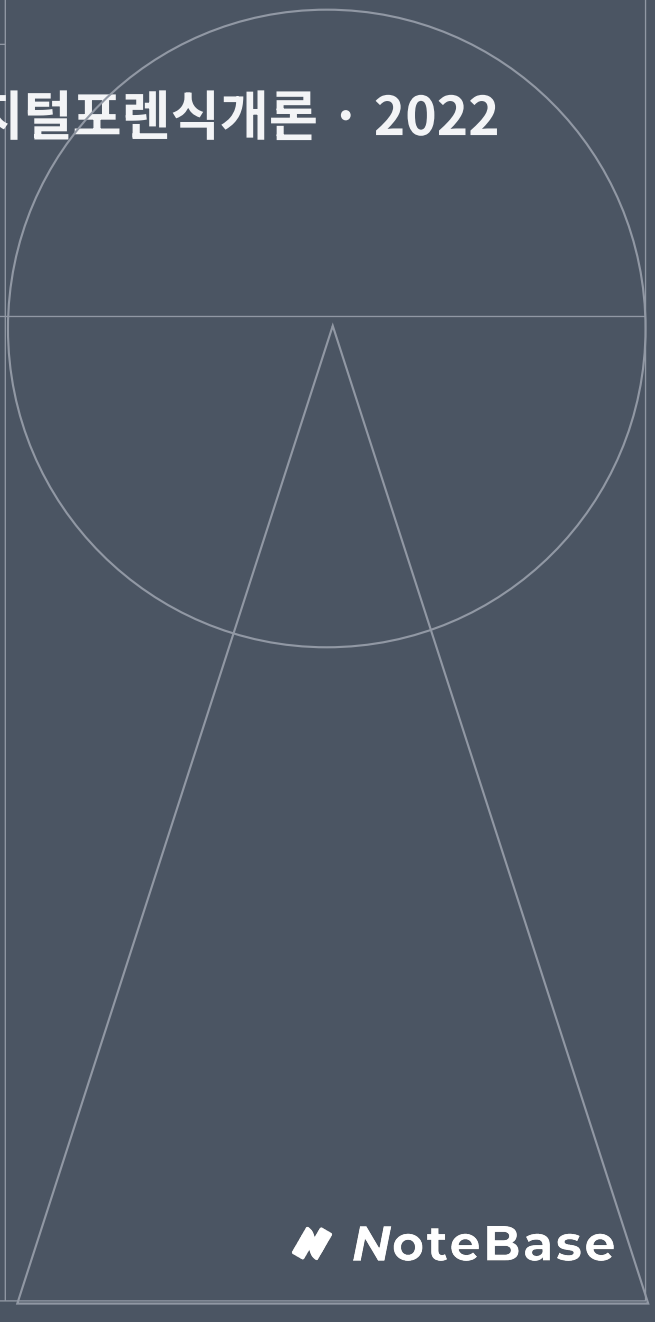
기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2022



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2022

공무원/경찰/경력채용 · 디지털포렌식개론 · 2022

문 1. 범죄와 관련된 사용자 PC의 윈도우 레지스트리 헤더 정보 중 가장 적절하지 않은 것은?

① 시그니처(signature)

② 마지막 수정시간

③ 카탈로그 파일(catalog file)

④ 하이브 포맷 버전 번호

정답 3번

간단한 해설

카탈로그 파일은 하이브 헤더의 정보가 아니다. 레지스트리 하이브 헤더에는 형식 식별용 시그니처, 마지막 기록 시각, 하이브 포맷의 버전 번호 등이 저장된다.

선지별 해설

① O: 하이브 파일의 헤더에는 파일 형식을 식별하는 **'regf' 시그니처**가 들어 있다. 이는 레지스트리 하이브임을 나타내는 고정 식별 값이다.

② O: 헤더에는 하이브의 마지막 기록 시점을 나타내는 **타임스탬프**가 저장된다. 개별 레지스트리 키의 수정시간과는 구별되는 하이브 수준의 시간 정보이다.

③ X: 카탈로그 파일은 레지스트리 하이브 헤더의 구성 필드가 아니다. Windows의 서명된 카탈로그 파일은 여러 파일의 암호학적 해시를 묶어 서명·무결성 확인에 사용하는 별도 파일이다. 하이브 헤더에는 시그니처, 시간, 버전 등 하이브 구조를 해석하는 정보가 들어 있다.

④ O: 헤더에는 하이브 파일 구조를 해석하는 데 사용하는 **주 버전과 부 버전 번호**가 있다. 이는 운영체제의 제품명이나 응용프로그램 버전이 아니라 하이브 저장 형식의 버전이다.

NoteBase

문 2. 문서의 인쇄 SPL(spool file) 포렌식 분석에 관한 설명으로 가장 적절하지 않은 것은?

· SPL 문서의 인쇄 작업이 끝나면 스풀(spool) 데이터인 ①shd 파일과 ②spp 파일은 자동으로 삭제된다.
· 삭제된 스풀 파일은 하드디스크의 ③미할당 영역과 ④페이징 파일에서 복구할 수 있어, 인쇄된 기밀 유출 문서를 알아낼 수 있다.

① ①

② ②

③ ③

④ ④

정답 2번

간단한 해설

인쇄 스풀 관련 파일은 관리 정보를 담는 SHD와 **인쇄 데이터를 담는 SPL**로 구별된다. 제시문의 spp는 올바른 확장자가 아니다.

보기별 해설

① O. SHD 파일은 인쇄 작업의 **문서명·사용자·프린터 등 관리 정보**를 담는 그림자 파일이다. 일반적인 정상 인쇄 처리에서는 작업이 끝나면 관련 스풀 파일이 삭제되지만, 작업 보존 설정이나 오류 상태 등에 따라 남을 수 있다.

