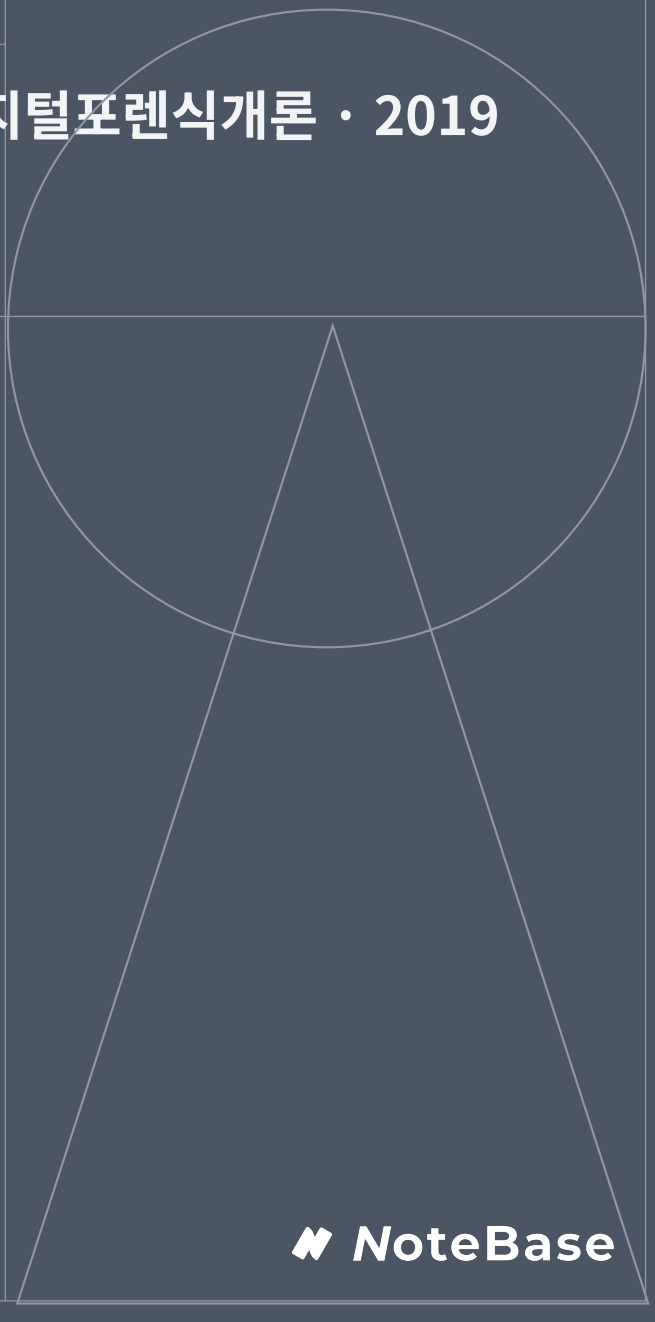
기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2019



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2019

공무원/경찰/경력채용 · 디지털포렌식개론 · 2019

문 1. 디지털 포렌식의 기본 원칙으로 가장 적절하지 않은 것은?

① 디지털 증거의 정확성을 위해 원본을 사용하여 분석해야 한다.

② 디지털 증거는 원본을 획득하되, 특별한 환경에서는 사본을 획득할 수 있도록 하고 있다.

③ 분석도구의 신뢰성 확보를 위하여 반드시 검증된 분석도구를 사용해야 한다.

④ 적법절차를 준수하여 당사자의 프라이버시 및 인권을 최대한 보호해야 한다.

정답 1번

간단한 해설

디지털 증거의 분석은 **원본 보존과 무결성 유지**가 핵심이다. 원본을 직접 사용해야 정확한 것이 아니라, 동일성을 확인한 분석용 사본을 사용하여 원본 변경 위험을 줄인다.

선지별 해설

① X — 원본을 직접 분석해야 정확하다는 설명은 부적절하다. 원본의 변경·훼손을 줄이기 위해 **원본은 보존하고 무결성을 확인한 분석용 사본**으로 작업하는 것이 기본이다. 복제 시 쓰기방지 장치 등을 사용하고 해시값과 처리 기록으로 동일성을 확인한다.

② O — 이 문항은 증거의 출처와 원본성을 확보하면서 여건에 따라 사본을 획득할 수 있다는 취지이다. **증거의 획득과 분석용 사본의 사용은 다른 단계**이므로, 원본 확보를 원본 직접 분석 의무로 연결하면 안 된다. 다만 이 표현을 모든 상황에서 원본 저장매체 자체를 우선 압수해야 한다는 보편적 법적 규칙으로 읽어서는 안 되며, 구체적인 수집 방식은 적법한 범위와 현장 조건에 따라 정한다.

③ O — 분석 결과를 신뢰하려면 **기능과 정확성이 검증된 도구**를 사용해야 한다. 도구의 버전·설정과 처리 절차를 기록하고, 필요한 경우 알려진 시험 자료나 다른 방법으로 결과를 교차 확인한다.

④ O — 증거 수집과 분석은 **적법절차와 권리 보호**를 전제로 한다. 허용된 목적과 범위 안에서 필요한 자료를 다루어 당사자의 사생활과 인권 침해를 최소화해야 한다.

NoteBase

문 2. 디지털 데이터 사본을 만드는 방법으로 가장 적절한 것은?

① 조사대상 매체는 반드시 읽기 전용으로 조사용 시스템에 부착해야 한다.

② 원본 디스크의 저장 용량보다 반드시 적은 용량의 디스크를 사용하여 복제본을 생성해야 한다.

③ 소프트웨어를 사용한 이미징(imaging)은 하드웨어를 사용한 방법보다 이미징 시간이 단축된다.

④ 사본 이미지 생성에 LinEn, dd는 사용할 수 없다.

정답 1번

간단한 해설

사본 생성 과정에서도 원본 데이터가 바뀌지 않아야 한다. 조사용 시스템에 원본 매체를 연결할 때 **쓰기 동작을 차단하고 읽기 전용으로 접근**하여 무결성을 보존한다.

