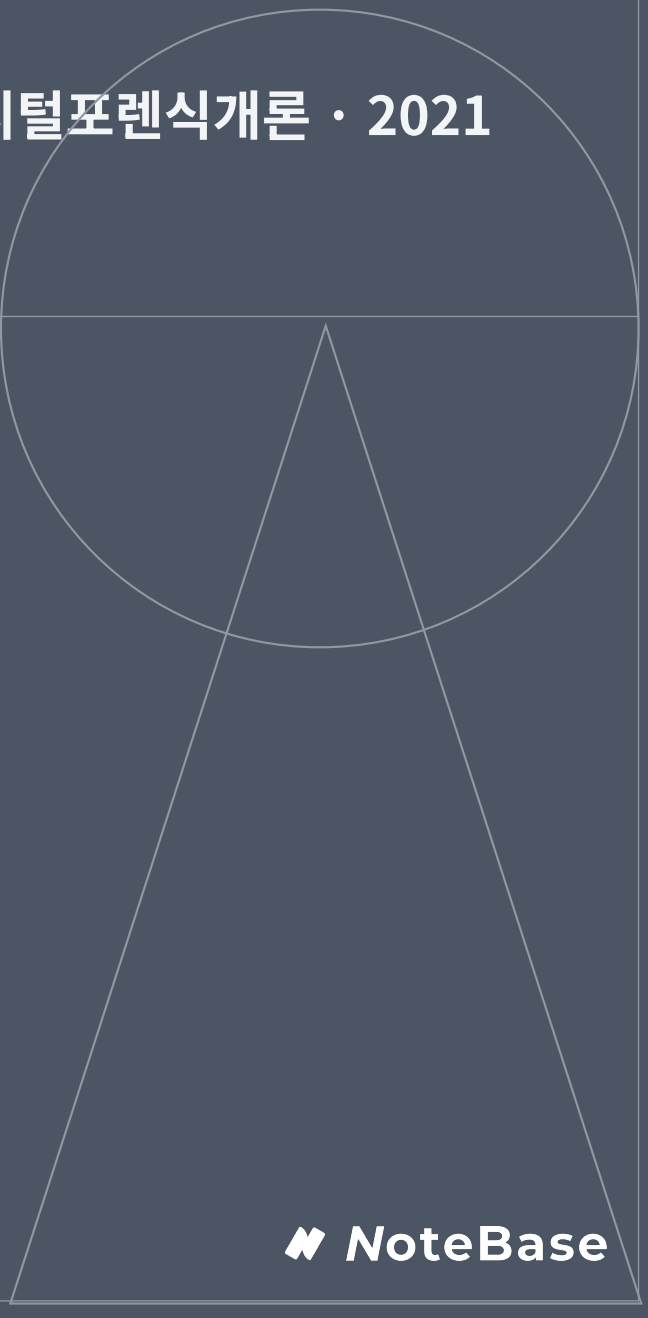
기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2021



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2021

공무원/경찰/경력채용 · 디지털포렌식개론 · 2021

문 1. 사이버범죄 포렌식 분석 보고서가 법정에서 증거로 채택되기 위한 기본원칙으로 가장 적절하지 않은 것은?

① 구현의 원칙: 법정에서 다시 네트워크에 접속하여 범행을 시연하면, 사이버범죄 현장과 같은 범죄 행위가 구현되어야 한다.

② 정당성의 원칙: 수사관이 해킹하여 수집한 범죄 집단의 디지털 증거는 증거능력이 인정되기 어렵다.

③ 무결성의 원칙: 수집 당시의 증거자료 해시값과 법정제출 시점의 증거자료 해시값은 반드시 일치해야 한다.

④ 연계보관성의 원칙: 수집된 증거자료의 이송-보관-분석-법정 제출의 각 단계에서 담당자의 확인이 있어야 한다.

정답 1번

①

재현성은 **동일한 증거를 같은 조건과 절차로 분석하면 동일한 결과를 얻을 수 있어야 한다**는 원칙이다. 법정에서 네트워크에 다시 접속하여 범죄행위 자체를 구현해야 한다는 뜻이 아니다.

②

정당성은 디지털 증거를 **적법한 절차로 수집해야 한다**는 원칙이다. 수사 목적이라도 위법한 해킹으로 수집한 증거는 원칙적으로 증거능력이 배제된다.

형사소송법 제308조의2(위법수집증거의 배제) 적법한 절차에 따르지 아니하고 수집한 증거는 증거로 할 수 없다.

③

무결성은 증거자료가 수집 이후 법정 제출까지 **변경·훼손되지 않고 보존되는 성질**이다. 동일한 증거자료의 해시값은 변하지 않아야 하므로, **수집 시점과 법정 제출 시점의 해시값을 비교**하여 이를 확인한다.

④

연계보관성은 증거의 수집부터 법정 제출까지 **각 단계의 담당자·인계인수·취급 내역을 기록하고 확인**하여 증거가 바뀌거나 섞이지 않았음을 추적할 수 있게 하는 원칙이다.

NoteBase

문 2. 전자적 증거(디지털 증거)의 특징에 대한 설명으로 가장 적절하지 않은 것은?

① 전자적 증거는 저장매체에 독립된 정보 내용이 증거가 된다.

② 전자적 증거는 삭제, 변경, 훼손 등 변조가 쉽다.

③ 인위적으로 생성되는 전자적 증거로는 문서 파일, 인터넷 사이트 접속 기록 등이 있다.

④ 전자적 증거는 공간을 초월하여 전송되므로 관할권의 문제와 국경을 넘을 경우 국가의 주권문제까지 연관 될 수 있다.

정답 3번

간단한 해설

인터넷 사이트 접속 기록은 보통 사용자가 직접 작성하는 문서와 달리 **시스템·프로그램이 자동으로 생성**한다. 사람이 사이트에 접속했다는 사실만으로 그 기록을 인위적 작성 자료로 분류하지 않는다.