② X. 인쇄할 데이터가 저장되는 스풀 파일의 확장자는 **SPL**이다. 따라서 제시문의 spp 파일은 spl 파일로 고쳐야 하며, SHD와 SPL의 역할을 구별해야 한다.

③ O. 파일을 삭제해도 데이터가 즉시 모두 덮어써지는 것은 아니므로 **미할당 영역에 남은 스풀 데이터**를 복구 대상으로 조사할 수 있다. 복구 여부는 덮어쓰기와 저장장치의 동작 등에 따라 달라진다.

④ O. 인쇄 처리 중 메모리에 있던 내용이 디스크로 페이징되었다면 **페이징 파일에 인쇄 데이터의 일부 흔적**이 남을 수 있다. 따라서 분석 대상이 될 수 있지만, 삭제된 스풀 파일 전체가 항상 페이징 파일에 보존되거나 완전히 복원된다는 뜻은 아니다.

따라서 밑줄 친 부분 중 잘못된 것은 ② spp 파일이며, 올바른 확장자는 spl이다.

NoteBase

문 3. 기밀 데이터 유출사건과 관련된 USB 장치 분석에 대한 설명으로 ㉠, ㉡에 알맞은 용어는?

USB를 윈도우 시스템에 연결시키면, 다양한 (㉠)가 (㉡)와 함께 레지스트리에 남게 된다.

① ㉠: 아티팩트, ㉡: setupapi.dev.log
② ㉠: 아티팩트, ㉡: setup.apidev.db
③ ㉠: 개인정보, ㉡: usb.read.log
④ ㉠: 개인정보, ㉡: usb.dev.db

정답 1번

간단한 해설

USB 사용으로 남는 흔적은 **아티팩트**이며, 장치 설치 기록을 담는 로그는 **setupapi.dev.log**이다. 다만 이 로그는 레지스트리 안에 저장되는 것이 아니라 별도의 파일이다.

빈칸별 해설

㉠ 아티팩트: 기기 사용이나 시스템 동작으로 남는 흔적을 뜻한다. USB 연결·장치 설치로 생성된 레지스트리 항목과 로그 등이 여기에 해당한다. 단순히 개인정보만을 가리키는 말이 아니다.

㉡ setupapi.dev.log: Windows의 장치 설치 과정을 기록하는 텍스트 로그이다. USB 장치 설치 흔적을 확인하는 자료로 사용하며, 기본 위치는 %SystemRoot%\inf이다. 다른 선지의 파일명은 이 장치 설치 로그의 이름과 일치하지 않는다.

원문의 '함께 레지스트리에 남게 된다'는 표현은 저장 위치를 정확히 구분하지 못한다. **setupapi.dev.log는 레지스트리 내부 항목이 아니라 별도의 로그 파일**이며, USB 관련 레지스트리 흔적과 함께 분석한다.

따라서 USB 사용 흔적을 뜻하는 ㉠은 아티팩트, 장치 설치 로그 이름인 ㉡은 setupapi.dev.log로, ①과 대응한다.

NoteBase

문 4. 윈도우 시스템의 WinPrefetchView를 이용하여 얻을 수 있는 정보 중 가장 적절하지 않은 것은?

① 응용프로그램 이름, 경로 정보

② 응용프로그램 마지막 수행 시간 정보

③ 응용프로그램 수행 시 참조된 DLL, INI 경로 정보

④ 응용프로그램 7초 모니터링 후, 프리패치 526개의 파일 생성 정보

정답 4번

간단한 해설

WinPrefetchView는 **이미 생성된 프리패치 파일을 분석해 실행·참조 파일 정보를 표시**한다. 일정 시간 감시한 뒤 정해진 개수의 프리패치 파일을 만드는 도구로 설명하면 안 된다.

선지별 해설

① O: WinPrefetchView는 프리패치 파일을 읽어 **응용프로그램의 이름과 경로**를 확인하는 데 사용된다. 표시 가능한 경로 정보는 프리패치 형식과 도구의 지원 버전 등에 영향을 받을 수 있다.

② O: 프리패치에 기록된 **최근 실행 시각**을 확인할 수 있다. 이는 프로그램 실행 흔적을 분석하는 자료이며, 기록된 시각만으로 실행한 사람까지 바로 확정하는 것은 아니다.

③ O: 프로그램이 실행되면서 읽어 들인 파일 목록에서 **참조된 DLL·INI 등의 경로**를 확인할 수 있다. 프로그램과 관련된 파일 접근 흔적을 보여 주는 것이지 해당 파일의 전체 내용이나 사용자의 모든 행위를 기록한 것은 아니다.

④ X: WinPrefetchView는 운영체제가 남긴 **기존 프리패치 파일의 정보를 읽어 보여 주는 도구**이다. 응용프로그램을 7초 동안 모니터링한 뒤 프리패치 파일 526개를 생성한다는 것은 이 도구에서 얻는 정보의 설명이 아니다. 프리패치 기록 방식과 보관 개수는 Windows 버전 등에 따라 달라질 수 있으므로, 제시된 시간과 개수를 보편적인 생성 규칙으로 볼 수도 없다.

NoteBase

문 5. 윈도우 시스템의 아이콘캐시(IconCache) 분석으로 가장 적절하지 않은 것은?

① IconCache는 Iconographic model을 사용하면 보임

② IconCache_##.db 형태로 저장

③ Fortools 라이브러리를 사용하면 확인이 가능

④ IconCache.db 분석에서 삭제된 응용프로그램의 존재 여부

정답 1번

간단한 해설

아이콘캐시는 **전용 분석 도구나 라이브러리로 데이터베이스를 해석**하여 조사한다. 'Iconographic model'을 사용한다는 ①은 적절하지 않다. 잔존 아이콘·경로는 삭제된 프로그램의 과거 존재를 추적하는 단서가 될 수 있다.