선지별 해설

① O: 원본 저장매체를 조사용 시스템에 연결해 사본을 만들 때는 시스템이 원본에 데이터를 기록하지 못하도록 **읽기 전용으로 접근**해야 한다. 쓰기방지장치 등의 방법으로 원본 변경을 막아야 사본 생성 과정에서 증거의 무결성을 보존할 수 있다.

② X: 원본 전체를 다른 디스크에 복제하려면 대상 디스크에 복제할 데이터를 담을 **충분한 용량**이 있어야 한다. 일반적인 비트 단위 디스크 복제에서는 원본과 같거나 더 큰 용량을 확보한다. 압축 이미지 파일의 크기가 줄어들 수 있다는 사실이 반드시 더 작은 디스크를 사용해야 한다는 뜻은 아니다.

③ X: 이미징 속도는 저장장치와 연결 인터페이스의 속도, 도구의 구현, 압축·검증 설정 등에 따라 달라진다. 소프트웨어 방식이라는 이유만으로 하드웨어 방식보다 **항상 시간이 짧다고 단정할 수 없다**.

④ X: LinEn과 dd는 모두 디스크 사본 이미지 생성에 사용할 수 있다. LinEn은 리눅스 환경의 EnCase 증거 획득 도구이며, dd는 디스크 장치의 데이터를 읽어 이미지 파일로 복사할 수 있는 도구이다.

NoteBase

문 3. 해수욕장에서 다른 사람의 신체를 촬영하고 있는 용의자를 체포한 후 관련 사진이 저장된 것을 발견하였으나 인터넷에서 다운받은 것이라 부인할 경우, 이를 반박할 수 있는 증거를 찾는 방법 중 가장 적절한 것은?

① 이미지 파일의 확장자

② 이미지 파일들의 목록

③ 이미지 파일의 용량

④ 이미지 파일의 메타데이터

정답 4번

간단한 해설

이미지의 **메타데이터에는 촬영 장비·시각·위치 등에 관한 단서**가 남을 수 있다. 이를 사건 및 장비 정보와 대조하는 것이 단순히 확장자나 용량을 확인하는 것보다 촬영 경위를 밝히는 데 적절하다.

핵심 풀이

쟁점은 사진이 저장되어 있다는 사실 자체가 아니라 **직접 촬영한 사진인지, 내려받은 사진인지**를 구별할 단서를 찾는 것이다. 이미지의 메타데이터는 이미지 자체에 관한 부가 정보로, Exif에는 촬영 장비의 제조사·모델, 원본 생성 시각, 기록된 경우 GPS 위치 등이 포함될 수 있다. 이를 압수한 장비와 사건의 시간·장소에 대조하면 직접 촬영했다는 주장을 뒷받침할 단서를 얻을 수 있다.

확장자는 JPEG 등 파일 형식을 나타낼 뿐 촬영과 다운로드를 구별하지 못한다. 이미지 파일들의 목록은 보유한 파일을 파악하는 자료이고, 용량은 해상도·압축 정도 등에 영향을 받으므로 그 자체로 촬영 경위를 정하지 못한다. 이들보다 촬영 경위에 관한 구체적 정보를 담을 수 있는 메타데이터가 적절하다.

다만 **메타데이터만으로 촬영자를 확정할 수는 없다**. 내려받은 사진에도 원래 메타데이터가 남을 수 있고, 값이 수정·삭제되거나 장비 시계가 부정확할 수도 있다. 따라서 다른 촬영 기록과 다운로드 흔적 등과 함께 확인해야 한다. 이러한 단서를 찾는 방법은 ④ 이미지 파일의 메타데이터에 해당한다.

NoteBase

문 4. 포렌식 분석 기법 및 분석 도구에 대한 설명으로 가장 적절한 것은?

① 포렌식 조사 분석은 잘 알려진 파일은 검색 대상에서 제외하고, 주목해서 검색할 대상을 선정하여 검색범위를 축소하는 것이 중요하다.

② FTK(Forensic Tool Kit)의 프로그램 중 사본 이미지 생성에 사용되는 프로그램은 Registry viewer이다.

③ ProDiscover는 리눅스에서만 동작한다.

④ 해시 값을 이용하여 불필요한 파일을 조사대상에서 제외하거나 특정 파일만을 찾아내는 방법은 시그니처 분석 방법이다.

정답 1번

간단한 해설

사건과 무관한 알려진 파일을 걸러 내면 **검색 범위를 줄여 분석에 집중**할 수 있다. 이미지 생성은 FTK Imager, 알려진 파일 식별은 해시 비교라는 기능 구분이 중요하다.

선지별 해설

① O. 알려진 운영체제·응용 프로그램 파일 등을 식별하고 사건과 무관한 대상을 걸러 내면 **조사 범위를 효율적으로 축소**할 수 있다. 여기서 제외하는 것은 관련성이 없다고 판단한 파일이며, 알려진 파일이라는 이유만으로 사건과 관련된 파일까지 일률적으로 배제해서는 안 된다.

② X. 사본 이미지 생성에는 **FTK Imager**를 사용한다. Registry Viewer는 레지스트리 파일의 키·값 등 운영체제 설정과 사용 흔적을 확인하는 도구이므로 이미지 생성 도구와 구별된다.

③ X. ProDiscover는 **Windows 기반 분석 도구**로도 제공되어 왔으므로 리눅스에서만 동작한다는 설명은 틀리다. 도구가 실행되는 운영체제와, 그 도구가 분석할 수 있는 파일시스템·대상 운영체제는 서로 다른 개념이다.

④ X. 알려진 해시 집합과 비교하여 파일을 제외하거나 특정 파일을 찾는 것은 **해시 분석·해시 기반 필터링**이다. 이 문제에서 구별하는 파일 시그니처 분석은 파일 내부의 형식 식별 패턴을 확인하여 실제 파일 형식이나 확장자 불일치를 판별하는 방법이다. 문헌에 따라 해시값도 넓은 의미의 파일 시그니처라고 부르므로, 해시는 절대로 시그니처가 아니라는 뜻으로 일반화해서는 안 된다.

따라서 제시된 기법·도구 구분에서 가장 적절한 설명은 ①이다.

NoteBase

문 5. 디지털 증거의 특징에 대한 설명으로 가장 적절하지 않은 것은?