선지별 해설

① O: 디지털 증거에서는 물리적 저장매체 자체와 구별되는 **정보의 내용**이 핵심이다. 같은 데이터를 다른 매체에 복제하더라도 내용의 동일성이 유지될 수 있다는 매체 독립성을 가진다.

② O: 디지털 데이터는 조작이나 시스템 동작으로 삭제·변경되기 쉽다. 따라서 원본 보존, 변경 방지, 해시값 비교 등의 방법으로 수집·분석 과정의 무결성을 확인해야 한다.

③ X: 사용자가 직접 작성한 문서 파일은 인위적으로 생성한 정보이지만, 인터넷 사이트 접속 기록은 일반적으로 **사용자 활동에 따라 시스템이나 프로그램이 자동 생성**한 정보이다. 접속 행위를 사람이 했다는 것과 접속 기록을 직접 작성했다는 것은 구분한다.

④ O: 디지털 정보는 네트워크를 통해 국경을 넘어 전송되거나 여러 국가의 서버에 저장될 수 있다. 반면 수사권 행사는 영토적 제한을 받으므로, 증거에 접근·수집하는 과정에서 관할권과 다른 국가의 주권 문제가 생길 수 있다.

NoteBase

문 3. 사이버 도박 범죄 현장에서 수사관의 휘발성 데이터 수집 방법에 대한 설명으로 가장 적절하지 않은 것은?

① 범죄 현장의 컴퓨터에서 사용자를 분리시키고, 현재 화면과 시스템을 사진으로 촬영한다.

② 데이터 증거수집은 우선 '디스크 정보→시스템 메모리→라우팅 테이블 정보' 순서로 한다.

③ 현재 네트워크에 연결된 시스템의 시간과 로그인, 사용자 정보를 확인한다.

④ 현재 네트워크에 연결된 시스템의 IP 주소를 확인한다.

정답 2번

간단한 해설

라우팅 테이블과 메모리 같은 **휘발성 정보는 디스크 정보보다 먼저 확보**하는 것이 원칙이다. 디스크를 우선 수집하다가 변동하거나 사라질 수 있는 정보를 놓치지 않아야 한다.

선지별 해설

① O: 사용자가 컴퓨터를 계속 조작하면 화면·프로세스·파일 등의 상태가 바뀔 수 있으므로 **추가 조작을 막고 현 상태를 기록**해야 한다. 화면과 시스템의 사진은 현장 상태를 설명하는 자료가 된다. 사용자를 분리한다는 것은 곧바로 전원을 끄라는 뜻이 아니다.

② X: 증거는 원칙적으로 **변경·소실이 빠른 휘발성 정보부터** 수집한다. 라우팅 테이블 등 현재 실행 상태와 시스템 메모리의 정보는 변동하거나 전원 차단으로 사라질 수 있으므로, 비교적 지속성이 있는 디스크 정보를 먼저 수집하도록 한 순서는 부적절하다. 구체적인 실행 순서는 시스템 상태와 수집의 영향을 고려하되, 휘발성 정보를 디스크보다 뒤로 미루지 않는 것이 핵심이다.

③ O: 시스템 시간은 기록된 사건 시각을 해석하는 기준이고, 로그인·사용자 정보는 **현재 세션과 사용 상태**를 파악하는 단서이다. 시간이 지나거나 세션이 끝나면 달라질 수 있으므로 현장에서 확인·기록한다. 시스템 시각과 신뢰할 수 있는 기준 시각의 차이도 함께 남겨야 한다.

④ O: 현재 IP 주소는 **시스템과 네트워크 접속 기록을 연결**하는 단서이다. 동적 주소 할당이나 연결 변경으로 달라질 수 있으므로 당시 값을 수집한다. IP 주소만으로 특정 사람의 행위를 확정하지 않고 다른 접속·사용 기록과 대조한다.

NoteBase

문 4. 수사관이 증거로 확보한 시스템에서 웹 브라우저와 관련된 데이터를 조사하고 있다. 이에 대한 설명으로 가장 적절하지 않은 것은?

① 웹 히스토리(Web History)에는 사용자가 방문한 웹 사이트의 내역이 저장된다.

② 쿠키(Cookie)에는 사용자가 만든 동영상이 자동으로 저장된다.

③ 웹 캐시(Web Cache)에는 웹 사이트 방문 시에 빠른 재접속을 위하여 이미지 파일 등이 자동으로 저장된다.

④ 임시 인터넷 파일(Temporary Internet File)에는 임시 파일의 URL, 임시 파일의 이름, 임시 파일의 저장위치 등이 저장된다.

정답 2번

간단한 해설

쿠키는 **세션 식별이나 사용자 설정 등에 쓰는 작은 데이터**이다. 사용자가 만든 동영상 파일을 자동으로 저장하는 기능이 아니다.

선지별 해설

① O: 웹 히스토리는 방문한 페이지의 URL과 방문 시각 등 웹 사이트 이용 내역을 저장하는 기록이다. 삭제나 사생활 보호 모드 등의 영향으로 모든 방문이 반드시 남는 것은 아니므로, 확보된 기록의 범위 안에서 이용 행위를 해석한다.

② X: 쿠키는 사이트가 세션 식별, 로그인 상태 유지, 사용자 환경설정 등에 이용하는 **작은 데이터**이다. 사용자가 만든 동영상 파일을 자동으로 보관하는 저장소가 아니다. 동영상 자체의 저장 여부는 별도의 파일 저장·다운로드·웹 캐시 등의 흔적에서 확인해야 한다.

③ O: 웹 캐시는 페이지의 이미지·스크립트 등 재사용 가능한 리소스를 저장하여, 다시 필요할 때 서버에서 같은 내용을 재전송받는 비용과 지연을 줄인다. 다만 **캐시 정책과 유효기간에 따라 저장·재사용 여부가 달라지며**, 모든 방문 자료가 항상 저장되는 것은 아니다.

