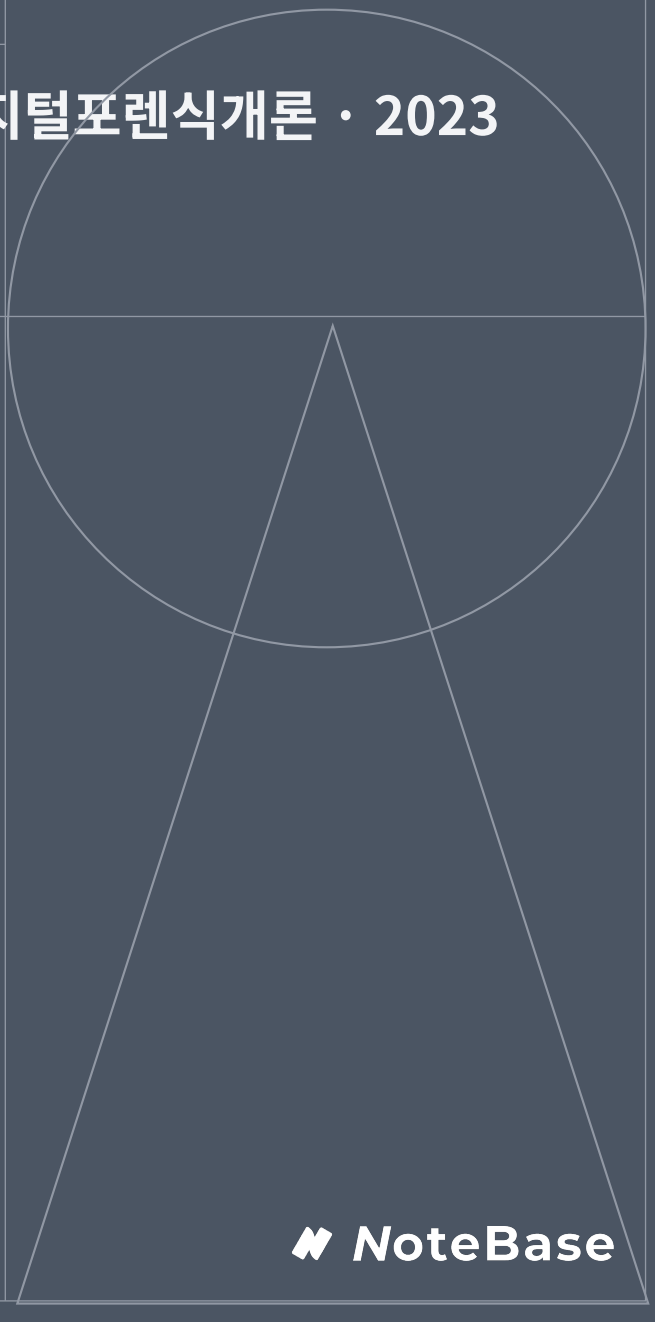
# 기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2023



NoteBase

# 기출OX 해설집

## 공무원/경찰/경력채용 · 디지털포렌식개론 · 2023

### 공무원/경찰/경력채용 · 디지털포렌식개론 · 2023

**문 1. 디지털 증거의 특징에 관한 설명으로 가장 적절하지 않은 것은?**

① 디지털 증거의 경우 해당 증거의 내용을 수사관의 지각으로 바로 인식할 수 없기 때문에 증거로 사용되기 위해서는 일정한 절차(가독화)를 거쳐야 하는 특징이 있다.

② 디지털 증거는 복제를 통해 원본과 동일한 사본을 만들 수 있으나 속성정보(메타데이터)가 변경되기 때문에 해시값도 변경된다.

③ 증거수집분석 등 일련의 취급과정에서 프로그램 조작자의 부주의로 인해 의도치 않게 증거물 파일의 내용이 쉽게 변경될 가능성이 높다.

④ 압수대상이 되는 디지털 증거는 단독으로 존재하기 보다는 사건과 관련 없는 개인적인 자료와 혼재되어 있는 경우가 많다.

**정답 2번**

**간단한 해설**

디지털 증거는 **동일한 비트열로 복제할 수 있으며, 같은 입력과 알고리즘의 해시값은 같다.** 파일시스템 속성 변경과 파일 내용 해시를 구별해야 하므로, 복제 시 해시값도 반드시 변경된다는 ②가 적절하지 않다.

NoteBase

**선지별 해설**

① (O) 저장매체의 비트열은 사람의 감각으로 곧바로 내용을 읽을 수 없으므로, **적절한 하드웨어와 소프트웨어로 해석·표시하는 가독화**가 필요하다. 화면 표시나 출력도 이러한 해석 과정을 거친 결과이다.

② (X) **같은 범위의 비트열을 정확히 복제하고 같은 해시 알고리즘을 적용하면 해시값은 같다.** 일반 파일 복사로 복사본의 생성시각 등 파일시스템 속성이 달라질 수는 있지만, 그 속성이 파일 내용 해시의 입력 범위 밖이라면 내용 해시는 달라지지 않는다. 반대로 해시 입력에 포함된 메타데이터가 바뀌면 입력이 달라진다. 복제하면 메타데이터와 해시가 반드시 변경된다는 일반화가 잘못이다.

③ (O) 디지털 자료는 쓰기 작업으로 쉽게 변할 수 있으며, **분석자의 부주의나 프로그램의 자동 기록**으로 의도하지 않은 변경이 발생할 수 있다. 원본을 보존하고 검증된 사본으로 분석하며 취급 과정을 기록하는 이유이다.

④ (O) 하나의 저장매체나 계정에는 여러 목적의 자료가 함께 저장되므로 **사건 관련 자료와 무관한 개인 자료가 혼재**할 수 있다. 따라서 분석 과정에서 관련성을 구분해야 한다. 이는 디지털 자료의 저장 특성에 관한 설명이며 구체적인 압수 절차나 법적 허용 범위를 단정하는 것은 아니다.

NoteBase

**문 2. 디지털 증거의 동일성·무결성·신뢰성에 관한 설명으로 가장 적절하지 않은 것은? (다툼이 있는 경우 판례에 의함)**

① 무결성과 동일성, 신뢰성이 인정되지 않으면 증거능력이 부정되어 증거로 사용할 수 없다.

② 무결성은 디지털 증거가 수집 및 분석과정을 거쳐 법정에 제출되기까지 변경이나 훼손 없이 유지되어야 한다는 것을 의미한다.

③ 동일성과 무결성을 증명하는 방법은 원본과 해시값이 동일하다는 피압수자의 확인서면에 의해 증명할 수 있다.

④ 컴퓨터의 기계적 정확성, 프로그램의 신뢰성을 확보하되, 수사기밀 유지를 위하여 결과보고서에는 사용한 하드웨어 장비나 소프트웨어 도구를 기재해서는 안 된다.

**정답 4번**

①

디지털 증거의 증거능력을 인정하려면 **원본과 제출 자료의 동일성, 수집·처리 과정의 무결성, 사용한 장비·프로그램과 처리 과정의 신뢰성**이 확보되어야 한다. 이러한 요건이 인정되지 않으면 증거로 사용할 수 없다.

(1) 압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체(이하 '정보저장매체'라고만 한다)에 입력하여 기억된 문자정보 또는 그 출력물(이하 '출력 문건'이라 한다)을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다. 특히 정보저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다(대법원 2007. 12. 13. 선고 2007도7257 판결 등 참조). (대법원 2013. 7. 26. 선고 2013도2511 판결)

NoteBase

②

무결성은 디지털 증거가 **수집된 때부터 분석·보관을 거쳐 법정에 제출될 때까지 변경되거나 훼손되지 않고 유지되는 것**을 의미한다. 이는 **제출된 자료가 수집 당시 원본의 내용을 그대로 반영한다는 동일성**을 뒷받침하기 위한 것이다.

