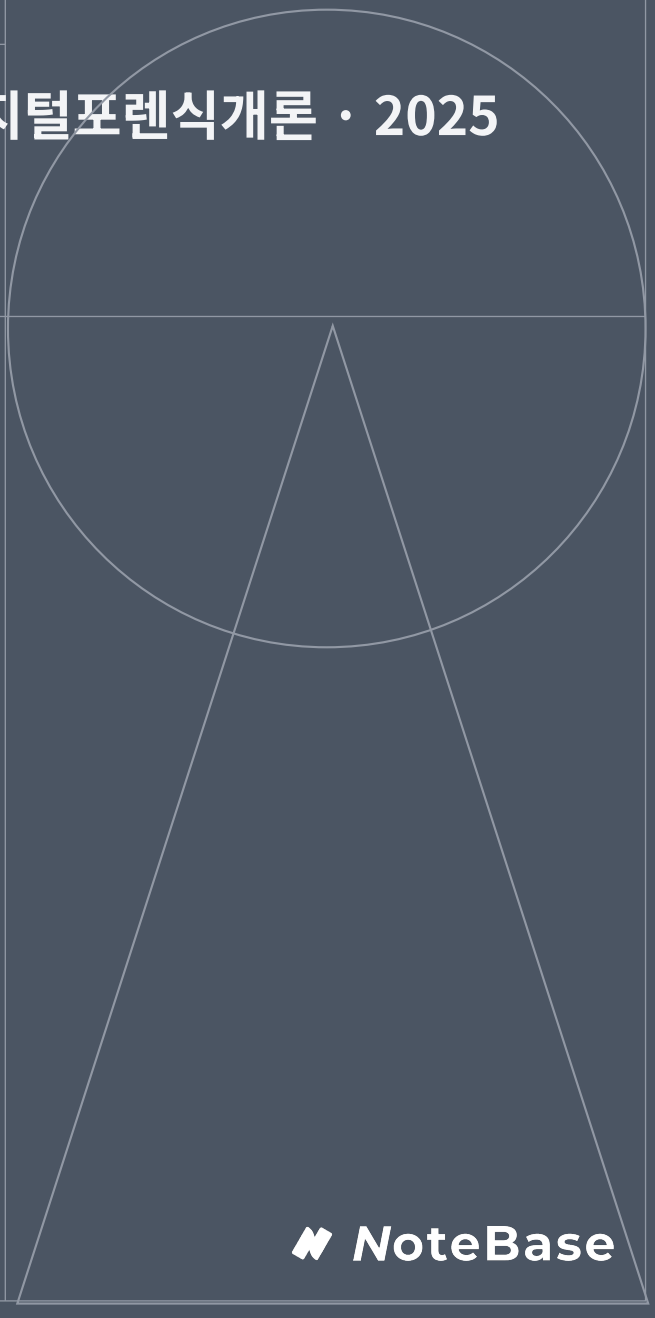
기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2025



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2025

공무원/경찰/경력채용 · 디지털포렌식개론 · 2025

문 1. 디지털 데이터 복제나 이미징에 관한 설명으로 가장 적절한 것은?

① 증거 손상 가능성 방지를 위해 물리적 쓰기 방지 장치를 연결한다.

② 복제하고자 하는 저장장치의 용량보다는 작은 용량으로 복제하는 것이 원칙이다.

③ 소프트웨어를 사용한 이미징은 수행할 수 없다.

④ 다양한 기능을 제공하는 통합포렌식 도구로 이미징 작업을 하여서는 아니 된다.

정답 1번

간단한 해설

복제·이미징에서는 **원본 변경을 막고 수집 결과의 무결성을 검증**하는 것이 중요하다. 물리적 쓰기 방지 장치는 원본에 대한 쓰기 요청을 차단하는 수단이다.

선지별 해설

① O: 물리적 쓰기 방지 장치는 원본 저장매체로 전달되는 **쓰기 요청을 차단하여 내용 변경을 방지**한다.
복제·이미징 과정에서 증거의 무결성을 보호하는 적절한 방법이다. 다만 장치의 호환성과 작동 상태를 확인해야 하며, 모든 물리적 고장까지 방지하는 장비라는 뜻은 아니다.

② X: 전체 저장장치를 복제하려면 **수집할 데이터를 온전히 담을 수 있는 용량**을 확보해야 한다. 디스크 간 비트 단위 복제라면 대상 디스크는 원본의 복제 범위를 수용해야 한다. 이미지 파일은 압축 등에 따라 작아질 수 있지만, 원본보다 작은 용량으로 만드는 것이 원칙인 것은 아니다.

③ X: 이미징은 **소프트웨어로도 수행**할 수 있다. 검증된 이미징 도구로 원본 데이터를 읽어 이미지 파일을 만들고, 해시값 비교 등으로 결과를 검증할 수 있다. 하드웨어 장비만 허용되는 작업이 아니다.

④ X: 이미징 기능이 있는 **통합 포렌식 도구도 사용할 수 있다**. 기능이 다양하다는 이유로 배제하지 않고, 해당 도구와 설정이 수집 목적에 적합한지, 원본 변경을 방지하는지, 결과의 완전성·무결성을 검증할 수 있는지를 확인해야 한다.

NoteBase

문 2. 다음 (㉠)에 들어갈 용어로 가장 적절한 것은?

(㉠)는 윈도우 운영체제에서 USB 장치와 관련된 기록을 저장하는 핵심 영역으로, 이 정보를 분석하여 USB 사용 이력을 파악할 수 있다.

① SECURITY 하이브
② SOFTWARE 하이브
③ DEFAULT 하이브
④ SYSTEM 하이브

정답 4번

간단한 해설

USB·USBSTOR 등 장치 열거 정보는 **SYSTEM 하이브의 제어 집합**에 남는다. 이를 분석하면 연결된 USB 장치의 식별 정보와 사용 흔적을 확인할 수 있다.