④ O: 임시 인터넷 파일을 관리하는 캐시 기록에는 원본 URL, 로컬 파일 이름·경로 등 저장된 자료를 식별하는 정보가 포함될 수 있다. 이를 통해 캐시 파일과 원래 웹 리소스를 연결한다. 이러한 정보는 **캐시의 관리 기록·메타데이터**에 해당하며, 모든 이미지나 임시 파일의 본문 안에 URL과 저장경로가 직접 들어 있다는 뜻은 아니다.

NoteBase

문 6. 메타 데이터(Meta data)는 NTFS가 볼륨을 관리하기 위한 파일이다. ㉠~㉣에 해당하는 용어를 순서대로 나열한 것으로 가장 적절한 것은?

㉠ MFT entry의 복사본을 별도로 저장
㉡ 볼륨에서 사용되는 속성에 대한 정보를 저장
㉢ 파일이나 디렉터리의 변경 사항에 대한 정보를 저장
㉣ 파일 시스템의 루트 디렉터리에 대한 정보를 저장

① ㉠: $UsnJrnl, ㉡: $MFTMirr, ㉢: $., ㉣: $AttrDef
② ㉠: $AttrDef, ㉡: $., ㉢: $UsnJrnl, ㉣: $MFTMirr
③ ㉠: $., ㉡: $UsnJrnl, ㉢: $MFTMirr, ㉣: $AttrDef
④ ㉠: $MFTMirr, ㉡: $AttrDef, ㉢: $UsnJrnl, ㉣: $.

정답 4번

간단한 해설

MFT 앞부분의 복사본은 **$MFTMirr**, 속성 정의는 **$AttrDef**, 변경 기록은 **$UsnJrnl**이다. 이 세 대응을 만족하는 선지는 ④이다. 마지막 $.은 원문이 루트 디렉터리를 가리키려 사용한 표기로, 실제 이름 표기인 점(.)과 구별해야 한다.

대응 관계 해설

㉠은 **$MFTMirr**이다. MFT의 복구에 필요한 앞부분 레코드의 복사본을 별도로 보관한다. 모든 사용자 파일의 MFT 엔트리를 전부 복제한 파일이라는 뜻은 아니며, 대표적으로 처음 네 레코드의 백업을 말한다.

㉡은 **$AttrDef**이다. NTFS가 사용하는 속성의 이름·식별번호·크기 제한 등 속성 정의 정보를 저장한다. 개별 파일 내용이나 파일 변경 이력을 보관하는 역할과 구별된다.

㉢은 **$UsnJrnl**이다. 파일이나 디렉터리의 생성·삭제·이름 변경 등 변경 사실을 기록하는 변경 저널이다. 변경 사유와 식별 정보 등을 남기는 것이지, 변경 전후의 모든 파일 내용을 그대로 백업하는 것은 아니다.

㉣은 **루트 디렉터리**를 가리킨다. 원문 선지는 이를 **$.**으로 표기했지만, 실제 루트 디렉터리의 이름 표기는 점(.)이며 루트 경로는 역슬래시로 나타낸다. 따라서 원문의 $. 표기는 정확한 파일명으로 외우지 말고, 이 문항에서 루트 디렉터리를 가리키려는 표기로 구별해야 한다.

앞의 세 대응인 **$MFTMirr → $AttrDef → $UsnJrnl**을 모두 만족하는 선지는 ④뿐이다. 여기에 원문이 $.으로 제시한 루트 디렉터리를 대응시키면 제시된 정답 ④가 된다.

NoteBase

문 7. 디지털 데이터를 포렌식 증거자료로 사용하기 위해 가장 쉽게 복구할 수 있는 경우로 가장 적절한 것은?

① 임의의 숫자로 증거 데이터를 덮어쓰고, 첫 번째 숫자의 보수로 다시 덮어쓴 후, 임의의 숫자로 덮어쓰는 방식을 7회 이상 반복한 자료

② 웹 검색에 사용되는 index.dat 파일을 삭제하고, 최근 사용문서, 열람문서 보관하는 기능도 삭제하며, 히스토리나 캐시에 들어있는 정보를 삭제하고, 자동삭제 기능으로 삭제한 자료

③ 윈도우에서 마우스 오른쪽 버튼을 클릭 '삭제'하여 휴지통으로 이동한 자료

④ 증거 데이터가 있는 하드디스크에 디가우징(degaussing) 방법을 적용한 자료

정답 3번

간단한 해설

파일을 **휴지통으로 이동한 것만으로는 내용을 완전히 지우지 않는다**. 휴지통에 남아 있는 파일은 복원할 수 있으므로 덮어쓰기나 디가우징을 한 자료보다 복구가 쉽다.

선지별 해설

① 반복 덮어쓰기: 저장된 원래 데이터를 다른 값으로 바꾸는 방식이다. 대상 영역에 덮어쓰기가 정상적으로 이루어졌다면 단순 삭제보다 원래 내용의 복구가 어렵다. 제시된 7회 이상이라는 횟수가 모든 매체에 필요한 보편적 기준이라는 뜻은 아니다.

② 사용 흔적 삭제: 접속 이력·캐시·최근 문서 기록 등을 제거한 상태이다. 남은 데이터나 다른 기록을 분석하여 일부 복구할 가능성은 있지만, 삭제 방식과 이후 덮어쓰기 여부에 따라 결과가 달라진다. 휴지통에 그대로 남아 있는 파일보다 복구 절차가 복잡하다.

③ 휴지통으로 이동: 문제에서 파일이 휴지통에 이동한 상태라고 명시했으므로, 휴지통을 비우거나 추가 삭제하지 않았다면 **파일 내용이 남아 있어 복원이 쉽다**. 원래 데이터 영역을 덮어쓰거나 자기적 기록을 제거한 경우와 구별한다.

