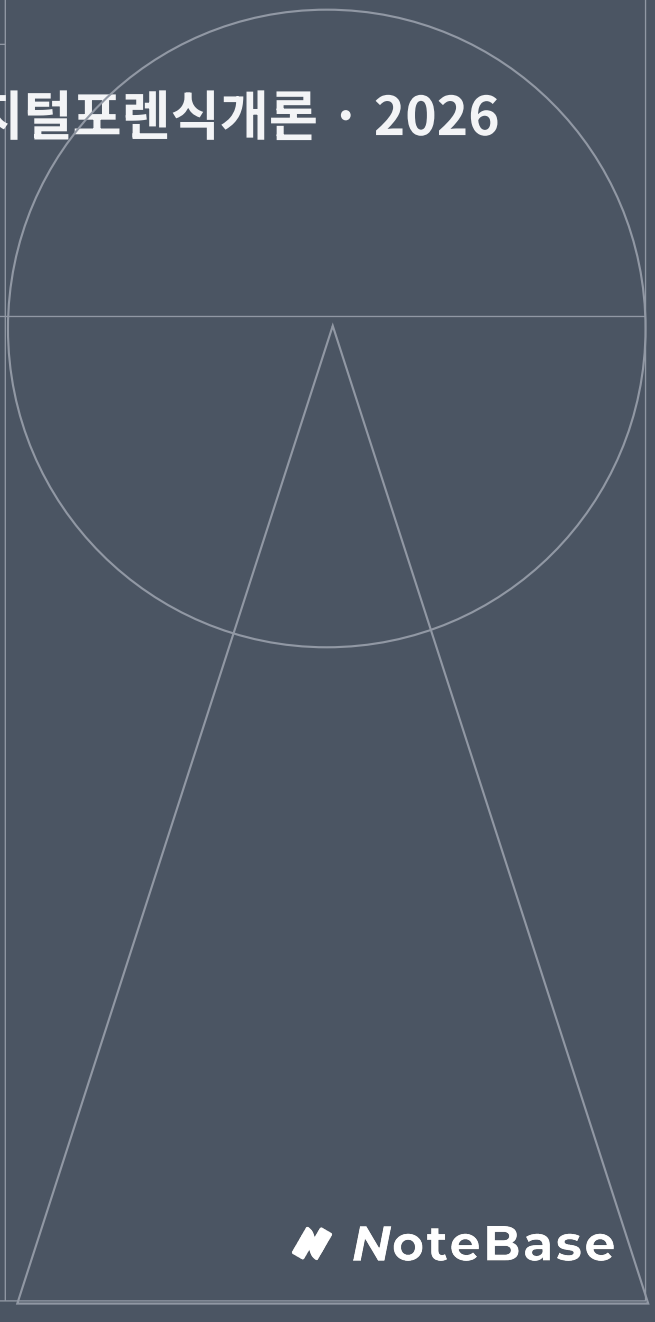
기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2026



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2026

공무원/경찰/경력채용 · 디지털포렌식개론 · 2026

문 1. 디지털 증거의 동일성·무결성을 확보하거나 증명하기 위한 방법과 가장 거리가 먼 것은?

① 해시값의 비교

② 선별압수 원칙의 준수

③ 압수·수색 과정을 촬영한 영상녹화물 재생

④ 연계보관성(Chain of Custody)의 준수

정답 2번

공통 해설

선별압수는 **사건과 관련된 전자정보로 압수 범위를 제한하여 수집 절차의 적법성을 확보**하는 원칙이다. 수집된 정보가 원본과 같고 변경되지 않았다는 **동일성·무결성을 직접 확보하거나 증명하는 방법과는 구별**된다.

형사소송법 제106조(압수)
①법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다. <개정 2011.7.18>
③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다. <신설 2011.7.18>

NoteBase

문 2. SSD(Solid State Drive)에 관한 설명으로 가장 적절하지 않은 것은?

① FTL(Flash Translation Layer)은 논리 주소를 플래시 메모리의 물리 주소로 매핑하는 기능을 수행한다.

② 플래시 메모리 셀의 쓰기 횟수가 제한되어 있어 SSD는 웨어 레벨링(Wear Leveling)을 수행한다.

③ 가비지 컬렉션(Garbage Collection) 기능으로 인해 SSD는 하드디스크에 비해 삭제된 데이터의 복구가 어렵다.

④ 트림(Trim)은 SSD 자체적으로 수행하는 기능이며, 비활성화시키는 것이 불가능하다.

정답 4번

간단한 해설

TRIM은 **호스트가 SSD에 불필요한 데이터 영역을 알리는 명령**이다. 운영체제에서 통지를 비활성화할 수 있으므로, SSD 자체 기능이며 끌 수 없다는 설명은 틀리다.

선지별 해설

① O: FTL은 호스트가 사용하는 논리 주소와 플래시 메모리의 실제 저장 위치를 연결하는 변환 계층이다. 데이터가 다른 물리 위치로 이동하더라도 논리 주소로 접근할 수 있도록 매핑 정보를 관리한다.

② O: 플래시 메모리는 프로그램·삭제를 반복할 수 있는 횟수에 한계가 있다. 웨어 레벨링은 쓰기·삭제 부담을 여러 블록으로 분산하여 **특정 블록만 먼저 마모되는 것을 줄이는** 기능이다.

③ O: 가비지 컬렉션은 필요한 데이터를 옮겨 보존하고 더 이상 유효하지 않은 데이터가 포함된 블록을 지워 재사용 가능한 공간을 확보한다. 이 과정에서 삭제 흔적이 사라질 수 있어, 삭제 데이터가 덮어쓰기 전까지 남는 일반적인 HDD보다 복구가 어려워질 수 있다.

④ X: TRIM은 운영체제 등 호스트가 더 이상 필요하지 않은 데이터 영역을 SSD에 알리는 명령이다. SSD 내부의 가비지 컬렉션과 동일한 기능이 아니며, **운영체제에서 TRIM 통지를 비활성화할 수 있다**. 다만 통지를 끄는 것이 이미 통지된 데이터의 복원이나 SSD 내부 가비지 컬렉션의 중단을 보장하지는 않는다.

NoteBase

문 3. 해시값(Hash Value)에 관한 설명으로 가장 적절하지 않은 것은?

① MD5, SHA-1, SHA-256은 해시 알고리즘이다.

② 한글 파일(.hwp)의 파일명을 변경하면 해당 파일의 해시값도 변경된다.

③ 피의자 甲으로부터 압수한 A파일이 공범인 乙의 PC에도 저장되어 있는지 확인하기 위해 해시값을 활용할 수 있다.

④ 해시는 일방향 알고리즘으로 해시값을 원래 입력된 데이터로 복원하기 어렵다.

정답 2번

간단한 해설

일반적인 파일 해시는 **파일 내용의 바이트**로 계산한다. 내용은 그대로 두고 파일명만 바꾸는 경우에는 같은 알고리즘으로 계산한 해시값이 바뀌지 않는다.

선지별 해설

① O: MD5, SHA-1, SHA-256은 모두 **입력 데이터의 해시값을 계산하는 알고리즘**이다. 다만 알고리즘의 분류가 같다는 것이 보안 강도도 같다는 뜻은 아니며, MD5와 SHA-1에는 충돌 저항성의 취약점이 알려져 있다.