선지별 해설

① (X) 아이콘캐시는 **데이터베이스 형식을 해석하여 내부 아이콘이나 경로를 추출**하는 방식으로 분석한다. 예를 들어 Thumbcache Viewer는 iconcache_*.db의 이미지를 추출·표시한다. 원문에 적힌 'Iconographic model'은 이러한 캐시 파일 분석 방법을 설명하는 표현으로 적절하지 않다. 이를 특정 분석 도구의 이름으로 임의로 바꾸어 이해해서는 안 된다.

② (O) 윈도우 버전에 따라 아이콘캐시는 **iconcache_숫자.db 등 여러 데이터베이스 파일**로 저장된다. 선지의 ##는 파일명에 붙는 숫자 등을 나타내는 표현이다. 모든 버전에서 이 형태만 사용하는 것은 아니며, 별도의 IconCache.db도 분석 대상이 된다.

③ (O) **Fortools는 아이콘캐시 분석 기능을 제공**한다. 다만 라이브러리의 Iconcache 분석 모듈과 thumbnail 분석 모듈은 지원하는 파일 형식이 다르므로, IconCache.db인지 iconcache_##.db인지에 맞게 기능을 선택해야 한다.

④ (O) 캐시에 관련 아이콘이나 실행 파일 경로가 남아 있으면, **현재 삭제된 응용프로그램이 과거에 존재했음을 추적하는 단서**로 활용할 수 있다. 캐시가 재생성·정리되면 흔적이 없을 수 있으므로 모든 삭제 프로그램을 확인할 수 있다는 뜻은 아니다. 또한 아이콘 등록은 보기·복사 등으로도 발생하므로, 캐시 흔적만으로 실행 사실까지 단정하지 않는다.

NoteBase

문 6. 윈도우 운영체제 이벤트 로그 분석에서 가장 적절하지 않은 것은?

· 범죄 관련 증거자료를 포렌식 분석관이 수집 분석할 때, 외부장치 연결, ①공유 폴더 사용/해제, 원격 연결/해제, 네트워크 연결/해제, ②파일/레지스트리 조작, 프로세스 생성, ③이벤트 로그 삭제의 행동 분석이 가능하다.
· 윈도우 시스템의 이벤트를 로그 형태로 관리하며, 이벤트 로그는 윈도우 기본 프로그램인 ④이벤트 리서처(Event Researcher)를 통해서 볼 수 있다.

① ①
② ②
③ ③
④ ④

정답 4번

간단한 해설

윈도우의 기본 이벤트 로그 열람 도구는 **이벤트 뷰어(Event Viewer)**이다. 공유 폴더 사용, 파일·레지스트리 조작, 로그 삭제 행위는 관련 이벤트가 기록되어 있다면 분석 대상이 된다.

보기별 해설

① O. 공유 폴더에 대한 **접근·공유 해제**는 이벤트 로그 분석 대상이다. 관련 감사가 설정되어 로그가 생성·보존되어 있다면 공유 접근(예: 5140)이나 공유 객체 삭제(예: 5144) 기록으로 행위를 추적할 수 있다.

② O. **파일 접근과 레지스트리 값 변경**도 감사 이벤트를 통해 조사할 수 있다. 예를 들어 파일 접근 권한 사용은 4663, 레지스트리 값 변경은 4657 등의 이벤트와 관련된다. 다만 감사 정책과 대상의 감사 설정 등 기록 조건을 충족해야 하며, 모든 조작이 기본적으로 빠짐없이 남는다는 뜻은 아니다.

③ O. **이벤트 로그를 지운 행위 자체**도 분석할 수 있다. 예를 들어 보안 감사 로그를 비우면 1102 이벤트가 생성되어 수행 계정 등을 확인하는 단서가 된다. 이는 지워진 과거 로그의 내용까지 모두 복원된다는 뜻은 아니다.

④ X. 윈도우에 기본 제공되는 로그 열람 도구의 이름은 **이벤트 뷰어(Event Viewer)**이다. 이벤트 리서처(Event Researcher)는 이 기본 도구의 올바른 명칭이 아니다.

따라서 가장 적절하지 않은 것은 기본 로그 열람 도구의 명칭을 잘못 제시한 ④이다.

NoteBase

문 7. 스마트폰 단말기에 관한 포렌식 분석에서 빈칸에 가장 적절한 것은?

스마트폰 단말기는 휴대폰 장치 및 가입자 식별 모듈로 구성되어 있다. ( )(은)는 모바일 장치나 단말기를 유일하게 식별하는 데 쓰이는 번호로 처음 6~8자리 숫자는 유형할당코드(type allocation code)이다. 유형할당코드는 무선 장치의 유형을 식별한다.

① 스마트폰 Model-Version

② 스마트폰 S/N(Serial Number)

③ IMEI(International Mobile Equipment Identity)

④ 스마트폰 국제 전화 번호

정답 3번

간단한 해설

단말기 자체를 식별하며 TAC를 포함하는 번호는 IMEI이다. 가입자의 전화번호나 단순한 모델명이 아니라 이동통신 장치의 국제 식별 번호이다.

빈칸별 해설

빈칸에는 IMEI가 들어간다. IMEI는 가입자가 아니라 **이동통신 단말기 자체를 식별**하는 국제 식별 번호이다. 앞부분의 TAC가 단말기의 유형을 식별한다는 단서가 이에 해당한다. 통상 15자리 IMEI는 8자리 TAC, 6자리 일련번호, 1자리 검사 숫자로 구성되며, 과거 체계에서는 TAC가 6자리였다.

모델·버전은 같은 제품군의 여러 단말기가 공유할 수 있고, 제조사의 S/N만으로는 지문에 제시된 TAC를 포함하는 국제 단말기 식별 체계를 뜻하지 않는다. 국제 전화번호는 통신 서비스의 전화번호로, 단말기 장치의 고유 식별 번호와 구별된다.

따라서 빈칸에 대응하는 선택지는 ③ IMEI이다.

NoteBase

문 8. 스마트폰에 들어있는 SIM 카드 포렌식 분석에서 가장 적절하지 않은 내용은?