빈칸별 해설

㉠은 SYSTEM 하이브이다. 이 하이브에는 운영체제의 제어 집합과 하드웨어·드라이버 관련 설정이 저장된다. 제어 집합의 Enum 아래에 있는 USB·USBSTOR 관련 키 등에서 **USB 장치의 식별 정보와 연결 흔적**을 조사할 수 있어 USB 사용 이력 분석의 핵심 자료가 된다. 오프라인 하이브에서는 Select 정보로 사용할 ControlSet을 확인하여 해석한다.

SECURITY는 보안 정책 등에, SOFTWARE는 설치된 소프트웨어와 운영체제 설정 등에 관련된다. DEFAULT는 로그온 전 환경 등에 쓰이는 사용자 설정 하이브이다. USB 장치 열거 정보를 저장하는 중심 하이브라는 단서에는 SYSTEM이 가장 적합하다. USB 흔적이 다른 하이브나 로그에도 남을 수 있으므로 SYSTEM만으로 모든 사용 행위를 확정한다는 뜻은 아니다.

따라서 ㉠에 들어갈 용어는 ④ SYSTEM 하이브이다.

NoteBase

문 3. 디지털 증거의 조사가 필요한 상황이라고 판단하기에 가장 적절하지 않은 것은?

① 경찰 조사를 받는 피혐의자가 사건관련 정보의 은닉을 목적으로 스마트폰에 저장된 내용을 삭제하였다.

② 택시기사가 손님이 택시에 두고 간 것으로 확인된 블루투스 이어폰을 오프라인에서 타인에게 판매하였다.

③ 미성년자 성폭행 피혐의자가 공범과 모바일 메신저를 통해 대화를 주고 받았다.

④ 타인의 정보를 이용해 웹사이트에 가입하여 인터넷상에서 활동하였다.

정답 2번

간단한 해설

①·③·④에는 사건과 연결된 전자정보의 삭제·통신·온라인 활동이 직접 제시되어 있다. ②는 **오프라인 물품 처분만 제시**되어 디지털 조사의 필요성을 판단할 직접 단서가 상대적으로 약하다. 디지털 증거가 절대 없다는 뜻은 아니다.

선지별 해설

① (O) 사건 관련 정보를 숨기기 위해 스마트폰 내용을 삭제했다면, **삭제된 자료의 잔존 흔적과 삭제 경위**를 확인할 필요가 있다. 기기·앱·백업 등에 남은 자료가 조사 대상이 될 수 있지만, 삭제된 내용이 언제나 복구된다는 뜻은 아니다.

② (X) 제시된 사실은 분실된 이어폰을 **오프라인에서 처분한 행위**이며, 다른 선지처럼 사건 관련 전자정보의 삭제·통신·온라인 활동이 직접 제시되어 있지 않다. 따라서 주어진 사정만으로 디지털 증거 조사의 필요성을 판단하기에는 상대적으로 가장 약하다. 이어폰이라는 이유만으로 디지털 흔적이 없다는 뜻은 아니며, 연결 이력이나 영상·결제기록 등이 사건과 관련되면 디지털 조사도 필요할 수 있다.

③ (O) 공범과 주고받은 모바일 메신저 대화는 **대화 내용·시각·상대방 및 행위자 사이의 관계**를 확인할 수 있는 디지털 자료이다. 단말기나 관련 저장소에 남은 기록을 조사할 직접적인 이유가 제시되어 있다.

④ (O) 타인의 정보를 사용한 가입과 온라인 활동은 **계정 가입정보·접속기록·활동 내역**을 통해 경위를 확인할 필요가 있는 상황이다. 다만 특정 계정이나 IP주소의 기록만으로 실제 행위자가 곧바로 확정되는 것은 아니므로 다른 자료와 함께 검토한다.

NoteBase

문 4. 다음 (㉠)에 들어갈 용어로 가장 적절한 것은?

(㉠)은(는) 운영체제 또는 응용프로그램이 자신이 생성한 파일임을 인식할 수 있도록 파일의 특정 위치에 고정하여 표시하는 파일 고유정보이다.

① 레지스트리(Registry)
② 시그니처(Signature)
③ MBR(Master Boot Record)
④ 파일 시스템(File System)

정답 2번

간단한 해설

파일의 정해진 위치에 기록되어 형식을 식별하게 하는 특징적인 바이트 패턴을 **파일 시그니처**라고 한다. 개별 파일마다 다른 값이 아니라 같은 형식의 파일들이 공유할 수 있는 정보이다.

빈칸별 해설

㉠ 시그니처(Signature): 파일 형식을 식별하는 데 사용하는 특징적인 바이트 패턴이다. 파일의 헤더 등 형식에서 정한 위치에 나타나므로, 지문의 '특정 위치에 고정하여 표시하는 정보'라는 단서와 연결된다. 확장자가 바뀌어도 내부 패턴을 검사하여 실제 형식을 추정할 수 있다.

여기서 '파일 고유정보'는 개별 파일 하나만을 구별하는 값이라는 뜻이 아니다. **같은 형식의 여러 파일이 같은 시그니처를 공유**할 수 있다. 또한 시그니처만으로 파일을 만든 프로그램이나 파일 전체의 무결성을 확정하지는 못한다.

레지스트리는 Windows의 구성 정보를 담는 데이터베이스이고, MBR은 전통적인 디스크의 부팅 정보와 파티션 정보를 담는 영역이다. 파일시스템은 파일의 저장·배치·관리 구조이므로, 파일 내부의 형식 식별 패턴을 가리키는 말과 구별된다.

따라서 ㉠에 들어갈 용어는 ② 시그니처이다.

NoteBase

문 5. 다음과 같은 상황일 경우, 범죄혐의를 입증할 수 있는 정보로 가장 적절한 것은?

