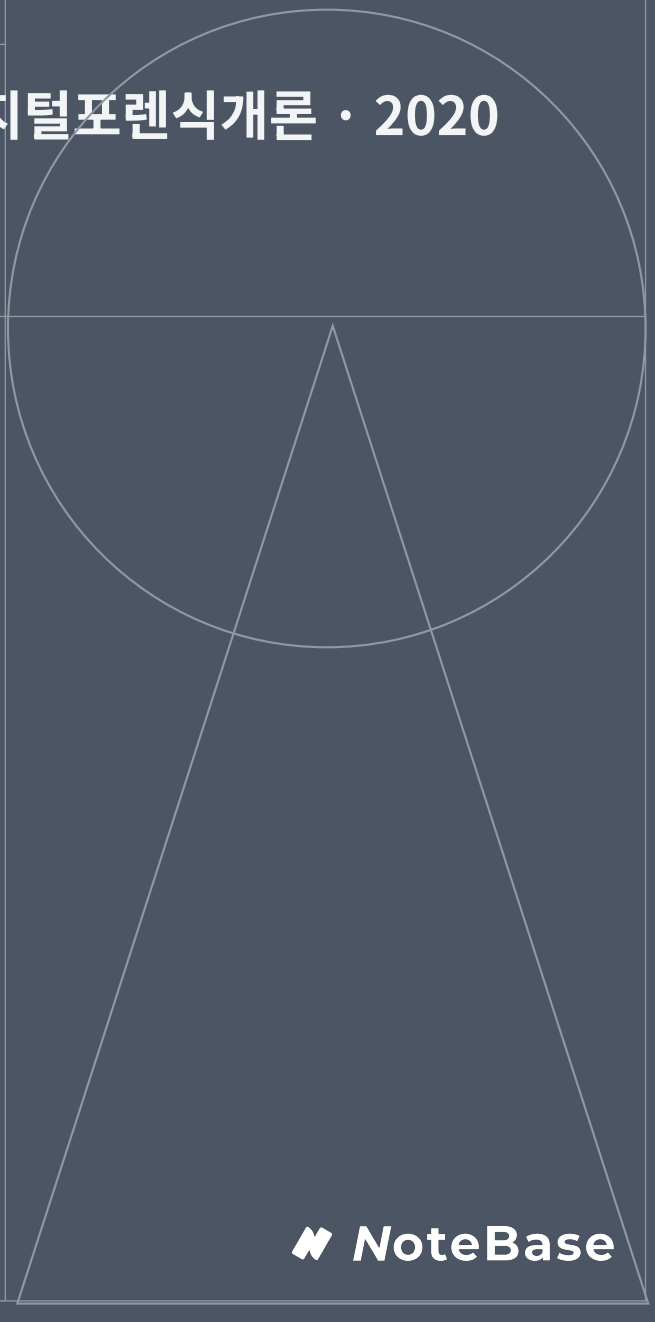
기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2020



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2020

공무원/경찰/경력채용 · 디지털포렌식개론 · 2020

문 1. 피의자는 회사의 중요한 설계도면 파일을 업무용 PC에서 개인 USB로 복사하고, 이후 USB를 자신의 개인 PC에 연결하여 해당 파일 복사 후 이메일을 통해 경쟁 회사로 유출하였으나 설계도면 파일을 유출하지 않았다며 부인하고 있다. 위 행위를 입증하기 위한 것으로 가장 적절하지 않은 것은?

① USB 연결 시간

② 파일의 해시(Hash)값

③ 업무용 PC의 파티션 정보

④ USB 시리얼 번호

정답 3번

간단한 해설

업무용 PC의 **파티션 정보**는 저장장치의 구성을 보여 줄 뿐, 도면 파일이 USB로 복사되고 이메일로 유출된 경로를 직접 나타내지는 않는다. 장치 연결 흔적과 파일 동일성을 보여 주는 자료에 비해 해당 행위와의 관련성이 낮다.

핵심 풀이

USB 연결 시간은 업무용 PC와 개인 PC에서 해당 장치를 사용한 시점을 연결하는 단서이다. 파일 생성·수정 시각이나 이메일 전송 기록과 대조하여 유출 과정의 시간적 흐름을 살핀다.

파일의 해시값은 파일 내용을 바탕으로 계산한 값이다. 업무용 PC의 도면과 USB·개인 PC·이메일 첨부파일의 해시를 비교하면 **동일한 내용의 파일인지 확인하는 근거**를 얻을 수 있다.

USB 시리얼 번호는 연결 기록에 나타난 장치를 식별하는 단서이다. 두 PC의 기록을 대조하여 같은 USB가 사용되었는지 확인하는 데 활용한다. 다만 연결 기록이나 식별값만으로 파일 복사와 유출이 모두 증명되는 것은 아니므로 다른 흔적과 종합한다.

업무용 PC의 파티션 정보는 저장장치의 구획·구성에 관한 정보이다. 파일을 찾는 데 도움이 될 수는 있지만, **도면의 복사·이동이나 이메일 전송 행위와 직접 연결되는 자료는 아니다**. 따라서 제시된 자료 중 유출 행위 입증에 가장 적절하지 않은 것은 ③이다.

NoteBase

문 2. 디지털 증거 수집을 위한 디스크 복제와 디스크 이미징(Imaging)의 설명으로 가장 적절하지 않은 것은?