· SIM 카드의 IMSI는 고유번호이다. ①MCC(Mobile Country Code)는 IMSI의 처음 3자리 숫자를 의미하며, 뒤에 오는 2~3자리 숫자는 ②MNC(Mobile Network Code)이다.
· IMSI의 마지막 부분은 최대 10자리 ③MSIN(Mobile Subscriber Identity Number)으로, 휴대폰 통신사에 의해 생성되며 통신망 가입자를 식별하는 역할을 하고 있다.
· ④MSISDN(Mobile Subscriber Integrated Services Digital Network)은 19~20자리 또는 더 작은 수로 SIM 카드에 새겨져 있다.

① ①
② ②
③ ③
④ ④

정답 4번

간단한 해설

MSISDN은 가입자의 전화번호이고, **ICCID는 SIM 카드의 식별번호**이다. 카드에 새겨진 식별번호를 MSISDN과 혼동한 부분이 잘못되었다.

보기별 해설

① O: MCC는 이동통신 국가 코드로 IMSI의 첫 3자리이다. IMSI는 이동통신 가입을 식별하는 번호이며 MCC, MNC, MSIN으로 구성된다.

② O: MNC는 이동통신망 코드로 MCC 다음에 위치하는 2자리 또는 3자리이다. 국가 코드와 결합하여 해당 이동통신망을 구분한다.

③ O: MSIN은 해당 통신망 안에서 가입을 식별하는 부분이다. IMSI가 최대 15자리이고 MCC가 3자리이므로, **MNC가 2자리이면 MSIN은 최대 10자리**, MNC가 3자리이면 최대 9자리이다.

④ X: MSISDN은 일반적으로 전화를 걸 때 사용하는 가입자의 전화번호이다. **SIM 카드 자체의 식별번호는 ICCID**이며, 카드 외부에 인쇄되기도 한다. 따라서 카드에 새겨진 식별번호를 MSISDN이라고 한 부분이 잘못되었다.

따라서 가장 적절하지 않은 내용은 ④이다.

NoteBase

문 9. 웹 아티팩트에 관한 설명으로 ㉠, ㉡에 가장 적절한 것은?

· 웹 침해사고 분석을 하는 경우 웹 아티팩트에는 (㉠)가 포함된다.
· 악성코드 유포 사이트로 사용자를 이동하게 만드는 소셜 엔지니어링 공격의 경우, (㉠)의 데이터는 특정 (㉡)로 이동하였음을 알려준다.
· (㉡)을(를) 추출한 후 내·외부의 자료를 근거로 이미 알려진 악성 웹 사이트 목록과 비교해 볼 수 있다.

① ㉠: Web history, ㉡: Mac Marshal
② ㉠: Da_destination.db, ㉡: URL
③ ㉠: Web history, ㉡: URL
④ ㉠: Da_destination.db, ㉡: Mac Marshal

정답 3번

간단한 해설

웹 방문 기록에서 URL을 추출해 악성 사이트 목록과 대조하는 과정이다. 기록의 종류와 기록에 담긴 방문 주소를 구별하면 된다.

빈칸별 해설

㉠ Web history: 웹 브라우저의 **방문 기록**은 사용자가 어떤 웹 페이지로 이동했는지 분석하는 웹 아티팩트이다. 제시문은 이 기록에서 방문 목적지를 추출하여 악성 사이트 목록과 비교하는 흐름을 설명하므로 Web history가 들어간다. 특정 데이터베이스 파일명인 Da_destination.db 자체를 웹 방문 기록의 일반 명칭으로 볼 수는 없다.

㉡ URL: **웹 자원의 주소**이므로 방문 기록에서 추출한 목적지를 이미 알려진 악성 웹 사이트 목록과 비교할 때 사용하는 값이다. Mac Marshal은 포렌식 분석 도구의 이름이지 방문한 웹 사이트의 주소가 아니다. URL이 목록과 일치한다는 사실은 조사 단서이며, 그것만으로 악성코드 실행이나 감염까지 확정하지는 않는다.

따라서 ㉠은 Web history, ㉡은 URL이므로 정답은 ③이다.

NoteBase

문 10. 윈도우 운영체제에서 바로 가기 Link File 분석으로 알 수 있는 것 중 가장 적절하지 않은 것은?

① 원본 파일시스템 경로

② LNK 파일 타임스탬프

③ 원본 파일 속성(읽기 전용)

④ LNK 파일이 아카이브된 메모리의 주소

정답 4번

간단한 해설

바로 가기 파일은 대상 파일의 경로·속성·시간 정보를 제공하지만, **아카이브된 메모리 주소를 기록하지 않는다**. 내부 데이터 위치를 나타내는 오프셋을 메모리 주소로 해석해서는 안 된다.

선지별 해설

① O: 바로 가기 파일에는 대상 파일을 찾기 위한 경로 정보가 남을 수 있다. LinkInfo의 로컬 경로 또는 네트워크 경로와 상대 경로 등을 분석하여 **원본 대상 파일의 위치**를 파악할 수 있다.

② O: LNK 파일의 파일시스템 메타데이터에서 LNK 자체의 생성·수정 등의 시각을 확인할 수 있다. 다만 **LNK 내부 헤더의 시간은 대상 파일의 시간**이므로, LNK 자체의 타임스탬프와 혼동하지 않아야 한다.

③ O: LNK 헤더의 FileAttributes에는 대상 파일의 속성이 기록된다. 읽기 전용 등의 속성 비트를 해석하면 링크에 저장된 원본 파일의 속성을 파악할 수 있다. 이는 기록 당시 정보이므로 원본의 현재 상태와 반드시 같다고 단정할 수는 없다.

④ X: LNK는 대상 경로와 속성, 시간 등 바로 가기를 해석하는 정보를 담으며, **아카이브된 메모리 주소를 저장하는 형식이 아니다**. 파일 내부의 오프셋은 구조 내 데이터 위치를 가리키는 값으로, 실행 중 메모리 주소와도 구별된다.