버스에서 다른 사람의 신체를 촬영한 피혐의자를 체포한 후, 압수한 스마트폰에서 관련 사진이 저장된 것을 발견하였으나 피혐의자는 인터넷에서 다운받은 것이라 부인하고 있다.

① 스마트폰의 H/W 정보
② 스마트폰의 운영체제 버전
③ 사진 파일의 확장자
④ 사진 파일의 메타데이터

정답 4번

간단한 해설

사진의 촬영 일시·기기·위치 등 메타데이터를 사건 및 압수 기기의 정보와 대조하면 생성 경위를 조사할 수 있다. 다만 메타데이터만으로 촬영자를 단정하지는 않는다.

핵심 풀이

쟁점은 사진이 **해당 스마트폰으로 촬영된 것인지, 외부에서 내려받은 것인지**를 가리는 것이다. 사진 파일 자체에 남은 촬영·생성 관련 정보가 다른 선택지보다 직접적인 조사 단서를 제공한다.

사진의 **메타데이터**에는 형식과 기기 설정에 따라 촬영 일시, 촬영 기기 제조사·모델, 위치 정보 등이 포함될 수 있다. 이를 압수 기기의 정보, 사건 발생 시간·장소, 다운로드·앱 기록 등과 대조하면 사진의 생성 경위를 판단하는 데 도움이 된다.

스마트폰의 H/W 정보와 운영체제 버전은 기기의 특성을 알려 주지만 해당 사진을 실제로 촬영했다는 사실을 곧바로 보여 주지는 않는다. 사진 파일의 확장자도 파일 형식을 나타내는 이름의 일부일 뿐, 촬영인지 다운로드인지 구별하는 결정적 정보가 아니다.

메타데이터는 누락·변경될 수 있고, 내려받은 사진에도 원래의 촬영 정보가 남을 수 있다. 따라서 메타데이터 하나만으로 행위자를 단정하지 않고 다른 흔적과 종합해야 한다. 제시된 선택지 중 가장 적절한 정보는 사진 파일의 메타데이터인 ④이다.

NoteBase

문 6. Thumbs.db 포렌식에 관한 설명으로 가장 적절하지 않은 것은?

① 이미지들을 모두 삭제해도 Thumbs.db 파일이 남아 있을 수 있다.

② Thumbs.db 파일은 윈도우 [파일 탐색기 옵션]이 기본값으로 설정되어 있어도 볼 수 있다.

③ Thumbs.db 파일은 이미지 파일이 포함된 폴더를 열어보는 순간 생성된다.

④ Thumbs.db 파일에는 동영상 파일의 미리보기 캐시가 저장될 수 있다.

정답 2번

간단한 해설

Thumbs.db는 일반적으로 **숨김 시스템 파일**이므로 기본 파일 탐색기 설정에서는 보이지 않는다. 원본을 삭제해도 별도로 저장된 썸네일 흔적은 남을 수 있다.

선지별 해설

① O. **원본 이미지 삭제와 캐시 삭제는 별개**이므로, 이미지를 모두 삭제해도 Thumbs.db 파일과 그 안의 미리보기 이미지가 남을 수 있다. 다만 캐시 정리나 파일 삭제 등으로 소실될 수도 있어 영구 보존을 의미하지 않는다.

② X. Thumbs.db는 일반적으로 **숨김 시스템 파일**이므로 기본 파일 탐색기 표시 설정에서는 보이지 않는다. 파일이 존재하는 것과 탐색기에 표시되는 것은 별개의 문제이다.

③ O(Thumbs.db를 사용하는 미리보기 환경을 전제로 한 설명). 해당 폴더의 이미지를 **썸네일로 표시·캐시하는 과정**에서 Thumbs.db가 생성될 수 있다는 취지이다. 그러나 폴더를 열기만 하면 언제나 즉시 생성된다는 보편 법칙은 아니다. 썸네일 설정·권한·윈도우 버전과 저장 위치에 따라 달라지며, 현대 윈도우의 로컬 미리보기에는 중앙화된 thumbcache 계열도 사용된다.

④ O. 지원되는 동영상에서 추출한 **대표 프레임의 미리보기**도 썸네일 캐시에 저장될 수 있다. 동영상 전체가 Thumbs.db에 복사된다는 뜻이 아니라, 내용을 대표하는 축소 이미지가 남을 수 있다는 의미이다.

따라서 기본 설정에서도 Thumbs.db를 볼 수 있다고 한 ②가 가장 적절하지 않다.

NoteBase

문 8. 윈도우 레지스트리 키를 설명한 정보로 가장 적절하지 않은 것은?

① 레지스트리에서 RunMRU라는 키는 최근 실행한 명령어 정보를 가지고 있다.

② 시작 프로그램과 관련된 레지스트리 키는 Run, RunOnce 등이 있다.

③ 컴퓨터 이름은 ActiveComputerName 키에서 확인할 수 있다.

④ 윈도우 레지스트리에서 키값을 단계적으로 확인할 경우, 하위 레벨에서 상위레벨 순으로 확인해야 한다.

정답 4번

간단한 해설

레지스트리 경로는 **상위 키에서 하위 키로** 이어지는 계층 구조이다. 하위 레벨부터 상위 레벨 순으로 확인해야 한다는 규칙은 없다.

선지별 해설

① O: RunMRU는 사용자가 Windows의 **'실행' 대화상자에서 실행한 명령**의 최근 사용 이력을 담는 키이다. 모든 프로그램 실행이나 명령 프롬프트의 모든 명령을 기록하는 키는 아니므로, 기록 대상의 범위를 구별해야 한다.

② O: Run과 RunOnce는 사용자 로그온 시 실행할 프로그램을 등록하는 데 쓰인다. **Run은 반복 실행, RunOnce는 일회 실행**을 위한 키이며, 시스템 전체 또는 사용자별 위치를 함께 확인한다.