④ 디가우징: 강한 자기장으로 자기식 하드디스크의 기록을 제거하는 방식이다. 매체에 적합한 조건으로 처리되었다면 데이터 복구가 매우 어렵고, 디스크 자체도 사용할 수 없게 될 수 있다.

따라서 제시된 경우 중 가장 쉽게 복구할 수 있는 것은 휴지통으로 이동한 자료인 ③이다.

NoteBase

문 8. 슬랙 공간(Slack Space)은 파일에 할당된 물리적 공간이 논리적으로는 사용할 수 없는 공간을 말한다. 이전에 사용한 데이터가 남아 있을 가능성이 없는 슬랙 공간으로서 가장 적절한 것은?

① 램 슬랙(RAM Slack)

② 파일 시스템 슬랙(File System Slack)

③ 드라이브 슬랙(Drive Slack)

④ 볼륨 슬랙(Volume Slack)

정답 1번

간단한 해설

램 슬랙은 일반적인 현대 운영체제에서 0으로 채워지는 영역이다. 마지막 사용 섹터의 빈 부분을 이렇게 채우므로, 과거 데이터가 남을 수 있는 미사용 섹터나 비할당 공간과 구별된다.

개념 구분

램 슬랙은 파일의 논리적 끝에서 그 파일이 마지막으로 사용한 섹터의 끝까지 남는 공간이다. 파일의 마지막 부분을 섹터 단위로 기록할 때 생기는 빈 부분이며, **일반적인 현대 운영체제에서는 0으로 채운다**. 따라서 사용하지 않은 디스크 영역을 그대로 남겨 두는 다른 슬랙과 달리, 종전 데이터가 잔존할 가능성이 없는 공간을 찾는 이 문항에서는 램 슬랙이 구별된다.

드라이브 슬랙은 마지막 사용 섹터의 다음부터 할당된 클러스터 끝까지의 공간이다. 파일 내용이 기록되지 않은 섹터가 남으므로 **과거에 기록된 데이터가 잔존할 수 있다**.

파일 시스템 슬랙은 볼륨 내부에서 파일 시스템의 할당 단위로 사용되지 못하고 남는 공간이다. 볼륨 크기와 파일 시스템이 실제 사용하는 공간의 차이에서 발생하며, 사용되지 않는 영역에 종전 데이터가 남을 수 있다.

볼륨 슬랙은 이 문항의 구분에서 디스크 전체 공간 중 파티션으로 할당되지 않고 남은 영역이다. 파티션 밖의 공간을 모두 지웠다는 보장이 없으므로 종전 데이터가 남을 수 있다.

이와 같은 일반적인 슬랙의 구분에 대응하는 선택지는 ①이다. 다만 RAM 슬랙의 0 채움은 모든 역사적 운영체제에 공통된 성질은 아니다. 일부 구형 운영체제에서는 파일과 무관한 RAM 내용이 기록되기도 하므로, '가능성이 없다'를 모든 운영체제에 대한 절대 명제로 확대해서는 안 된다.

NoteBase

문 9. 스마트폰 압수 현장에서 수사관의 주의 사항에 대한 설명으로 가장 적절하지 않은 것은?

① 압수수색 현장에서 스마트폰의 잠금해제에 대한 정보를 확인해야 한다.

② 압수수색 후 현장에서 스마트폰의 전원을 다시 켜서, 스마트폰의 정상작동 여부를 확인해야 한다.

③ 사용자가 스마트폰 보안설정을 한 경우, 암호정보를 확보해야 한다.

④ 스마트폰을 비행기 모드로 설정하고, WiFi를 비활성 모드로 한다.

정답 2번

간단한 해설

꺼진 스마트폰을 현장에서 다시 켜면 **부팅과 통신으로 증거 데이터가 변경될 수 있다**. 정상작동 확인을 위해 임의로 전원을 켜기보다 발견 상태를 기록·보존하고 적절한 획득 절차를 적용한다.

선지별 해설

① O: 잠금 상태와 해제 방식·관련 정보를 현장에서 확인하면 이후 증거 획득 가능성을 판단하는 데 도움이 된다. 잠금해제 정보를 모른 채 임의로 반복 입력하면 접근 제한이나 데이터 손실 위험을 높일 수 있으므로, 상태를 기록하고 적법한 절차로 필요한 정보를 확인한다.

② X: 정상작동 여부를 확인한다는 이유만으로 **꺼진 스마트폰의 전원을 다시 켜서는 안 된다**. 부팅 과정에서 파일·로그가 바뀌거나 통신이 재개되어 증거 상태에 영향을 줄 수 있다. 발견 당시 전원·잠금 상태를 기록하고 불필요한 조작을 피한 뒤 전문가의 획득 절차에 따른다. 이는 이미 켜진 기기를 무조건 끄라는 뜻도 아니다.

③ O: 보안설정이 적용되어 있으면 암호정보는 잠금해제나 암호화된 데이터 접근에 중요하므로, 법적으로 허용되는 절차와 범위에서 확보할 필요가 있다. 해당 정보의 확보 필요성을 말하는 것이지, 이 문장만으로 강제 제공 의무나 무제한 접근 권한이 생기는 것은 아니다.

④ O: 비행기 모드 설정과 WiFi 비활성화는 **외부 통신에 따른 원격 삭제·변경을 막기 위한 격리 조치**이다. 이미 켜져 있고 조작 가능한 기기에서 상태를 기록하며 적용한다. 비행기 모드만으로 모든 무선 기능이 꺼진다고 단정하지 말고 Bluetooth 등의 상태도 확인한다. 꺼진 기기를 이 설정을 위해 켜거나, 잠긴 기기를 무리하게 조작하지는 않는다.

NoteBase

문 10. 파일 카빙(File Carving)은 삭제된 파일을 복구하는 방법 중 하나이다. 파일 카빙에 대한 설명으로 가장 적절하지 않은 것은?

① 파일 카빙은 파일의 메타 데이터를 활용하지 않고 파일의 고유한 정보를 이용하여 복구한다.