① 디스크 이미징은 원본 저장매체의 사본을 파일 형태로 만든다.

② 디스크 복제는 디스크 영역 중 비할당영역을 포함하지 않고 사본을 만들며, 디스크 이미징은 디스크 영역 중 비할당영역을 포함하여 사본을 만든다.

③ 디스크 복제와 디스크 이미징은 원본과 사본의 동일함을 증명하기 위한 방법으로 해시값을 이용한다.

④ 디스크 이미징으로 생성한 사본파일은 분석을 위한 분석 전용 소프트웨어가 필요하다.

정답 2번

간단한 해설

디스크 복제와 이미징은 저장 대상을 매체 또는 파일로 구분한 것이며, **물리적 비트 단위 획득에서는 둘 다 비할당영역을 포함**할 수 있다. 따라서 복제는 비할당영역을 포함하지 않는다고 한 ②가 가장 적절하지 않다.

선지별 해설

① (O) 디스크 이미징은 원본 저장매체의 데이터를 **이미지 파일 형태**로 저장하는 방식이다. 이 문항에서 디스크 복제는 다른 저장매체에 직접 복사하는 방식과 대비된다. 이미지 형식에 따라 하나의 파일이나 분할 파일로 보관할 수 있다.

② (X) 포렌식 목적의 물리적 비트 단위 복제라면 **디스크 복제와 이미징 모두 비할당영역을 포함**하여 수집할 수 있다. 두 방식의 차이를 비할당영역 포함 여부로 나누는 것은 틀리다. 실제 수집 범위는 물리적 획득인지 논리적 획득인지, 선택한 범위와 도구 설정 등에 따라 결정된다.

③ (O) 원본에서 읽은 데이터와 획득한 사본 데이터의 **해시값을 비교하여 동일성과 무결성을 검증**한다. 비교할 때는 같은 데이터 범위와 해시 알고리즘을 사용해야 한다. 압축·메타데이터가 포함된 이미지 컨테이너 파일 전체의 해시를 원본 디스크 해시와 그대로 비교하는 것이 아니라, 획득된 증거 데이터에 대한 검증값을 확인한다.

④ (O) 이미지 파일 내부의 파일시스템과 삭제 흔적 등을 분석하려면 **그 이미지 형식과 내부 구조를 해석할 수 있는 분석 도구**가 필요하다는 취지이다. 다만 특정 상용 전용 제품만 사용해야 한다는 뜻은 아니다. 지원되는 raw 이미지는 읽기 전용으로 마운트하거나 매체에 복원하여 접근하는 방법도 있으며, 포렌식 분석에는 목적에 맞는 도구를 사용한다.

NoteBase

문 3. 피의자가 아동 음란물 사이트에 접속해서 아동 음란물을 다운받아 소지한 혐의를 부인하고 있다. 피의자의 혐의를 입증할 수 있는 방법으로 가장 적절하지 않은 것은?

① 피의자가 사용한 PC의 인터넷 히스토리(History) 정보에서 해당 아동 음란물 사이트 URL이 발견되었다.

② 피의자가 사용한 PC의 다운로드 폴더에서 해당 아동 음란물과 해시값이 동일한 파일이 저장된 것을 확인하였다.

③ 피의자가 해당 PC를 사용한 시간과 그 PC에서 아동 음란물 사이트 접속한 시간이 일치하여 피의자가 해당 아동 음란물에 접속한 사실을 확인하였다.

④ 피의자가 사용한 PC의 숨김 폴더에 SafeBack 프로그램이 설치된 것을 확인하였다.

정답 4번

간단한 해설

SafeBack은 **디스크 이미징 도구**이므로 설치 사실만으로 특정 사이트 접속이나 문제의 파일 소지를 입증할 수 없다. 대상 파일과 접속·사용 흔적을 직접 연결하는 자료가 필요하다.

선지별 해설

① O: 인터넷 방문 기록에 해당 사이트 URL이 남아 있으면 **사이트 접속과 관련된 흔적**으로 활용할 수 있다. 다만 URL 기록만으로 특정 파일의 다운로드나 피의자 본인의 고의적 접속까지 모두 확정할 수는 없으므로 다른 기록과 함께 해석해야 한다.

② O: 다운로드 폴더에서 대상 파일과 해시값이 일치하는 파일을 발견하면 **해당 파일이 PC에 저장되어 있음을 뒷받침**하는 자료가 된다. 적절한 해시 비교와 파일 검증을 전제로 파일 동일성을 판단하되, 누가 어떤 경위로 저장했는지는 별도의 다운로드 기록·사용 흔적 등을 함께 확인해야 한다.

③ O: 피의자의 PC 사용 시간과 사이트 접속 기록의 시간을 대조하는 것은 **사용자와 접속 행위를 연결하는 정황**을 찾는 방법이다. 다만 시각 일치만으로 행위자를 단정하는 것은 아니며, 기록의 시간대·시계 오차, 공용 사용이나 원격 접속 가능성 등을 점검하고 다른 자료와 종합해야 한다.

④ X: SafeBack은 디스크를 비트 단위로 복제하거나 이미지를 만드는 **디스크 이미징 도구**이다. 숨김 폴더에 이 프로그램이 설치되어 있다는 사실만으로 특정 사이트 접속이나 문제의 파일 다운로드·소지를 입증할 수 없다. 프로그램의 존재와 실제 대상 파일·접속 흔적은 구별해야 한다.