② X: 일반적인 파일 해시는 **파일 이름이 아니라 파일 내용의 바이트**를 입력으로 계산한다. 한글 파일의 내용은 그대로 두고 파일명만 변경했다면 같은 알고리즘으로 계산한 해시값은 변하지 않는다. 문서를 다시 저장하면서 내부 데이터까지 바뀐 경우와 단순 이름 변경을 구별해야 한다.

③ O: 압수한 A파일과 다른 PC의 파일에 **같은 해시 알고리즘**을 적용해 값을 비교하면 동일한 내용의 파일을 찾는 데 활용할 수 있다. 해시 충돌 가능성은 이론적으로 존재하므로 해시가 같다는 이유만으로 모든 상황에서 동일성이 수학적으로 보장된다고 하지는 않는다.

④ O: 암호학적 해시는 **주어진 해시값에서 원래 입력을 알아내기 어렵게 하는 일방향성**을 목표로 한다. 암호문을 키로 복호화하듯 원문을 되돌리는 기능은 없다. 다만 가능한 입력이 적거나 쉽게 추측되면 후보의 해시를 계산해 대조할 수 있으므로 어떤 입력도 절대 알아낼 수 없다는 뜻은 아니다.

NoteBase

문 4. 윈도우 10(Windows 10)에서 유저어시스트(UserAssist) 정보를 분석하고자 할 때 반드시 확보해야 할 파일로 가장 적절한 것은?

① index.dat

② NTUSER.DAT

③ SOFTWARE

④ thumbs.db

정답 2번

간단한 해설

UserAssist는 **사용자별 레지스트리 영역**에 저장되는 실행 흔적이다. 해당 영역을 담는 하이브 파일이 NTUSER.DAT이므로 분석 대상 사용자의 파일을 확보해야 한다.

핵심 풀이

UserAssist는 Windows 탐색기 등을 통한 사용자별 프로그램 실행 흔적을 담는 레지스트리 아티팩트이다. HKEY_CURRENT_USER의 Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist 아래에 저장되며, 해당 사용자의 이 영역을 보존하는 하이브 파일이 **NTUSER.DAT**이다.

따라서 분석할 사용자의 프로필에서 NTUSER.DAT를 확보해야 하며, 선택지는 ②이다. UserAssist에는 실행 횟수나 최근 실행 시각 등의 정보가 남을 수 있지만 모든 방식의 프로그램 실행을 빠짐없이 기록하는 것은 아니다.

index.dat는 구형 Internet Explorer의 인터넷 이용 흔적과 관련된 파일이고, SOFTWARE는 시스템의 소프트웨어 설정 등을 담는 별도 하이브이다. thumbs.db는 섬네일 캐시이므로 사용자별 UserAssist 레지스트리 정보를 담는 NTUSER.DAT와 구별된다.

NoteBase

문 5. 파일 시그니처에 관한 아래의 설명에 대한 옳고 그름의 표시 (O, X)가 가장 적절한 것은?

㉠ 주로 파일의 동일성·무결성을 확인하기 위해 시그니처 분석이 활용된다.
㉡ 파일의 확장자가 변경되거나 위장된 경우 파일 시그니처 분석을 통해 실제 파일 형식을 식별할 수 있으며, 확장자와 시그니처가 일치하지 않을 경우 EnCase에서는 Unknown으로 표시된다.
㉢ 헤더 시그니처와 푸터 시그니처의 구조를 이용하여 은닉된 데이터를 찾아낼 수 있다.
㉣ ZIP 파일(.zip) 형식은 Microsoft Word 문서 파일(MS 오피스 2007 버전 이후)과 같은 다양한 컨테이너 파일 형식의 기본이 되며, ZIP 파일(.zip)과 DOCX 파일(.docx)은 시그니처 값 “50 4B 03 04”를 공유한다.

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

정답 4번

간단한 해설

파일 형식 시그니처는 형식 식별과 카빙에 활용하며, 파일 전체의 동일성·무결성 검증과는 구별한다. EnCase의 Unknown은 단순한 확장자 불일치와 같지 않고, DOCX는 ZIP 기반이므로 대표 헤더 패턴을 공유할 수 있다.

NoteBase

보기별 해설

㉠ X. 이 문제의 시그니처 분석은 헤더·푸터 등 **파일 형식 식별 패턴**을 확인하는 분석이다. 파일 전체의 동일성·무결성 확인에는 주로 해시값 비교를 사용한다. 디지털 서명이나 해시를 넓은 의미에서 시그니처라고 부르는 경우와 이 문항의 형식 시그니처를 혼동하면 안 된다.

㉡ X. 확장자가 바뀌어도 시그니처로 실제 형식을 추정할 수 있다는 앞부분은 맞다. 그러나 EnCase의 **Unknown은 시그니처와 확장자 모두 등록된 형식으로 인식되지 않는 경우**를 가리킨다. 알려진 헤더와 다른 확장자가 붙은 경우는 Alias가 될 수 있고, 확장자에 기대되는 헤더와 맞지 않는 미인식 데이터는 Bad Signature가 될 수 있으므로 단순 불일치를 Unknown이라고 단정한 뒷부분이 틀렸다.

㉢ O. **헤더·푸터 패턴과 파일 구조**를 이용하면 미할당 영역이나 다른 파일 안에 포함된 데이터의 시작·끝을 찾아 카빙할 수 있다. 따라서 은닉·잔존 데이터를 찾는 데 활용되지만, 모든 형식에 고정 푸터가 있거나 모든 은닉·암호화 데이터를 이 방법만으로 복원할 수 있다는 뜻은 아니다.

㉣ O. DOCX 같은 Office Open XML 문서는 **ZIP 기반 패키지**이다. ZIP 로컬 파일 헤더의 대표 바이트열은 50 4B 03 04이므로 일반적인 ZIP과 DOCX가 이를 공유할 수 있다. 이 네 바이트만으로 DOCX를 확정할 수는 없고 내부 파일과 구조를 추가 확인해야 한다.

따라서 ㉠ X, ㉡ X, ㉢ O, ㉣ O의 조합은 ④이다.

NoteBase

문 6. Apple사의 휴대전화용(用) 파일시스템으로 가장 적절한 것은?

① EXT4

② NTFS

③ APFS

④ ZFS

정답 3번

간단한 해설

iPhone은 iOS 10.3부터 **APFS(Apple File System)**를 기본 파일시스템으로 사용한다. APFS는 Apple 플랫폼의 파일 저장과 관리를 위해 개발되었다.

핵심 풀이

APFS(Apple File System)는 Apple이 개발한 파일시스템으로, iPhone의 **iOS 10.3부터 기본 파일시스템**으로 사용된다. 이전의 HFS+를 대체했으며, 플래시 저장장치에 적합하도록 설계되었다. 휴대전화 전용은 아니고 macOS 등 다른 Apple 플랫폼에서도 사용한다.

EXT4는 Linux 계열에서 널리 사용하는 파일시스템이고, NTFS는 Windows의 대표적인 파일시스템이다.
ZFS는 저장장치 풀 관리와 데이터 무결성 기능 등을 제공하는 파일시스템으로, iPhone의 기본 파일시스템에 해당하지 않는다.

따라서 Apple 휴대전화의 파일시스템으로 가장 적절한 것은 ③ APFS이다.

NoteBase

문 7. 윈도우 10(Windows 10)의 링크 파일(.lnk)에 관한 설명으로 가장 적절하지 않은 것은?