(1) 압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체(이하 '정보저장매체'라고만 한다)에 입력하여 기억된 문자정보 또는 그 출력물(이하 '출력 문건'이라 한다)을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다. 특히 정보저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다(대법원 2007. 12. 13. 선고 2007도7257 판결 등 참조). 이 경우 출력 문건과 정보저장매체에 저장된 자료가 동일하고 정보저장매체 원본이 문건 출력 시까지 변경되지 않았다는 점은, 피압수·수색 당사자가 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체의 해쉬(Hash) 값이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법에 의하여 증명하는 것이 원칙이나, 그와 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우에는, 정보저장매체 원본에 대한 압수, 봉인, 봉인해제, '하드카피' 또는 '이미징' 등 일련의 절차에 참여한 수사관이나 전문가 등의 증언에 의해 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이의 해쉬 값이 동일하다거나 정보저장매체 원본이 최초 압수 시부터 밀봉되어 증거 제출 시까지 전혀 변경되지 않았다는 등의 사정을 증명하는 방법 또는 법원이 그 원본에 저장된 자료와 증거로 제출된 출력 문건을 대조하는 방법 등으로도 그와 같은 무결성·동일성을 인정할 수 있다고 할 것이며, 반드시 압수·수색 과정을 촬영한 영상녹화물 재생 등의 방법으로만 증명하여야 한다고 볼 것은 아니다. (대법원 2013. 7. 26. 선고 2013도2511 판결)

NoteBase

③

**피압수·수색 당사자가 원본과 복제·이미징 매체의 해시값이 같다는 취지로 서명한 확인서면**을 법원에 제출하여 동일성과 무결성을 증명할 수 있다.

특히 정보저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다(대법원 2007. 12. 13. 선고 2007도7257 판결 등 참조). 이 경우 출력 문건과 정보저장매체에 저장된 자료가 동일하고 정보저장매체 원본이 문건 출력 시까지 변경되지 않았다는 점은, 피압수·수색 당사자가 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체의 해쉬(Hash) 값이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법에 의하여 증명하는 것이 원칙이나, 그와 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우에는, 정보저장매체 원본에 대한 압수, 봉인, 봉인해제, '하드카피' 또는 '이미징' 등 일련의 절차에 참여한 수사관이나 전문가 등의 증언에 의해 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이의 해쉬 값이 동일하다거나 정보저장매체 원본이 최초 압수 시부터 밀봉되어 증거 제출 시까지 전혀 변경되지 않았다는 등의 사정을 증명하는 방법 또는 법원이 그 원본에 저장된 자료와 증거로 제출된 출력 문건을 대조하는 방법 등으로도 그와 같은 무결성·동일성을 인정할 수 있다고 할 것이며, 반드시 압수·수색 과정을 촬영한 영상녹화물 재생 등의 방법으로만 증명하여야 한다고 볼 것은 아니다. (대법원 2013. 7. 26. 선고 2013도2511 판결)

④

분석 결과의 신뢰성을 검증하고 처리 과정을 재현할 수 있도록 **사용한 하드웨어 장비와 소프트웨어 도구를 결과보고서에 기록**해야 한다. 수사기밀 유지를 이유로 이를 기재해서는 안 된다는 설명은 잘못이다.

NoteBase

**문 3. 세계의 다양한 언어와 문자를 지원하는 국제 코드 규약인 유니코드에서 가장 일반적으로 사용되며 영문은 1바이트, 한글은 3바이트로 표현하는 코드로 가장 적절한 것은?**

① ASCII

② EBCDIC

③ BASE64

④ UTF-8

**정답 4번**

**간단한 해설**

**UTF-8**에서는 기본 영문자를 1바이트, 일반적인 완성형 한글 음절을 코드 포인트당 3바이트로 표현한다. 문자에 따라 길이가 달라지는 유니코드 인코딩 방식이다.

**핵심 풀이**

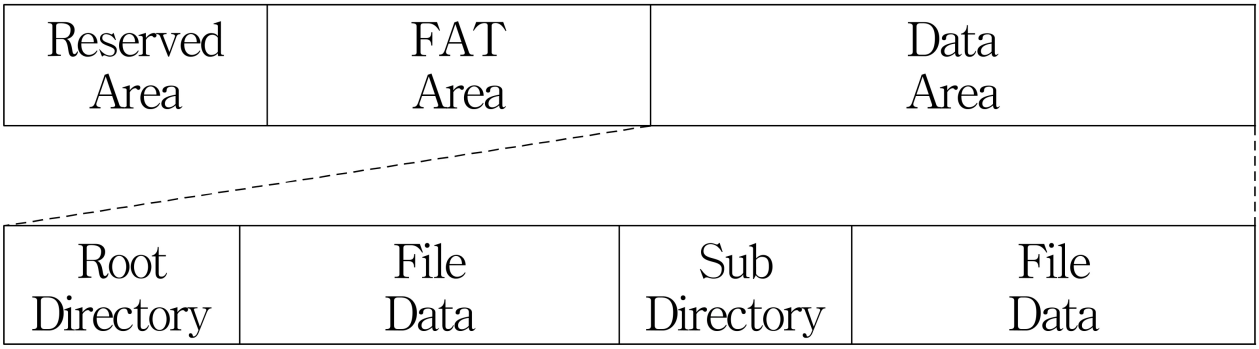
**UTF-8**은 유니코드 코드 포인트를 1~4바이트로 표현하는 가변 길이 인코딩이다. 기본 영문자처럼 ASCII 범위인 U+0000~U+007F의 문자는 1바이트로 표현되므로 ASCII와 호환된다.

일반적인 완성형 한글 음절은 U+AC00~U+D7A3에 속하므로 UTF-8에서 **음절 코드 포인트 하나당 3바이트**가 된다. 예를 들어 A는 1바이트, 가는 3바이트이다. 다만 한글 음절을 여러 자모로 분해하여 저장하면 그 코드 포인트들의 바이트 수를 합산해야 하므로, 화면에 보이는 한 글자가 언제나 총 3바이트라는 뜻은 아니다.

따라서 제시된 바이트 길이 특성에 맞는 것은 ④ UTF-8이다.

NoteBase

**문 4. 다음 그림에서 설명하는 구조를 사용하여 USB, 디지털카메라, 메모리카드에서 사용되는 파일시스템에 관한 설명으로 가장 적절하지 않은 것은?**




① Boot 섹터는 파일시스템의 첫 번째 섹터에 위치한다.

② FAT Area는 클러스터의 할당 상태를 판단하며 백업용 FAT는 없다.

③ Data Area에는 실제 파일의 데이터가 존재한다.

④ Directory Entry는 파일과 디렉터리마다 할당된 데이터 구조체이며, 메타데이터가 포함된다.

**정답 2번**

**간단한 해설**

FAT 영역에는 클러스터의 할당·연결 정보가 기록되며, 보통 **FAT 사본을 함께 두어 중복성**을 확보한다. 따라서 백업용 FAT가 없다는 설명은 틀리다.

NoteBase

**선지별 해설**

그림은 예약 영역, FAT 영역, 데이터 영역으로 나뉘며, 루트 디렉터리도 데이터 영역에 놓인 FAT32 구조를 보여준다.

① O: 부트 섹터는 FAT 볼륨의 첫 번째 섹터에 있으며 예약 영역에 포함된다. 이곳에는 부팅 관련 정보와 파일시스템의 구조를 해석하는 데 필요한 BPB가 들어 있다. 볼륨의 첫 섹터가 물리 디스크 전체의 첫 섹터와 반드시 같은 것은 아니다.

② X: FAT는 클러스터의 사용 상태와 파일을 구성하는 클러스터들의 연결 관계를 기록한다. 일반적인 FAT 구성은 **중복성을 위한 FAT 사본**을 두므로 백업용 FAT가 없다는 설명은 틀리다. FAT 개수는 BPB에 기록되며 통상 두 개를 사용한다.

③ O: 데이터 영역에는 파일의 실제 내용이 클러스터 단위로 저장된다. 그림에서 File Data뿐 아니라 Root Directory와 Sub Directory도 이 영역에 표시되어 있으므로, 파일 내용만 저장하는 영역이라고 한정해서는 안 된다.

④ O: 디렉터리 엔트리는 파일·하위 디렉터리를 관리하기 위한 항목이다. 이름, 속성, 시간 정보, 시작 클러스터 등 **메타데이터**를 기록하여 실제 데이터의 위치와 특성을 파악하게 한다.

NoteBase

**문 5. 「디지털 증거의 처리 등에 관한 규칙」의 내용으로 옳지 않은 것은?**

① 디지털 증거의 수집은 수사목적을 달성하는데 필요한 최소한의 범위에서 이루어져야 하며, 「형사소송법」 등 관계 법령에 따른 적법절차를 준수하여야 한다.

② 디지털 증거 처리의 각 단계에서 업무처리자 변동 등의 이력이 관리되어야 한다.