NoteBase

문 4. 피의자는 지하철에서 자신의 휴대폰을 사용하여 타인의 신체를 몰래 촬영한 혐의를 받고 있다. 피의자의 휴대폰에서 범죄 혐의와 관련된 디지털 증거를 획득하는 방법으로 가장 적절하지 않은 것은?

① Falcon을 이용한 획득

② JTAG을 이용한 획득

③ Chip-off를 이용한 획득

④ 데이터 케이블을 이용한 획득

정답 1번

간단한 해설

이 문제의 'Falcon'은 일반 저장매체의 복제·이미징 장비로, **휴대폰 내부 데이터 획득을 위한 JTAG·Chip-off·케이블 기반 추출과 구별**된다. 단순히 USB로 연결할 수 있다는 사실만으로 휴대폰 내부 메모리에 접근할 수 있는 것은 아니다.

핵심 풀이

휴대폰 내부의 촬영 파일을 확보하려면 단말기 운영체제나 메모리에 접근할 수 있는 획득 방법이 필요하다. 이 문제의 'Falcon'은 2020년 출제 맥락의 저장매체 이미징 장비를 가리킨다. SAS·SATA·USB 등으로 연결한 저장매체를 복제하는 장비라는 점에서, **휴대폰 내부 데이터에 직접 접근하는 전용 획득 방법과 구별**된다. 따라서 제시된 방법 중 가장 적절하지 않은 것은 ①이다. 휴대폰에 USB 단자가 있다는 사실만으로 일반 디스크처럼 내부 저장공간 전체를 읽을 수 있는 것은 아니다.

JTAG은 기판의 시험·디버깅 인터페이스를 통해 메모리 데이터를 읽는 방법이다. 해당 단말기의 인터페이스 접근과 장비 지원이 가능해야 하며, 모든 휴대폰에서 성공하는 것은 아니다.

Chip-off는 메모리 칩을 기판에서 분리하여 리더로 읽는 방식이다. 휴대폰 데이터 획득에 활용될 수 있지만 **칩 손상 위험과 암호화의 제약**을 고려해야 한다. 칩의 원시 데이터를 읽었다고 해서 암호화된 촬영 파일이 곧바로 해독되는 것은 아니다.

데이터 케이블을 이용한 획득은 휴대폰과 분석 장비를 연결하고 지원되는 통신 방식과 포렌식 도구로 파일이나 데이터를 추출하는 방법이다. 잠금 상태·접근 권한·기종·운영체제와 도구의 지원 범위에 따라 획득 가능 범위가 달라진다.

NoteBase

문 5. 디지털 증거 수집에 대한 설명으로 가장 적절하지 않은 것은?

① 영장에 의한 압수·수색의 경우 범죄사실의 관련성과 피의자에게 혐의가 있다고 인정되는 경우에 한정한다.

② 영장에 의하지 않은 압수·수색 중 증거의 계속 사용을 위해 사후영장을 반드시 요하는 경우는 임의제출물의 압수인 경우다.

③ 도박·음란·기타 불법사이트 운영 사건 등 디지털 저장매체에 저장된 원본 디지털 데이터가 다시 범죄에 이용될 우려가 있는 경우 디지털 저장매체 자체를 압수할 수 있다.

④ 디지털 데이터를 압수하는 경우에는 범죄사실과 관계가 있다고 인정할 수 있는 범위를 정하여 출력하거나 복제하는 방법으로 압수하여야 한다.

정답 2번

①

영장에 의한 수사상 압수·수색은 **피의자가 죄를 범하였다고 의심할 만한 정황**이 있고, **해당 사건과 관계가 있다고 인정할 수 있는 것**에 한정하여 허용된다.

형사소송법 제215조(압수, 수색, 검증)
② 사법경찰관이 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 검사에게 신청하여 검사의 청구로 지방법원판사가 발부한 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.

②

소유자·소지자·보관자가 임의로 제출한 물건은 영장 없이 압수할 수 있으며, **별도의 사후영장도 필요하지 않다**. 현행범 체포현장이나 범죄 현장에서 임의제출한 경우에도 같다.

검사 또는 사법경찰관은 피의자 등이 유류한 물건이나 소유자·소지자 또는 보관자가 임의로 제출한 물건을 영장 없이 압수할 수 있다(형사소송법 제218조). 따라서 현행범 체포현장이나 범죄 현장에서도 소지자 등이 임의로 제출하는 물건을 형사소송법 제218조에 따라 영장 없이 압수하는 것이 허용되고, 이 경우 검사나 사법경찰관은 별도로 사후에 영장을 받을 필요가 없다(대법원 2016. 2. 18. 선고 2015도13726 판결, 대법원 2019. 11. 14. 선고 2019도13290 판결, 대법원 2020. 4. 9. 선고 2019도17142 판결 참조). (대법원 2022. 8. 31. 선고 2019도15178 판결)

NoteBase

③

불법사이트 운영에 사용되어 원본 데이터가 다시 범죄에 이용될 우려가 있는 저장매체는 **범행에 제공된 물건으로서 몰수 대상이 될 수 있으므로, 전자정보와 별도로 저장매체 자체에 대한 영장을 발부받아 압수할 수 있다**.