① 잠재성: 내용 확인을 위해서는 판독장치가 필요하다.

② 취약성: 위·변조 및 삭제가 용이하다.

③ 복제성: 원본과 사본의 구분이 어렵다.

④ 다양성: 자료가 방대하다.

정답 4번

간단한 해설

자료가 방대하다는 것은 **대량성**이다. 다양성은 증거가 여러 기기·매체·파일 형식 등으로 존재한다는 특징이므로 양과 종류를 구별해야 한다.

선지별 해설

① O — **잠재성**은 저장매체에 기록된 디지털 내용을 사람의 감각만으로 곧바로 확인하기 어렵다는 특징이다. 내용을 해석·표시하려면 적절한 판독 장치와 소프트웨어가 필요하다.

② O — **취약성**은 디지털 데이터가 변경·삭제되기 쉬워 증거의 상태가 훼손될 수 있다는 뜻이다. 따라서 원본 보존, 접근 통제, 쓰기방지와 해시값 검증 등으로 무결성을 관리한다.

③ O — **복제성**은 동일한 비트 내용의 사본을 만들 수 있다는 특징이다. 내용만으로 원본과 정확한 사본을 구별하기 어려우므로, 원본·사본의 관계는 획득 경위와 처리 기록 등으로 관리한다. 저장매체 자체나 모든 부수 메타데이터까지 항상 구별 불가능하다는 뜻은 아니다.

④ X — 자료의 양이 방대하다는 설명은 **대량성**에 해당한다. 다양성은 저장매체·기기·파일 형식·운영환경 등 증거의 종류와 형태가 여러 가지라는 뜻으로, 자료의 양과 구별해야 한다.

NoteBase

문 6. 윈도우의 “Thumbs.db”에 대한 설명으로 가장 적절한 것은?

① 삭제된 이미지 파일의 존재 여부를 확인할 수는 없다.

② 기본적으로 숨김 속성으로 설정되어 있다.

③ Thumbs.db는 사용자가 직접 생성한다.

④ 사진이나 이미지를 삭제하면 Thumbs.db 파일은 삭제되므로 주기적인 백업이 필요하다.

정답 2번

간단한 해설

Thumbs.db는 Windows가 이미지 미리보기를 위해 관리하는 **숨김 속성의 썸네일 캐시**이다. 따라서 ②가 가장 적절하다. 원본 이미지가 삭제되어도 캐시의 흔적은 남을 수 있다.

선지별 해설

① (X) 원본 이미지가 삭제되어도 **캐시에 썸네일이 남아 있을 수 있다**. 남은 미리보기는 해당 이미지가 존재했음을 조사하는 단서가 된다. 다만 캐시 정리·덮어쓰기 등에 따라 흔적이 사라질 수 있고, 썸네일만으로 원본 전체가 복구되는 것은 아니다.

② (O) Thumbs.db는 이미지 미리보기를 빠르게 표시하기 위한 **썸네일 캐시 파일이며 기본적으로 숨김 속성**을 가진다. 숨김 파일 표시 설정에 따라 탐색기에서 보이지 않을 수 있다. Windows 버전과 저장 위치에 따라 캐시 방식은 달라지므로, 모든 최신 Windows의 로컬 폴더에 반드시 이 파일이 생긴다는 뜻은 아니다.

③ (X) 사용자가 직접 작성하는 파일이 아니라, 캐시 사용이 허용된 환경에서 **Windows 탐색기가 썸네일을 저장하며 자동으로 생성·관리**하는 파일이다. 사용자의 폴더 열람이 생성 계기가 될 수 있다는 것과 사용자가 파일 자체를 직접 만든다는 것은 다르다.

④ (X) **원본 사진 삭제와 Thumbs.db 삭제는 별개**이다. 원본이 삭제되어도 캐시 파일과 일부 썸네일이 남을 수 있으므로, 사진을 삭제하면 캐시도 반드시 삭제된다는 전제가 틀렸다. 포렌식에서는 남아 있는 캐시를 보존하여 분석하되, 그 보존 가능성이 항상 보장되는 것은 아니다.

NoteBase

문 7. 리눅스가 설치된 PC의 압수·수색 과정에서 발견된 로그파일 중 “시스템의 정기적인 작업에 대한 로그”가 기록된 것으로 가장 적절한 것은?

① secure 로그 파일

② dmesg 로그 파일

③ xferlog 로그 파일

④ cron 로그 파일

정답 4번

간단한 해설

cron은 정해진 일정에 따라 작업을 실행하는 서비스이다. **시스템의 정기적인 작업**과 관련된 이력은 cron 로그에서 확인한다.

개념 구분

cron은 설정된 일정에 따라 명령이나 스크립트를 실행하는 서비스이다. 따라서 **정기적으로 실행되는 작업**의 이력을 확인하는 단서는 cron 로그이다. 전통적인 로그 파일 구성에서는 /var/log/cron에 관련 메시지를 저장한다.

secure 로그는 로그인이나 권한 사용 등 **보안·인증 관련 메시지**를 기록하는 데 쓰인다. 정기 작업의 실행 이력과는 주된 기록 대상이 다르다.

dmesg 관련 로그는 부팅 과정의 장치 인식 등 커널 메시지를 확인하는 데 쓰인다. 예약된 작업의 일정이나 실행을 기록하는 로그와 구별된다.

xferlog는 주로 FTP 서비스의 **파일 전송 내역**을 기록한다. 파일 업로드·다운로드와 관련된 정보를 확인하는 자료이지 정기 작업 전용 로그가 아니다.

배포판과 로그 설정에 따라 저장 위치나 방식은 달라질 수 있으나, 제시된 정기 작업에 대응하는 항목은 ④ cron 로그 파일이다.

NoteBase

문 8. 디지털 포렌식 증거 수집에 대한 설명으로 가장 적절하지 않은 것은?

① 증거 수집 절차는 “증거획득→증거분석→증거보관→증거제출”이다.

② 컴퓨터시스템 전체를 확보한 경우에는 BIOS에 설정되어 있는 시스템 날짜와 시간을 조사기관의 증거분석실에서 확인할 수 있다.

③ 휘발성 정보를 수집하기 위해 PC 종료 후, 디스크 복제를 수행한다.