③ O: ActiveComputerName 키의 ComputerName 값에서 **현재 사용 중인 컴퓨터 이름**을 확인할 수 있다. 이름 변경 후 재부팅 전에는 별도로 설정된 이름과 활성 이름이 다를 수 있으므로 실제 활성 이름을 구별하는 데 의미가 있다.

④ X: 레지스트리는 루트 키 아래에 하위 키와 값이 이어지는 계층 구조이다. 경로를 단계적으로 따라갈 때는 **상위 키에서 하위 키로** 내려가 대상 값을 찾는다. 분석 도구의 검색 기능 등을 사용할 수도 있으며, 하위에서 상위 순으로만 확인해야 한다는 의무적 순서는 없다.

NoteBase

문 9. 모바일 포렌식에서 데이터 수집 방법에 관한 설명으로 가장 적절하지 않은 것은?

① 물리적 수집 방법은 삭제된 데이터를 포함한 장치에 존재하는 모든 데이터를 얻을 수 있다.

② 데이터 수집은 모바일 장치와 주변 장치, 매체로부터 정보를 추출하는 과정을 의미한다.

③ 논리적 수집 방법을 통해 할당되지 않은 공간에 존재하는 데이터도 수집할 수 있다.

④ 모바일 폰 내부의 데이터는 SIM 카드, 메모리 등에서 수집한다.

정답 3번

간단한 해설

논리적 수집은 접근 가능한 파일 등 논리적 객체를 대상으로 한다. 삭제 흔적이 남아 있는 **미할당 영역까지 확보하려면 물리적 수집**과 구별해야 한다.

선지별 해설

① O: 물리적 수집은 저장매체를 낮은 수준에서 복사하여 할당 영역뿐 아니라 미할당 영역까지 확보하는 방식이다. 따라서 삭제된 파일의 내용이 아직 남아 있으면 함께 얻을 수 있다. 이는 전체 저장 영역을 수집 대상으로 한다는 뜻이며, 암호화·손상·덮어쓰기 등과 무관하게 모든 자료의 획득과 해독이 언제나 성공한다는 보장은 아니다.

② O: 데이터 수집은 모바일 장치와 관련 주변 장치·저장매체에서 분석에 필요한 정보를 추출하는 과정이다. 수집 대상과 방법을 정하고 자료를 확보한 뒤, 확보된 내용이 제대로 수집되었는지 확인해야 한다.

③ X: 논리적 수집은 운영체제나 제공 인터페이스를 통해 접근 가능한 파일·디렉터리 등 논리적 객체를 수집한다. **파일시스템의 미할당 영역까지 그대로 복사하는 것은 물리적 수집**의 범위이다. 할당된 데이터베이스 파일 안에 삭제 흔적이 남아 논리적으로 수집될 수는 있지만, 이것을 미할당 영역 수집과 혼동해서는 안 된다.

④ O: 모바일 데이터는 단말기 내부 메모리와 SIM 카드 등 여러 저장 위치에서 수집할 수 있다. 각 저장 위치에는 서로 다른 정보가 들어갈 수 있으므로, 단말기 본체와 SIM 카드 등을 구분하여 적절한 방법으로 조사한다.

NoteBase

문 10. 디지털 증거의 법적 증거 효력에 관한 설명으로 가장 적절하지 않은 것은?

① 디지털 증거 압수·수색 집행 현장에 피의자가 참여할 수 없는 경우, 피의자를 대신하여 변호인, 소지자 등 그 밖의 이해관계인을 참여시켜 영장 집행을 할 수 있다.

② 디지털 증거는 디지털 증거의 무결성, 신뢰성, 원본성 등이 기본적으로 보장되어야 한다.

③ 복제본을 이용한 증거 분석을 통해 디지털 증거의 무결성을 보호한다.

④ 피압수자 등과 함께 생성된 복제본에 대한 해시값을 확인할 필요는 없다.

정답 4번

①

피의자가 직접 참여하지 못하더라도 **변호인이나 소지자 등 적법한 참여인을 참여시켜 영장을 집행할 수 있다**.
타인의 주거 등에서는 주거주·간수자 또는 이에 준하는 사람을 참여시키고, 이들을 참여시키지 못하면 이웃 사람이나 지방공공단체 직원을 참여시킨다.

형사소송법 제121조(영장집행과 당사자의 참여) 검사, 피고인 또는 변호인은 압수 · 수색영장의 집행에 참여할 수 있다.

형사소송법 제123조(영장의 집행과 책임자의 참여)
② 제1항에 규정한 장소 외에 타인의 주거, 간수자 있는 가옥, 건조물(建造物), 항공기 또는 선박 · 차량 안에서 압수 · 수색영장을 집행할 때에는 주거주(住居主), 간수자 또는 이에 준하는 사람을 참여하게 하여야 한다.
③ 제2항의 사람을 참여하게 하지 못할 때에는 이웃 사람 또는 지방공공단체의 직원을 참여하게 하여야 한다.

형사소송법 제219조(준용규정) 제106조, 제107조, 제109조부터 제112조까지, 제114조, 제115조제1항 본문, 같은 조 제2항, 제118조부터 제132조까지, 제134조, 제135조, 제140조, 제141조, 제333조제2항 및 제486조는 사법경찰관의 본장의 규정에 의한 압수, 수색 또는 검증에 준용한다. 이 경우 사법경찰관이 제130조, 제132조 및 제134조에 따른 처분을 할 때에는 검사의 의견을 들어야 하고, 정당한 사유가 없으면 그 의견에 따라야 한다.

NoteBase

②

디지털 증거는 **수집 이후 내용이 변경되지 않았다는 무결성, 처리 도구·방법의 신뢰성, 원본과 제출된 자료의 동일성**이 보장되어야 한다. 원본성은 원본 매체 자체만 제출해야 한다는 뜻이 아니라, 복제본이라면 원본의 내용이 그대로 재현되었음을 입증해야 한다는 의미이다.