NoteBase

문 11. 타임라인 분석에서 가장 적절하지 않은 것은?

· 해킹사고를 조사할 때 응용 프로그램이나 ①파일의 실행 시점은 매우 중요하다.
· 타임스탬프는 응용 프로그램이나 ②메모리 이미지를 검사할 때와 마찬가지로, 또 다른 조사를 수행할 때도 찾을 수 있다.
· 또한, 메모리 이미지에서 특정 ③이미지 파일을 식별하면, 응용 프로그램이나 파일의 ④접근 날짜와 시간을 비교할 수 있고, 시스템에서 관찰됐던 다른 활동과 상호 연관시킬 수 있다.

① ①
② ②
③ ③
④ ④

정답 3번

간단한 해설

메모리 분석에서는 **실행 파일·DLL 등 프로그램 관련 대상을 식별하고 시간 흔적을 대조**한다. 이 문맥의 대상을 단순한 이미지 파일로 바꾼 표현을 구별해야 한다.

보기별 해설

① O: 응용프로그램이나 실행 파일의 **실행 시점**은 침해 행위의 전후 관계를 재구성하는 핵심 단서이다. 다른 로그·파일 활동과 시각을 대조하여 사건의 흐름을 분석한다.

② O: **메모리 이미지에서도 시간 관련 자료**를 찾을 수 있다. 예를 들어 프로세스 생성 시각 같은 정보가 남을 수 있으며, 디스크의 로그나 파일시스템 기록과 함께 타임라인을 구성하는 데 활용한다.

③ X: 이 문맥에서 식별하여 실행·접근 흔적과 연결하려는 대상은 **실행 파일이나 DLL 등 프로그램 관련 파일**이다. 이를 단순히 이미지 파일로 표현한 부분이 의도한 분석 대상을 적절하게 가리키지 못한다. 다만 그림 파일이나 이미지 자료도 메타데이터 등으로 타임라인 분석에 기여할 수 있으므로, 이미지 파일은 어떤 경우에도 분석할 수 없다는 뜻은 아니다.

④ O: 파일 등의 **접근 날짜와 시간**을 다른 시스템 활동의 기록과 대조하면 사건 사이의 시간적 관련성을 분석할 수 있다. 시각의 의미와 갱신 조건, 시간대·시계 오차를 확인해야 하며, 접근 시각을 곧 실행 시각이나 행위자의 확정 증거로 취급해서는 안 된다.

프로그램 관련 실행 파일·DLL을 식별하는 문맥에 맞지 않는 부분은 ③이다.

NoteBase

문 12. 산업기밀 유출 사고로 압수·수색한 하드디스크 이미징 작업을 수행할 때, 가장 적절하지 않은 것은?

① dd 명령어로 파일과 볼륨을 복사하여 이미지를 만들 수 있다.

② 라이브 이미징을 수행하면, 파티션과 마스터 부트 레코드까지 복사된다.

③ 이미지 파일 생성 후에 저장되는 경로에 대한 설정과 파일 압축 크기 설정이 가능하다.

④ 가상화 소프트웨어의 스냅샷 기능을 활용하여 이미지를 만들 수 있다.

정답 2번

간단한 해설

라이브 여부는 수집 당시 시스템의 실행 상태를 뜻한다. 파티션과 MBR까지 포함되는지는 실제 수집 범위에 따라 달라지므로, 라이브 이미징이라는 이유만으로 모두 복사된다고 단정할 수 없다.

선지별 해설

① O: dd는 지정한 입력에서 데이터를 읽어 출력으로 복사하는 도구이다. 파일이나 볼륨·디스크 장치를 입력으로 지정하고 이미지 파일로 저장할 수 있다. 수집 범위는 입력 대상으로 무엇을 선택했는지에 따라 달라진다.

② X: 라이브 이미징은 **시스템이 실행 중인 상태에서 수집**한다는 뜻이지, 디스크의 모든 영역을 반드시 복사한다는 뜻은 아니다. 파티션 구조와 MBR의 포함 여부는 물리 디스크 전체를 수집하는지, 특정 볼륨·파일만 수집하는지에 달려 있다. 라이브 방식에서도 전체 물리 디스크를 대상으로 하면 MBR을 포함할 수 있으므로, 라이브 이미징은 MBR을 절대 복사하지 못한다고 이해해서도 안 된다.

③ O: 이미지 생성 도구에서는 결과 파일의 저장 경로와 지원 형식의 압축 수준·분할 크기 등을 설정할 수 있다. 구체적인 옵션은 도구와 이미지 형식에 따라 다르며, 설정만으로 모든 형식에서 압축이 가능한 것은 아니다.

④ O: 가상화 소프트웨어의 스냅샷은 특정 시점의 가상머신·가상디스크 상태를 보존하는 데 활용할 수 있다. 다만 **스냅샷 파일 하나가 항상 완전한 독립 이미지인 것은 아니며**, 기본 디스크와 차등 이미지 등 관련 파일을 함께 보존해야 상태를 재구성할 수 있다.

NoteBase

문 13. 섬네일(Thumbnail)은 원본파일이 삭제되더라도 지워지지 않아 증거자료로 사용할 수 있다. 섬네일을 분석한 형식과 설명으로 가장 적절하지 않은 것은?

① Thumbcache_32.db - 32×32 픽셀보다 작은 섬네일이 저장되며 모두 GIF 형식이다.

② Thumbcache_96.db - 32×32~96×96 픽셀 사이의 섬네일이 저장되며 모두 BMP 형식이다.

③ Thumbcache_256.db - 96×96~256×256 픽셀 사이의 섬네일이 저장되며 모두 JPEG 또는 PNG 형식이다.

④ Thumbcache_1024.db - 256×256~1024×1024 픽셀 사이의 섬네일이 저장되며 모두 JPEG 형식이다.