③ 증거분석관은 신속한 분석과 결과보고서의 신뢰성을 확보하기 위하여 분석의뢰물 원본을 대상으로 직접 분석하여야 한다.

④ 전자정보에 대한 압수·수색·검증영장을 신청하는 경우에는 혐의사실과의 관련성을 고려하여 압수·수색·검증할 전자정보의 범위 등을 명확히 하여야 한다.

**정답 3번**

①

디지털 증거는 **수사목적 달성에 필요한 최소한의 범위**에서 수집하고, **관계 법령에 따른 적법절차**를 준수해야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제9조(디지털 증거 수집 시 원칙) 디지털 증거의 수집은 수사목적을 달성하는데 필요한 최소한의 범위에서 이루어져야 하며, 「형사소송법」 등 관계 법령에 따른 적법절차를 준수하여야 한다.

②

각 단계의 보관 주체 사이에 증거가 연속적으로 승계되었는지 확인할 수 있도록 **업무처리자 변동 등의 이력을 관리**해야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제5조(디지털 증거 처리의 원칙) 디지털 증거의 처리는 다음 각 호의 원칙에 따라 이루어져야 한다.
3. 디지털 증거 처리의 각 단계별 보관 주체들 간의 연속적인 승계 절차를 위하여 업무처리자 변동 등 이력을 관리할 것

NoteBase

③

분석의뢰물의 변경을 방지하기 위해 **복제하여 분석하는 것이 원칙**이다. **수사상 긴박한 사정이 있거나 복제본을 획득할 수 없는 부득이한 사정**이 있는 경우에는 쓰기방지 등 변경 방지 조치를 한 후 직접 분석할 수 있다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제34조(분석의뢰물의 분석) ① 증거분석관은 분석의뢰물이 변경되지 않도록 분석의뢰물을 복제하여 디지털 증거분석을 수행하여야 한다. 이 경우 분석의뢰물과 복제한 전자정보의 해시값을 비교 · 기록하여 동일성을 유지하여야 한다. ② 증거분석관은 수사상 긴박한 사정이 있거나 복제본을 획득할 수 없는 부득이한 사정이 있는 경우에는 쓰기방지 장치를 사용하는 등 분석의뢰물이 변경되지 않도록 조치한 후 의뢰받은 분석의뢰물을 직접 분석할 수 있다.

④

전자정보의 압수·수색·검증영장을 신청할 때에는 **혐의사실과의 관련성을 고려하여 대상 전자정보의 범위를 명확히** 해야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제10조(압수 · 수색 · 검증영장의 신청)
② 경찰관은 전자정보에 대한 압수 · 수색 · 검증영장을 신청하는 경우에는 혐의사실과의 관련성을 고려하여 압수 · 수색 · 검증할 전자정보의 범위 등을 명확히 하여야 한다. 이 경우 영장 집행의 실효성 확보를 위하여 다음 각 호의 사항을 고려하여야 한다. 1. 압수 · 수색 · 검증 대상 전자정보가 원격지의 정보저장매체등에 저장되어 있는 경우 등 특수한 압수 · 수색 · 검증방식의 필요성 2. 압수 · 수색 · 검증영장에 반영되어야 할 압수 · 수색 · 검증 장소 및 대상의 특수성

NoteBase

**문 6. 디스크를 병렬처리하여 성능과 안전성을 향상시키는 저장 방식인 RAID(Redundant Array of Inexpensive Disks)에 관한 설명으로 가장 적절하지 않은 것은?**

① 레벨: RAID 0, 특징: 병렬기록, 스트라이핑 모드

② 레벨: RAID 1, 특징: 중복기록, 미러링 모드

③ 레벨: RAID 3, 특징: 패리티 정보기반 병렬 분산 저장

④ 레벨: RAID 5, 특징: 최소한 2개 이상의 디스크 필요

**정답 4번**

**간단한 해설**

RAID 5는 데이터와 분산 패리티를 서로 다른 디스크에 배치하므로 **최소 3개의 디스크**가 필요하다. 디스크 2개만으로 구성하는 방식이 아니다.

**선지별 해설**

① O: RAID 0은 데이터를 여러 디스크에 나누어 기록하는 **스트라이핑** 방식으로 병렬 입출력 성능을 높인다. 미러링이나 패리티가 없어 한 디스크가 고장 나면 배열의 데이터를 잃을 수 있으므로, 자체적인 장애 복구 기능은 없다.

② O: RAID 1은 동일한 데이터를 두 디스크 이상에 중복 기록하는 **미러링** 방식이다. 한 디스크가 고장 나도 다른 복제본으로 데이터를 사용할 수 있는 대신, 복제본을 저장하는 만큼 실제 가용 용량이 줄어든다.

③ O: RAID 3은 데이터를 바이트 단위로 여러 디스크에 나누어 병렬 저장하고 **별도의 전용 디스크에 패리티**를 기록한다. 데이터와 패리티를 이용하여 디스크 한 개의 장애를 복구할 수 있다. 패리티 자체를 여러 디스크에 분산하는 RAID 5와는 다르다.

④ X: RAID 5는 블록 단위 스트라이핑과 분산 패리티를 사용하며 **최소 3개의 디스크**가 필요하다. 최소 구성에서 데이터 블록 둘과 그에 대한 패리티 블록을 서로 다른 디스크에 배치한다. 따라서 최소 필요 개수를 2개로 제시한 설명은 맞지 않는다.

NoteBase

**문 7. SSD(Solid State Drive)에 관한 설명 중 옳고 그름의 표시 (O, X)가 바르게 된 것은?**

㉠ 비휘발성으로 전원이 없어도 데이터 저장 상태를 유지할 수 있다.
㉡ HDD와 비교하면 작동 시 소음이 없으며 전력 소모가 많은 대용량 플래시 메모리이다.
㉢ 임의접근 방법을 사용하므로 데이터 입·출력을 저속으로 수행할 수 있다.
㉣ HDD와 비교하면 외부의 충격, 진동, 자성에 강하여 데이터 손실의 가능성이 낮다.

① ㉠(O) ㉡(X) ㉢(X) ㉣(X)
② ㉠(X) ㉡(X) ㉢(O) ㉣(X)
③ ㉠(O) ㉡(O) ㉢(X) ㉣(X)
④ ㉠(O) ㉡(X) ㉢(X) ㉣(O)

**정답 4번**

**간단한 해설**

SSD는 **비휘발성 플래시 기반의 빠른 저장장치**이며, 기계적 구동부가 없어 소음·충격 면에서 유리하다. 전력 소모가 많고 임의 접근이 저속이라는 설명을 바로잡아야 한다.

**보기별 해설**

㉠ O: 일반적인 SSD의 NAND 플래시는 **비휘발성 저장매체**이므로 전원이 꺼져도 기록된 데이터를 유지한다. 다만 아직 플래시에 기록되지 않은 휘발성 캐시의 데이터까지 갑작스러운 정전으로부터 항상 보호된다는 뜻은 아니다.

㉡ X: SSD는 회전 원판이나 이동 헤드가 없어 **기계적 구동 소음이 없고, 일반적인 비교에서는 전력 소모가 적다**. 따라서 전력 소모가 많다는 부분이 잘못되었다. 실제 소비전력은 제품과 작업 부하에 따라 달라지므로 모든 SSD가 모든 HDD보다 항상 적게 소비한다는 의미는 아니다.

㉢ X: SSD는 HDD의 헤드 이동·회전 대기 없이 전자적으로 접근하므로 **임의 접근 지연이 짧고 빠른 입출력**에 유리하다. 임의 접근을 사용하기 때문에 저속이라는 설명은 이러한 특성과 반대이다.

㉣ O: SSD는 움직이는 기계 부품이 없고 자기 기록 방식도 아니므로 **충격·진동과 자기장에 의한 기록 손상에 비교적 강하다**. 이 비교는 그러한 외부 요인에 관한 것으로, SSD에 고장이나 데이터 손실 가능성이 전혀 없다는 뜻은 아니다.

따라서 ㉠ O, ㉡ X, ㉢ X, ㉣ O로 표시한 ④가 정답이다.

NoteBase

**문 8. 디지털 증거의 압수·수색·검증에 관한 설명으로 가장 적절하지 않은 것은? (다툼이 있는 경우 판례에 의함)**

① 전자정보 압수는 원칙적으로 범죄 혐의사실과 관련된 전자정보에 한하여 문서로 출력하거나 휴대한 정보저장매체에 해당 전자정보만을 복제하는 방식으로 하여야 한다.