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)

③

원본을 직접 분석하면 데이터가 변경되거나 훼손될 수 있으므로, **원본은 보존하고 원본과 동일한 복제본을 만들어 분석**하여 원본 증거의 무결성을 보호한다.

NoteBase

④

원칙적으로 **피압수자 등이 원본과 복제본의 해시값이 동일함을 확인하고 서명한 서면**으로 동일성·무결성을 증명한다. 따라서 해시값 확인을 불필요한 절차로 볼 수 없다. 다만 이러한 증명이 불가능하거나 현저히 곤란하면 참여 수사관·전문가의 증언이나 법원의 원본 대조 등으로도 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)

NoteBase

문 11. 다음 중 쉽게 복구가 가능한 데이터로 가장 적절한 것은?

① 완전 삭제 프로그램을 사용하여 삭제한 데이터

② 데이터를 삭제한 후 대용량 파일을 디스크 전체에 덮어쓰는 방식으로 삭제한 데이터

③ 키보드의 Del(Delete) 버튼으로 삭제하여 휴지통으로 이동시킨 데이터

④ 강력한 자석을 사용하여 하드디스크 드라이브(HDD)에서 삭제한 데이터

정답 3번

간단한 해설

휴지통으로 이동한 파일은 내용이 그대로 보존되어 복원할 수 있다. 실제 덮어쓰기나 자기 기록 훼손과 구별하면 된다.

핵심 풀이

핵심은 **파일 내용이 보존된 채 휴지통으로 이동한 경우**와 저장된 내용을 덮어쓰거나 자기 기록을 훼손한 경우를 구별하는 것이다. 휴지통에 실제로 남아 있는 파일은 일반적인 복원 기능으로 원래 위치에 되돌릴 수 있어 쉽게 복구할 수 있다.

완전 삭제 프로그램이 대상 매체에 적합한 방식으로 정상 작동했다면 통상적인 복구가 어렵다. 삭제 후 원래 데이터 영역을 실제로 덮어쓴 경우에도 그 영역의 이전 내용을 쉽게 복구할 수 없다. 다만 프로그램 이름만으로 완전 삭제 성공이 보장되는 것은 아니며, 매체 특성과 수행·검증 결과에 따라 잔존 여부가 달라진다.

HDD를 충분한 자기장으로 적절히 소자하여 기록을 훼손한 경우도 휴지통 이동처럼 간단히 복원할 수 있는 상황이 아니다. 단순히 자석을 가까이 대는 것만으로 모든 HDD 데이터가 확실히 삭제된다고 일반화해서는 안 된다.

제시문은 Del 키를 누른 뒤 파일이 **실제로 휴지통으로 이동한 상태**를 명시한다. 따라서 휴지통을 비우거나 다른 손상이 생기지 않았다는 해당 상황에서 가장 쉽게 복구할 수 있는 것은 ③이다.

NoteBase

문 12. 모바일 포렌식 조사 기록 작성에 포함되는 정보로 가장 적절하지 않은 것은?

① 증거를 수집하기 위해 사용되는 포렌식 도구

② 통신사 가입 대리점 및 판매사원 정보

③ 가입자 세부 사항과 통화내역 기록

④ 모바일 식별번호(ICCID, IMEI 등)

정답 2번

간단한 해설

모바일 조사 기록에는 **수집 도구, 관련 가입자·통화자료, 카드·단말기 식별번호** 등을 남긴다. 대리점과 판매사원 정보는 사건별로 추가할 수는 있지만 공통 핵심 항목은 아니므로 ②이다.

핵심 풀이

모바일 포렌식 조사 기록은 **분석 대상의 식별, 사용한 방법, 확인한 증거와 결과**를 추적할 수 있게 작성한다. 통신사 가입 대리점과 판매사원 정보는 이러한 기록의 공통적인 핵심 항목과 직접 연결되지 않으므로, 제시된 항목 중 가장 적절하지 않은 것은 ②이다.

사용한 **포렌식 도구와 버전·설정**은 수집 방법과 결과의 재현·검토를 위해 기록한다.

가입자 세부 사항과 통화내역은 사건 관련 신원·통신 관계·시간적 경위를 분석하는 증거가 될 수 있으므로, 확보한 자료와 그 출처를 기록한다.

ICCID는 UICC/SIM 카드 식별번호, IMEI는 이동통신 단말기 식별번호이다. 서로 같은 번호가 아니며, 조사 대상 카드와 단말기를 구분하여 다른 증거·기록과 대응시키는 데 도움이 된다.

대리점이나 판매사원 정보가 사건의 가입·구입 경위와 직접 관련되면 추가로 기록할 수 있다. 따라서 ②는 **어떤 사건에서도 기록하면 안 되는 정보라는 뜻이 아니라**, 일반적인 모바일 포렌식 조사 기록의 핵심 항목으로는 상대적으로 적절하지 않다는 의미이다.

NoteBase

문 13. 침해 사고가 발생한 컴퓨터의 전자우편(E-mail)을 수사하는 기법으로 전자우편 헤더 분석을 사용할 수 있다. 전자우편 헤더에서 확인할 수 있는 것으로 가장 적절하지 않은 것은?

① 발신자가 이용한 전자우편 주소

② 전자우편을 발송한 시간

③ 발신자의 인적사항과 연락처

④ 발신자의 IP 주소

정답 3번

간단한 해설

메일 헤더에는 **전자우편 주소·시간·IP 주소**의 단서가 나타날 수 있지만, 그것만으로 **실제 발신자의 신원과 연락처**가 확인되는 것은 아니다. 별도의 계정·접속 기록 등과 교차 검증해야 한다.

핵심 풀이

메일 헤더는 **주소·시간·전달 경로의 기술적 단서**를 담는다. From 등의 필드에는 발신 측이 제시한 전자우편 주소가, Date에는 메시지 작성자가 표시한 전송 준비 시각이, Received에는 서버가 기록한 접속 상대 IP와 수신 시각 등이 나타날 수 있다.