① 링크 파일 저장 경로에는 암캐시(Amcache) 파일도 저장되어 있으므로 응용 프로그램의 삭제시간, 해시값을 확인하고자 할 때 링크 파일을 분석한다.

② 사용자가 파일이나 폴더에 액세스하는 경우 등에 자동으로 링크 파일이 생성되지만, 사용자가 링크 파일을 직접 생성할 수도 있다.

③ 링크 파일 분석으로 원본 파일의 타임 스탬프와 원본 파일의 크기 등을 알 수 있다.

④ 원본 파일이 삭제되어 더 이상 존재하지 않는 경우에도 링크 파일은 남아있을 수 있다.

정답 1번

간단한 해설

Amcache.hve와 LNK는 **저장 위치와 구조가 다른 별개의 아티팩트**이다. 링크 파일 분석을 응용프로그램의 삭제 시각·해시값 확인과 직접 연결하는 설명은 적절하지 않다.

선지별 해설

① X: Amcache는 일반적인 링크 파일 저장 폴더의 구성물이 아니라 **별도 레지스트리 하이브 Amcache.hve**로 관리되는 아티팩트이다. 보통 Windows의 AppCompat\Programs 아래에 있으며 프로그램·파일 관련 정보를 조사하는 자료이다. LNK 분석으로 응용프로그램의 삭제 시각과 해시값을 곧바로 확인한다는 설명은 두 아티팩트를 혼동한 것이다.

② O: Windows는 최근 사용 항목 등 이용 흔적을 관리하는 과정에서 링크 파일을 자동 생성할 수 있다. 사용자도 '바로 가기 만들기' 기능으로 **직접 링크 파일을 생성**할 수 있으므로, 모든 LNK가 자동 생성되었다고 단정해서는 안 된다.

③ O: LNK 헤더에는 대상 파일의 생성·접근·수정 시각과 파일 크기 등이 저장될 수 있다. 이는 **링크에 기록된 대상 파일 정보**이며, LNK 자체의 파일시스템 시간이나 원본의 현재 상태와 구별하여 해석한다.

④ O: 링크 파일과 대상 파일은 별개의 파일이므로, 대상 파일이 삭제되어도 LNK가 자동으로 함께 삭제되는 것은 아니다. 남아 있는 대상 경로와 속성 등을 통해 **현재 사라진 원본의 과거 흔적**을 조사할 수 있다.

NoteBase

문 8. 윈도우 아티팩트(Windows Artifact)에 관한 <보기 1>의 용어와 <보기 2>의 설명을 가장 적절하게 연결한 것은?

<보기 1>
(가) 프리패치(prefetch)
(나) 점프리스트(jump list)
(다) 쉘백(shellbag)
(라) 섬네일(thumbnail)

<보기 2>
㉠ 사용자가 열람한 폴더 정보를 기록
㉡ 작업 표시줄의 앱 아이콘을 우클릭했을 때 표시되는 최근 사용한 파일 등의 정보를 저장
㉢ 응용 프로그램의 실행에 필요한 시스템 자원 정보를 저장
㉣ 원본 이미지를 축소하여 보여주는 것

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

정답 4번

간단한 해설

프리패치는 **실행 자원**, 점프리스트는 **앱별 최근 항목**, 쉘백은 **폴더 탐색 정보**, 섬네일은 **축소 미리보기**에 대응하므로 ④이다.

NoteBase

대응 관계 해설

(가) 프리패치 → ㉢: 프로그램 시작을 빠르게 하기 위해 **실행 초기에 참조한 파일·디렉터리 등 자원 정보**를 기록한다. 포렌식에서는 프로그램 실행 흔적을 살피는 단서가 된다. 단순히 최근 문서 목록을 보여 주는 기능과는 구별한다.

(나) 점프리스트 → ㉡: 작업 표시줄의 앱 아이콘에서 접근할 수 있는 **최근 또는 자주 사용한 항목, 고정된 항목** 등의 정보를 관리한다. 특정 응용프로그램과 관련 파일 사이의 사용 관계를 파악하는 데 활용할 수 있다.

(다) 쉘백 → ㉠: 탐색기 등의 폴더 보기와 관련된 정보를 레지스트리에 남기는 아티팩트이다. **사용자가 탐색한 폴더 경로와 보기 설정** 등을 확인하는 데 도움이 된다. 모든 접근을 빠짐없이 기록하는 감사 로그나 폴더 안의 모든 파일을 열었다는 증거로 단정하지 않는다.

(라) 섬네일 → ㉣: 원본 이미지 등의 내용을 작은 크기로 미리 보여 주는 **축소 미리보기**이다. 생성된 미리보기는 캐시에 남을 수 있으나, 섬네일의 존재만으로 원본 전체나 사용자의 의도까지 확정할 수는 없다.

따라서 (가)㉢, (나)㉡, (다)㉠, (라)㉣의 대응을 제시한 ④가 정답이다.

NoteBase

문 9. 전자정보를 압수·수색·검증하고자 할 때 사전 고려 대상으로 가장 적절하지 않은 것은?

① 이동통신단말장치 제조업자의 조직 현황

② 사건의 개요, 압수·수색·검증 장소 및 대상

③ 압수·수색·검증할 컴퓨터 시스템의 네트워크 구성 형태

④ 압수·수색·검증에 필요한 인원 및 시간

정답 1번

①

사전에 파악해야 할 것은 **압수 대상과 시스템 환경, 필요한 인원·시간·장비**이며, 이동통신단말장치 제조업자의 조직 현황은 규정된 고려사항이 아니다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제11조(압수 · 수색 · 검증의 준비) 경찰관은 전자정보를 압수 · 수색 · 검증하고자 할 때에는 사전에 다음 각 호의 사항을 고려하여야 한다. 1. 사건의 개요, 압수 · 수색 · 검증 장소 및 대상 2. 압수 · 수색 · 검증할 컴퓨터 시스템의 네트워크 구성 형태, 시스템 운영체제, 서버 및 대용량 저장장치, 전용 소프트웨어 3. 압수대상자가 사용 중인 정보저장매체등 4. 압수 · 수색 · 검증에 필요한 인원 및 시간 5. 디지털 증거분석 전용 노트북, 쓰기방지 장치 및 하드디스크 복제장치, 복제용 하드디스크, 하드디스크 운반용 박스, 정전기 방지장치 등 압수 · 수색 · 검증에 필요한 장비

②

압수 범위와 집행 계획을 정하기 위해 **사건의 개요와 압수·수색·검증의 장소·대상**을 사전에 고려해야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제11조(압수 · 수색 · 검증의 준비) 경찰관은 전자정보를 압수 · 수색 · 검증하고자 할 때에는 사전에 다음 각 호의 사항을 고려하여야 한다.
1. 사건의 개요, 압수 · 수색 · 검증 장소 및 대상

③

전자정보의 저장 위치와 적절한 확보 방법을 파악하기 위해 **대상 컴퓨터 시스템의 네트워크 구성 형태**를 사전에 고려해야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제11조(압수 · 수색 · 검증의 준비) 경찰관은 전자정보를 압수 · 수색 · 검증하고자 할 때에는 사전에 다음 각 호의 사항을 고려하여야 한다.
2. 압수 · 수색 · 검증할 컴퓨터 시스템의 네트워크 구성 형태, 시스템 운영체제, 서버 및 대용량 저장장치, 전용 소프트웨어

NoteBase

④

현장 집행에 필요한 자원을 준비할 수 있도록 **압수·수색·검증에 필요한 인원과 시간**을 사전에 고려해야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제11조(압수 · 수색 · 검증의 준비) 경찰관은 전자정보를 압수 · 수색 · 검증하고자 할 때에는 사전에 다음 각 호의 사항을 고려하여야 한다.
4. 압수 · 수색 · 검증에 필요한 인원 및 시간

NoteBase

문 10. 디지털 증거에 관한 설명으로 가장 적절하지 않은 것은?