(경찰청) 디지털 증거의 처리 등에 관한 규칙 제10조(압수 · 수색 · 검증영장의 신청)
③ 경찰관은 다음 각 호의 어느 하나에 해당하여 필요하다고 판단하는 경우 전자정보와 별도로 정보저장매체등의 압수 · 수색 · 검증영장을 신청할 수 있다.
1. 정보저장매체등이 「형법」 및 그 밖의 법률에서 정하는 몰수사유에 해당하는 경우

④

전자정보는 원칙적으로 **범죄사실과 관련된 범위를 정하여 출력하거나 복제**하는 방식으로 압수한다. 다만, 이러한 방식이 불가능하거나 압수 목적을 달성하기에 현저히 곤란한 때에는 저장매체 자체를 압수할 수 있다.

형사소송법 제106조(압수)
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>

형사소송법 제215조(압수, 수색, 검증)
② 사법경찰관이 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 검사에게 신청하여 검사의 청구로 지방법원판사가 발부한 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.

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

문 6. 다음 웹 로그의 내용 중 ㉠, ㉡, ㉢, ㉣에 해당하는 용어를 순서대로 나열한 것으로 가장 적절한 것은?

㉠ 웹 서버 사용자가 사이트에 접근 시 사용자 IP 정보, 시간 정보, 요청 정보가 기록된다.
㉡ 웹 서버 내부에서 발생하는 에러와 사용자의 접속실패에 관한 정보가 기록된다.
㉢ 현재 웹 서버를 이용하기 전에 어떤 경유지를 거쳐서 도착하게 되었는지에 대한 정보를 알려준다.
㉣ 웹 서버 사용자에 대한 정보를 확인할 수 있는 로그로 사용자의 브라우저 종류와 버전, 운영체제의 종류 등에 대해서 알 수 있다.

① 엑세스 로그(Access Log) - 에러 로그(Error Log) - 에이전트 로그(Agent Log) - 레퍼러 로그(Referrer Log)
② 에이전트 로그(Agent Log) - 엑세스 로그(Access Log) - 에러 로그(Error Log) - 레퍼러 로그(Referrer Log)
③ 레퍼러 로그(Referrer Log) - 에러 로그(Error Log) - 엑세스 로그(Access Log) - 에이전트 로그(Agent Log)
④ 엑세스 로그(Access Log) - 에러 로그(Error Log) - 레퍼러 로그(Referrer Log) - 에이전트 로그(Agent Log)

정답 4번

간단한 해설

접속 IP·시각·요청은 엑세스 로그, 서버 오류는 에러 로그에 대응한다. **이전 페이지의 유입 정보는 레퍼러 로그**, 브라우저·운영체제 등 클라이언트 환경 정보는 에이전트 로그로 구분한다.

NoteBase

대응 관계 해설

㉠ 엑세스 로그(Access Log): 서버가 처리한 요청을 기록한다. 접속 IP, 요청 시각, 요청한 자원과 응답 상태 등을 통해 웹 이용 내역을 파악한다.

㉡ 에러 로그(Error Log): 서버 내부 오류와 요청 처리 중 발생한 문제의 진단 정보를 기록한다. 접속 실패의 원인을 조사하는 데 쓰이며, 실제 기록 범위는 서버 설정과 오류 수준에 따라 달라진다.

㉢ 레퍼러 로그(Referrer Log): 요청의 Referer 정보로 **현재 자원에 연결해 준 이전 페이지**를 파악하는 단서이다. 네트워크 라우터의 전체 경로를 뜻하지 않으며, 해당 정보가 없거나 제한될 수도 있다.

㉣ 에이전트 로그(Agent Log): User-Agent 정보로 브라우저 종류·버전이나 운영체제 등 클라이언트 환경을 파악한다. **클라이언트가 보고한 정보**이므로 실제 환경과 반드시 일치한다고 단정하지 않는다.

따라서 ㉠~㉣은 엑세스 로그 - 에러 로그 - 레퍼러 로그 - 에이전트 로그이며, ④와 일치한다.

NoteBase

문 7. 디지털 포렌식 분석에서 키워드, 시그니처 등으로 대상 파일들을 검색한다. 이에 대한 내용으로 가장 적절하지 않은 것은?

① 동일한 키워드라도 인코딩 방식에 따라 전혀 다른 값이 되기 때문에 검색하고자 하는 키워드의 형태를 결정해서 검색을 수행해야 한다.

② 단순한 일회성 검색은 로우 서치(Raw Search)를 이용하고, 키워드를 바꾸어 가며 여러 번 수행하는 검색은 인덱스 서치(Index Search)를 이용하는 것이 바람직하다.

③ 윈도우 기반 파일에서 시그니처에 따른 파일 확장자는 MBR Entry에 있으며, 확장자에 따라 연결되는 어플리케이션 정보는 레지스트리(Registry)에 저장하고 있다.

④ 데이터 은닉을 위해 파일의 확장자를 변경하는 경우가 있으므로 파일 확장자와 시그니처가 일치하는지 여부를 확인해야 한다.

정답 3번

간단한 해설

MBR 엔트리는 파티션 정보를 담으며 개별 파일의 확장자를 저장하지 않는다. 파일명에 붙은 확장자, 파일 내용의 시그니처, 레지스트리의 연결 프로그램 정보는 구별해야 한다.