② 정보저장매체 원본을 압수·수색·검증현장에서 수사기관 사무실 등으로 반출한 경우에는 피압수자에게 참여권을 보장하여야 한다.

③ 압수된 정보의 상세목록에는 정보의 파일 명세가 특정되어 있어야 하고, 서면으로 교부하거나 압수한 전자정보를 전자파일 형태로 복사해 주는 방식으로도 교부할 수 있다.

④ 압수·수색·검증현장에서 정보저장매체 원본을 반출한 경우에는 수사 종결 때까지 원본을 증거물 보관실에 보관한 후, 반환하여야 한다.

**정답 4번**

①

전자정보는 원칙적으로 **범죄 혐의사실과 관련된 부분만 선별하여 출력하거나 수사기관이 휴대한 저장매체에 복제**한다. 이러한 방법이 불가능하거나 압수 목적 달성이 현저히 곤란한 경우에만 매체나 전체 복제본의 반출이 예외적으로 허용된다.

따라서 수사기관의 전자정보에 대한 압수·수색은 원칙적으로 영장 발부의 사유로 된 범죄 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복제하는 방식으로 이루어져야 하고, 저장매체 자체를 직접 반출하거나 그 저장매체에 들어 있는 전자파일 전부를 하드카피나 이미징 등 형태(이하 '복제본'이라 한다)로 수사기관 사무실 등 외부로 반출하는 방식으로 압수·수색하는 것은 현장의 사정이나 전자정보의 대량성으로 인하여 관련 정보 획득에 긴 시간이 소요되거나 전문 인력에 의한 기술적 조치가 필요한 경우 등 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에 한하여 예외적으로 허용될 수 있을 뿐이다. (대법원 2015. 7. 16.자 2011모1839 전원합의체 결정)

NoteBase

②

원본을 수사기관 사무실로 옮긴 뒤 이루어지는 복제·탐색·출력도 **하나의 영장에 따른 압수·수색 과정**이므로 피압수자나 변호인에게 **참여할 기회를 보장**해야 한다.

따라서 저장매체에 대한 압수·수색 과정에서 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란한 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 또는 복제본을 수사기관 사무실 등으로 옮겨 이를 복제·탐색·출력하는 경우에도, 그와 같은 일련의 과정에서 형사소송법 제219조, 제121조에서 규정하는 피압수·수색 당사자(이하 '피압수자'라 한다)나 그 변호인에게 참여의 기회를 보장하고 혐의사실과 무관한 전자정보의 임의적인 복제 등을 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차를 준수하여야 한다. (대법원 2015. 7. 16.자 2011모1839 전원합의체 결정)

③

상세목록은 피압수자가 압수 범위를 확인하여 권리를 행사할 수 있도록 **정보의 파일 명세를 특정**해야 한다. 그 목록은 **출력한 서면뿐 아니라 전자파일을 복사하거나 이메일로 전송하는 방식으로도 교부**할 수 있다.

압수물 목록은 피압수자 등이 압수처분에 대한 준항고를 하는 등 권리행사절차를 밟는 가장 기초적인 자료가 되므로, 수사기관은 이러한 권리행사에 지장이 없도록 압수 직후 현장에서 압수물 목록을 바로 작성하여 교부해야 하는 것이 원칙이다(대법원 2009. 3. 12. 선고 2008도763 판결 참조). 이러한 압수물 목록 교부 취지에 비추어 볼 때, 압수된 정보의 상세목록에는 정보의 파일 명세가 특정되어 있어야 하고, 수사기관은 이를 출력한 서면을 교부하거나 전자파일 형태로 복사해 주거나 이메일을 전송하는 등의 방식으로도 할 수 있다. (대법원 2018. 2. 8. 선고 2017도13263 판결)

④

전자정보 확보를 위해 반출한 원본은 **복제본을 획득한 뒤 영장에 정한 절차에 따라 지체 없이 반환**해야 한다. 원본을 계속 보유할 특별한 사정도 없이 수사 종결까지 보관하는 것은 허용되지 않는다.

가) 이 사건 영장에 첨부된 '압수 대상 및 방법의 제한'에는 [별지]와 같이 원칙적으로 저장매체의 소재지에서 수색·검증 후 혐의사실과 관련된 전자정보만을 범위를 정하여 문서로 출력하거나 수사기관이 휴대한 저장매체에 복제하여야 하고(이하 '원칙적 방법'이라 한다), 예외적으로 저장매체 소재지에서 복제본 형태로 반출하여 전자정보를 압수할 수 있으며(이하 '제1 예외적 방법'라 한다), 제1 예외적 방법이 불가능하거나 현저히 곤란한 경우에는 피압수자 등의 참여 아래 저장매체 원본을 봉인하여 저장매체의 소재지 이외의 장소로 반출할 수 있지만, 그 경우 피압수자 등의 참여권을 보장한 가운데 원본을 개봉하여 복제본을 획득하고, 원본은 지체 없이 반환하되, 특별한 사정이 없는 한 원본 반출일로부터 10일을 도과하여서는 안 된다(이하 '제2 예외적 방법'이라 한다)는 내용이 명시되어 있다. (대법원 2022. 7. 14.자 2019모2584 결정)

NoteBase

**문 9. 다음 전자정보 중 전문증거에 해당하는지 확인해 볼 필요가 있는 증거를 모두 고른 것은?**

㉠ 운영체제 이벤트 로그기록
㉡ 웹 히스토리
㉢ 사용자 작성의 문서파일
㉣ 송·수신된 이메일 내용
㉤ 방화벽 로그

① ㉠㉡
② ㉡㉢
③ ㉢㉣
④ ㉣㉤

**정답 3번**

㉠

운영체제 이벤트 로그는 시스템에서 발생한 사건을 **자동으로 기록한 비진술증거**이다. 사람의 진술을 담은 자료가 아니므로 전문법칙의 적용 대상이 아니다.

형사소송법 제310조의2(전문증거와 증거능력의 제한) 제311조 내지 제316조에 규정한 것 이외에는 공판준비 또는 공판기일에서의 진술에 대신하여 진술을 기재한 서류나 공판준비 또는 공판기일 외에서의 타인의 진술을 내용으로 하는 진술은 이를 증거로 할 수 없다.

㉡

웹 히스토리는 브라우저가 웹사이트 방문 내역을 **자동으로 저장한 기록**이다. 방문 사실을 기록한 비진술증거이므로 전문법칙의 적용 대상이 아니다.

형사소송법 제310조의2(전문증거와 증거능력의 제한) 제311조 내지 제316조에 규정한 것 이외에는 공판준비 또는 공판기일에서의 진술에 대신하여 진술을 기재한 서류나 공판준비 또는 공판기일 외에서의 타인의 진술을 내용으로 하는 진술은 이를 증거로 할 수 없다.

NoteBase

㉣

사용자가 작성한 문서파일에는 **사람의 진술이 담길 수 있으므로**, 그 내용과 입증 목적을 살펴 전문증거 해당 여부를 확인해야 한다.

형사소송법 제310조의2(전문증거와 증거능력의 제한) 제311조 내지 제316조에 규정한 것 이외에는 공판준비 또는 공판기일에서의 진술에 대신하여 진술을 기재한 서류나 공판준비 또는 공판기일 외에서의 타인의 진술을 내용으로 하는 진술은 이를 증거로 할 수 없다.

형사소송법 제313조(진술서등)
①전2조의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자 · 사진 · 영상 등의 정보로서 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함한다. 이하 이 조에서 같다)은 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다. 단, 피고인의 진술을 기재한 서류는 공판준비 또는 공판기일에서의 그 작성자의 진술에 의하여 그 성립의 진정함이 증명되고 그 진술이 특히 신빙할 수 있는 상태하에서 행하여 진 때에 한하여 피고인의 공판준비 또는 공판기일에서의 진술에 불구하고 증거로 할 수 있다. <개정 2016.5.29>

㉤

송·수신된 이메일 내용에는 **발신자가 작성한 진술이 담길 수 있으므로**, 그 내용과 입증 목적을 살펴 전문증거 해당 여부를 확인해야 한다.

형사소송법 제310조의2(전문증거와 증거능력의 제한) 제311조 내지 제316조에 규정한 것 이외에는 공판준비 또는 공판기일에서의 진술에 대신하여 진술을 기재한 서류나 공판준비 또는 공판기일 외에서의 타인의 진술을 내용으로 하는 진술은 이를 증거로 할 수 없다.