정답 1번

간단한 해설

Thumbcache_32.db의 작은 섬네일은 **GIF가 아니라 BMP 형식**이다. 원본 이미지의 형식과 캐시에 저장된 축소 이미지의 형식을 혼동한 설명이다.

선지별 해설

문제는 Windows의 전통적인 크기별 섬네일 캐시 분류를 묻는다. 파일명에 붙은 수는 섬네일 크기 등급을 나타내며, 원본 이미지의 파일 형식과 캐시에 저장된 섬네일의 형식은 구별해야 한다.

① X: Thumbcache_32.db의 작은 섬네일은 **GIF가 아니라 BMP 형식**으로 저장되는 분류이다. 원본 파일이 GIF일 수 있다는 사실과 캐시 내부 섬네일이 GIF라는 주장은 다르다.

② O: Thumbcache_96.db는 96×96 크기 등급의 섬네일 캐시로, 제시된 분류에서는 32×32~96×96 픽셀 범위의 섬네일을 BMP로 저장한다. 작은 크기 등급을 비트맵 형식으로 저장한다는 점에서 32 등급과 연결된다.

③ O: Thumbcache_256.db는 256×256 크기 등급이며, 제시된 분류에서는 96×96~256×256 픽셀 범위의 섬네일을 **JPEG 또는 PNG**로 저장한다. 데이터의 시그니처를 확인하면 두 형식을 구별할 수 있다.

④ O: Thumbcache_1024.db는 더 큰 미리보기용 캐시로, 제시된 분류에서는 256×256~1024×1024 픽셀 범위의 섬네일을 JPEG로 저장한다. 이 크기별 구성을 모든 Windows 버전에 동일하게 적용하는 것은 아니며, 실제 분석에서는 버전과 엔트리의 형식도 확인한다.

NoteBase

문 15. Chrome 웹브라우저의 Cache 폴더의 저장내용으로 가장 적절하지 않은 것은?

① data_0 파일에는 인덱스 정보가 저장

② data_0 파일에는 오프셋 0x001부터 0x512바이트 단위로 저장

③ 캐시 데이터가 적은 경우 data_1, data_2, data_3에 저장

④ 캐시 데이터가 큰 경우 f_0001부터 연속된 파일에 캐시 데이터가 저장

정답 2번

간단한 해설

data_0는 8,192바이트의 헤더 뒤인 **0x2000부터 36바이트 단위**로 캐시 항목의 관리 정보를 저장한다. 0x001부터 0x512바이트 단위로 저장한다는 설명은 시작 위치와 단위를 잘못 제시한 것이다.

선지별 해설

이 문항은 data_0부터 data_3 및 f_ 형식의 파일을 사용하는 Chrome의 블록 파일 기반 캐시 구조를 묻는다.

① O: data_0에는 캐시 항목을 관리하는 랭킹 노드가 저장된다. 각 노드에는 해당 캐시 항목의 위치를 가리키는 주소가 들어 있으므로, 선지의 '인덱스 정보'는 이러한 **캐시 항목의 위치·관리 정보**를 뜻한다. URL 해시로 항목을 찾는 주 해시 테이블을 저장하는 별도의 index 파일과는 구별된다.

② X: data_0의 블록은 8,192바이트 헤더 뒤인 **오프셋 0x2000부터 0x24바이트, 즉 36바이트 단위**로 저장된다. 따라서 시작 위치를 0x001, 저장 단위를 0x512바이트라고 한 설명은 모두 잘못되었다.

③ O: 작은 캐시 데이터는 고정 크기 블록을 사용하는 data_1, data_2, data_3에 저장된다. 각 파일의 기본 블록 크기는 각각 256바이트, 1,024바이트, 4,096바이트이며, 데이터 크기에 맞는 블록을 사용한다.

④ O: 블록 파일의 저장 한도를 넘는 큰 캐시 데이터는 **f_로 시작하는 별도 파일**에 저장된다. 파일명 뒤에는 순차적으로 부여되는 16진수 번호가 붙는다. 선지의 '연속된 파일'은 이러한 번호 체계를 가리키며, 하나의 데이터를 반드시 여러 파일에 분할하거나 디스크의 연속된 영역에 저장한다는 뜻은 아니다.

NoteBase

문 16. 「디지털 증거의 처리 등에 관한 규칙(경찰청훈령 제1030호)」 제13조에서 압수·수색·검증 시 참여 보장에 관한 내용으로 가장 적절하지 않은 것은?

① 전자정보를 압수·수색·검증할 경우에는 피의자 또는 변호인, 소유자, 소지자, 보관자의 참여를 보장하여야 한다. 이 경우, 압수·수색·검증 장소가 「형사소송법」 제123조제1항, 제2항에 정한 장소에 해당하는 경우에는 「형사소송법」 제123조에 정한 참여인의 참여를 함께 보장하여야 한다.

② 경찰관은 제13조 제1항에 따른 피의자 또는 변호인의 참여를 압수·수색·검증의 전 과정에서 보장하고, 미리 집행의 일시와 장소를 통지하여야 한다. 다만, 위 통지는 참여하지 아니한다는 의사를 명시한 때 또는 참여가 불가능하거나 급속을 요하는 때에는 예외로 한다.

③ 경찰관은 피압수자 등이 전자정보의 압수·수색·검증 절차 참여과정에서 알게 된 사건관계인의 개인정보를 공지하여, 피압수자 등에게 협조를 요청할 수 있다.

④ 전자정보 압수·수색·검증에 따른 참여의 경우 경찰관은 참여인과 압수정보와의 관련성, 전자정보의 내용, 개인정보보호 필요성의 정도에 따라 압수·수색·검증 시 참여인 및 참여 범위를 고려하여야 한다.