선지별 해설

① O: 같은 문자열도 UTF-8·UTF-16 등 **인코딩에 따라 저장되는 바이트 표현이 달라질 수 있다**. 원시 데이터에서 키워드를 찾을 때는 예상되는 인코딩과 문자열 표현을 고려해야 한다. 다만 서로 다른 인코딩에서 모든 문자의 바이트가 반드시 달라지는 것은 아니며, 일부 문자 범위는 같은 표현을 사용할 수 있다.

② O: 로우 서치는 원시 데이터를 직접 훑으므로 색인 생성 없이 일회성 검색을 수행하는 데 적합하다. 인덱스 서치는 먼저 검색용 색인을 구축하는 비용이 들지만, 이후 **여러 키워드를 반복 검색할 때 색인을 재사용**할 수 있다. 실제 효율과 검색 범위는 도구·데이터·색인 설정에 따라 달라진다.

③ X: MBR의 파티션 엔트리는 **파티션의 위치·크기·종류** 등을 담는 것이지 개별 파일의 확장자를 저장하는 곳이 아니다. 확장자는 파일명의 일부로 파일시스템에서 관리되며, 파일 형식의 시그니처는 파일 내용에서 확인한다. Windows에서 확장자와 연결 프로그램의 대응 정보가 레지스트리에 저장된다는 뒷부분과 구별해야 한다.

④ O: 파일명을 바꾸어 확장자를 변경해도 실제 파일 내용과 형식이 함께 바뀌는 것은 아니다. 따라서 **확장자와 내용의 시그니처를 대조**하면 형식을 위장한 파일을 찾는 데 도움이 된다. 불일치는 조사 단서이지 그 자체로 은닉 의도의 확정 증거는 아니며, 시그니처가 없는 형식이나 여러 형식이 같은 표식을 쓰는 경우에는 내부 구조도 함께 분석한다.

NoteBase

문 8. 사용자의 인터넷 사용 흔적을 찾는 방법은 디지털 포렌식에서 유용하게 사용된다. 다음 내용 중 ㉠, ㉡, ㉢에 순서대로 들어갈 단어로 가장 적절한 것은?

· (㉠)는 웹 사이트를 재접속할 때, 웹 페이지 데이터를 다시 다운받지 않고 다운받은 데이터를 사용하게 함으로써 빠른 웹 페이지 로딩을 가능하게 한다.
· 브라우저 입장에선 사용자가 뒤로가기 버튼을 눌렀을 때 어디로 돌아가야 할지 기억할 필요가 있는데, 이러한 목적으로 만들어진 기능이 (㉡)이다.
· (㉢)는 인터넷 사용자가 웹 사이트를 방문할 때, 웹 서버로부터 전송받아 저장되는 파일로서 웹 서비스 도메인, 만료시간, 보안 속성 등의 정보로 구성될 수 있다.

① 히스토리(History) - 웹 캐시(Cache) - 쿠키(Cookie)
② 웹 캐시(Cache) - 쿠키(Cookie) - 히스토리(History)
③ 웹 캐시(Cache) - 히스토리(History) - 쿠키(Cookie)
④ 쿠키(Cookie) - 히스토리(History) - 웹 캐시(Cache)

정답 3번

간단한 해설

받은 페이지 데이터를 재사용하는 것은 **웹 캐시**, 뒤로 가기를 위한 탐색 이력은 **히스토리**, 도메인·만료시간 등의 속성과 함께 관리되는 데이터는 **쿠키**이다. 따라서 ㉠·㉡·㉢은 ③의 순서이다.

빈칸별 해설

㉠은 **웹 캐시(Cache)**이다. 브라우저는 이전에 받은 이미지·스크립트 등 응답 데이터를 저장해 두었다가 재사용함으로써 전송량과 로딩 시간을 줄인다. 다만 캐시의 유효성이나 서버 정책에 따라 재검증 또는 재다운로드가 필요할 수 있으므로, 재방문 때 항상 네트워크 요청이 사라지는 것은 아니다.

㉡은 **히스토리(History)**이다. 브라우저는 탐색한 페이지의 순서를 관리하여 뒤로 가기와 앞으로 가기를 제공한다. 제시문은 이러한 세션 탐색 이력을 가리키며, 포렌식에서 확인하는 디스크상의 방문 기록과 저장 범위·수명이 항상 같은 것은 아니다.

㉢은 **쿠키(Cookie)**이다. 서버가 전달한 작은 이름·값 데이터와 도메인, 경로, 만료시간, Secure 등의 속성을 브라우저가 관리하고, 조건에 맞는 요청에 포함해 보낸다. 이는 웹 페이지 자체를 저장하는 캐시와 다르다. 쿠키는 브라우저에 따라 데이터베이스나 메모리 등에 보관되므로, 각각이 반드시 독립된 파일 하나로 저장된다는 뜻은 아니다.

따라서 순서는 **웹 캐시 → 히스토리 → 쿠키**이며, 이 대응을 모두 만족하는 선지는 ③이다.

NoteBase

문 9. 윈도우 10 PC 바탕화면에 원본 파일을 생성하고, 다음 날 복사-붙여넣기로 복사본 파일을 생성하였다. 이 복사본 파일의 속성 정보에 대한 설명 중 가장 적절한 것은?

① 복사본 파일의 '수정한 날짜'는 원본 파일의 '수정한 날짜'와 동일하다.