형사소송법 제313조(진술서등)
①전2조의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자 · 사진 · 영상 등의 정보로서 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함한다. 이하 이 조에서 같다)은 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다. 단, 피고인의 진술을 기재한 서류는 공판준비 또는 공판기일에서의 그 작성자의 진술에 의하여 그 성립의 진정함이 증명되고 그 진술이 특히 신빙할 수 있는 상태하에서 행하여 진 때에 한하여 피고인의 공판준비 또는 공판기일에서의 진술에 불구하고 증거로 할 수 있다. <개정 2016.5.29>

NoteBase

ⓞ

방화벽 로그는 네트워크 통신의 허용·차단 내역 등을 **방화벽이 자동으로 기록한 비진술증거**이다. 사람의 진술을 담은 자료가 아니므로 전문법칙의 적용 대상이 아니다.

형사소송법 제310조의2(전문증거와 증거능력의 제한) 제311조 내지 제316조에 규정한 것 이외에는 공판준비 또는 공판기일에서의 진술에 대신하여 진술을 기재한 서류나 공판준비 또는 공판기일 외에서의 타인의 진술을 내용으로 하는 진술은 이를 증거로 할 수 없다.

NoteBase

**문 10. 하나의 클러스터보다 작은 데이터가 저장될 때 클러스터 일부만 사용되고 나머지 공간은 사용되지 않는다. 이 공간을 분석하는 기술로 가장 적절한 것은?**

① 윈도우(windows) 레지스트리 분석

② 타임라인(timeline) 분석

③ 슬랙(slack) 분석

④ 파일 시그니처(signature) 분석

**정답 3번**

**간단한 해설**

파일에 할당된 클러스터에서 실제 파일 내용 뒤에 남는 영역은 **파일 슬랙**이다. 따라서 이를 조사하는 기술은 ③ **슬랙 분석**이다.

**핵심 풀이**

파일에 할당된 마지막 클러스터에서 **파일의 실제 데이터가 끝난 뒤 남는 영역**이 파일 슬랙이다. 문항처럼 한 클러스터보다 작은 파일을 저장하여 일부 공간이 남는 경우가 이에 해당하므로, 정답은 ③ **슬랙 분석**이다.

예를 들어 4,096바이트 클러스터에 1,000바이트 파일을 저장하면, 단순한 클러스터 할당 모형에서 남는 3,096바이트가 파일 슬랙이다. **파일에 할당되었지만 현재 파일의 내용으로 사용하지 않는 공간**이라는 점에서, 어떤 파일에도 할당되지 않은 미할당 영역과 구별한다.

슬랙에 이전 자료의 잔존 내용이 남아 있다면 분석 단서로 활용할 수 있으나, 덮어쓰기나 초기화 여부에 따라 흔적이 없을 수도 있다. **레지스트리 분석**은 시스템·사용자 설정 등의 흔적, **타임라인 분석**은 사건의 시간적 흐름, **파일 시그니처 분석**은 파일 내부 식별 패턴을 조사하므로, 제시된 공간 자체를 가리키는 용어는 슬랙이다.

NoteBase

**문 11. 다음 설명 중 ㉠과 ㉡에 해당하는 모바일포렌식 용어가 올바르게 짝지어진 것은?**

최근 가장 중요한 수사 분야인 모바일포렌식에서는 ㉠스마트폰 단말기 고유정보와 ㉡가입자 고유정보를 파악할 수 있는 15자리로 구성된 2가지 모듈을 사용한다.

① ㉠ IMEI ㉡ MEID

② ㉠ IMEI ㉡ IMSI

③ ㉠ IDEN ㉡ IMSI

④ ㉠ MCC ㉡ ICCID

**정답 2번**

**간단한 해설**

**IMEI는 단말 장비**를, **IMSI는 이동통신 가입자**를 식별한다. 장비 식별번호와 가입자 식별번호의 역할을 구분하면 된다.

**대응 관계 해설**

㉠ 단말기 고유정보: **IMEI**(International Mobile Equipment Identity)는 이동통신 단말 장비를 식별하는 번호이다. 일반적으로 표시되는 15자리 IMEI는 기기 유형 할당 코드, 일련번호, 검사 숫자로 구성되며 가입자 식별번호와는 역할이 다르다.

㉡ 가입자 고유정보: **IMSI**(International Mobile Subscriber Identity)는 이동통신 가입을 식별하는 번호로, MCC(국가 코드), MNC(망 코드), MSIN(가입자 식별 부분)으로 구성된다. 단말기 장비 자체를 식별하는 IMEI와 구별한다.

제시문의 “15자리로 구성된 2가지 모듈”은 용어와 길이를 단순화한 표현이다. IMEI와 IMSI는 모듈 자체가 아니라 **식별번호**이며, 표준상 IMSI의 길이는 반드시 15자리가 아니라 **최대 15자리**이다. 이 표현상의 부정확함과 별개로 단말기와 가입자라는 핵심 식별 대상의 대응은 명확하다.

따라서 ㉠ IMEI와 ㉡ IMSI를 연결한 ②가 해당한다.

NoteBase

**문 12. 네트워크 침해사고 관련 증거 확보방식 중 패킷 캡처에 활용되는 장비와 애플리케이션에 관한 설명으로 적절하지 않은 것은?**

① FTK imager : 네트워크 트래픽 캡처의 메모리 이미징을 수행한다.

② 네트워크 탭 : 손상된 호스트와 스위치를 인라인하여 패킷 캡처를 수행한다.

③ tcpdump : root 권한으로 실행되면서 네트워크 트래픽을 모니터링한다.

④ wireshark : GUI 기반 도구로 패킷 캡처와 분석을 수행한다.

**정답 1번**

**간단한 해설**

FTK Imager의 메모리 수집은 **시스템 RAM의 덤프**이며 네트워크 패킷 캡처가 아니다. 패킷 수집·분석은 tcpdump나 Wireshark 같은 도구의 역할이다.

**선지별 해설**

① X: FTK Imager는 저장매체의 포렌식 이미지를 만들고 시스템의 **물리 메모리를 덤프**하는 도구이다. 메모리 수집 기능을 네트워크 인터페이스의 패킷 캡처 기능으로 볼 수 없다. 네트워크 트래픽을 수집하려면 tcpdump나 Wireshark 같은 패킷 캡처 도구를 사용한다.

② O: 네트워크 탭은 조사 대상 호스트와 스위치 사이의 통신 구간에 인라인으로 설치하여 지나가는 트래픽의 복사본을 분석 장비에 제공한다. 호스트의 메모리를 복제하는 것이 아니라 **통신 링크의 패킷을 관찰**하는 장비이다.

③ O: tcpdump는 명령줄에서 네트워크 패킷을 캡처하고 필터링·출력하는 도구이다. 실시간 인터페이스 캡처에는 보통 root 또는 이에 해당하는 캡처 권한이 필요하다. 이미 저장된 캡처 파일을 읽는 작업까지 반드시 root여야 하는 것은 아니다.

④ O: Wireshark는 **GUI 기반 패킷 캡처·프로토콜 분석** 도구이다. 캡처한 패킷의 헤더와 계층별 필드를 해석하고 필터를 적용하여 통신 내용을 분석할 수 있다.

NoteBase

**문 13. 다음 윈도우포렌식에 관한 설명에서 ㉠과 ㉡에 해당하는 것으로 가장 적절한 것은?**

컴퓨터의 원본이미지가 삭제되어 복원하지 못한다고 하더라도 윈도우에서 미리보기를 선택하면 자동으로 생성되는 로딩속도가 빠른 ㉠소용량의 작은 미리보기용 이미지를 차선의 증거로 사용할 수 있다. 이 파일은 폴더 옵션에서 “보호된 운영체제 파일 숨기기” 항목의 체크 상태를 해제하여 볼 수 있으며, 이 파일의 존재를 통해 ㉡시스템에서 특정 시점에 원본 이미지가 존재하였다는 사실을 증명할 수 있다.