그러나 표시된 주소나 IP만으로 **실제 발신자의 신원과 전화번호 등 연락처**를 확정할 수는 없다. 표시 이름은 임의로 지정될 수 있고 헤더 일부는 위조될 수 있다. 또한 웹메일·중계 서비스 이용 시 IP가 개인 단말이 아니라 서버의 주소일 수도 있다.

따라서 헤더는 발신자를 추적할 출발점이지만 신원 확인 자료 그 자체는 아니다. 실제 사용자와 연결하려면 서비스의 계정·접속 기록 등 별도 자료와 교차 검증해야 하며, 날짜·시간 역시 시간대와 기록 주체를 구분하여 해석한다.

따라서 헤더에서 확인할 수 있는 정보로 가장 적절하지 않은 것은 ③ 발신자의 인적사항과 연락처이다.

NoteBase

문 14. 응용프로그램 프리패치 파일을 분석하여 얻는 정보에 관한 설명으로 가장 적절하지 않은 것은?

① 응용프로그램 이름

② 응용프로그램 최초 수행(실행)시간

③ 응용프로그램 설치 및 삭제시간

④ 응용프로그램 수행(실행) 횟수

정답 3번

간단한 해설

프리패치는 **프로그램의 실행 흔적**을 남기는 자료이며, 설치·삭제 시각을 직접 기록하는 로그가 아니다. 실행 기록과 프로그램의 설치·제거 이력을 구별해야 한다.

개념 구분

프리패치는 응용프로그램의 시작을 빠르게 하기 위한 자원 접근 기록이므로, 실행 파일 이름과 실행 횟수, 실행 시각 등의 **프로그램 실행 흔적**을 분석하는 자료이다. 설치 프로그램의 작업 이력이나 삭제 시각을 직접 기록하는 설치·삭제 로그가 아니다.

최초 실행 시각은 프리패치가 처음 생성되는 시점과 관련하여 추정할 수 있다. 다만 프리패치 파일이 삭제·재생성되거나 수집 과정에서 메타데이터가 바뀌면, 현재 파일의 생성 시각을 그 프로그램의 생애 최초 실행 시각으로 단정할 수 없다. 내부의 최근 실행 시각과도 구별해야 한다.

설치·삭제 시각을 확인하려면 설치 로그, 이벤트, 레지스트리 등 다른 자료를 대조해야 한다. 따라서 프리패치 분석으로 직접 얻는 정보로 가장 부적절한 것은 ③ 응용프로그램 설치 및 삭제시간이다.

NoteBase

문 15. 다음과 같은 상황일 경우, 이 행위의 직접 증거로 가장 적절하지 않은 것은?

피혐의자가 회사의 중요자료를 회사 공용 PC에서 자신의 USB를 이용하여 자신의 개인 PC에 저장한 행위를 부인하고 있다.

① 공용 PC와 개인 PC의 레지스트리에 동일하게 저장되어있는 USB 제조사명·제품명·시리얼 번호 등

② 유출된 중요자료와 동일한 해시값을 가진 개인 PC에 저장된 파일

③ 회사 공용 PC 레지스트리에 기록된 피혐의자의 USB가 연결된 시간으로부터 수 분 이내에 USB에 저장된 중요자료

④ 피혐의자의 개인 PC 폴더에 저장된 회사 업무 수행과 관련된 일반 참고자료

정답 4번

간단한 해설

개인 PC에 일반 업무 참고자료가 있다는 사실은 **문제의 중요자료를 해당 USB로 옮겼다는 사실과 직접 연결되지 않는다**. USB 식별 정보, 동일 파일의 해시값, 연결·저장 시각은 해당 이동 행위와 더 구체적으로 관련된다.

NoteBase

핵심 풀이

판단 대상은 일반적인 회사 업무 수행이 아니라, '회사 중요자료를 공용 PC에서 USB를 거쳐 개인 PC로 옮긴 행위'이다. 따라서 **해당 USB, 해당 중요자료, 이동 시점**과 연결되는 흔적인지를 비교해야 한다.

①의 제조사명·제품명·시리얼 번호 등 식별 정보가 두 PC에서 일치하면 같은 USB의 연결 가능성을 뒷받침한다. 제조사명과 제품명만 같다고 동일 장치로 단정할 수는 없으므로 시리얼 번호 등 여러 정보와 연결 기록을 함께 확인한다.

②의 해시값 일치는 개인 PC에 있는 파일과 유출된 중요자료의 내용 동일성을 뒷받침한다. 다만 해시값만으로 누가 어떤 경로로 옮겼는지까지 확정하지는 않는다.

③은 USB 연결 시각과 중요자료 저장 시각이 가깝다는 점에서 복사 행위의 시간적 연관성을 뒷받침한다. 시간 정보의 의미와 시계 오차 등도 함께 검토해야 한다.

④의 일반 참고자료는 회사 업무와 관련된 자료라는 사실만 보여 준다. 그것이 문제의 중요자료인지, 공용 PC에서 해당 USB로 이동했는지와는 직접 연결되지 않는다. 따라서 제시된 행위와의 관련성이 가장 약한 것은 ④이다.

각 흔적은 서로 결합하여 판단해야 하며, 하나만으로 행위자와 전송 경로가 모두 입증되는 것은 아니다. 여기서는 해당 행위에 대한 구체적 관련성을 비교한 것이며, ①~③을 모두 엄밀한 법적 의미의 직접증거라고 단정하는 것은 아니다.

NoteBase

문 16. 디지털 포렌식 기본원칙에 의한 조치로 가장 적절하지 않은 것은? (다툼이 있는 경우 판례에 의함)

① 甲이 지구대에 임의동행된 상태에서 경찰관이 甲의 집을 수색하여 사진 등 자료를 확보한 후 임의동행을 근거로 디지털 증거로 제출하였다.