④ 네트워크 증거수집 시에는 반드시 소유자나 관련자의 확인을 받아야 한다.

정답 3번

출제 포인트

디지털 증거 수집에서 휘발성 정보와 비휘발성 정보의 차이, 전원 종료 전 수집의 필요성을 묻는다.

핵심 개념

휘발성 정보는 전원이 꺼지면 사라지는 정보로, RAM의 내용과 실행 중인 프로세스·현재 네트워크 연결 상태 등이 해당한다. 비휘발성 정보는 전원이 꺼져도 저장매체에 남는 정보로, 디스크에 저장된 파일 등이 해당한다. 디스크 복제는 저장매체의 내용을 복사하는 작업이며 RAM 수집을 대신하지 못한다.

선지별 해설

① O. 제시된 획득→분석→보관→제출은 증거를 확보하여 내용을 분석하고, 증거와 분석 결과를 관리한 뒤 제출하는 흐름이다. 다만 원본 보호와 무결성 유지는 분석이 끝난 뒤에만 하는 일이 아니라 전 과정에서 필요하다.
② O. 컴퓨터시스템 전체를 확보하면 메인보드의 시계와 BIOS 설정도 확인할 수 있으므로, 증거분석실에서 시스템 날짜와 시간을 확인할 수 있다. 이 시계는 통상 별도 배터리로 유지되며, 확인한 시스템 시간이 실제 시간과 일치하는지는 별도로 대조한다.
③ X. 틀린 표현은 “휘발성 정보를 수집하기 위해 PC 종료 후”이다. PC를 종료하면 RAM의 내용과 실행 상태 등 휘발성 정보가 소실되므로, 이후 디스크를 복제해도 이를 보존할 수 없다. 올바르게는 PC가 켜진 상태에서 필요한 휘발성 정보를 먼저 수집한 뒤 디스크 복제를 수행한다.
④ O. 네트워크에는 여러 장비와 이용자의 정보가 함께 존재하므로, 소유자나 관련자를 통해 수집 대상과 범위를 확인하는 절차가 필요하다. 이 선지의 확인은 대상 네트워크와 관련 정보를 특정하기 위한 절차로 이해한다.

오답 포인트

③의 “디스크 복제”가 모든 정보를 보존한다는 착각이 함정이다. 디스크를 정확히 복제하더라도 종료와 함께 사라진 RAM의 내용까지 복제되는 것은 아니다.

NoteBase

다시 나오면 이렇게 판단

수집할 정보가 전원 종료 후에도 남는지를 먼저 구분한다. RAM이나 실행 상태처럼 종료 시 사라지는 정보가 필요하면 전원을 끄기 전에 수집하며, 디스크 정보는 별도의 복제로 확보한다.

암기 포인트

휘발성 정보는 종료 전에 수집한다. 디스크 복제는 RAM 수집을 대신하지 못한다.

NoteBase

문 9. 안티-포렌식에서 데이터를 식별하지 못하도록 정보를 은닉하는 방법으로 가장 적절하지 않은 것은?

① Safeback

② Slacker

③ Steganography

④ RuneFS

정답 1번

간단한 해설

Safeback은 정보를 숨기는 도구가 아니라 **디스크 이미지를 획득하는 포렌식 도구**이다. 나머지는 데이터를 눈에 띄지 않게 저장하거나 그 존재를 감추는 방식과 관련된다.

개념 구분

Safeback은 원본 디스크나 파티션의 내용을 **비트스트림 사본·이미지로 획득**하는 포렌식 도구이다. 분석할 증거를 복제·보존하는 역할이며, 데이터를 식별하지 못하도록 숨기는 도구로 분류하지 않는다.

Slacker는 파일에 할당된 공간 중 실제 파일 내용이 차지하지 않는 **슬랙 공간에 데이터를 은닉**하는 도구이다. 정상적인 파일 내용만 확인할 때 드러나지 않는 공간을 이용한다.

Steganography는 이미지 등 다른 매체에 정보를 넣어 **정보의 존재 자체를 감추는** 기법이다. 내용을 읽기 어렵게 만드는 암호화와 구별된다.

RuneFS는 파일시스템에서 **불량 블록으로 관리되는 영역을 이용한 은닉** 기법·도구로 알려져 있다. 파일시스템의 일반적인 파일 접근에서 잘 드러나지 않는 저장 영역을 활용한다.

따라서 정보 은닉 방법으로 가장 적절하지 않은 것은 ① Safeback이다.

NoteBase

문 10. 디지털 포렌식에서 삭제된 파일의 복구와 관련된 설명으로 가장 적절하지 않은 것은?

① 파일 카빙(file carving)은 파일의 시그니처 구조, 논리구조, 형식 등에 의존하여 파일을 복구해야 한다.

② 파일이 삭제되더라도 해당 데이터 클러스터가 다른 파일로 사용되지 않았다면 복구 가능하다.

③ 복구 대상 컴퓨터에 복구 소프트웨어를 설치하여 복구한다.

④ 삭제된 파일의 속성은 다른 파일이 그 디렉토리 엔트리를 재사용하기 전까지 이름을 제외하고 대부분 보존된다.

정답 3번

간단한 해설

복구 대상 컴퓨터에 소프트웨어를 설치하면 **삭제 데이터가 남아 있는 영역을 덮어쓸 위험**이 있다. 원본에 대한 쓰기를 막고 복제본을 별도 환경에서 분석해야 한다.

선지별 해설

① O: 파일 카빙은 파일시스템의 메타데이터에 의존하는 복구와 달리 **파일 내용의 시그니처·내부 구조·형식**을 분석하여 파일을 찾아 복원한다. 파일의 시작·끝 표식이나 형식상 유효한 구조 등이 복구 단서가 된다.

② O: 일반적인 논리적 삭제에서는 저장 영역이 사용 가능한 것으로 표시되어도 기존 데이터가 남을 수 있다. 따라서 **데이터가 덮어써지지 않고 남아 있으면 복구 가능성**이 있다. 다만 다른 파일이 사용하지 않았다는 사정만으로 복구가 보장되지는 않으며, TRIM·보안 삭제·손상이나 조각난 파일의 연결 정보 소실 등도 영향을 준다.

