 및 로그 분석, 스니핑 된 트래픽 로깅 파일)

**데이터베이스 포렌식**

대상물: 정보시스템의 데이터 베이스 (데이터베이스로부터 데이터를 추출 및 분석 기업의 분식회계, 횡령, 탈세수사 시 필수임)

**Mobile 포렌식**

대상물: 휴대폰, PDA, 전자수첩 USB 저장장치, 미디어 (휴대용 기기에서 필요한 정보를 입수 및 분석, 휴대용 기기의 은닉 용이성으로 세심한 분석이 필요함)

**Cryptograph 포렌식**

대상물: 암호화 시스템 (문서나 시스템에서 암호를 추출, 증거수집에서 비인가 접근을 막기 위해 문서나 시스템에 암호를 설정한 경우 암호 분석)

**회계 포렌식**

대상물: 회계 시스템 (저장된 회계 데이터를 추출하고 회계 전문가가 분석할 수 있도록 데이터를 정제함, 기업의 부정과 관련된 수사 시 필요)

**3. 디지털 포렌식 5대 원칙을 서술 하시오**

정당성의 원칙: 획득한 디지털 자료 증거가 적법한 절차를 거쳐 획득, 위법한 방법으로 수집된 증거는 법적 효력을 상실(위법 수집 증거배제 법칙)

재현의 원칙: 피해 당시와 동일 조건에서 현장 검증 시 동일한 결과 도출

신속성의 원칙: 컴퓨터 시스템의 휘발성 정보수집 가능성은 신속한 조치에 의해 결정되므로 신속히 수행

연계 보관성의 원칙(Chain of Custody): 디지털 증거물의 획득-> 이송 -> 분석 -> 보관 -> 법정 제출의 각 단계에 따른 책임자 명시

무결성의 원칙: 획득한 디지털 증거가 위조 또는 변조되지 않았음을 증명