② 원본이 압수된 시점부터 문건이 출력될 때까지 변경되지 않도록 조치하였다.

③ 원본과 사본 사이에 자료의 내용이 동일함을 입증하였다.

④ 증거를 획득하고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정별 담당자를 명시하였다.

정답 1번

①

임의동행만으로는 주거에 대한 무영장 수색이 허용되지 않는다. 영장이나 법률상 무영장 수색 요건을 갖추지 않은 채 자료를 확보하는 것은 적법절차 원칙에 어긋난다.

형사소송법 제215조 제2항은 “사법경찰관이 범죄수사에 필요한 때에는 검사에게 신청하여 검사의 청구로 지방법원 판사가 발부한 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.”고 규정하고 있는바,사법경찰관이 위 규정을 위반하여 영장없이 물건을 압수한 경우 그 압수물은 물론 이를 기초로 하여 획득한 2차적 증거 역시 유죄 인정의 증거로 사용할 수 없는 것이고, 이와 같은 법리는 헌법과 형사소송법이 선언한 영장주의의 중요성에 비추어 볼 때 위법한 압수가 있은 직후에 피고인으로부터 작성받은 그 압수물에 대한 임의제출동의서도 특별한 사정이 없는 한 마찬가지라고 할 것이다. (대법원 2010. 7. 22. 선고 2009도14376 판결)

②

디지털 증거의 무결성을 확보하려면 **압수 시점부터 문건 출력 시점까지 원본이 변경되지 않았음**이 담보되어야 한다.

(1) 압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 할 것인데, 그 동일성을 인정하기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보되어야 하고 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 ‘하드카피’·‘이미징’한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 ‘하드카피’·‘이미징’한 매체 사이에 자료의 동일성도 인정되어야 한다. (대법원 2007. 12. 13. 선고 2007도7257 판결)

NoteBase

③

원본 대신 복제하거나 이미징한 사본을 이용할 때에는 **원본과 사본에 저장된 자료의 동일성**이 인정되어야 한다.

(1) 압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 할 것인데, 그 동일성을 인정하기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보되어야 하고 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 '하드카피'·'이미징'한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 '하드카피'·'이미징'한 매체 사이에 자료의 동일성도 인정되어야 한다. (대법원 2007. 12. 13. 선고 2007도7257 판결)

④

증거 획득부터 법정 제출까지 단계별 담당자와 취급 이력을 기록하여 **증거의 이동·보관 경로를 끊김 없이 추적할 수 있게 하는 것이 연계보관성 원칙**이다.

NoteBase

문 17. 하드디스크 드라이브에 관한 설명으로 가장 적절하지 않은 것은?

① RAID는 여러개의 하드디스크 드라이브를 연결하여 입출력 성능 개선 및 컴퓨터 응용에서 발생될 수 있는 데이터 손실 등을 방지하기 위한 기술로 응용되고 있다.

② 하드디스크 드라이브는 전원 연결단자, 헤드, 플래터 등으로 구성된 정보저장 장치이다.

③ 하드디스크 드라이브 인터페이스 중 SCSI는 단일 SCSI 포트에 여러개의 장치들을 연결할 수 있다는 이점이 있다.

④ Sector의 수보다 Head의 수가 더 많다.

정답 4번

간단한 해설

헤드는 읽기·쓰기 부품, 섹터는 기록 공간의 단위이다. 하나의 헤드가 많은 섹터에 접근하므로 디스크 전체의 섹터 수보다 헤드 수가 많다는 설명은 틀리다.

선지별 해설

① O: RAID는 여러 디스크를 묶어 **입출력 성능이나 장애 내성**을 높이는 데 활용된다. 구체적 효과는 RAID 수준에 따라 다르며, RAID 0처럼 중복성을 제공하지 않는 방식도 있다. RAID는 모든 데이터 손실을 막거나 별도 백업을 대체하는 기술은 아니다.

② O: HDD에는 데이터를 자기적으로 기록하는 **플래터와 이를 읽고 쓰는 헤드**, 전원을 공급받는 연결 단자 등이 있다. 회전하는 기록 매체와 기계적 접근 부품을 사용하는 저장장치이다.

③ O: 전통적인 병렬 SCSI에서는 **하나의 버스에 여러 장치를 연결**하고 장치 식별자로 구별할 수 있다. 연결 가능한 장치 수와 종단 처리 등은 인터페이스 규격에 따라 정해지며, 이를 모든 저장장치 연결 방식에 그대로 적용하지는 않는다.

④ X: 헤드는 기록면을 읽고 쓰는 부품이고, 섹터는 기록 공간을 나눈 데이터 저장 단위이다. 하나의 헤드가 접근하는 기록면에도 수많은 섹터가 있으므로 **디스크 전체 섹터 수가 헤드 수보다 훨씬 많다**. 주소 표현에 쓰는 논리적 CHS 값과 실제 물리적 헤드·섹터 구조를 혼동하지 않아야 한다.

NoteBase

문 18. 다음 헤더 정보(Hex) 중 ZIP 파일로 가장 적절한 것은?

① 50 4B 03 04

② 41 4C 5A 01

③ 50 4B 05 06

④ 43 4C 5A 02

정답 1번

간단한 해설

ZIP의 일반적인 로컬 파일 헤더 시그니처는 **50 4B 03 04**이다. 50 4B 05 06은 같은 ZIP 형식에서도 중앙 디렉터리의 종료를 나타내는 별도 레코드이다.

개념 구분

일반적인 ZIP 파일의 로컬 파일 헤더는 **50 4B 03 04** 바이트로 시작한다. 앞의 50 4B는 ASCII의 'PK'에 해당하며, ZIP 안에 저장된 파일의 로컬 헤더임을 식별한다. 따라서 통상적인 파일 헤더를 묻는 이 문항의 답은 ①이다.