② 복사본 파일의 '만든 날짜'는 원본 파일의 '만든 날짜'와 동일하다.

③ 복사본 파일의 '액세스한 날짜'는 원본 파일의 '만든 날짜'와 동일하다.

④ 복사본 파일의 '액세스한 날짜'는 원본 파일의 '액세스한 날짜'와 동일하다.

정답 1번

간단한 해설

일반적인 파일 복사에서는 **수정한 날짜는 원본 값을 유지**하고, 만든 날짜는 복사본이 생성된 시점으로 정해진다. 생성 시각과 내용의 마지막 수정 시각을 구별해야 한다.

선지별 해설

① O. 일반적인 탐색기 복사·붙여넣기는 원본의 내용을 새 파일로 복제하면서 **마지막 수정 시각은 원본 값으로 유지**한다. 파일 내용이 새로 수정된 것이 아니므로, 복사본의 수정한 날짜가 원본과 동일하다.

② X. 복사본은 다음 날 새로 만들어진 파일이므로 **만든 날짜는 복사본 생성 시점**이 된다. 원본을 처음 만든 시각이 그대로 유지되는 것으로 보면 안 된다. 이 때문에 복사본에서는 만든 날짜가 수정한 날짜보다 나중일 수 있다.

③ X. 액세스한 날짜는 접근 시각에 관한 정보이지 **원본의 생성 시각을 뜻하지 않는다**. 복사본의 접근 시각을 전날 원본을 만든 시각과 동일하다고 볼 근거가 없다.

④ X. 복사본의 접근 시각은 복사본 생성·접근 상황과 운영체제의 갱신 정책에 영향을 받으므로 **원본의 접근 시각을 그대로 보존한다고 일반화할 수 없다**. 특히 NTFS의 마지막 접근 시각 갱신은 지연되거나 비활성화될 수 있으므로, 접근 시각이 항상 즉시 변경된다고 단정해서도 안 된다.

따라서 문제의 일반적인 복사·붙여넣기 조건에서 가장 적절한 설명은 ①이다.

NoteBase

문 10. 증거 분석관이 인가되지 않은 USB 접속 흔적을 파악하기 위해 윈도우의 레지스트리를 분석 중이다. 관련된 내용 설명으로 가장 적절하지 않은 것은?

① USBSTOR는 SubKey를 통해 시스템에서 사용했던 USB 장치를 확인할 수 있다.

② Unique Instance ID는 동일 Device Class ID를 갖는 경우, 장치별로 구별되지 않는다.

③ Device Class ID에서는 연결된 USB의 제조사, 제품명, 버전을 확인할 수 있다.

④ Enum\USB에는 시스템에 접속되었던 모든 USB 장치에 대한 정보를 포함하고 있다.

정답 2번

간단한 해설

같은 Device Class ID를 가진 장치라도 **Unique Instance ID로 개별 인스턴스를 구별**한다. 장치 종류를 나타내는 정보가 같다는 것과 개별 장치가 구별되지 않는다는 것은 다르다.

선지별 해설

① O: USBSTOR의 하위 키에는 USB 저장장치의 종류와 개별 장치 인스턴스 정보가 남는다. 이를 통해 시스템에서 사용한 USB 저장장치의 흔적을 확인할 수 있다.

② X: Unique Instance ID는 같은 Device Class ID 아래에서도 **개별 장치 인스턴스를 구별**하는 데 쓰인다. 같은 제조사·모델의 장치라는 이유만으로 인스턴스까지 구별되지 않는 것은 아니다.

③ O: 이 문항의 Device Class ID는 USBSTOR 아래 장치 종류를 나타내는 키를 가리킨다. Ven, Prod, Rev 등의 구성 요소로 제조사·제품명·리비전 정보를 확인한다. 이는 같은 종류의 장치가 공유할 수 있는 정보이며, 개별 장치 인스턴스 식별과는 다르다.

④ O: Enum\USB는 저장장치에 한정하지 않고 **USB로 열거된 장치 전반**의 정보를 다루므로 USBSTOR보다 대상 범위가 넓다. 여기서 '모든'은 USB 장치 종류 전반이라는 의미이며, 삭제된 과거 기록까지 언제나 완전하게 보존된다는 뜻은 아니다. 실제 접속 흔적은 남아 있는 기록을 기준으로 판단한다.

NoteBase

문 11. 슬랙 공간(Slack Space)과 발생 원인의 연결이 가장 적절하지 않은 것은?

① 램(RAM) 슬랙 - 섹터 크기

② 파일 시스템(File System) 슬랙 - 클러스터 크기

③ 드라이브(Drive) 슬랙 - 볼륨 크기

④ 볼륨(Volume) 슬랙 - 파티션 크기

정답 3번

간단한 해설

드라이브 슬랙은 **파일의 마지막 할당 클러스터 안에서 남는 섹터 공간**이다. 볼륨 크기가 아니라 클러스터 단위 할당 때문에 생긴다.

선지별 해설

① O: 램 슬랙은 **파일의 논리적 끝부터 마지막 사용 섹터의 끝**까지 남는 공간이다. 파일 크기가 섹터 경계에 맞지 않을 때 생기므로 섹터 크기와 관련된다. 이름에 RAM이 들어가더라도 현재 운영체제에서 반드시 메모리 내용이 남는다는 뜻은 아니다.