③ X: 복구 대상 컴퓨터에 소프트웨어를 설치하면 설치 파일이나 운영체제의 쓰기가 **복구하려는 삭제 데이터 영역을 덮어쓸 수 있다**. 원본에 대한 쓰기를 방지하면서 이미지를 확보하고, 별도의 분석 환경에서 복제본을 대상으로 복구하는 것이 적절하다. 복구 결과도 원본 매체가 아닌 별도 매체에 저장해야 한다.

④ O: 디렉터리 엔트리를 이용하는 전통적인 FAT의 삭제 동작을 대표적으로 설명한 것이다. 삭제된 엔트리가 재사용되기 전에는 크기·시각·시작 클러스터 등 **여러 속성 정보가 남아 복구에 활용**될 수 있다. FAT에서는 짧은 파일명 첫 바이트가 삭제 표시로 바뀌며, 이름 전체가 반드시 사라지는 것은 아니다. 보존되는 정보와 삭제 방식은 파일시스템에 따라 다르므로 모든 파일시스템의 보편적 규칙으로 확대해서는 안 된다.

NoteBase

문 11. 윈도우 레지스트리를 이용하여 확인할 수 있는 정보로 가장 적절하지 않은 것은?

① 사용한 USB 장치의 제조사, 모델명, 고유번호 정보

② 설치 후 삭제된 프로그램 정보

③ 외부 시스템 연결 정보

④ 데몬(daemon)을 관리하는 inetd 정보

정답 4번

간단한 해설

Windows 레지스트리에는 장치·프로그램·원격 연결 관련 흔적이 남을 수 있다. **inetd는 Unix 계열의 슈퍼서버**이므로 Windows 레지스트리의 일반적인 조사 항목과 구별된다.

선지별 해설

① O — USB 저장장치 관련 레지스트리 키에는 **장치 식별 정보**가 남을 수 있다. 이를 통해 제조사·제품명·일련번호 등을 조사할 수 있으나, 장치와 운영체제에 따라 값의 존재와 의미가 달라지므로 모든 장치에서 완전한 고유번호가 보장되는 것은 아니다.

② O — 프로그램을 제거해도 관련 설정이나 사용 흔적 등이 레지스트리에 남을 수 있어 **과거 설치·사용 여부**를 추정하는 단서가 된다. 삭제된 모든 프로그램의 기록이 반드시 남는 것은 아니며, 잔존 정보와 다른 흔적을 종합해야 한다.

③ O — 원격 데스크톱 클라이언트의 최근 접속 대상 등 **외부 시스템 연결 관련 흔적**을 레지스트리에서 확인할 수 있다. 다만 저장된 접속 대상 정보만으로 모든 실제 연결의 성공 여부나 정확한 접속 시각까지 입증되는 것은 아니다.

④ X — **inetd**는 전통적인 Unix 계열의 인터넷 슈퍼서버로, 설정 파일인 /etc/inetd.conf 등을 이용해 네트워크 서비스를 관리한다. Windows 레지스트리가 기본적으로 관리하는 서비스 정보와 구별해야 한다.

NoteBase

문 12. 압수·수색 현장에서 시스템 관리자가 비협조적일 경우, 디지털 포렌식 수사관이 데이터베이스를 찾기 위한 방법으로 가장 적절하지 않은 것은?

① 리눅스의 경우 “ps” 명령으로 “mysql” 프로세스를 확인할 수 있다.

② MySQL, MS-SQL 등이 동작 중이라면 특정 네트워크 포트를 검색하여 존재 여부를 확인할 수 있다.

③ MS-SQL의 경우 “my.cnf”라는 환경 설정 파일을 검색하고, MySQL의 경우 파일 확장자가 “.mdf”인 파일을 검색하여 존재 여부를 확인할 수 있다.

④ 윈도우의 경우 cmd 창에서 “tasklist” 명령으로 “mysql” 프로세스를 확인할 수 있다.

정답 3번

간단한 해설

두 데이터베이스의 파일 특징이 뒤바뀌었다. **my.cnf는 MySQL 설정 파일**이고, **.mdf는 MS-SQL의 주 데이터 파일에 쓰이는 확장자**이다.

선지별 해설

① O: 리눅스의 ps는 실행 중인 프로세스 정보를 조회하는 명령이므로 MySQL 관련 프로세스를 찾는 데 사용할 수 있다. 다만 MySQL 서버의 일반적인 실행 파일명은 **mysqld**이며, mysql은 클라이언트 프로그램 이름이기도 하다. 실제 서버 여부는 프로세스의 실행 경로와 인수 등을 함께 확인한다.

② O: 실행 중인 데이터베이스 서버가 네트워크 연결을 수신한다면 **수신 대기 포트**가 존재 여부를 찾는 단서가 된다. 다만 포트는 설정에 따라 바뀔 수 있고 다른 서비스가 사용할 수도 있으므로, 포트 번호만으로 제품을 확정하지 말고 연결된 프로세스와 설정을 대조한다.

③ X: 두 제품의 파일 특징을 서로 바꾸어 연결했다. **my.cnf는 MySQL의 설정 파일**이며, **.mdf는 MS-SQL의 주 데이터 파일에 일반적으로 쓰이는 확장자**이다. 따라서 MySQL을 찾을 때는 해당 설정 파일을, MS-SQL을 찾을 때는 .mdf 등의 데이터 파일을 단서로 삼아야 한다.

④ O: 윈도우의 tasklist는 실행 중인 프로세스 목록을 표시하므로 MySQL 관련 실행 파일을 확인하는 데 사용할 수 있다. 서버 프로세스는 일반적으로 **mysqld.exe**이므로, 선지의 mysql을 관련 프로세스를 찾는 취지로 이해하되 클라이언트인 mysql.exe와 서버를 구별해야 한다.

NoteBase

문 13. 전체 드라이브를 암호화할 수 있으며 자신의 시스템에 인증 받지 못한 변경에 대한 보호 기능을 갖는 윈도우용 안티-포렌식 응용프로그램으로 가장 적절한 것은?