① 디지털 증거는 범죄와 관련하여 증거로서의 가치가 있는 전자정보이다.

② 디지털 증거는 정보저장매체등에 저장된 전자정보와 동일성이 유지되어야 한다.

③ 디지털 증거 처리 과정에서 이용된 장비의 기계적 정확성, 프로그램의 신뢰성, 처리자의 전문적인 기술능력과 정확성이 담보되어야 한다.

④ 압수된 디지털 저장 매체로부터 출력한 문서는 진술증거로 사용할 수 없다.

정답 4번

①

디지털 증거는 **범죄 관련성과 증거가치를 갖춘 전자정보**이다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제2조(정의) 이 규칙에서 사용하는 용어의 뜻은 다음과 같다.
3. "디지털 증거"란 범죄와 관련하여 증거로서의 가치가 있는 전자정보를 말한다.

②

디지털 증거를 처리하는 과정에서도 **그 내용이 저장매체에 저장된 전자정보와 같게 유지**되어야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제5조(디지털 증거 처리의 원칙) 디지털 증거의 처리는 다음 각 호의 원칙에 따라 이루어져야 한다.
2. 디지털 증거는 정보저장매체등에 저장된 전자정보와 동일성이 유지되도록 할 것

③

디지털 증거의 처리에는 **장비의 정확한 작동, 프로그램의 신뢰성, 처리자의 전문적인 기술능력과 처리 정확성**이 담보되어야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제5조(디지털 증거 처리의 원칙) 디지털 증거의 처리는 다음 각 호의 원칙에 따라 이루어져야 한다.
4. 디지털 증거 처리 과정에서 이용된 장비의 기계적 정확성, 프로그램의 신뢰성, 처리자의 전문적인 기술능력과 정확성이 담보되도록 할 것

NoteBase

④

압수된 디지털 저장매체의 출력 문서도 **진술증거로 사용할 수 있다**. 원본과의 동일성이 인정되어야 하며, 기재 내용의 진실성을 증명하려는 경우에는 **전문법칙에 따른 증거능력 요건**을 갖추어야 한다.

그리고 압수된 디지털 저장매체로부터 출력된 문건이 진술증거로 사용되는 경우에는 그 기재 내용의 진실성에 관하여 전문법칙이 적용되므로, 형사소송법 제313조 제1항에 의하여 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다(대법원 1999. 9. 3. 선고 99도2317 판결 참조). (대법원 2007. 12. 13. 선고 2007도7257 판결)

NoteBase

문 11. 디스크 이미징(Disk Imaging)에 관한 설명으로 가장 적절하지 않은 것은?

① 디스크의 모든 물리적 섹터를 복제한다.

② 증거 손상 방지를 위해 쓰기 방지 조치를 한다.

③ 드래그 앤드 드롭(Drag-and-drop)을 통해 복사하는 것이다.

④ 이미징된 디스크 섹터에 삭제 데이터가 남아 있는 경우 복구가 가능하다.

정답 3번

간단한 해설

디스크 이미징은 **미할당 공간과 슬랙 공간을 포함한 매체 데이터의 비트 단위 복제**이다. 탐색기에서 드래그 앤드 드롭으로 선택한 파일만 복사하는 것과는 수집 범위가 다르다.

선지별 해설

① O: 이 문항의 디스크 이미징은 파일 목록만 복사하는 것이 아니라 **매체의 섹터 데이터를 비트 단위로 복제**하는 물리적 이미징을 뜻한다. 따라서 할당된 파일뿐 아니라 미할당 공간과 슬랙 공간도 수집 대상에 포함된다. 실제 장치에서 접근할 수 없는 영역이나 불량 섹터까지 항상 읽을 수 있다는 뜻은 아니므로 수집 범위와 오류는 기록해야 한다.

② O: 원본에 새 데이터가 기록되면 기존 증거가 변경되거나 덮어써질 수 있다. 따라서 이미징 과정에서는 **쓰기 방지 조치**로 원본의 변경을 막고, 수집 결과의 무결성을 확인한다.

③ X: 드래그 앤드 드롭은 일반적으로 파일 시스템이 인식하는 **선택한 파일을 논리적으로 복사**하는 방식이다. 미할당 영역이나 삭제 흔적까지 포함해 매체를 비트 단위로 복제하는 디스크 이미징과 다르다.

④ O: 삭제된 파일의 내용이 섹터에 남아 있고 그 영역이 이미지에 포함되었다면 **잔존 데이터를 분석해 복구**할 수 있다. 다만 덮어쓰기·손상·암호화 등 상태에 따라 복구 범위가 달라지며, 이미징 자체가 이미 사라진 내용을 되살리는 것은 아니다.

NoteBase

문 12. 다음에서 설명하는 슬랙 공간(Slack Space)으로 가장 적절한 것은?

파일시스템은 하나의 큰 파일을 저장할 때 여러 클러스터들로 나누어서 저장하게 된다. 이때 가장 마지막 클러스터에서 파일의 가장 뒷부분을 저장한 후 남는 공간 중 램(RAM) 슬랙 공간을 제외한 나머지 부분이다.

① 섹터 슬랙(Sector Slack)
② 볼륨 슬랙(Volume Slack)
③ 파일 시스템 슬랙(File System Slack)
④ 드라이브 슬랙(Drive Slack)

정답 4번

간단한 해설

파일 슬랙에서 RAM 슬랙을 제외하면 **마지막 사용 섹터 뒤부터 마지막 클러스터 끝까지**의 공간이 남는다. 이 공간을 드라이브 슬랙이라고 한다.

핵심 풀이

파일에 마지막으로 할당된 클러스터에서 실제 파일 내용 뒤에 남는 공간은 파일 슬랙이다. 이를 나누면 파일의 끝에서 마지막 사용 섹터의 끝까지가 RAM 슬랙이고, **그 섹터의 끝에서 마지막 클러스터의 끝까지** 남는 부분이 드라이브 슬랙이다.

지문은 마지막 클러스터의 남은 공간에서 RAM 슬랙을 제외한다고 하였으므로, 파일의 마지막 사용 섹터 뒤에 남은 미사용 섹터들이 대상이다. 이 부분에는 덮어쓰이지 않은 과거 데이터가 남아 있을 수 있다.

섹터 슬랙은 섹터 내부의 남은 공간을 가리키는 데 사용되어 지문이 제외한 RAM 슬랙과 구별 기준이 같다. 볼륨 슬랙·파일시스템 슬랙은 문헌에 따라 용어 범위가 달라질 수 있으나, 일반적으로 볼륨·파티션·파일시스템의 경계에서 생기는 여유 영역을 구분하는 데 쓰인다. 이 문제처럼 개별 파일의 마지막 클러스터 안에서 RAM 슬랙을 뺀 공간과는 다르다.

따라서 지문이 설명하는 것은 ④ 드라이브 슬랙이다.

NoteBase

문 13. 활성 시스템(Live System)의 휘발성 데이터 조사 방법에 관한 설명으로 가장 적절하지 않은 것은?