② O: 이 문항의 분류에서 파일 시스템 슬랙은 파일시스템 영역 끝부분에서 **온전한 클러스터를 구성하지 못하고 남은 섹터**를 가리킨다. 클러스터 단위로 공간을 관리하기 때문에 생기는 잔여 공간이므로 클러스터 크기와 연결된다.

③ X: 드라이브 슬랙은 **파일의 마지막 사용 섹터 끝부터 마지막 할당 클러스터 끝**까지 남는 공간이다. 따라서 볼륨 전체 크기가 아니라 클러스터 단위 할당과 관련된다. 램 슬랙과 드라이브 슬랙을 합친 것이 파일 슬랙이다.

④ O: 이 문항이 구별하는 볼륨 슬랙은 디스크를 파티션으로 나눈 뒤 **파티션에 포함되지 않고 남는 영역**을 말한다. 파티션으로 정한 범위와 크기에 따라 생기는 공간이라는 연결이다. 자료에 따라 볼륨 슬랙이라는 명칭을 파일시스템 끝과 파티션 끝 사이의 공간에 쓰기도 하므로, 이름만 외우기보다 어떤 경계 사이의 잔여 공간인지 구별해야 한다.

NoteBase

문 12. 범죄혐의와 관련된 윈도우 10 PC를 디지털 증거 분석하고 있다. 윈도우 이벤트 로그(Event Log)에 대한 설명으로 가장 적절하지 않은 것은?

① 이벤트 로그가 기록되는 로그 파일의 확장자는 .evtx이다.

② 이벤트 로그 '최대 이벤트 로그 크기에 도달할 때'의 기본 설정(Default)은 '필요한 경우 이벤트 덮어쓰기(가장 오래된 이벤트 먼저)'이다.

③ 시스템 로그는 윈도우 시스템 구성요소에서 기록한 이벤트로서, 응용 프로그램 개발자가 이벤트를 정의한다.

④ 보안 로그는 로그온 횟수, 로그인 오류 정보 등을 기록한 이벤트로서 관리자가 이벤트 유형을 지정하고 보안 로그에 기록한다.

정답 3번

간단한 해설

시스템 로그는 **윈도우 구성요소의 동작과 오류**를 기록한다. 응용 프로그램 개발자가 기록할 이벤트를 정한다는 설명은 응용 프로그램 로그에 해당한다.

선지별 해설

① O: 윈도우 10의 이벤트 로그는 기본적으로 '.evtx' 형식의 파일에 저장된다. 이벤트의 발생 시각·이벤트 ID·공급자·메시지 등은 시스템 활동을 추적하는 단서가 된다.

② O: 기본 설정에서는 로그가 최대 크기에 도달하면 **가장 오래된 이벤트부터 덮어써** 새 이벤트를 기록한다. 따라서 기록이 없다고 해서 해당 행위가 없었다고 단정할 수 없다. 실제 PC에서는 관리자가 보존 정책을 변경했을 수 있으므로 해당 로그의 설정도 확인한다.

③ X: 시스템 로그에 윈도우 구성요소의 이벤트가 기록된다는 부분은 맞지만, '응용 프로그램 개발자가 이벤트를 정의한다'는 설명을 잘못 결합했다. 시스템 로그는 드라이버나 시스템 서비스 등 **운영체제 구성요소의 동작·오류**를 기록한다. 응용 프로그램 개발자가 기록할 사건을 정하는 것은 응용 프로그램 로그의 설명이다.

④ O: 보안 로그에는 감사 정책에 따라 로그온 성공·실패나 자원 접근 같은 보안 관련 사건이 기록된다. 관리자는 **감사할 사건의 종류와 성공·실패 여부를 설정**하며, 실제 로그 항목은 그 정책에 따라 시스템이 생성한다. 관리자가 각 사건을 수작업으로 적는다는 뜻은 아니다. 로그온 횟수는 남아 있는 관련 이벤트를 집계하여 파악할 수 있다.

NoteBase

문 13. 디지털 증거의 무결성에 대한 내용으로 가장 적절하지 않은 것은?

① 디지털 증거의 해시값을 확인 후, 소유자(관련자)의 서명을 받아야 한다.

② 저장매체를 압수한 경우 디지털 증거의 무결성 증명을 위해 피의자의 서명을 받아 봉인하고, 서명 봉인 과정을 영상 녹화한다.

③ 피고인이 재판과정에서 무결성을 부정하는 경우, 압수한 저장장치의 해시값과 사본파일의 해시값을 비교할 수 있도록 법원에 검증을 요구한다.

④ 디지털 증거의 무결성을 위해서는 디지털 포렌식 전 과정이 지체없이 신속하게 진행되어야 한다.

정답 4번

①

원본과 사본의 **해시값이 동일함을 확인하고 당사자의 서명을 받은 확인서**를 확보하는 것이 원칙이다. 이는 수집 당시 확인한 내용을 기록하여 디지털 증거의 무결성·동일성을 입증하기 위한 조치이다.

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

②

서명·봉인과 그 과정의 영상녹화는 압수 당시의 상태와 이후 봉인의 연속성을 확인하여 증거가 변경되지 않았음을 입증하는 방법이다.