정답 3번

①

전자정보 압수·수색·검증에서는 **피의자·변호인과 소유자·소지자·보관자 등의 참여권을 보장**해야 한다.
공무소나 타인의 주거 등 법정 장소에서는 **책임자·주거주·간수자 등 법정 참여인의 참여도 함께 보장**해야 한다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제16조(압수 · 수색 · 검증 시 참여 보장)
① 경찰관은 전자정보 압수 · 수색 · 검증의 전 과정에서 피압수자등의 참여를 보장해야 한다.

(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.
1. 피압수자, 「형사소송법」 제123조에서 정한 참여인 또는 변호인(이하 "피압수자등"이라 한다)이 협조하지 않거나, 협조를 기대할 수 없는 경우

형사소송법 제123조(영장의 집행과 책임자의 참여)
① 공무소, 군사용 항공기 또는 선박 · 차량 안에서 압수 · 수색영장을 집행하려면 그 책임자에게 참여할 것을 통지하여야 한다.
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.

NoteBase

②

피압수자등의 참여는 **압수·수색·검증의 전 과정에서 보장**하며 집행 일시와 장소를 미리 통지해야 한다. 다만, **불참 의사를 명시하거나 참여가 불가능하거나 급속을 요하는 경우**에는 사전 통지를 생략할 수 있다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제16조(압수 · 수색 · 검증 시 참여 보장) ① 경찰관은 전자정보 압수 · 수색 · 검증의 전 과정에서 피압수자등의 참여를 보장해야 한다. ② 경찰관은 제1항에 따른 참여를 보장하기 위하여 미리 집행의 일시와 장소를 통지해야 한다. 다만, 위 통지는 피압수자등이 참여하지 않는다는 의사를 명시한 때 또는 참여가 불가능하거나 급속을 요하는 때에는 예외로 한다.

③

협조 요청의 내용은 참여 과정에서 알게 된 사건관계인의 **개인정보와 수사비밀 등을 누설하지 않도록 하는 것**이다. 개인정보를 공지하여 협조를 요청한다는 설명은 이와 반대이다.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제16조(압수 · 수색 · 검증 시 참여 보장)
⑤ 경찰관은 피압수자등이 전자정보의 압수 · 수색 · 검증절차 참여과정에서 알게 된 사건관계인의 개인정보와 수사비밀 등을 누설하지 않도록 피압수자등에게 협조를 요청할 수 있다.

④

참여인과 압수정보의 관련성, 전자정보의 내용, 개인정보보호 필요성의 정도를 고려하여 **참여인 및 참여 범위를 정해야 한다**.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제16조(압수 · 수색 · 검증 시 참여 보장)
③ 제1항에 따른 참여의 경우 경찰관은 참여인과 압수정보와의 관련성, 전자정보의 내용, 개인정보보호 필요성의 정도에 따라 압수 · 수색 · 검증 시 참여인 및 참여 범위를 고려하여야 한다.

NoteBase

문 17. 파일의 미리보기, 삭제 및 제거에 관한 설명 중 ㉠, ㉡에 가장 적절한 것은?

· 윈도우 운영체제에서는 로딩속도가 빠른 작은 이미지들을 따로 만들어 놓고 실제 이미지 대신 미리보기를 해준다. 미리보기 이미지가 생성되어 저장된 것을 (㉠)(이)라 한다.
· (㉡)를 사용하는 운영체제는 파일 저장을 더욱 효율적으로 하고자 삭제된 파일 복구가 어렵게 제거하는 경우가 있다.

① ㉠: 링크파일, ㉡: SAS 드라이브(Serial Attached SCSI Drive)
② ㉠: 임시인터넷파일, ㉡: 솔리드 스테이트 드라이브(Solid State Drive)
③ ㉠: index.dat, ㉡: SAS 드라이브(Serial Attached SCSI Drive)
④ ㉠: thumbs.db, ㉡: 솔리드 스테이트 드라이브(Solid State Drive)

정답 4번

간단한 해설

thumbs.db는 작은 미리보기 이미지를 저장하는 썸네일 캐시 파일이다. **SSD**에서는 TRIM과 내부 정리 동작에 따라 삭제 데이터의 복구가 어려워질 수 있다.

빈칸별 해설

㉠: **thumbs.db**. 원본 이미지를 매번 읽는 대신 작은 미리보기 이미지를 재사용하도록 저장하는 썸네일 캐시 파일이다. 다만 윈도우의 모든 버전과 모든 위치에서 이 파일만 사용하는 것은 아니며, 버전·환경에 따라 thumbcache 계열 파일 등도 사용된다. 보기 중 제시된 썸네일 저장 파일에 해당하는 것은 thumbs.db이다.

㉡: **솔리드 스테이트 드라이브(SSD)**. 운영체제가 TRIM 등으로 더 이상 필요하지 않은 논리 영역을 알리면 SSD는 해당 공간을 내부 정리 대상으로 삼을 수 있다. 이후 가비지 컬렉션 등으로 데이터가 지워지면 삭제 파일 복구가 어려워질 수 있다. 이는 삭제 즉시 모든 SSD에서 반드시 복구 불가능해진다는 뜻은 아니며, 명령 지원·설정과 실제 처리 상태에 따라 결과가 달라진다.

따라서 ㉠ thumbs.db와 ㉡ 솔리드 스테이트 드라이브를 짝지은 ④가 해당한다.

NoteBase

문 18. 다음 중 포렌식 도구에 관한 설명으로 가장 적절하지 않은 것은?

① FTK는 포렌식 응용 프로그램으로 네트워크를 통한 이미징이 가능하다.

② BitLocker는 디스크 데이터를 복제하고 암호화 키를 제공하는 하드웨어 장비로, 데이터의 이미징과 완전 삭제, 복구를 지원한다.

③ EnCase는 주로 하드 드라이브와 기타 저장매체를 사용하는 디지털 증거조사에 관한 작업을 수행하며, 분석관이 요약 형식으로 사건 데이터를 출력할 수 있도록 보고기능을 갖고 있다.