① 와이핑(Wiping)

② 비트락커(BitLocker)

③ 린 엔(LinEn)

④ 어뎁토(Adepto)

정답 2번

간단한 해설

드라이브 암호화와 부팅 환경 보호 기능을 제공하는 것은 ② **BitLocker**이다. 와이핑은 삭제 기법이고, LinEn·Adepto는 증거 획득 도구이므로 구별된다.

핵심 풀이

Windows의 **BitLocker**는 드라이브의 데이터를 암호화하여 허가되지 않은 접근으로부터 보호하는 기능이다. 따라서 전체 드라이브 암호화라는 핵심 단서에 해당하는 것은 ②이다. 파일의 내용을 없애는 것이 아니라, 정당한 키 없이 내용을 읽기 어렵게 만드는 방식이다.

TPM과 연계한 운영체제 드라이브 보호에서는 **부팅 환경의 무결성**을 확인한다. 부팅 구성이나 주요 시작 파일 등에 예상하지 못한 변경이 감지되면 정상적인 키 해제 대신 복구 절차가 필요할 수 있다. 이는 모든 시스템 변경을 막는다는 뜻은 아니며, 구성과 보호 방식에 따라 동작이 달라진다.

와이핑은 데이터를 덮어쓰는 등으로 복구를 어렵게 하는 삭제 기법이다. LinEn과 Adepto는 증거 획득·이미징에 사용하는 도구로, 제시된 Windows 드라이브 암호화 기능과 구별된다. 문제의 **안티-포렌식**이라는 표현은 암호화가 분석을 어렵게 할 수 있다는 맥락이며, BitLocker 자체의 본래 목적은 정상적인 데이터 보호이다.

NoteBase

문 14. 웹 브라우저 사용 흔적의 분석을 위하여, 수집된 WebcacheV24.dat 파일에 대한 설명으로 가장 적절하지 않은 것은?

① ESE(Extensible Storage Engine)라는 구조를 사용한다.

② C:\Users\<username>\AppData\Local\Microsoft\Internet Explorer\IECompatData\ 폴더에서 파일을 수집한다.

③ 인터넷 익스플로러 10 버전에서 사용한다.

④ 윈도우의 Taskhost 프로세스가 핸들링하고 있어서 일반적인 복사로 획득할 수 없다.

정답 2번

간단한 해설

WebCacheV24.dat는 사용자 프로필의 **Microsoft\Windows\WebCache 폴더**에서 수집한다. Internet Explorer\IECompatData 폴더와 혼동하면 안 된다.

선지별 해설

① O. WebCacheV24.dat는 **ESE 데이터베이스 형식**으로 웹 사용 흔적을 관리한다. ESE는 Extensible Storage Engine의 약자로 Jet Blue라고도 하며, 종전의 index.dat 구조와 구별된다.

② X. 수집 위치는 사용자 프로필 아래의 **AppData\Local\Microsoft\Windows\WebCache** 폴더이다. 전체 경로는 C:\Users\사용자명\AppData\Local\Microsoft\Windows\WebCache\이며, 선지의 Internet Explorer\IECompatData\ 경로가 아니다.

③ O. 인터넷 익스플로러 10은 종전 index.dat 방식에서 **ESE 기반 WebCache 데이터베이스**를 사용하는 방식으로 바뀌었다. WebCacheV24.dat는 이 환경에서 확인되는 파일명이며, 환경·버전에 따라 WebCacheV01.dat 등 다른 이름도 나타날 수 있다.

④ O. 실행 중인 시스템에서는 Taskhost와 관련된 서비스가 데이터베이스를 사용하여 **잠금 상태에서 일반 파일 복사가 제한**된다. 이는 사용 중인 파일의 획득 제약을 설명한 것으로, 오프라인 상태나 잠금이 해제된 뒤에도 영구히 복사할 수 없다는 뜻은 아니다. 수집 시 파일 상태와 일관성을 고려해야 한다.

따라서 저장 경로를 잘못 제시한 ②가 가장 적절하지 않은 설명이다.

NoteBase

문 15. 디지털 포렌식에서 해시(hash)에 대한 설명으로 가장 적절하지 않은 것은?

① 해시는 일방향 알고리즘으로, 해시 값을 이용하여 본래 데이터로 복원하는 것은 원론적으로 불가능하다.

② 디지털 데이터의 무결성을 검증하기 위하여 적용하는 알고리즘이다.

③ 해시 검색은 외장장치 연결 흔적 등의 시스템 사용 흔적을 분석하기 위하여 사용한다.

④ 두 개 파일의 해시 값이 동일하다면 동일한 파일이라고 추론 가능하다.

정답 3번

간단한 해설

해시는 **무결성 검증과 알려진 파일의 식별**에 이용된다. 외장장치 연결과 같은 사용 흔적은 레지스트리·로그 등 관련 아티팩트를 분석해야 한다.

선지별 해설

① O — 해시는 암호화처럼 복호화하여 원문을 되찾는 방식이 아닌 **일방향 요약 함수**이다. 다만 원문의 '원론적으로 불가능'은 해시값만으로 원문을 유일하게 복원하는 역함수가 없다는 취지로 읽어야 한다. 안전한 암호학적 해시의 역상 저항성은 입력을 찾는 것이 계산상 어렵다는 성질이며, 후보가 적으면 추측한 입력의 해시를 대조할 수 있다.

② O — 수집 전후나 원본·사본의 해시값을 비교하여 **데이터의 변경 여부와 무결성**을 검증하는 데 이용한다. 동일한 알고리즘과 동일한 바이트 범위를 대상으로 계산하고, 기준 해시값 자체도 신뢰할 수 있게 보관해야 한다.

③ X — **해시 검색**은 파일의 해시값을 알려진 해시 목록과 비교하여 동일한 내용의 파일 후보를 식별·선별하는 방법이다. 외장장치 연결 등 시스템 사용 흔적은 레지스트리·이벤트 로그 등 해당 아티팩트를 분석해야 하며, 해시 검색 자체가 그 행위를 해석하는 것은 아니다.

④ O — 충돌 저항성이 충분한 해시를 적절히 사용하면 해시값 일치는 **내용의 동일성을 추론하는 강한 근거**가 된다. 그러나 서로 다른 입력이 같은 해시값을 갖는 충돌은 가능하므로 수학적인 절대 증명은 아니며, 파일명·경로 등 해시 계산 대상 밖의 정보까지 같다는 뜻도 아니다.