① 휘발성 정도가 높은 데이터부터 수집한다.

② 물리 메모리 덤프 시 네트워크 연결 정보, 프로세스 정보, 로그온 사용자 정보를 수집할 수 있다.

③ 압수하기 용이하지 않은 경우, 시스템 전원을 끄지 않고 조사를 수행할 수 있다.

④ 라이브 포렌식 도구를 사용하면 주기억장치나 캐시에 저장된 휘발성 데이터가 변경되지 않는다.

정답 4번

간단한 해설

라이브 포렌식은 실행 자체가 메모리 등 시스템 상태에 영향을 줄 수 있다. 휘발성 자료를 우선 확보하되, 도구의 영향을 최소화하고 수집 절차를 기록해야 한다.

선지별 해설

① O. 시간이 지나거나 전원이 꺼질 때 사라지기 쉬운 **휘발성이 높은 데이터부터** 수집하는 것이 기본 원칙이다. 실제 순서는 증거의 중요도, 시스템 상태, 도구의 영향 등을 함께 고려하여 정한다.

② O. 물리 메모리 덤프에는 실행 중인 **프로세스·네트워크 연결·로그온 세션**과 관련된 구조나 흔적이 포함될 수 있다. 이후 메모리 분석으로 이를 추출할 수 있지만, 시스템 버전과 획득 상태 등에 따라 모든 정보가 완전하게 복원되는 것은 아니다.

③ O. 장비를 바로 분리·반출하기 어렵거나 운영 중단이 곤란한 환경에서는 **전원을 유지한 상태로 라이브 조사**를 수행할 수 있다. 다만 수집 권한과 범위를 지키고, 시스템 변경 위험과 휘발성 자료 확보의 필요성을 검토하면서 절차를 기록해야 한다.

④ X. 라이브 포렌식 도구도 실행되면 **메모리와 캐시 등 시스템 상태에 영향을 준다.** 운영체제와 다른 프로세스 역시 계속 동작하므로 휘발성 데이터가 전혀 변경되지 않는다고 보장할 수 없다. 검증된 도구로 영향을 최소화하고 실행 시각·명령·변경 가능성을 기록해야 한다.

따라서 가장 적절하지 않은 것은 라이브 도구 사용 시 휘발성 데이터가 변경되지 않는다고 한 ④이다.

NoteBase

문 14. 다음과 같은 상황일 경우, 특정 파일의 내용을 신속하게 찾아내는 방법을 통해 피의자 甲의 혐의에 관한 단서를 찾고자 할 때 가장 적절한 분석 방법은?

사법경찰관 P는 피의자 甲이 2026년 1월 초순경, 고등학교 선배이자 OO시청 시장인 피의자 乙에게 OO시청 공무원 채용 시험에 응시한 아들의 최종 합격을 청탁하며 응시 원서와 3천만 원을 전달한 것이 의심되는 사건에서 피의자 甲과 피의자 乙의 정보저장매체 등을 압수수색하여 실체적 진실을 발견하고자 한다. 피의자 甲과 피의자 乙은 평소에도 문자메시지를 자주 주고받는 사이로 피의자 甲이 피의자 乙에게 휴대전화 문자메시지를 통해 아들의 응시 원서를 전달했다는 제보도 있는 상황이다.

① 파일 해시(Hash) 검색을 통한 분석 방법

② 시스템 레지스트리(Registry) 분석을 통한 방법

③ '채용 청탁' 관련 키워드(Keyword) 검색을 통한 분석 방법

④ 파일 시그니처(Signature) 검색을 통한 분석 방법

정답 3번

간단한 해설

사건과 관련된 **문자메시지·문서의 내용**을 찾으려는 목적이므로 ③ 키워드 검색이 가장 적합하다. 해시는 알려진 파일의 식별, 시그니처는 형식 식별에 주로 쓰이므로 내용 검색과 구별한다.

핵심 풀이

이 사례의 목표는 파일 형식이나 알려진 파일의 동일성을 확인하는 것이 아니라, **채용 청탁과 응시 원서 전달에 관한 내용**을 빠르게 찾는 것이다. 따라서 관련 표현을 검색하여 후보 자료를 추리는 **③ 키워드 검색**이 가장 직접적이다.

문자메시지와 문서에서 채용·청탁·응시 원서 등 사건 관련 표현이나 인명·기관명 등을 검색하고, 검색된 항목의 앞뒤 문맥과 시각·상대방을 함께 확인한다. **검색 결과는 단서이지 혐의의 자동 확정이 아니다.** 단어가 없더라도 다른 표현이나 이미지 형태로 내용이 존재할 수 있으므로 검색 실패도 자료 부재를 뜻하지 않는다.

해시 검색은 **이미 알고 있는 해시값과 같은 파일**을 찾는 데 적합하지만, 제시문은 기준 파일의 해시값을 제공하지 않는다. 레지스트리 분석은 시스템·사용자 설정과 활동 흔적을 조사하며, 파일 시그니처 검색은 파일 형식을 나타내는 내부 패턴 등을 찾는 데 쓰인다. 이들은 보조 분석으로 활용할 수 있어도, 사건 관련 문장의 내용을 직접 검색하는 목적에는 키워드 검색이 더 적합하다.

NoteBase

문 15. 파일 카빙(File Carving)에 관한 설명으로 가장 적절하지 않은 것은?

① 파일의 내용이 저장 매체의 공간 여러 부분에 조각나 저장된 경우에도 수행할 수 있다.

② 파일시스템 메타데이터가 손상되어, 삭제된 데이터가 저장된 주소를 알 수 없을 때는 사용할 수 없다.

③ 파일의 헤더(Header), 푸터(Footer), 내부 데이터 구조에 대한 정보를 활용하여 파일을 식별하고 추출한다.

④ 삭제된 파일의 데이터가 저장되었던 영역에 새로운 데이터를 덮어쓰게 되면 삭제된 데이터를 복구하지 못할 수 있다.

정답 2번

간단한 해설

파일 카빙은 **메타데이터 대신 파일 내용의 패턴과 구조**를 이용한다. 따라서 메타데이터가 손상되어 저장 주소를 알 수 없는 경우에도 남은 데이터를 탐색하여 복구를 시도할 수 있다.

선지별 해설

① O: 파일 카빙은 단편화된 파일에도 적용할 수 있다. 파일 형식의 내부 구조 등을 이용해 떨어진 조각의 연결 관계를 분석하는 방식이 있다. 다만 단순히 헤더부터 연속 영역을 추출하는 방식은 단편화에 취약하며, 모든 조각을 반드시 복구하는 것은 아니다.

② X: 파일 카빙은 **파일시스템 메타데이터에 의존하지 않고 내용의 특징으로 파일을 찾는** 방법이다. 따라서 파일의 저장 위치를 알려 주는 메타데이터가 손상되었거나 없어도 사용할 수 있다. 실제 데이터 자체가 남아 있고 식별·재구성할 단서가 있어야 한다.

③ O: 파일 형식별 헤더·푸터의 패턴이나 내부 구조·길이 정보 등을 이용하여 파일 후보의 시작·끝과 구성 관계를 판단한다. 모든 파일 형식에 명확한 헤더와 푸터가 모두 존재하는 것은 아니므로, 형식별 구조에 맞게 분석한다.

④ O: 새로운 데이터가 기존 파일의 내용을 덮어쓰면 복구에 필요한 바이트가 사라질 수 있다. 카빙은 **남아 있는 데이터를 식별·재구성**하는 방법이지, 덮어써져 없어진 내용을 자동으로 되살리는 방법은 아니다.