② 램 슬랙 카빙은 미들 시그니처(Middle Signature)를 활용하는 방법이다.

③ 파일 구조체 카빙은 파일 포맷 내부에 여러 개의 시그니처가 존재할 수 있으므로 파일 구조를 분석하여 카빙하는 방법이다.

④ 파일 카빙은 디스크의 비할당영역에 있는 파일 조각을 조합하여 삭제된 내용을 복구하는 방법이다.

정답 2번

간단한 해설

램 슬랙 카빙은 **파일 끝과 섹터 경계 사이의 패딩**을 복구 단서로 이용한다. 파일 내부에 있는 미들 시그니처를 사용하는 방식과 구별해야 한다.

선지별 해설

① O. 파일 카빙은 파일명·위치·할당 정보와 같은 **파일시스템 메타데이터에 의존하지 않고** 데이터 자체의 시그니처와 내부 구조 등을 이용하여 파일을 찾아 복구한다. 여기서 메타데이터를 사용하지 않는다는 말은 파일 내부의 크기 필드나 구조 정보까지 모두 배제한다는 뜻이 아니다.

② X. 램 슬랙 카빙은 파일 끝에서 마지막 섹터 끝까지의 **램 슬랙에 나타나는 패딩을 파일 경계의 단서**로 활용하는 방식이다. 예를 들어 해당 영역이 0x00으로 채워지는 환경에서는 이 패턴을 헤더 등 다른 단서와 함께 활용할 수 있다. 파일 내부의 미들 시그니처를 이용하는 방법과 동일하지 않으며, 0 바이트가 있다는 사실만으로 파일 끝을 확정해서도 안 된다.

③ O. 파일 내부에 여러 시그니처가 있으면 단순 패턴 검색만으로 파일 경계를 잘못 판단할 수 있다. 파일 구조체 카빙은 **파일 포맷의 내부 구조와 필드 관계**를 분석하여 유효한 데이터를 구분하고 복구 범위를 판단한다.

④ O. 비할당 영역에 남은 파일 데이터나 조각을 찾아 삭제 내용을 복구하는 것은 파일 카빙의 대표적인 활용이다. 다만 **조각의 존재가 완전한 복구를 보장하지는 않으며**, 단편화·덮어쓰기와 포맷 특성에 따라 복구가 제한된다. 카빙 대상도 비할당 영역에만 한정되지는 않는다.

따라서 램 슬랙 카빙을 미들 시그니처 활용 방법으로 설명한 ②가 가장 적절하지 않다.

NoteBase

문 11. 스마트폰 데이터의 논리적인 추출 방법으로 가장 적절하지 않은 것은?

① 탈옥(jailBreak)

② 루팅(Rooting)

③ Backup 메커니즘을 이용한 데이터추출

④ Rawshark의 필드 집합 출력

정답 4번

간단한 해설

Rawshark의 필드 집합 출력은 **네트워크 패킷 데이터의 분석** 기능이다. 스마트폰의 파일·앱 데이터 등을 논리적으로 추출하는 방법과는 다르다.

선지별 해설

① O: 탈옥은 iOS의 접근 제한을 완화하여 일반 상태에서 접근하기 어려운 파일이나 데이터에 접근하는 데 활용될 수 있다. 탈옥 자체가 추출 완료를 뜻하는 것은 아니며, 이 문항에서는 데이터 추출을 가능하게 하는 접근권한 확보 수단으로 제시되었다.

② O: 루팅은 안드로이드에서 높은 권한을 확보하여 보호된 파일·앱 데이터에 접근할 수 있게 하는 수단이다. 이후 확보한 권한으로 데이터를 수집하며, 루팅 자체와 논리적 데이터 추출 작업은 구분한다. 탈옥·루팅은 기기 상태를 변경할 수 있으므로 증거 보존에 미치는 영향도 고려한다.

③ O: 백업 메커니즘은 운영체제나 앱이 제공하는 기능으로 파일·설정·앱 데이터 등을 수집하는 데 활용한다. 저장매체 전체를 물리적으로 복제하는 방식이 아니라 **백업이 허용하는 논리적 데이터 범위**를 확보한다.

④ X: Rawshark는 원시 pcap 패킷 데이터를 해석하여 지정한 필드 등을 출력하는 네트워크 분석 도구이다. **패킷 필드 출력은 스마트폰 내부 데이터의 논리적 추출과 다르다**. 스마트폰 데이터 수집에는 백업 기능이나 기기·앱 인터페이스 등을 이용한다.

NoteBase

문 12. 윈도우 레지스트리에서 <보기 1>과 <보기 2>를 가장 적절하게 연결한 것은?

<보기 1>
(가) HKEY_CURRENT_CONFIG
(나) HKEY_LOCAL_MACHINE
(다) HKEY_CLASSES_ROOT

<보기 2>
㉠ 시스템 전체에 적용되는 하드웨어와 소프트웨어의 설정 데이터를 저장
㉡ 시스템이 시작할 때 사용되는 하드웨어 프로파일 정보를 저장
㉢ 파일 확장자에 대한 정보, 각 파일과 프로그램 간의 연결정보, 마우스 오른쪽 단추의 등록 정보를 저장

① (가): ㉡, (나): ㉠, (다): ㉢
② (가): ㉢, (나): ㉡, (다): ㉠
③ (가): ㉢, (나): ㉠, (다): ㉡
④ (가): ㉠, (나): ㉢, (다): ㉡

정답 1번

간단한 해설

CURRENT_CONFIG는 현재 하드웨어 프로파일, LOCAL_MACHINE은 시스템 전체 설정, CLASSES_ROOT는 파일 형식·프로그램 연결을 기준으로 구별한다.

대응 관계 해설

(가) HKEY_CURRENT_CONFIG → ㉡: **현재 사용 중인 하드웨어 프로파일**의 정보를 제공한다. 시스템을 시작할 때 선택된 하드웨어 구성과 관련된 키이므로, 시스템 전체의 모든 설정을 가리키는 ㉠과 구별한다.