NoteBase

문 16. 슬랙 공간(slack space)에 대한 설명으로 가장 적절하지 않은 것은?

① 파일 시스템 할당 크기와 볼륨 크기 간의 차이로 인해 발생되는 공간을 파일 시스템 슬랙이라고 한다.

② 램 슬랙을 이용하면 파일의 끝을 알 수 있고, 삭제된 파일을 복구할 때 유용하게 사용된다.

③ 파일 슬랙을 이용하면 특정 파일이 해당 매체에 존재하였는지를 규명할 수 있다.

④ 볼륨 슬랙은 파티션 크기의 변경을 통해 임의로 생성이 불가능하다.

정답 4번

간단한 해설

파티션의 크기나 배치를 조정하면 파티션에 포함되지 않는 공간을 의도적으로 남길 수 있다. 따라서 볼륨 슬랙은 **파티션 크기 변경을 통해 생성할 수 있다**.

선지별 해설

① O: 파일 시스템이 관리하도록 할당된 영역이 볼륨 전체를 채우지 못하면 그 경계 사이에 남는 공간이 생긴다. 이러한 **파일 시스템 영역과 볼륨 크기의 차이**에서 생기는 공간을 파일 시스템 슬랙이라고 한다.

② O: 램 슬랙은 파일의 실제 데이터가 끝나는 지점부터 해당 섹터의 끝까지 남는 공간이다. 따라서 파일 끝과 섹터 경계를 구별하는 분석 단서가 되며, 다른 파일 구조 정보와 함께 삭제 파일의 경계를 판단하고 복구하는 데 활용할 수 있다. 다만 0으로 채워지는 경우도 있어 **슬랙만으로 파일 끝이나 복구를 항상 확정할 수는 없다**.

③ O: 파일 슬랙은 파일의 실제 끝부터 마지막으로 할당된 클러스터의 끝까지 남는 공간이다. 덮어쓰이지 않은 과거 파일의 일부가 남아 있다면 그 내용을 분석하여 **해당 매체에 파일이 존재했던 흔적**을 확인할 수 있다. 다만 흔적이 항상 남거나 파일 전체가 복구되는 것은 아니다.

④ X: 볼륨 슬랙은 볼륨을 파티션들로 나누고 남는 공간으로, 파티션의 크기나 배치를 조정하여 의도적으로 남길 수 있다. 따라서 **파티션 크기 변경으로 생성이 가능**하며, 임의로 생성할 수 없다는 설명은 틀리다.

NoteBase

문 17. 네트워크 증거 수집 시에, 정보를 획득하기 위한 명령으로 가장 적절하지 않은 것은?

① netstat -r: 라우팅 테이블 정보

② net share: 외부 접속 사용자 목록

③ set user: 현재 로그인한 사용자의 도메인, 이름, 프로파일

④ ipconfig: IP 설정 정보

정답 2번

간단한 해설

net share는 외부 접속 사용자 목록이 아니라 **로컬 컴퓨터의 공유 자원**을 보여 준다. 연결된 클라이언트 세션과 사용자 정보는 net session으로 확인할 수 있다.

선지별 해설

① O: netstat -r은 **IP 라우팅 테이블**을 표시한다. 목적지 네트워크로 패킷을 보낼 때 사용하는 경로와 게이트웨이 등의 정보를 확인하는 데 이용한다.

② X: 인수 없이 실행한 net share는 **해당 컴퓨터가 공유하는 자원 목록**을 표시한다. 외부에서 접속한 사용자 목록을 표시하는 명령으로 설명한 것은 잘못이다. 로컬 컴퓨터에 연결된 클라이언트의 세션과 사용자 정보를 확인하는 대표적인 명령은 net session이며, 모든 종류의 외부 접속을 이 명령 하나로 확인할 수 있다는 뜻은 아니다.

③ O: Windows 명령 프롬프트에서 set user는 이름이 USER로 시작하는 **현재 프로세스의 환경 변수**를 표시한다. 일반적인 사용자 환경에서는 USERDOMAIN, USERNAME, USERPROFILE을 통해 도메인·사용자 이름·프로파일 경로를 확인할 수 있다. 이는 환경 변수 값의 조회이므로 변경 가능성이 있으며, 시스템 전체의 로그인 세션을 나열하거나 사용자 신원을 독립적으로 인증하는 명령은 아니다.

④ O: 인수 없이 실행한 ipconfig는 어댑터의 **IP 주소·서브넷 마스크·기본 게이트웨이** 등 기본 TCP/IP 설정을 표시한다. 더 상세한 어댑터와 DNS 등의 설정은 ipconfig /all로 확인할 수 있다.

NoteBase

문 18. 침해 사고가 발생한 컴퓨터의 전자우편(E-mail) 분석 시, 전자우편 헤더에서 확인할 수 있는 것으로 가장 적절하지 않은 것은?

① 송신자가 이용한 메일 서버

② 전자우편을 보낸 시간

③ 전자우편이 경유한 라우터 목록

④ 송신자의 IP 주소

정답 3번

간단한 해설

전자우편 헤더는 메일 서버의 전달 기록과 시각 등을 담지만, **패킷이 경유한 라우터 목록**을 담는 기록은 아니다. 메일 서버 경로와 네트워크 계층의 라우터 경로를 구별해야 한다.

핵심 풀이

전자우편 헤더의 Received 필드는 메일을 받은 서버가 덧붙이는 전달 기록이다. 이를 분석하면 송신자가 이용한 메일 서버와 메일 전달에 관여한 서버의 정보를 확인하는 단서를 얻을 수 있다.

Date 필드는 작성자가 메일을 완성하여 전송할 준비가 되었다고 표시한 시각을 담는다. 보낸 시각을 파악하는 자료가 되지만 실제 네트워크 전송 시각과 반드시 같지는 않으므로, **Received의 처리 시각과 함께 대조**한다.

Received 등의 헤더에는 연결한 호스트의 IP 주소가 기록될 수 있어 송신 측 IP를 추적하는 단서가 된다. 다만 웹메일이나 중계 서버를 이용하면 서버 주소만 보일 수 있으므로 **최초 사용자의 IP가 항상 노출되는 것은 아니다**.