NoteBase

문 16. 모바일 포렌식에 관한 설명으로 가장 적절하지 않은 것은?

① 디지털포렌식의 한 분야로서 스마트폰, 태블릿 등 모바일 기기에서 디지털 증거를 복구·수집·조사하는 일련의 과정이다.

② 스마트폰은 복수의 장치에 의해 접근, 삭제, 동기화될 수도 있어 수집·조사에 어려움이 있다.

③ 스마트폰은 잠금 해제에 관한 정보를 확보할 필요가 없다.

④ 전원이 켜져 있는 스마트폰을 압수한 경우 '비행기 모드'를 활성화하여 네트워크로부터의 연결을 차단하는 것이 필요하다.

정답 3번

간단한 해설

스마트폰의 잠금·암호화 상태는 **증거 데이터에 대한 접근 가능성**에 영향을 준다. 따라서 잠금 해제 관련 정보를 확보할 필요가 없다는 설명은 적절하지 않다.

선지별 해설

① O: 모바일 포렌식은 스마트폰·태블릿 같은 **모바일 기기의 디지털 증거**를 보존·수집·복구·조사하는 디지털포렌식 분야이다. 기기와 운영체제, 저장 방식, 잠금 상태에 맞는 절차가 필요하다.

② O: 스마트폰의 데이터는 연동된 기기나 서비스의 **동기화·원격 접근·삭제**에 의해 달라질 수 있다. 따라서 압수 당시 상태를 보존하고 외부 통신이나 연동으로 증거가 변하는 위험을 관리해야 한다.

③ X: 잠금 상태와 암호화는 저장 데이터에 접근하고 증거를 수집하는 데 영향을 준다. 따라서 적법한 범위에서 **잠금 해제에 필요한 정보와 현재 잠금 상태를 확보·확인**할 필요가 있다. 모든 기기에 같은 해제 방법을 적용할 수 있다는 뜻은 아니다.

④ O: 이 선지는 켜진 기기를 **네트워크에서 격리해 원격 변경을 방지**한다는 취지이다. 비행기 모드는 그 방법 중 하나지만, 반드시 유일한 방법은 아니며 기기별로 Wi-Fi·블루투스 등 실제 통신 차단 상태를 확인해야 한다. 조작에 따른 변경 위험을 고려해 차폐 등 적합한 방법을 선택하고 조치 내용을 기록한다.

NoteBase

문 17. 「디지털 증거의 처리 등에 관한 규칙(경찰청훈령 제1178호)」 상 '디지털 증거분석 결과보고서'에 기재해야 할 사항으로 가장 적절하지 않은 것은?

① 증거분석을 실시한 증거분석실 규모
② 사건번호 등 분석의뢰정보 및 분석의뢰자정보
③ 분석에 사용된 장비·도구 및 준비과정
④ 증거분석에 의해 획득한 자료 및 이에 대한 상세 내용 등 증거분석결과

정답 1번

①

분석에 사용된 장비·도구와 준비과정 등은 기재해야 하지만, **증거분석실의 규모는 필수 기재사항에 포함되지 않는다**.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제37조(결과보고서 작성) 증거분석관은 분석을 종료한 때에는 다음 각호의 사항을 기재한 디지털 증거분석 결과보고서를 작성하여야 한다. 1. 사건번호 등 분석의뢰정보 및 분석의뢰자정보 2. 증거분석관의 소속 부서 및 성명 3. 분석의뢰물의 정보 및 의뢰 요청사항 4. 분석의뢰물의 접수일시 및 접수자 등 이력정보 5. 분석에 사용된 장비 · 도구 및 준비과정 6. 증거분석과정 및 그 과정을 기록한 사진 · 영상자료 7. 증거분석에 의해 획득한 자료 및 이에 대한 상세 내용 등 증거분석결과 8. 그 밖에 분석과정에서 행한 조치 등 특이사항

②

디지털 증거분석 결과보고서에는 **사건번호 등 분석의뢰정보 및 분석의뢰자정보를 기재해야 한다**.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제37조(결과보고서 작성) 증거분석관은 분석을 종료한 때에는 다음 각호의 사항을 기재한 디지털 증거분석 결과보고서를 작성하여야 한다.
1. 사건번호 등 분석의뢰정보 및 분석의뢰자정보

③

디지털 증거분석 결과보고서에는 **분석에 사용된 장비·도구 및 준비과정을 기재해야 한다**.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제37조(결과보고서 작성) 증거분석관은 분석을 종료한 때에는 다음 각호의 사항을 기재한 디지털 증거분석 결과보고서를 작성하여야 한다.
5. 분석에 사용된 장비 · 도구 및 준비과정

NoteBase

④

디지털 증거분석 결과보고서에는 **증거분석으로 획득한 자료와 그 상세 내용 등 증거분석결과를 기재해야 한다**.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제37조(결과보고서 작성) 증거분석관은 분석을 종료한 때에는 다음 각호의 사항을 기재한 디지털 증거분석 결과보고서를 작성하여야 한다.
7. 증거분석에 의해 획득한 자료 및 이에 대한 상세 내용 등 증거분석결과

NoteBase

문 18. 「디지털 증거의 처리 등에 관한 규칙(경찰청훈령 제1178호)」의 내용으로 가장 적절하지 않은 것은?

① 정보저장매체등에 저장된 전자정보 전부가 아니라 일부를 하드카피 또는 이미징 등의 기술적 방법으로 별도의 다른 정보저장매체에 저장한 것도 “복제본”에 해당한다.

② 경찰관은 혐의사실과 관련될 개연성이 있는 전자정보가 삭제·폐기·조작된 정황이 발견되는 경우 정보저장매체등에 저장된 전자정보 전부를 복제하여 그 복제본을 외부로 반출한 후 전자정보의 압수·수색·검증을 진행할 수 있다.

③ 원본을 반출하는 경우 뿐만 아니라 복제본을 반출하는 경우에도 피압수자등의 참여를 보장한 상태에서 이를 봉인하여야 한다.

④ 유류물인 정보저장매체등을 압수하는 경우에도 선별압수 및 참여에 관한 규정을 준수하여야 한다.

정답 4번

①

복제본은 전자정보 **전부뿐 아니라 일부**를 하드카피·이미징 등의 기술적 방법으로 별도의 정보저장매체에 저장한 것도 포함한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제2조(정의) 이 규칙에서 사용하는 용어의 뜻은 다음과 같다.
6. "복제본"이란 정보저장매체등에 저장된 전자정보 전부 또는 일부를 하드카피 또는 이미징 등의 기술적 방법으로 별도의 다른 정보저장매체에 저장한 것을 말한다.