(나) HKEY_LOCAL_MACHINE → ㉠: **컴퓨터 전체에 적용되는 설정**을 담는다. 특정 로그인 사용자만의 환경 설정이 아니라 하드웨어와 설치된 소프트웨어 등 시스템 차원의 구성 정보를 다루므로 ㉠에 대응한다.

(다) HKEY_CLASSES_ROOT → ㉢: **파일 형식과 프로그램의 연결 및 셸 동작**에 관한 정보를 제공한다. 파일 확장자별 연결 프로그램과 오른쪽 클릭 메뉴 등의 등록 정보가 해당한다. 컴퓨터별·사용자별 클래스 등록 정보를 합쳐 보여 주는 키라는 점에서 현재 하드웨어 프로파일을 나타내는 (가)와 다르다.

따라서 (가)–㉡, (나)–㉠, (다)–㉢으로 연결되므로 정답은 ①이다.

NoteBase

문 13. 스마트폰 포렌식 분석 보고서에 필수적으로 포함되어야 할 사항으로 가장 적절하지 않은 것은?

① 스마트폰 제조사, 모델

② 스마트폰 판매자 정보

③ 스마트폰 증거분석관 정보

④ 스마트폰 접수일시

정답 2번

간단한 해설

분석 보고서에는 **대상 기기 식별 정보, 분석자 정보, 증거 접수일시** 등 분석과 증거 관리에 필요한 사항을 기록한다. 판매자 정보는 사건에 따라 추가할 수 있는 사항이지 공통 필수 항목은 아니므로 ②가 가장 적절하지 않다.

선지별 해설

① (O) **제조사와 모델**은 분석 대상 스마트폰을 식별하고 적용한 분석 방법의 적합성을 확인하기 위한 기본 정보이다. 동일 모델의 다른 기기와도 구별할 수 있도록 일련번호 등 추가 식별 정보를 함께 기록할 수 있다.

② (X) **판매자 정보는 모든 스마트폰 분석 보고서의 공통 필수 항목이 아니다.** 기기의 매매 경위가 사건과 관련되면 기록할 수 있지만, 분석 대상의 식별·분석 책임·증거 접수 이력을 설명하기 위해 항상 필요한 정보는 아니다. 따라서 필수 포함 사항으로 가장 적절하지 않은 것은 ②이다.

③ (O) **증거분석관 정보**는 누가 분석을 수행하고 결과에 책임을 지는지 확인하기 위한 정보이다. 분석자와 작성자를 명확히 기록하면 수행 절차와 보고 내용에 대한 검토·확인이 가능하다.

④ (O) **접수일시**는 분석기관이 증거를 인계받은 시점을 나타낸다. 인계·보관·분석 과정의 시간적 연결을 확인하고 증거 관리 이력을 추적하기 위한 기본 기록이다.

NoteBase

문 14. 안티 포렌식(Anti Forensic) 기법에 대한 설명으로 가장 적절한 것은?

① 삭제된 증거 데이터를 복구한다.

② 암호화된 데이터 파일의 패스워드를 전수 조사한다.

③ 증거 자료에 대한 이미지를 생성할 때 반드시 BitLocker를 꺼야 한다.

④ 운영체제에서 자동으로 생성되는 정보 중에서 증거가 될 만한 모든 정보를 생성 즉시 자동으로 삭제한다.

정답 4번

간단한 해설

안티 포렌식은 **증거를 은닉·훼손하거나 흔적을 제거하여 분석을 어렵게 하는 행위**이다. 삭제 자료 복구나 패스워드 탐색처럼 증거를 확보하는 작업과 구별한다.

선지별 해설

① X: 삭제된 데이터를 복구하는 것은 남아 있는 정보를 찾아 **증거를 확보하는 포렌식 작업**이다. 증거를 숨기거나 없애 분석을 어렵게 하는 안티 포렌식과 목적이 반대이다.

② X: 암호화 파일의 패스워드 후보를 전수 조사하는 것은 파일 내용을 읽기 위해 **접근 가능성을 회복하려는 분석 작업**이다. 암호화를 이용해 내용을 감추는 행위와 암호를 알아내려는 행위를 구별해야 한다.

③ X: 이미징할 때 **BitLocker를 반드시 꺼야 하는 것은 아니다**. 암호화된 저장장치의 비트열 자체를 보존하는 것과 복구 키 등을 이용해 내용을 해독하는 것은 별개의 문제이다. 원본의 암호화를 해제하여 상태를 바꾸는 일을 모든 이미지 생성의 필수 조건으로 삼을 수 없으며, 이 설명은 안티 포렌식 기법의 정의에도 해당하지 않는다.

④ O: 증거가 될 수 있는 운영체제의 생성 정보를 없애는 행위는 **분석에 필요한 흔적을 줄여 증거 수집을 방해**하므로 안티 포렌식의 취지에 해당한다. 다만 이는 제시된 삭제 행위의 목적을 분류한 것이며, 실제로 모든 정보를 즉시 완전히 삭제하거나 다른 저장 위치의 흔적까지 없앨 수 있다는 보장은 아니다.

NoteBase

문 16. 포렌식은 원래 범인이 남긴 흔적을 대상으로 과학의 힘을 빌려 법적인 문제를 해결하는 작업을 의미한다. 괄호 안에 들어갈 용어로 가장 적절한 것은?

( )은(는) 접촉하는 두 물체 사이에는 반드시 흔적이 남는다는 이론이다. 범죄자가 범죄 현장을 드나들 때 무엇인가를 가지고 가며 범죄자는 흔적을 남긴다는 것이다. 디지털 세계에서도 범인은 파일 개방, 방문 기록, 프로세스 실행기록, 파일 삭제 흔적 등 다양한 흔적을 남기게 된다.

