**1번 답**

**디지털 포렌식의 종류는 분석 목적에 따라 크게 사고 대응 포렌식과 입증을 위해 정보 추출 포렌식으로 나뉩니다. 사고 대응 포렌식은 사고 내용을 분석하여 조치를 취하고 추가적인 피해가 없게 막고, 서비스를 재개하는데 목적을 두고, 정보 추출 포렌식은 컴퓨터나 저장매체에 남아 있는 범행 흔적이나 정보를 복구하거나 검색하는 과정을 함으로써 정보를 추출합니다.**

**2번 답**

**1) 매체 독립성**

**- 디지털 증거는 유체물이 아닌 각종 디지털 저장매체에 저장되어 있거나 네트워크를 통하여 전송 중인 정보 그 자체**

**- 정보는 값이 같다면 어느 매체에 저장되어 있뜬지 동일한 가치**

**- 따라서 디지털 증거는 사본과 원본의 구별이 불가능함**

**2) 비가시성, 비가독성**

**- 디지털 증거 그 자체는 사람의 지각으로 바로 인식이 불가능**

**- 일정한 변환절차를 거쳐 모니터 화면으로 출력되거나 프린터를 통하여 인쇄된 형태로 출력되었을 때 가시성과 가독성을 가짐**

**- 따라서, 디지털 증거와 출력된 자료와의 동일성 여부가 중요**

**3) 취약성**

**- 삭제, 변경 등이 용이**

**- 하나의 명령으로 하드디스크 전체를 포맥하거나 파일 삭제가 가능**

**- 파일을 열어보는 것만으로 파일 속성이 변경됨**

**- 수사기관에 의한 증거조작의 가능성도 배제할 수 없으므로 디지털 증거에 대한 무결성 문제가 대두**

**4) 대량성**

**- 방대한 분량의 정보를 하나의 저장매체에 저장가능함**

**- 수사기관에 의해 압수되는 경우 업무수행에 지장을 줄 수 있음**

**5) 전문성**

**- 디지털 증거의 수집과 분석에 전문적인 기술이 사용되므로, 디지털 증거의 압수, 분석 등에 있어 디지털 포렌식 전문가가 필수적임**

**- 여기에서 디지털 증거에 대한 신뢰성 문제가 대두**

**6) 네트워크 관련성**

**- 네트워크를 통해 서로 연결되어 있기 때문에, 디지털 증거의 관할권을 어느 정도까지 인정할 것인지 문제 발생.**

**- 국경을 넘는 경우 국가의 주권문제까지 연관**

**3번 답**

**1) 정당성의 원칙**

**- 디지털 증거는 법적 절차에 의해 수집되어야 한다. 위법한 방법으로 수집 시 법적 효력이 상실한다.**

**2) 무결성의 원칙**

**- 디지털 증거는 습득 후 어떠한 일이 발생하여도 변조가 되어서는 안된다,**

**3) 연계성의 원칙**

**- 디지털 증거의 습득, 이송, 분석, 보관, 법정 제출 각 단계에서 담당자와 업무자를 명확히 하여야 한다.**

**4) 신속성의 원칙**

**- 모든 과정은 지체없이 신속하게 진행되어야 한다.**

**5) 재현의 원칙**

**- 피해 직전과 같은 환경에서 현장 재현 시 피해 당시와 동일한 결과가 나와야 한다.**