②

혐의사실과 관련될 개연성이 있는 전자정보의 삭제·폐기·조작 정황으로 **현장 선별압수가 불가능하거나 압수 목적 달성이 현저히 곤란한 경우**, 전자정보 전부를 복제하여 외부로 반출한 뒤 압수·수색·검증을 진행할 수 있다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제12조(압수 · 수색 · 검증영장의 집행 방법)
② 경찰관은 다음 각 호의 사유로 인해 압수 · 수색 · 검증 현장에서 제1항에 따라 선별압수하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란한 경우에는 정보저장매체등에 저장된 전자정보 전부를 복제하여 그 복제본을 외부로 반출한 후 전자정보의 압수 · 수색 · 검증을 진행할 수 있다.
2. 혐의사실과 관련될 개연성이 있는 전자정보가 삭제 · 폐기 · 조작된 정황이 발견되는 경우

NoteBase

③

원본과 복제본 모두 피압수자등의 참여를 보장한 상태에서 봉인해야 한다. 복제본에는 해시값 확인이나 압수·수색·검증 과정 촬영 등 동일성과 무결성을 담보할 조치도 해야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제19조(복제본 반출 시 조치)
① 경찰관은 제12조제2항에 따라 복제본을 획득하는 경우에는 피압수자등의 참여를 보장한 상태에서 이를 봉인하고, 복제본의 해시값을 확인하거나 압수 · 수색 · 검증 과정을 촬영하는 등 디지털 증거의 동일성과 무결성을 담보할 수 있는 적절한 방법과 조치를 해야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제20조(정보저장매체등 원본 반출 시 조치)
① 경찰관은 제12조제3항에 따라 정보저장매체등 원본을 반출하는 경우에는 피압수자등의 참여를 보장한 상태에서 정보저장매체등 원본을 봉인해야 한다.

④

유류물인 정보저장매체등을 압수할 때에는 디지털 증거 수집 규정을 준용하지만, **선별압수 및 참여에 관한 부분은 제외**한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제28조(유류물인 정보저장매체등) 제15조제2항에 따라 유류물인 정보저장매체등을 압수하는 경우에는 본 장의 규정을 준용한다. 다만, 선별압수 및 참여에 관한 부분은 제외한다.

NoteBase

문 19. 디지털포렌식 분석을 위한 도구에 관한 <보기 1>의 용어와 <보기 2>의 설명을 가장 적절하게 연결한 것은?

<보기 1>
(가) Autopsy
(나) EnCase Forensic
(다) Volatility
(라) DFT(Digital Forensic Tool)

<보기 2>
㉠ Sleuth Kit를 윈도우 시스템에서 GUI 형태로 이용할 수 있도록 개발한 오픈소스 기반 디지털포렌식 도구
㉡ OpenText사의 디지털포렌식 조사·분석 소프트웨어로 미국 NIST의 CFTT 검증을 받은 도구
㉢ 메모리 덤프 및 분석을 위해 사용하는 파이썬(Python) 기반 오픈소스 디지털포렌식 도구
㉣ 국가보안기술연구소가 국내 수사환경에 적합하도록 개발한 디지털포렌식 도구

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

정답 1번

간단한 해설

도구의 개발 주체와 분석 대상을 구분한다. **Autopsy는 GUI 플랫폼, EnCase는 OpenText 제품, Volatility는 메모리 분석, DFT는 국가보안기술연구소 도구**에 대응한다.

NoteBase

대응 관계 해설

(가) Autopsy → ㉠: Autopsy는 The Sleuth Kit 등의 기능을 **그래픽 사용자 인터페이스로 활용**하게 하는 오픈소스 디지털포렌식 플랫폼이다. 명령줄 기반 분석 기능을 시각적으로 이용한다는 단서가 대응을 결정한다.

(나) EnCase Forensic → ㉡: OpenText의 디지털 증거 수집·조사·분석 소프트웨어이다. EnCase는 NIST의 CFTT 시험 대상이 된 이력이 있으므로 해당 설명과 연결된다. 다만 CFTT는 **정해진 도구 버전·기능에 대한 시험**으로 이해해야 하며 모든 버전과 분석 결과를 무조건 보증한다는 뜻은 아니다.

(다) Volatility → ㉢: Python 기반 오픈소스 메모리 포렌식 프레임워크로, 메모리 덤프에서 프로세스·모듈 등 실행 상태 정보를 추출·분석한다. 핵심은 **휘발성 메모리 이미지의 분석**이며, 실행 중인 시스템에서 메모리를 획득하는 도구와 분석하는 도구의 역할은 구별한다.

(라) DFT → ㉣: 국가보안기술연구소가 개발한 국가용 디지털포렌식 도구이다. **국내 수사환경을 위한 개발 주체**라는 단서가 앞선 해외 상용 도구 및 오픈소스 도구와 구별된다.

따라서 (가)–㉠, (나)–㉡, (다)–㉢, (라)–㉣의 대응이며, 이 조합은 ①과 일치한다.

NoteBase

문 20. '패킷감청'을 수행하여 디지털 증거를 수집하고자 한다. 다음과 같은 제한을 가하는 패킷감청의 근거 법률로 가장 적절한 것은? (다툼이 있는 경우 판례에 의함)

법은 "범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할 만한 충분한 이유가 있는 경우" 보충적 수사 방법으로 활용하도록 요건을 정하고 있고, 법원의 허가 단계에서 특정 피의자 내지 피내사자의 범죄수사를 위해 그 대상자가 사용하는 특정 인터넷회선에 한하여 필요한 범위 내에서만 감청이 이루어지도록 제한이 되어 있다.

① 형사소송법

② 전기통신사업법

③ 통신비밀보호법

④ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정답 3번

NoteBase

②

제시된 패킷감청의 근거 법률은 **통신비밀보호법**이다. 법정 대상범죄에 대한 충분한 혐의와 다른 방법으로 증거 수집 등이 어려운 보충성을 요구하고, 법원이 피의자·피내사자별로 대상과 범위 등을 특정하여 감청을 허가하도록 한다.

통신비밀보호법 제5조(범죄수사를 위한 통신제한조치의 허가요건)
①통신제한조치는 다음 각호의 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있다. <개정 1997.12.13, 2000.1.12, 2001.12.29, 2007.12.21, 2013.4.5, 2015.1.6, 2016.1.6, 2019.12.31>
1. 형법 제2편중 제1장 내란의 죄, 제2장 외환의 죄중 제92조 내지 제101조의 죄, 제4장 국교에 관한 죄중 제107조, 제108조, 제111조 내지 제113조의 죄, 제5장 공안을 해하는 죄중 제114조, 제115조의 죄, 제6장 폭발물에 관한 죄, 제7장 공무원의 직무에 관한 죄중 제127조, 제129조 내지 제133조의 죄, 제9장 도주와 범인은닉의 죄, 제13장 방화와 실화의 죄중 제164조 내지 제167조 · 제172조 내지 제173조 · 제174조 및 제175조의 죄, 제17장 아편에 관한 죄, 제18장 통화에 관한 죄, 제19장 유가증권, 우표와 인지에 관한 죄중 제214조 내지 제217조, 제223조(제214조 내지 제217조의 미수범에 한한다) 및 제224조(제214조 및 제215조의 예비 · 음모에 한한다), 제24장 살인의 죄, 제29장 체포와 감금의 죄, 제30장 협박의 죄중 제283조제1항, 제284조, 제285조(제283조제1항, 제284조의 상습범에 한한다), 제286조[제283조제1항, 제284조, 제285조(제283조제1항, 제284조의 상습범에 한한다)의 미수범에 한한다]의 죄, 제31장 약취(略取), 유인(誘引) 및 인신매매의 죄, 제32장 강간과 추행의 죄중 제297조 내지 제301조의2, 제305조의 죄, 제34장 신용, 업무와 경매에 관한 죄중 제315조의 죄, 제37장 권리행사를 방해하는 죄중 제324조의2 내지 제324조의4 · 제324조의5(제324조의2 내지 제324조의4의 미수범에 한한다)의 죄, 제38장 절도와 강도의 죄중 제329조 내지 제331조, 제332조(제329조 내지 제331조의 상습범에 한한다), 제333조 내지 제341조, 제342조[제329조 내지 제331조, 제332조(제329조 내지 제331조의 상습범에 한한다), 제333조 내지 제341조의 미수범에 한한다]의 죄, 제39장 사기와 공갈의 죄 중 제350조, 제350조의2, 제351조(제350조, 제350조의2의 상습범에 한정한다), 제352조(제350조, 제350조의2의 미수범에 한정한다)의 죄, 제41장 장물에 관한 죄 중 제363조의 죄
2. 군형법 제2편중 제1장 반란의 죄, 제2장 이적의 죄, 제3장 지휘권 남용의 죄, 제4장 지휘관의 항복과 도피의 죄, 제5장 수소이탈의 죄, 제7장 군무태만의 죄중 제42조의 죄, 제8장 항명의 죄, 제9장 폭행 · 협박 · 상해와 살인의 죄, 제11장 군용물에 관한 죄, 제12장 위령의 죄중 제78조 · 제80조 · 제81조의 죄
3. 국가보안법에 규정된 범죄
4. 군사기밀보호법에 규정된 범죄
5. 「군사기지 및 군사시설 보호법」에 규정된 범죄
6. 마약류관리에관한법률에 규정된 범죄중 제58조 내지 제62조의 죄
7. 폭력행위등처벌에관한법률에 규정된 범죄중 제4조 및 제5조의 죄
8. 「총포 · 도검 · 화약류 등의 안전관리에 관한 법률」에 규정된 범죄중 제70조 및 제71조제1호 내지 제3호의 죄