① 로카르드의 교환 법칙(Locard’s Exchange Principle)
② 증거 규칙(Rules of Evidence)
③ 정당성(Legitimacy)의 원칙
④ 전문 증거(Hearsay Evidence)

정답 1번

간단한 해설

'접촉하는 두 물체 사이에 흔적이 남는다'는 단서는 **로카르드의 교환 법칙**을 가리킨다. 디지털 행위가 실행기록이나 파일 관련 흔적을 남길 수 있다는 설명도 같은 관점에 연결된다.

빈칸별 해설

괄호에는 '로카르드의 교환 법칙'이 들어간다. **접촉하는 대상 사이에 흔적이 교환·전이된다**는 관점이 지문의 핵심이다. 범인이 현장에 흔적을 남기는 동시에 현장의 물질을 가져갈 수 있다는 설명이 이에 해당한다.

디지털 환경에서는 파일 열기, 웹 사이트 방문, 프로세스 실행, 파일 삭제 등의 행위가 로그·메타데이터·잔존 데이터 같은 흔적을 남길 수 있다는 관점으로 연결된다. 지문의 '반드시 흔적이 남는다'는 표현을 **모든 행위의 기록이 언제나 보존되어 복구된다는 보장**으로 확대해서는 안 된다. 기록 설정, 덮어쓰기, 삭제와 수집 시점에 따라 실제 확보 가능한 흔적은 달라진다.

증거 규칙은 증거를 재판에서 사용할 수 있는지와 그 취급을 판단하는 법적 기준을 가리킨다. 정당성의 원칙은 적법한 권한과 절차에 따라 증거를 수집·처리해야 한다는 원칙이다. 전문 증거는 법정 밖 진술을 그 내용의 진실성을 입증하는 데 사용하는 문제와 관련된다. 이들은 접촉에 따른 흔적의 교환을 설명하는 법칙과 구별된다.

따라서 괄호에 들어갈 용어와 일치하는 선택지는 ①이다.

NoteBase

문 17. 안드로이드 스마트폰의 포렌식 분석에 대한 설명으로 가장 적절하지 않은 것은?

① Manifest.mbdb에는 파일의 도메인, access 시간이 기록되어 있다.

② 캐시(cache) 파티션에 App 설치 파일 등 임시파일이 있다.

③ 데이터는 SQLite, Local file 형식으로 저장되어 있다.

④ Preference에는 주로 환경설정 값이 저장되어 있다.

정답 1번

간단한 해설

Manifest.mbdb는 **iOS의 구형 iTunes 백업 파일**로, 안드로이드의 표준 데이터 저장 구조와 구별된다.
데이터가 어떤 운영체제와 백업 형식에서 생성되었는지 확인해야 한다.

선지별 해설

① X. Manifest.mbdb는 **구형 iOS의 iTunes 백업**에서 파일 목록과 도메인·경로·시간 등의 정보를 관리하는 파일이다. 파일 도메인과 접근 시각이 기록된다는 특성은 이 백업 형식에 관한 것이며, 안드로이드의 표준 분석 자료로 제시한 점이 잘못되었다.

② O. 전통적인 안드로이드 파티션 구성에서는 **cache 영역이 다운로드·설치 과정의 임시 자료** 등에 사용된다. 다만 기기와 운영체제 구성에 따라 별도 cache 파티션이 없을 수 있으며, 모든 앱 설치 파일이 항상 이곳에 남는다는 뜻은 아니다.

③ O. 안드로이드 앱은 **SQLite 데이터베이스와 로컬 파일** 등을 이용하여 데이터를 저장할 수 있다. 따라서 데이터베이스의 테이블·레코드와 앱별 파일을 함께 분석한다. 모든 앱이 같은 형식으로 저장하는 것은 아니다.

④ O. Preference 계열 자료에는 **환경설정 등 키-값 형태의 정보**가 저장된다. 예를 들어 SharedPreferences에는 문자열·논리값·수치 등 작은 설정 값을 기록할 수 있어 앱의 설정 상태를 확인하는 데 활용된다.

따라서 iOS 백업의 Manifest.mbdb를 안드로이드 설명에 포함한 ①이 가장 적절하지 않다.

NoteBase

문 18. 디스크 이미징(Disk Imaging)에 대한 설명으로 가장 적절하지 않은 것은?

① 디스크의 모든 물리적 섹터를 복제한다.

② 비트스트림 사본은 CRC(Cyclic Redundancy Check) 계산법을 사용하여 원본 데이터와 차이가 없는 지를 확인한다.

③ 디스크 섹터에 삭제 파일 정보가 남아 있는 경우 복구가 가능하다.

④ Source Read & Destination Write 저장 방식이다.

정답 4번

출제 포인트

파일·디렉터리 단위의 일반 복사와 디스크 전체를 비트 단위로 복제하는 디스크 이미징의 차이를 묻는다.

핵심 개념

디스크 이미징은 원본 저장매체를 섹터 단위로 읽어 비트스트림 사본을 만드는 작업이다. 현재 사용 중인 파일뿐 아니라 미할당 영역과 파일 끝의 잔여 공간도 포함한다. 일반적인 논리적 복사는 파일·디렉터리를 대상으로 하므로 이러한 잔여 데이터를 모두 보존하지 못한다.

