* 1. 디지털 증거

디지털 형태로 저장되거나 전송되는 증거가치가 있는 정보

* 1. 디지털 증거 = 전자 증거 (Electronic Evidence)

전자기기에 저장되어 있거나, 전가 기기에 의해 전송되는 증거 가치가 있는 정보

* 1. 분류 (증거가 존해가게 된 과정에서 사용자의 개입여부에 따라 나뉨)
     1. 컴퓨터가 생성한 증거 (computer-generated records) :

컴퓨터가 운영체제를 포함한 시스템의 모든 것을 유지하고 관리하기 위한 데이터

ex) system logs (사용자의 개입없이 자동 생성, 작성한 데이터 관한 출처 증명, 진위 판정 등 활용 가능)

* 1. 컴퓨터에 저장된 증거 (computer-stored records) :

사용자가 인식하는 상태에서 생성하고 저장한 데이터

ex) 엑셀

사용자가 법정엥서 자신의 것임을 인정하는 경우에만 법저긍로 유효한 증거가 됨

조사하는 분석관이 혐의자가 소유하거나 사용하였더 데이터가 맞다고 하는 진술이나 객관적 증거를 확보 해야 하고, 해당 데이터는 신뢰할 만한 사실을 입증 요구

* 1. 디지털 증거의 3개 유형 ( Guid To Computer Forensics And Investigation의 저자 Bill Nelson이 범죄와의 관계를 고려해 분류)
     1. 범죄의 도구로서의 디지털 증거

공격자의 시스템이나 문서의 위변조에 이용된 컴퓨터는 각각 해당 범죄의 도구로 이용된 디지털 증거

* 1. 해킹 공격과 위변조란 혐의자의 행위를 분석해야 하므로 디바이스 전체에 대한 획득을 전제로 함

* 1. 범죄의 목표가 된 디지털 증거

해킹 사건에서 피해 시스템이나 데이터 절취 사건에서 목표가 된 데이터가 포함된 디지털 디바이스가 대표적

* 1. 침해로 인한 피해의 흔적에 대한 조사와 피해 복구가 함께 고려되어야 함

* 1. 데이터가 기록된 장소로서의 디지털 증거

어떤 범죄든 사건과 직접적으로 관련 없는 제3자의 디지털 디바이스는 단순히 사건과 관련된 데이터가 기록된 장소로서 의미만 지님

ex) 기업주가 거액의 회삿돈을 횡령한 사건에서 공범이 아닌 회사 직원들의 컴퓨터는 사건과 관련된 데이터가 기록되어 있을 가능성 있지만, 아무런 관련 없는 데이터 물론이고 개인의 사적인 데이터가 존재할 수 있으므로 데이터에 대한 선별작업이 중요