① ㉠ timeline ㉡ timeline cache
② ㉠ thumbnail ㉡ thumbnail cache
③ ㉠ metadata ㉡ metadata cache
④ ㉠ signature ㉡ signature cache

**정답 2번**

**간단한 해설**

**썸네일은 작은 미리보기 이미지이고, 썸네일 캐시는 이를 재사용하기 위해 저장한 자료**이다. 원본이 없어져도 남은 캐시가 조사 단서가 될 수 있다.

**빈칸별 해설**

㉠ thumbnail: **원본을 작게 나타낸 미리보기 이미지**를 말한다. 원본보다 적은 데이터로 내용을 빠르게 확인하는 데 쓰이며, 원본을 복원하지 못해도 남아 있는 썸네일이 시각적 단서가 될 수 있다. 사건의 시간 순서인 timeline, 자료의 속성 정보인 metadata, 식별용 패턴인 signature와 구별한다.

㉡ thumbnail cache: 생성한 썸네일을 다시 사용하도록 보관하는 **미리보기 이미지의 캐시**이다. 원본이 삭제된 뒤에도 캐시가 남으면 그 내용이 과거에 처리되었음을 뒷받침하는 단서가 될 수 있다. 다만 캐시만으로 원본의 정확한 존재 시점·저장 위치·행위자까지 항상 확정할 수는 없고, 관련 파일·기록과 함께 검증해야 한다. 캐시의 저장 방식과 파일 위치는 Windows 버전에 따라 다르며, 숨김 설정 해제만으로 캐시 내부 이미지가 일반 이미지처럼 바로 열리는 것도 아니다.

따라서 ㉠은 thumbnail, ㉡은 thumbnail cache이므로 정답은 ②이다.

NoteBase

**문 14. 디지털포렌식 도구에 관한 설명으로 가장 적절하지 않은 것은?**

① Autopsy는 Windows와 Linux 파일시스템 내용분석은 가능하나 Android의 파일시스템 내용분석은 불가능하다.

② Encase는 포렌식 소프트웨어가 갖추어야 할 증거 보존 및 분석 기능을 갖춘 강력한 포렌식 도구이다.

③ TCT는 UNIX 계열 시스템에서 수행되는 강력한 포렌식 도구로 확장된 기능은 TCTUtils에서 제공한다.

④ BlackLight는 Mac, Windows, Android와 iOS에 대한 포렌식 도구이다.

**정답 1번**

**간단한 해설**

Autopsy는 **Android 자료의 분석도 지원**한다. 확보된 파일시스템 덤프나 SQLite 파일 등을 분석할 수 있으므로 Android 분석 자체가 불가능하다는 설명은 틀리다.

**선지별 해설**

① X: Autopsy는 Windows·Linux 계열 자료뿐 아니라 **Android에서 확보한 파일시스템 덤프와 파일도 분석**할 수 있다. Android Analyzer는 SQLite 데이터베이스 등을 해석하여 문자 메시지, 통화 기록, 연락처 같은 정보를 추출한다. 다만 모든 기기·버전을 지원한다는 뜻은 아니며, 분석 기능과 기기에서 데이터를 직접 획득하는 기능은 구별해야 한다.

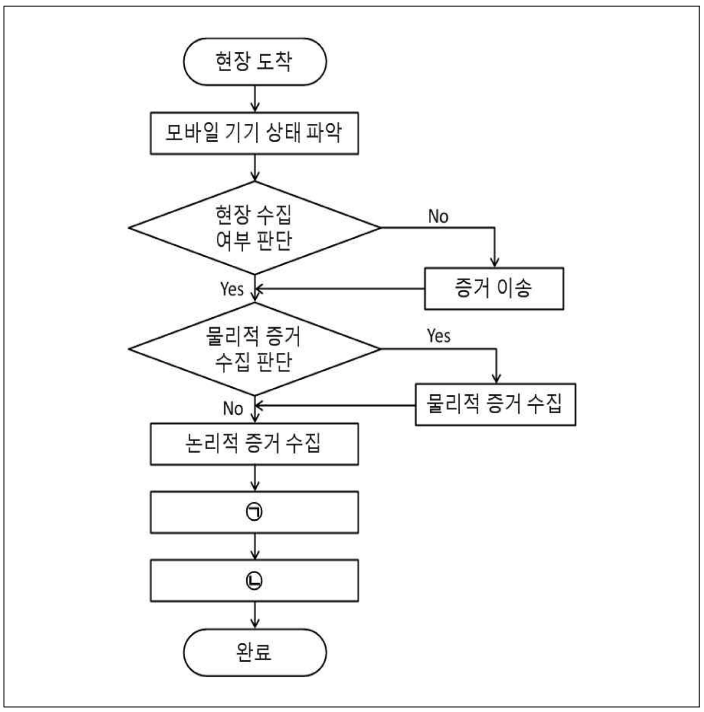
② O: EnCase는 디지털 증거를 수집·보존하고 검색·복구·분석하여 보고서로 정리하는 포렌식 도구이다. 증거 이미지 형식과 무결성 확인 기능을 통해 원본과 분석 자료의 동일성을 관리하는 데 활용된다.

③ O: TCT는 UNIX 계열 시스템의 자료 수집과 파일시스템 분석에 사용하는 도구 모음이다. TCTUtils는 TCT의 기능을 확장하여 파일·디렉터리 이름을 조사하고, 이름과 inode·데이터 블록 사이의 대응 관계를 분석하도록 돕는다.

④ O: BlackLight는 Mac과 Windows뿐 아니라 Android·iOS에서 확보한 자료도 분석하는 포렌식 도구이다. 컴퓨터의 파일·사용 흔적과 모바일 추출 자료의 메시지·응용프로그램 데이터 등을 함께 조사할 수 있다. 지원 범위는 자료 형식과 제품 버전에 따라 달라진다.

NoteBase

**문 15. 모바일 포렌식 절차에 관한 흐름도에서 ㉠과 ㉡에 들어갈 단계로 가장 적절한 것은?**




① ㉠ 분석 ㉡ 보존

② ㉠ 분석 ㉡ 검사

③ ㉠ 분석 ㉡ 보고서 작성

④ ㉠ 보존 ㉡ 보고서 작성

**정답 3번**

**간단한 해설**

수집한 증거의 의미를 **분석**한 뒤, 수행 방법과 판단 근거를 **보고서로 정리**해야 한다. 보존은 결과 작성 단계만의 활동이 아니라 취급 과정 전반에서 지켜야 한다.

NoteBase

**올바른 순서**

현장 도착 → 모바일 기기 상태 파악 → 현장 수집 여부 판단(현장 수집이 아니면 증거 이송) → 물리적 증거 수집 판단(필요하면 물리적 증거 수집) → 논리적 증거 수집 → ㉠ 분석 → ㉡ 보고서 작성 → 완료

현장 도착 후 기기의 상태를 확인하여 **현장에서 수집할지, 이송하여 수집할지** 결정한다. 그림의 No 경로는 증거 이송을 거친 뒤 수집 판단 단계로 합류한다. 이 과정에서도 증거 상태와 취급 이력을 보존해야 하며, 보존을 수집 후에 처음 시작하는 별도 최종 단계로 보지 않는다.

물리적 증거 수집 판단에서는 그림의 Yes 경로만 해당 수집 단계를 거치고, No 경로와 합류하여 논리적 증거 수집으로 이어진다. **그림의 분기 조건을 따라 필요한 자료를 확보**하는 부분이다. 모든 실제 모바일 조사에서 물리적·논리적 획득을 반드시 같은 순서로 수행한다는 일반 법칙을 뜻하지는 않는다.

㉠ 분석: 확보한 자료에서 사건 관련 정보를 찾아 관계와 의미를 해석한다. **수집된 자료를 근거로 판단**해야 하므로 흐름도에서는 수집 뒤에 놓인다. 자료를 추출·검사하는 작업과 의미를 해석하는 분석은 실제 과정에서 연계될 수 있다.

㉡ 보고서 작성: 사용한 방법, 확인한 자료, 분석 결과와 한계를 정리하여 다른 사람이 검토할 수 있게 한다. **분석 결과를 설명하는 보고서**이므로 분석 다음에 놓인다. 과정 기록은 처음부터 계속할 수 있지만, 그림의 마지막 단계는 결과를 종합하는 보고서 작성이다.

NoteBase

**문 16. 디지털 포렌식 이미지에 관한 설명 중 옳고 그름의 표시 (O, X)가 바르게 된 것은?**

㉠ 포렌식 이미지는 증거로부터 동일하게 이미지화한 데이터이다.
㉡ 포렌식 이미지는 이미지 파일 자체에 대한 이름, 크기, 타임스탬프 및 이미지 자체에 포함된 기타 정보 등을 포함한다.
㉢ 포렌식 이미지는 섹터 0부터 접근 가능한 마지막 섹터의 하드디스크 섹터를 복사하지 않고 파일을 복사한다.
㉣ 포렌식 이미지를 만들기 위하여 사용하는 가장 오래된 도구는 Windows에서 사용하는 dd 유틸리티이다.