선지별 해설

O는 적절한 설명, X는 이 문항에서 가장 적절하지 않은 설명을 뜻한다.
① O. 디스크 전체의 물리적 이미징은 파일의 존재 여부와 관계없이 섹터 단위로 데이터를 복제한다. 따라서 파일 목록에 나타나지 않는 영역도 사본에 포함된다.
② O. CRC는 데이터로부터 계산한 체크값을 비교하여 오류나 변경을 검출하는 방법이다. 비트스트림 사본의 데이터 검증에 사용될 수 있다. 실제 EnCase 증거 파일은 CRC와 해시값을 이용해 데이터의 변경 여부를 검사한다. 다만 CRC만으로 모든 변조 가능성이 배제된다는 뜻은 아니다.
③ O. 파일이 삭제되어도 해당 섹터의 내용이 덮어써지지 않고 남아 있으면 이미징된 사본에서 복구할 수 있다. 이미징은 삭제 파일의 잔여 데이터가 있는 영역까지 보존하기 때문이다. 삭제된 모든 파일이 반드시 복구된다는 의미는 아니다.
④ X. “Source Read & Destination Write”는 원본을 읽고 대상에 쓰는 일반적인 동작을 나타낼 뿐, 디스크 이미징의 핵심인 섹터 단위 전체 복제를 구체적으로 설명하지 못한다. 이 문항의 일반 복사와 이미징의 대비에서는 가장 적절하지 않은 설명이다. 올바르게는 “Bit Stream Clone, 즉 섹터 단위의 비트스트림 복제 방식”이라고 설명한다. 이미징도 실제로 읽기와 쓰기를 수행하므로 그 동작 자체가 잘못이라는 뜻은 아니다.

오답 포인트

④의 읽기·쓰기라는 표현만 보면 모든 복제에 해당하므로 맞다고 판단하기 쉽다. 이 문제의 구별 기준은 읽고 쓰는 동작 자체가 아니라 파일·디렉터리를 복사하는지, 잔여 영역까지 섹터 단위로 복제하는지이다.

다시 나오면 이렇게 판단

복제 범위를 먼저 확인한다. 파일·디렉터리만 대상으로 하면 논리적 복사이고, 미할당 영역과 삭제 데이터의 잔여 부분까지 포함하면 물리적 비트스트림 이미징이다. 삭제 파일의 복구 가능성은 데이터가 실제로 남아 있는지로 판단한다.

암기 포인트

일반 복사는 파일 중심, 디스크 이미징은 섹터 중심이다. 삭제 데이터가 남아 있어야 복구가 가능하다.

NoteBase

문 19. Access Point를 통하여 해킹을 당하고 있다. IEEE 802.11 패킷 수집을 위해 포렌식 수사관이 사용해야 할 도구로 가장 적절한 것은?

① FTK(Forensic Tool Kit)

② Autopsy

③ Airpcap

④ ProDiscover

정답 3번

간단한 해설

IEEE 802.11 무선 LAN 프레임 캡처에 특화된 도구는 ③ **AirPcap**이다. FTK·Autopsy·ProDiscover의 일반적인 증거 분석 기능과 구별한다.

핵심 풀이

제시된 도구 가운데 IEEE 802.11 무선 프레임 수집에 직접 대응하는 것은 ③ **AirPcap**이다. AirPcap은 무선 캡처용 어댑터와 드라이버를 이용해 무선 LAN 트래픽을 수집하고, Wireshark 같은 분석 도구에서 확인할 수 있도록 하는 제품군이다.

FTK, Autopsy, ProDiscover는 저장매체나 시스템의 디지털 증거를 획득·검색·분석하는 포렌식 도구이다. 이 문항은 일반적인 디지털 증거 분석 기능이 아니라, 접근 지점 주변의 802.11 무선 프레임을 수집하는 기능을 묻고 있으므로 AirPcap을 선택한다.

캡처 가능한 범위는 **지원 무선 규격·채널·어댑터와 드라이버** 등의 조건에 영향을 받는다. 또한 암호화된 프레임을 수집했다는 사실만으로 그 내부 데이터가 자동 복호화되는 것은 아니다. 이는 제시된 도구의 역할을 구별하는 설명이지, AirPcap만이 무선 캡처의 유일한 방법이라는 뜻은 아니다.

NoteBase

문 20. 해시(Hash)와 관련된 설명으로 가장 적절하지 않은 것은?

① 잘 알려진 파일들의 해시 값을 모아놓은 것을 참조 데이터 셋(Reference Data Set)이라 한다.

② 원본 데이터에 대한 이미지 파일의 무결성 입증에 사용된다.

③ 해시 함수에 입력한 데이터의 크기에 따라 출력 해시 값의 길이는 가변적이다.

④ 특정 파일의 존재 여부를 확인하는 검사에 사용되는 데이터 세트로서 NSRL(National Software Reference Library)을 공개하고 있다.

정답 3번

간단한 해설

고정 길이 해시 함수는 **입력 크기와 관계없이 정해진 길이의 요약값**을 만든다. 해시값 비교는 데이터 무결성 확인과 알려진 파일 식별에 활용된다.

선지별 해설

① O: 이미 알려진 파일의 해시값을 모아 두면 조사 대상 파일의 해시값과 비교하여 **기지 파일을 식별**할 수 있다. NSRL이 제공하는 참조 데이터 세트(RDS)는 이러한 해시값과 파일 식별용 메타데이터를 포함한다.

② O: 동일한 알고리즘으로 원본과 이미지에 담긴 **대응 데이터 영역의 해시값을 비교**하여 복제 과정의 변경 여부를 확인할 수 있다. 압축·메타데이터가 추가된 이미지 컨테이너 파일 전체가 원본 디스크와 같은 바이트열이라고 가정하는 것은 아니며, 검증 대상 영역과 방식이 일치해야 한다.

③ X: SHA-256 같은 고정 길이 해시 함수는 입력 데이터의 크기가 달라도 **출력 길이가 일정**하다. SHA-256의 결과는 항상 256비트이다. 출력 길이를 지정하는 확장 출력 함수도 있지만, 이는 입력 파일이 커질수록 해시값 길이가 자동으로 늘어난다는 뜻이 아니다.

④ O: NIST의 **NSRL은 알려진 소프트웨어 파일의 식별 정보**를 수집하고, 이를 바탕으로 RDS를 공개한다. 조사 대상 파일의 해시값을 그 자료와 대조하면 등록된 파일을 식별하는 데 활용할 수 있다. 엄밀히는 공개 참조 데이터 세트의 명칭이 RDS이고 NSRL은 이를 구축·제공하는 라이브러리 및 사업의 명칭이다.

NoteBase