메일 서버 사이의 전달 경로와 IP 패킷이 통과한 라우터 경로는 서로 다르다. 일반적인 전자우편 헤더는 **경유한 라우터 전체 목록을 기록하지 않는다**. 따라서 가장 적절하지 않은 항목은 ③이다.

NoteBase

문 19. 디지털 포렌식에서 증거 입증을 위해서는 우선 무결성이 입증되어야 하는데, 현장에서 무결성 입증을 위한 절차 중 가장 적절하지 않은 것은?

① 생성된 이미지 파일에 대한 해시 값을 계산하여 피압수자가 해시 값이 기재된 서면에 서명하게 한다.

② 피압수자가 입회한 상태에서 봉인을 푼 다음, 인케이스(EnCase)와 같은 인증된 포렌식 도구를 사용하여 압수한 저장매체에 대한 이미지 파일을 생성한다.

③ 하드 디스크 등의 저장매체를 압수한 뒤, 피압수자의 서명이 없어도 봉인 후 운송할 수 있다.

④ 피의자가 공판과정에서 무결성을 부정하는 경우에는 압수한 저장장치의 해시 값과 이미지 파일의 해시 값을 비교할 수 있도록 법원에 검증을 요구한다.

정답 3번

간단한 해설

증거의 무결성은 **압수부터 운송·분석까지의 변경 방지와 확인 기록**으로 뒷받침한다. 통상적인 확인·서명 절차를 이유 없이 생략하는 것은 적절하지 않지만, 서명이 없다는 사실만으로 무결성이 반드시 부정되는 것은 아니다.

선지별 해설

① O — 이미지 생성 후 해시값을 계산하고 원본과의 동일성을 확인하여 **당사자의 확인·서명 기록**을 남기는 것은 무결성 입증에 도움이 된다. 단순히 숫자를 적는 데 그치지 않고 어떤 대상과 범위를 어떤 방법으로 계산·대조했는지 확인해야 한다.

② O — 입회하에 봉인 상태를 확인하고 해제한 뒤, **신뢰성이 검증된 도구**로 이미징하는 것은 처리 과정을 설명할 근거가 된다. 원문의 '인증된'은 도구의 신뢰성을 강조한 표현이며, 특정 제품명이나 인증만으로 결과의 정확성이 자동 보장되는 것은 아니다. 쓰기방지와 작업 기록 등도 함께 확보한다.

③ X — 이 문항이 묻는 통상적인 무결성 확보 절차에서는 **당사자 등의 확인·서명을 받아 봉인**하고 운송·인계 상태를 기록해야 하므로, 그 확인을 이유 없이 생략해도 된다는 설명이 가장 부적절하다. 다만 서명 거부 등으로 확인서면 확보가 불가능하거나 현저히 곤란한 때까지 압수·운송이 절대 불가능하다는 뜻은 아니다. 대법원 2013도2511은 절차 참여자의 증언이나 원본 대조 등 다른 방법으로도 무결성·동일성을 입증할 수 있다고 보았다.

④ O — 무결성이 다투어지면 **법원의 검증을 통해 원본과 사본을 대조**하는 방법을 사용할 수 있다. 해시 비교는 같은 바이트 범위를 대상으로 해야 하며, 압축·메타데이터를 포함하는 이미지 컨테이너 파일 전체의 해시를 원본 매체의 해시와 무조건 같다고 보는 것은 잘못이다.

NoteBase

문 20. 디지털 포렌식 조사 과정이 필요한 경우로 가장 적절하지 않은 것은?

① 치료 중인 환자가 잘못된 약품 투여로 사망하자, 담당 의사가 컴퓨터에 저장되어 있는 환자의 처방전 내용을 변경하였다.

② 버스 안에서 휴대폰 카메라로 옆자리에 앉은 다른 사람의 신체를 몰래 촬영한 후, 촬영한 사진 파일을 삭제하였다.

③ 검찰에서 압수·수색이 나올 것을 염려하여, 공무원에게 제공한 뇌물 내역을 정리한 엑셀 파일을 삭제하였다.

④ 타인의 주민등록증을 이용하여 스마트폰 대리점 직원을 속이고 스마트폰을 개통하였다.

정답 4번

간단한 해설

디지털 자료의 변경·삭제가 명시된 사례는 흔적 분석이나 복구의 필요성이 직접 드러난다. 신분증을 이용한 명의도용 개통은 제시문상 **신원·서류·진술 확인이 중심**이라는 점에서 구별된다.

선지별 해설

① O. 컴퓨터에 저장된 처방전이 변경되었으므로 **변경 전 내용과 변경 흔적**을 확인하는 디지털 포렌식 조사가 직접 필요하다. 저장된 기록·백업·수정 이력 등을 대조하여 언제 어떤 내용이 바뀌었는지 분석할 수 있다.

② O. 삭제된 사진은 휴대폰의 저장 영역이나 관련 흔적에 남아 있을 가능성이 있으므로 **삭제 사진의 복구·잔존 흔적 분석**이 필요하다. 다만 삭제된 파일이 언제나 복구되는 것은 아니며, 저장 방식·덮어쓰기·암호화 상태 등에 따라 결과가 달라진다.

③ O. 삭제한 엑셀 파일에 뇌물 내역이 담겨 있으므로 **파일 복구와 관련 기록의 분석**이 직접적인 조사 과제이다. 원본의 상태를 보존하면서 사본·백업·잔존 데이터 등을 확인하여 내용을 검토할 수 있다.

④ X. 제시된 사실에서는 타인의 신분증을 사용한 경위, 본인 확인 절차, 신청·계약 서류와 직원 진술 등의 확인이 중심이다. 앞의 사례들과 달리 **디지털 자료의 변경·삭제 분석 필요성이 직접 제시되지 않았다**는 점에서 상대적으로 덜 적절하다. 다만 실제 사건에서는 전자 가입 기록이나 접속 기록 등도 증거가 될 수 있으므로, 명의도용 개통 사건에는 디지털 포렌식이 전혀 필요 없다고 일반화해서는 안 된다.

따라서 제시된 상황의 직접적인 조사 필요성을 비교하면 ④가 가장 적절하지 않다.

NoteBase