① ㉠(O) ㉡(O) ㉢(X) ㉣(X)
② ㉠(X) ㉡(X) ㉢(O) ㉣(O)
③ ㉠(O) ㉡(X) ㉢(X) ㉣(O)
④ ㉠(O) ㉡(X) ㉢(O) ㉣(X)

**정답 1번**

**간단한 해설**

물리 디스크 이미징은 파일만 복사하는 것이 아니라 **접근 가능한 섹터를 비트 단위로 복제**한다. dd 역시 Windows 고유 도구가 아니라 유닉스 계열에서 비롯된 복사 유틸리티이다.

NoteBase

**보기별 해설**

㉠ O: 포렌식 이미지는 증거 매체의 내용을 분석·보존하기 위하여 복제한 데이터이다. 물리 이미징은 읽을 수 있는 원본 영역의 **비트 단위 내용**을 보존하는 방식이며, 획득 후 해시값 등을 비교하여 동일성을 확인한다.

㉡ O: 포렌식 이미지도 파일로 저장되므로 이미지 파일 자체의 이름·크기·타임스탬프 같은 메타데이터가 존재하고, 그 내부에는 획득한 증거 데이터와 형식에 따른 정보가 들어 있다. 다만 **이미지 파일 자체의 시간과 내부 원본 파일의 시간은 별개**이며, 생성된 이미지의 메타데이터가 원본의 메타데이터와 자동으로 같아지는 것은 아니다.

㉢ X: 일반적인 물리 디스크 이미징은 파일만 골라 복사하는 것이 아니라 **첫 섹터부터 마지막 접근 가능 섹터까지**를 복제한다. 따라서 할당되지 않은 영역이나 슬랙 등 파일 단위 복사에서 빠질 수 있는 데이터도 포함한다. 파일을 선택해 복사하는 논리적 획득과 구별된다.

㉣ X: dd는 본래 **유닉스 계열의 복사·변환 유틸리티**로, 장치 데이터를 복사하는 기능을 디스크 이미징에 활용할 수 있다. Windows 고유의 기본 유틸리티라고 설명하는 것은 맞지 않는다. Windows용 이식판이 있다는 사실과 도구의 기원은 구별해야 한다.

㉠·㉡은 O, ㉢·㉣은 X이므로 해당 배열은 ①이다.

NoteBase

**문 17. 컴퓨터에서 USB 사용 흔적과 프린터 출력 정보를 확인하고자 할 때 수집해야할 전자정보를 모두 고른 것은?**

㉠ 레지스트리
㉡ 쿠키(cookie) 정보
㉢ 웹 캐시(web cache)
㉣ $RECYCLE.BIN 폴더
㉤ 스풀(spool) 파일

① ㉠㉡
② ㉢㉣
③ ㉣㉤
④ ㉠㉤

**정답 4번**

**간단한 해설**

USB 장치 사용 흔적은 **레지스트리**에서, 프린터 출력 관련 데이터와 작업 정보는 **스풀 파일**에서 확인할 수 있다. 자료가 남아 있는지와 실제 행위의 의미는 다른 증거와 함께 검토해야 한다.

NoteBase

**보기별 해설**

㉠ 레지스트리: **USB 사용 흔적**의 대표적인 분석 대상이다. 예를 들어 SYSTEM 하이브의 USBSTOR 관련 정보에서 연결된 USB 저장장치의 식별 정보를 확인할 수 있다. 장치 연결 흔적만으로 특정 파일의 복사까지 곧바로 입증되는 것은 아니므로 다른 자료와 함께 해석한다.

㉡ 쿠키 정보: 웹사이트의 세션·설정 등 **웹 이용 상태**와 관련된다. USB 장치 연결이나 프린터 출력 정보를 직접 확인하기 위해 제시된 대표 자료에는 해당하지 않는다.

㉢ 웹 캐시: 웹에서 받은 응답이나 자원을 재사용하기 위해 저장하는 **웹 콘텐츠 자료**이다. 주된 분석 목적은 웹 이용 흔적이며, 문제에서 묻는 USB 연결·인쇄 작업의 대표 기록과 구별된다.

㉣ $RECYCLE.BIN 폴더: **휴지통으로 이동한 파일과 삭제 관련 정보**를 조사하는 대상이다. 특정 사건에서 보조 증거가 될 가능성은 있지만, 이 문제의 USB 사용 흔적과 프린터 출력 정보에 직접 대응하는 대표 자료는 아니다.

㉤ 스풀 파일: 인쇄 작업을 처리하기 위해 저장된 **출력 데이터와 작업 정보**를 조사하는 대상이다. 윈도우의 SPL·SHD 파일 등이 이에 해당한다. 정상 인쇄 후 삭제될 수 있으므로 항상 완전한 출력 기록이 남는다고 단정해서는 안 된다.

따라서 USB 사용 흔적과 프린터 출력 정보에 각각 대응하는 ㉠·㉤을 묶은 ④가 해당한다.

NoteBase

**문 18. 디지털 증거 압수·수색·검증 과정에서 별도의 범죄혐의와 관련된 전자정보(별건 정보)를 우연히 발견한 경우 취해야 할 조치에 관한 설명으로 가장 적절하지 않은 것은?**

① 별건 정보는 영장의 범위를 벗어나기 때문에 별건 범죄혐의와 관련된 추가 탐색은 중단하여야 한다.

② 적법한 탐색 과정에서 별건 정보를 발견한 경우에는 별도의 압수·수색·검증영장 없이 별건 정보를 압수할 수 있다.

③ 영장에 기재된 범죄 혐의사실과 관련된 전자정보 탐색은 진행할 수 있다.

④ 별건 정보에 대한 압수·수색절차에서도 피압수자에게 참여권을 보장하고 압수목록을 교부하여야 한다.

**정답 2번**

①

별건 정보는 기존 영장의 대상에 포함되지 않으므로, 이를 우연히 발견하면 **별건 범죄혐의에 관한 추가 탐색을 중단**하여야 한다. 별건 정보의 압수·수색에는 별도의 영장이 필요하다.

가. 전자정보에 대한 압수·수색에 있어 그 저장매체 자체를 외부로 반출하거나 하드카피·이미징 등의 형태로 복제본을 만들어 외부에서 그 저장매체나 복제본에 대하여 압수·수색이 허용되는 예외적인 경우에도 혐의사실과 관련된 전자정보 이외에 이와 무관한 전자정보를 탐색·복제·출력하는 것은 원칙적으로 위법한 압수·수색에 해당하므로 허용될 수 없다. 그러나 전자정보에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관으로서는 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여도 적법하게 압수·수색을 할 수 있다고 할 것이다. (대법원 2015. 7. 16.자 2011모1839 전원합의체 결정)

②

적법한 탐색 중 우연히 발견한 별건 정보라도 **별도 범죄혐의에 대한 압수·수색영장을 발부받아야** 적법하게 압수할 수 있다. 우연한 발견만으로 기존 영장의 범위가 확대되지는 않는다.

그러나 전자정보에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관으로서는 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여도 적법하게 압수·수색을 할 수 있다고 할 것이다. (대법원 2015. 7. 16.자 2011모1839 전원합의체 결정)

NoteBase

③

중단하여야 하는 것은 기존 영장의 범위를 벗어난 별건 정보의 추가 탐색이다. **기존 영장에 기재된 범죄혐의와 관련된 전자정보의 탐색은 그 영장의 범위 안에서 계속**할 수 있다.

가. 전자정보에 대한 압수·수색에 있어 그 저장매체 자체를 외부로 반출하거나 하드카피·이미징 등의 형태로 복제본을 만들어 외부에서 그 저장매체나 복제본에 대하여 압수·수색이 허용되는 예외적인 경우에도 혐의사실과 관련된 전자정보 이외에 이와 무관한 전자정보를 탐색·복제·출력하는 것은 원칙적으로 위법한 압수·수색에 해당하므로 허용될 수 없다. 그러나 전자정보에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관으로서는 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여도 적법하게 압수·수색을 할 수 있다고 할 것이다. (대법원 2015. 7. 16.자 2011모1839 전원합의체 결정)

④

별건 정보에 대한 압수·수색은 최초 압수·수색과 구별되는 별개의 절차이다. 따라서 특별한 사정이 없는 한 **피압수자에게 참여권을 보장하고 압수한 전자정보 목록을 교부**하여야 한다.