50 4B 05 06은 ZIP과 무관한 값이 아니라 **중앙 디렉터리 종료 레코드**의 시그니처이다. 빈 ZIP에서는 이 레코드가 처음에 올 수도 있지만, 일반적인 로컬 파일 헤더와는 역할이 다르다.

41 4C 5A 01은 ALZ 계열 압축 형식의 식별자로 ZIP 로컬 헤더가 아니다.

43 4C 5A 02 역시 ZIP의 표준 로컬 파일 헤더 시그니처가 아니다.

NoteBase

문 19. 디지털 포렌식에서 해시(hash)함수의 특징에 관한 설명으로 가장 적절하지 않은 것은?

① 해시는 키가 없고 복호화가 불가능한 특징을 가지는 암호화 방식이다.

② SHA-1은 데이터 무결성을 보장하기 위한 해시 함수이다.

③ 1Bit라도 다른 입력 데이터는 다른 해시값을 갖는다.

④ SHA 해시함수는 128Bit의 출력 해시값을 생성한다.

정답 4번

간단한 해설

SHA-1은 **160비트**, SHA-256은 **256비트** 등 알고리즘마다 출력 길이가 다르므로, 모두 128비트라는 ④가 잘못이다. 해시의 변경 탐지 성질을 충돌이 절대 없다는 보장으로 해석해서는 안 된다.

선지별 해설

① O(일반적인 비키드 해시의 단방향성이라는 취지): 일반적인 암호학적 해시는 비밀키 없이 메시지 요약값을 계산하며, 원문을 되돌리는 복호화 연산이 없다. 다만 원문의 '암호화 방식'은 **복호화 가능한 암호화와 구별해야 하는 표현**이다. HMAC처럼 키를 결합한 구성도 있으므로 모든 해시 관련 기법에 키가 없다는 뜻으로 확대하지 않는다.

② O(사용 목적의 설명): SHA-1은 데이터를 요약하여 변경 여부를 확인하는 무결성 검사에 사용되어 온 해시 함수이다. 그러나 **충돌 취약성이 알려져 있어 안전성을 무조건 보장하지 않는다.** 특히 공격자가 서로 다른 자료를 만들 수 있는 상황에서는 SHA-1의 과거 용도와 현재의 보안 적합성을 구별해야 한다.

③ O(일반적인 변경 탐지의 취지): 좋은 암호학적 해시는 작은 입력 변화가 출력에 크게 영향을 주므로, 한 비트 수준의 변경도 해시 비교로 탐지하는 데 활용한다. 다만 원문을 **서로 다른 입력 사이의 충돌이 절대로 없다는 뜻**으로 읽으면 엄밀하지 않다. 유한한 길이의 해시에는 충돌이 가능하며, 충돌 저항성은 같은 값을 내는 서로 다른 입력을 찾기 어렵다는 성질이다.

④ (X) **SHA 계열의 출력이 모두 128비트인 것은 아니다.** SHA-1은 160비트, SHA-224는 224비트, SHA-256은 256비트, SHA-384는 384비트, SHA-512는 512비트의 요약값을 만든다. 알고리즘별 출력 길이를 혼동한 ④가 가장 적절하지 않다.

NoteBase

문 20. 디지털 증거 수집에 관한 설명으로 가장 적절하지 않은 것은?

① 하드디스크 드라이브 이미징(Imaging)은 원본 내 모든 섹터의 모든 데이터가 저장된다.

② 파일, 디렉터리 등을 마우스로 드래그 앤드 드롭(Drag-and-drop)을 통해 복사하여 디지털 증거를 수집한 경우에도 삭제된 데이터를 복구할 수 있다.

③ 증거 수집·복제 전에 증거가 위치하고 있는 장소에 대한 사진을 촬영한다.

④ 하드디스크 드라이브 분리 전 현장에서 시스템 정보를 기록하는 것이 중요하다.

정답 2번

간단한 해설

드래그 앤드 드롭 복사는 원본 디스크의 미할당 영역과 슬랙까지 수집하지 않는다. 삭제 데이터 분석에는 이러한 잔존 영역을 포함하는 **비트스트림 이미징**과 단순 파일 복사를 구별해야 한다.

선지별 해설

① O. 여기서 이미징은 디스크의 **전체 섹터를 대상으로 하는 비트스트림 복제**를 말한다. 정상적으로 읽을 수 있는 대상 영역을 복제하면 현재 파일뿐 아니라 미할당 영역과 슬랙의 잔존 데이터도 포함된다. 다만 불량 섹터나 접근 불가능한 영역까지 언제나 성공적으로 읽는다는 보장은 아니며, 획득 범위와 읽기 오류를 기록해야 한다.

② X. 일반적인 드래그 앤드 드롭은 **현재 접근 가능한 파일·폴더의 논리적 복사**이므로, 삭제 파일이 남아 있을 수 있는 원본의 미할당 영역이나 슬랙을 함께 획득하지 않는다. 따라서 그 단순 복사본만으로 원본 매체의 삭제 데이터를 복구할 수 있다고 볼 수 없다. 복사된 개별 파일 내부의 잔존 정보 분석과 원본 디스크의 삭제 파일 복구는 구별해야 한다.

③ O. 수집·복제 전에 **증거의 위치와 현장 상태를 사진으로 기록**하면 발견 당시의 배치·연결 관계를 보존하고 이후 절차를 설명하는 데 도움이 된다. 장비를 옮기거나 분리하기 전에 현장 맥락을 남기는 것이 중요하다.

④ O. 하드디스크를 분리하기 전에 **시스템 구성과 장비 식별·연결 상태**를 기록해야 원래 환경을 파악하고 수집 과정을 추적할 수 있다. 단순 기록을 위해 불필요하게 장비를 조작하여 증거를 변경하지 않도록 주의한다.

따라서 가장 적절하지 않은 것은 단순 파일 복사로 원본 매체의 삭제 데이터도 복구할 수 있다고 한 ②이다.

NoteBase