④ X-Ways Forensics는 네트워크 접속이나 원격 캡처의 기능 없이 포렌식을 수행한다.

정답 2번

간단한 해설

BitLocker는 **Windows의 드라이브 암호화 기능**이지 디스크 복제·삭제·복구용 하드웨어 장비가 아니다. 포렌식 분석 도구와 암호화 기능의 역할을 구별해야 한다.

선지별 해설

① O: FTK 제품군은 디지털 증거 수집·분석을 위한 소프트웨어이며, 지원되는 원격 수집 구성에서는 **네트워크를 통한 이미징**이 가능하다. 실제 이용 가능 범위는 제품 에디션과 에이전트·라이선스 등 구성 조건에 따라 달라진다.

② X: BitLocker는 Windows의 **드라이브 암호화 기능**이다. 디스크 복제·이미징·완전 삭제·복구를 수행하는 하드웨어 장비의 명칭이 아니다. 복구 키로 암호화된 드라이브에 다시 접근하는 기능과, 삭제 파일을 복구하거나 디스크를 복제하는 포렌식 장비의 기능을 혼동한 설명이다.

③ O: EnCase는 저장매체 등에서 디지털 증거를 수집하고 분석하는 도구이며, **조사 결과를 정리해 보고서로 출력**하는 기능을 제공한다. 분석 결과를 사건 단위로 검토·제시하는 작업을 지원한다.

④ O: 이 선택지는 **기본적인 로컬 디스크·이미지 분석 중심의 사용**을 설명한 것으로 이해해야 한다. X-Ways Forensics는 네트워크 원격 수집 기능을 사용하지 않고도 포렌식을 수행할 수 있다. 다만 원격 기능이 어떤 구성에서도 전혀 없다는 뜻은 아니다. 별도 옵션이나 F-Response 등의 연계를 통한 원격 분석이 가능하므로, 기본 구성과 확장 구성을 구별해야 한다.

NoteBase

문 19. 윈도우10 시스템의 기본 전자우편(e-mail) 프로그램 대상 포렌식 분석으로 확인할 수 있는 것 중 가장 적절하지 않은 것은?

① 전자우편(e-mail) 관련 메타데이터는 store.vol 파일에서 일부 찾을 수 있다.

② 윈도우 기본 아티팩트 폴더 안에는 일정규칙을 가진 .dat파일이 있다.

③ 발송한 전자우편(e-mail)이 경유한 라우터 IP주소를 알 수 있다.

④ 레지스트리 경로에서 기본 전자우편 연동 프로토콜을 확인한다.

정답 3번

간단한 해설

전자우편의 전송 흔적은 **메일 서버의 중계 기록이지 네트워크 라우터의 경유 목록이 아니다**. 따라서 메일 프로그램의 자료만으로 발송 메일이 거친 라우터의 IP주소를 확인할 수 있다는 설명은 부적절하다.

선지별 해설

① O: Windows 10의 기존 기본 메일 앱은 UnistoreDB의 **store.vol 데이터베이스**에 메시지와 계정 등에 관한 정보를 저장한다. 메시지·수신자·첨부파일 관련 테이블을 분석하면 전자우편 메타데이터의 일부를 확인할 수 있다.

② O: 해당 메일 앱의 Unistore 데이터 폴더에는 정해진 저장 구조와 이름 규칙에 따라 생성된 .dat 파일이 존재한다. 데이터베이스의 참조와 이 파일들을 함께 분석하여 메일 본문 등 관련 데이터를 연결할 수 있다. 확장자가 .dat라고 해서 모든 파일의 내용 형식이 같은 것은 아니다.

③ X: 전자우편의 Received 헤더는 **메일을 수신·중계한 메일 서버**에 관한 전송 흔적을 남긴다. IP 패킷이 경유한 네트워크 라우터를 빠짐없이 기록하는 구조가 아니므로, 메일 앱 분석만으로 발송 메일의 경유 라우터 IP주소를 알 수 있다고 할 수 없다.

④ O: 레지스트리의 **mailto 프로토콜 연결 정보**를 살펴보면 메일 링크를 처리하는 기본 프로그램의 등록·연결 상태를 확인할 수 있다. 이는 SMTP·IMAP 같은 메일 전송·접근 프로토콜 설정 자체와는 구별된다.

NoteBase

문 20. 다음은 디지털 증거의 증거능력에 관한 소위 '왕재산 사건'의 판례이다. ㉠~㉢에 가장 적절한 것은?

· (중략) 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 (㉠)이 담보되어야 한다.
· (중략) 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 검증된 프로그램의 (㉡), (중략) 피압수·수색 당사자가 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체의 (㉢)이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법으로 증명하는 것이 원칙(중략)

① ㉠: 무결성, ㉡: 신뢰성, ㉢: Hash값
② ㉠: 동일성, ㉡: 신뢰성, ㉢: Hash값
③ ㉠: 신뢰성, ㉡: Hash값, ㉢: 무결성
④ ㉠: Hash값, ㉡: 무결성, ㉢: 신뢰성

정답 1번

㉠

출력 문건을 증거로 사용하려면 원본에 저장된 내용과의 동일성이 인정되어야 하므로, **정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 무결성**이 담보되어야 한다.

(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. (대법원 2013. 7. 26. 선고 2013도2511 판결)

NoteBase

㉡, ㉢

원본과 복제매체의 동일성을 확인하는 과정에서는 **컴퓨터의 기계적 정확성과 프로그램의 신뢰성**이 담보되어야 한다. 동일성·무결성은 **원본과 복제매체의 Hash값이 같다는 취지로 피압수·수색 당사자가 서명한 확인서면을 법원에 제출하여 증명하는 것이 원칙**이다. 이 방법이 불가능하거나 현저히 곤란하면 절차에 참여한 수사관·전문가의 증언이나 법원의 원본 자료와 출력 문건 대조 등으로도 증명할 수 있다.

(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