그러나 전자정보에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관으로서는 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여도 적법하게 압수·수색을 할 수 있다고 할 것이다.
나아가 이러한 경우에도 별도의 압수·수색 절차는 최초의 압수·수색 절차와 구별되는 별개의 절차이고, 별도 범죄혐의와 관련된 전자정보는 최초의 압수·수색영장에 의한 압수·수색의 대상이 아니어서 저장매체의 원래 소재지에서 별도의 압수·수색영장에 기해 압수·수색을 진행하는 경우와 마찬가지로 피압수자는 최초의 압수·수색 이전부터 해당 전자정보를 관리하고 있던 자라 할 것이므로, 특별한 사정이 없는 한 그 피압수자에게 형사소송법 제219조, 제121조, 제129조에 따라 참여권을 보장하고 압수한 전자정보 목록을 교부하는 등 피압수자의 이익을 보호하기 위한 적절한 조치가 이루어져야 할 것이다. (대법원 2015. 7. 16.자 2011모1839 전원합의체 결정)

NoteBase

**문 19. 다음 사례에 대한 증거수집 및 분석방법으로 가장 적절하지 않은 것은?**

A는 서울역 지하철에서 스마트폰으로 타인의 신체를 몰래 사진 촬영한 후, 자신의 컴퓨터에 저장하였다. A는 컴퓨터에 저장된 해당 사진파일을 인터넷 커뮤니티 사이트에 올리고 확장자명을 hwp로 변경·저장하였다. 사법경찰관 P는 A를 성폭력범죄의 처벌등에관한특례법 위반죄로 수사하면서 A의 컴퓨터에서 사진 파일을 찾고 범죄사실을 증명하고자 한다.

① 해시(hash) 분석을 통해 인터넷 커뮤니티 사이트에 올려진 사진 파일의 해시값과 동일한 파일을 찾는다.

② 시그니처(signature) 분석을 통해 확장자명이 변경된 파일을 찾는다.

③ 웹 브라우저에서 히스토리 정보를 통해 웹 사이트의 접속날짜, 시간, URL 등을 확인한다.

④ 메인 메모리(main memory) 분석을 통해 썸네일(thumbnail)과 삭제된 파일을 분석하고, IP기록을 확인한다.

**정답 4번**

**간단한 해설**

저장된 사진과 삭제 흔적, 썸네일을 찾는 기본 분석 대상은 **디스크의 파일·파일시스템·캐시**이다. 메인 메모리는 실행 중인 상태와 일시적으로 남은 정보를 보완적으로 조사하는 자료이므로, 이러한 저장 흔적의 일반적인 분석 대상으로 설명하는 것은 가장 적절하지 않다.

NoteBase

**선지별 해설**

① O: 파일 내용으로 계산한 해시값을 비교하면 같은 내용을 가진 파일의 후보를 찾을 수 있다. 사례처럼 **확장자명만 hwp로 바꾼 경우 파일 내용의 해시는 바뀌지 않으므로** 게시된 사진과 비교하는 방법이 유효하다. 다만 사이트가 사진을 재압축하거나 변환했다면 해시값이 달라질 수 있어 원본 확보 여부를 함께 확인한다.

② O: 파일 시그니처는 파일 내부의 특정 바이트 패턴으로 형식을 식별하는 단서이다. 이름의 확장자가 hwp여도 내부에는 원래 이미지 형식의 특징이 남으므로, 확장자와 실제 형식의 불일치를 찾아 위장한 사진 파일을 선별할 수 있다.

③ O: 브라우저의 방문 기록에는 접속한 URL과 방문 시각 등이 저장될 수 있다. 해당 커뮤니티의 주소와 접근 시점을 확인하여 사진 게시 전후의 활동을 재구성하는 데 활용한다. 방문 기록만으로 사진 업로드 자체가 확정되는 것은 아니므로 파일·게시물 등 다른 증거와 대조한다.

④ X: 사례의 저장된 사진과 삭제 흔적을 찾으려면 디스크의 파일시스템·미할당 영역, 썸네일 캐시 및 브라우저·네트워크 기록 등을 우선 분석하는 것이 적절하다. 이를 일반적으로 **메인 메모리 분석의 대상으로 묶은 점**이 적절하지 않다. 메모리에서는 실행 중인 프로세스와 네트워크 연결, 캐시된 파일 조각 등이 발견될 수 있으므로 사진 조각이나 IP 관련 정보의 발견 자체가 불가능한 것은 아니다. 다만 휘발성·잔존 상태에 좌우되는 이런 자료를 저장장치에 남은 파일과 과거 기록의 통상적인 분석 대상으로 대신할 수는 없다.

NoteBase

**문 20. 다음 사례에 관한 설명으로 가장 적절하지 않은 것은?**

인천 국제공항 테러를 목적으로 A와 B는 X회사에서 서비스하는 컴퓨터 메신저를 통해 범행을 실시간으로 모의하고 있다. 사법경찰관 P는 이와 같은 첩보를 입수하고 A와 B의 메신저 아이디를 확인한 후, 관련 증거를 수집하고자 한다.

① A와 B의 대화 내용을 네트워크상에서 실시간 수집·확인하기 위해서는 압수·수색·검증영장을 발부 받아야 한다.
② 와이어샤크(wireshark) 포렌식 도구를 이용하여 패킷을 수집·분석할 수 있다.
③ 법원의 허가를 받아 A와 B의 통신사실 확인자료를 전기통신사업자에게 요청할 수 있다.
④ IP 패킷 헤더를 통해 A와 B가 사용하고 있는 IP 주소를 파악할 수 있다.

**정답 1번**

①

메신저 대화 내용을 네트워크에서 실시간으로 수집·확인하는 것은 **전기통신의 감청**에 해당한다. 이를 위한 절차는 압수·수색·검증영장 발부가 아니라 원칙적으로 **법원의 통신제한조치 허가**이다.

통신비밀보호법 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2001.12.29, 2004.1.29, 2005.1.27>
7. "감청"이라 함은 전기통신에 대하여 당사자의 동의없이 전자장치 · 기계장치등을 사용하여 통신의 음향 · 문언 · 부호 · 영상을 청취 · 공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송 · 수신을 방해하는 것을 말한다.

통신비밀보호법 제6조(범죄수사를 위한 통신제한조치의 허가절차)
③ 사법경찰관(군사법경찰관을 포함한다. 이하 같다)은 제5조제1항의 요건이 구비된 경우에는 검사(군검사를 포함한다. 이하 같다)에 대하여 각 피의자별 또는 각 피내사자별로 통신제한조치에 대한 허가를 신청하고, 검사는 법원에 대하여 그 허가를 청구할 수 있다. <개정 2026.9.29>
⑤법원은 청구가 이유 있다고 인정하는 경우에는 각 피의자별 또는 각 피내사자별로 통신제한조치를 허가하고, 이를 증명하는 서류(이하 "허가서"라 한다)를 청구인에게 발부한다. <개정 2001.12.29>

②

와이어샤크는 네트워크 인터페이스에서 **패킷을 실시간으로 수집하고 프로토콜별 구조와 내용을 분석**할 수 있는 도구이다.

NoteBase

③

사법경찰관은 수사에 필요한 경우 **관할 지방법원 또는 지원의 허가를 받아 전기통신사업자에게 통신사실 확인자료의 열람·제출을 요청**할 수 있다. 허가를 받기 위한 서면에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 적는다.

통신비밀보호법 제13조(범죄수사 등을 위한 통신사실 확인자료제공의 절차)
①수사처검사등 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자(이하 "전기통신사업자"라 한다)에게 통신사실 확인자료의 열람이나 제출(이하 "통신사실 확인자료제공"이라 한다)을 요청할 수 있다. <개정 2026.9.29>
④제1항부터 제3항까지에 따라 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체 없이 그 허가를 받아 전기통신사업자에게 송부하여야 한다. <개정 2005.5.26, 2019.12.31, 2021.9.24, 2026.9.29>

④

IP 패킷 헤더에는 **출발지 IP 주소와 목적지 IP 주소**가 포함된다. A와 B가 각각 송수신한 관련 패킷을 분석하면 이들이 사용한 IP 주소를 파악할 수 있다.

NoteBase