NoteBase

9. 「특정범죄 가중처벌 등에 관한 법률」에 규정된 범죄중 제2조 내지 제8조, 제11조, 제12조의 죄
10. 특정경제범죄가중처벌등에관한법률에 규정된 범죄중 제3조 내지 제9조의 죄
11. 제1호와 제2호의 죄에 대한 가중처벌을 규정하는 법률에 위반하는 범죄
12. 「국제상거래에 있어서 외국공무원에 대한 뇌물방지법」에 규정된 범죄 중 제3조 및 제4조의 죄

통신비밀보호법 제6조(범죄수사를 위한 통신제한조치의 허가절차)
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>
⑥제5항의 허가서에는 통신제한조치의 종류 · 그 목적 · 대상 · 범위 · 기간 및 집행장소와 방법을 특정하여 기재하여야 한다. <개정 2001.12.29>

NoteBase

③

통신비밀보호법은 법정 대상범죄를 계획·실행 중이거나 이미 실행하였다고 의심할 충분한 이유와 다른 방법으로 범죄 저지·범인 체포·증거 수집이 어려운 경우라는 보충성 요건을 정한다. 법원은 피의자·피내사자별로 감청을 허가하며, 허가서에 대상·범위·기간·방법 등을 특정한다.

통신비밀보호법 제5조(범죄수사를 위한 통신제한조치의 허가요건)
①통신제한조치는 다음 각호의 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있다. <개정 1997.12.13, 2000.1.12, 2001.12.29, 2007.12.21, 2013.4.5, 2015.1.6, 2016.1.6, 2019.12.31>
1. 형법 제2편중 제1장 내란의 죄, 제2장 외환의 죄중 제92조 내지 제101조의 죄, 제4장 국교에 관한 죄중 제107조, 제108조, 제111조 내지 제113조의 죄, 제5장 공안을 해하는 죄중 제114조, 제115조의 죄, 제6장 폭발물에 관한 죄, 제7장 공무원의 직무에 관한 죄중 제127조, 제129조 내지 제133조의 죄, 제9장 도주와 범인은닉의 죄, 제13장 방화와 실화의 죄중 제164조 내지 제167조 · 제172조 내지 제173조 · 제174조 및 제175조의 죄, 제17장 아편에 관한 죄, 제18장 통화에 관한 죄, 제19장 유가증권, 우표와 인지에 관한 죄중 제214조 내지 제217조, 제223조(제214조 내지 제217조의 미수범에 한한다) 및 제224조(제214조 및 제215조의 예비 · 음모에 한한다), 제24장 살인의 죄, 제29장 체포와 감금의 죄, 제30장 협박의 죄중 제283조제1항, 제284조, 제285조(제283조제1항, 제284조의 상습범에 한한다), 제286조[제283조제1항, 제284조, 제285조(제283조제1항, 제284조의 상습범에 한한다)의 미수범에 한한다]의 죄, 제31장 약취(略取), 유인(誘引) 및 인신매매의 죄, 제32장 강간과 추행의 죄중 제297조 내지 제301조의2, 제305조의 죄, 제34장 신용, 업무와 경매에 관한 죄중 제315조의 죄, 제37장 권리행사를 방해하는 죄중 제324조의2 내지 제324조의4 · 제324조의5(제324조의2 내지 제324조의4의 미수범에 한한다)의 죄, 제38장 절도와 강도의 죄중 제329조 내지 제331조, 제332조(제329조 내지 제331조의 상습범에 한한다), 제333조 내지 제341조, 제342조[제329조 내지 제331조, 제332조(제329조 내지 제331조의 상습범에 한한다), 제333조 내지 제341조의 미수범에 한한다]의 죄, 제39장 사기와 공갈의 죄 중 제350조, 제350조의2, 제351조(제350조, 제350조의2의 상습범에 한정한다), 제352조(제350조, 제350조의2의 미수범에 한정한다)의 죄, 제41장 장물에 관한 죄 중 제363조의 죄
2. 군형법 제2편중 제1장 반란의 죄, 제2장 이적의 죄, 제3장 지휘권 남용의 죄, 제4장 지휘관의 항복과 도피의 죄, 제5장 수소이탈의 죄, 제7장 군무태만의 죄중 제42조의 죄, 제8장 항명의 죄, 제9장 폭행 · 협박 · 상해와 살인의 죄, 제11장 군용물에 관한 죄, 제12장 위령의 죄중 제78조 · 제80조 · 제81조의 죄
3. 국가보안법에 규정된 범죄
4. 군사기밀보호법에 규정된 범죄
5. 「군사기지 및 군사시설 보호법」에 규정된 범죄
6. 마약류관리에관한법률에 규정된 범죄중 제58조 내지 제62조의 죄
7. 폭력행위등처벌에관한법률에 규정된 범죄중 제4조 및 제5조의 죄
8. 「총포 · 도검 · 화약류 등의 안전관리에 관한 법률」에 규정된 범죄중 제70조 및 제71조제1호 내지 제3호의 죄

NoteBase

9. 「특정범죄 가중처벌 등에 관한 법률」에 규정된 범죄중 제2조 내지 제8조, 제11조, 제12조의 죄
10. 특정경제범죄가중처벌등에관한법률에 규정된 범죄중 제3조 내지 제9조의 죄
11. 제1호와 제2호의 죄에 대한 가중처벌을 규정하는 법률에 위반하는 범죄
12. 「국제상거래에 있어서 외국공무원에 대한 뇌물방지법」에 규정된 범죄 중 제3조 및 제4조의 죄

통신비밀보호법 제6조(범죄수사를 위한 통신제한조치의 허가절차)
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>
⑥제5항의 허가서에는 통신제한조치의 종류 · 그 목적 · 대상 · 범위 · 기간 및 집행장소와 방법을 특정하여 기재하여야 한다. <개정 2001.12.29>

NoteBase