(2) 기록에 의하여 살펴보면, 국가정보원에서 피고인들 혹은 가족, 직원이 입회한 상태에서 원심 판시 각 디지털 저장매체를 압수한 다음 입회자의 서명을 받아 봉인하였고, 국가정보원에서 각 디지털 저장매체에 저장된 자료를 조사할 때 피고인들 입회하에 피고인들의 서명무인을 받아 봉인 상태 확인, 봉인 해제, 재봉인하였으며, 이러한 전 과정을 모두 녹화한 사실, 각 디지털 저장매체가 봉인된 상태에서 서울중앙지방검찰청에 송치된 후 피고인들이 입회한 상태에서 봉인을 풀고 세계적으로 인정받는 프로그램을 이용하여 이미징 작업을 하였는데, 디지털 저장매체 원본의 해쉬(Hash) 값과 이미징 작업을 통해 생성된 파일의 해쉬 값이 동일한 사실, 제1심법원은 피고인들 및 검사, 변호인이 모두 참여한 가운데 검증을 실시하여 이미징 작업을 통해 생성된 파일의 내용과 출력된 문건에 기재된 내용이 동일함을 확인한 사실을 알 수 있는바, 그렇다면 출력된 문건은 압수된 디지털 저장매체 원본에 저장되었던 내용과 동일한 것으로 인정할 수 있어 증거로 사용할 수 있고, 같은 취지의 원심의 판단은 정당하다. (대법원 2007. 12. 13. 선고 2007도7257 판결)

NoteBase

③

무결성이 다투어지면 **법원의 검증을 통해 원본과 사본의 해시값을 대조**하여 내용의 동일성과 변경 여부를 확인할 수 있다.

(2) 원심판결 이유에 의하면, 원심은 공소외 1 회사 사무실 또는 피고인들의 주거지에 대한 압수·수색을 집행하였던 국가정보원 수사관들, 국가정보원 사무실에서의 '이미징' 절차에 참여하였던 전문가들의 각 증언 등에 의하여 인정되는 다음과 같은 사정들, 즉 국가정보원 수사관들은 피고인들 혹은 가족, 직원이 참여한 상태에서 원심 판시 각 정보저장매체를 압수한 다음 참여자의 서명을 받아 봉인하였고, 국가정보원에서 일부 정보저장매체에 저장된 자료를 '이미징' 방식으로 복제할 때 피고인들 또는 위 전문가들로부터 서명을 받아 봉인상태 확인, 봉인 해제, 재봉인하였으며, 이들은 정보저장매체 원본의 해쉬 값과 '이미징' 작업을 통해 생성된 파일의 해쉬 값이 동일하다는 취지로 서명하였던 사정들과 함께, 제1심법원이 피고인들 및 검사, 변호인이 모두 참여한 가운데 검증을 실시하여 그 검증과정에서 산출한 해쉬 값과 압수·수색 당시 쓰기방지장치를 부착하여 '이미징' 작업을 하면서 산출한 해쉬 값을 대조하여 그 해쉬 값이 동일함을 확인하거나, '이미징' 작업을 통해 생성된 파일의 문자정보와 그 출력 문건이 동일함을 확인하였던 사정, 일부 정보저장매체의 경우 원심에서 시행한 검증결과 부분의 봉인봉투 안에 전자정보에 관한 전문가로서 '이미징' 과정에 참여하였던 전문가가 서명한 것으로 보이는 이전의 봉인해제 봉투가 존재하는 사실을 확인한 사정 등을 종합하면, 원심 판시와 같이 증거로 제출된 출력 문건들은 압수된 정보저장매체 원본에 저장되었던 내용과 동일한 것일 뿐만 아니라, 정보저장매체 원본이 문건 출력 시까지 변경되지 않았다고 인정할 수 있으므로 그 출력 문건들을 증거로 사용할 수 있다고 판단하였다.
원심판결 이유를 위 법리와 기록에 비추어 살펴보면, 원심의 이러한 판단은 정당한 것으로 수긍할 수 있고, 거기에 전자증거의 무결성·동일성 그리고 신뢰성에 대한 입증 방법이나 그 입증의 정도 등에 관한 법리를 오해한 위법이 없으며, 나아가 위와 같은 정보저장매체 등이 수사기관에 의하여 조작되었다거나 피고인들이 그 정보저장매체를 소유 내지 소지한 것이 아니라는 취지의 주장을 배척한 원심의 조치에도 상고이유에서 주장하는 바와 같은 위법이 있다고 할 수 없다. (대법원 2013. 7. 26. 선고 2013도2511 판결)

④

전 과정을 지체 없이 진행하는 것은 **신속성의 원칙**이다. 무결성은 수집·보관·분석·제출 과정에서 **증거가 위조·변조되지 않았음을 보장**하는 것이다.

NoteBase

문 14. 피의자의 범죄혐의와 관련된 윈도우 PC를 디지털 증거 분석 중이다. 그 중 레지스트리의 하이브(Hive) 파일에 대한 설명으로 가장 적절하지 않은 것은?

① SAM은 로컬 계정 정보와 그룹 정보로 시스템 계정만 접근 가능하다.

② HARDWARE는 시스템의 하드웨어 장치 드라이버 매핑정보를 가지고 있다.

③ SYSTEM은 시스템 부팅에 필요한 전역 구성정보를 가지고 있다.

④ SECURITY는 패스워드들의 해시 정보를 가지고 있다.

정답 4번

간단한 해설

로컬 사용자 계정의 암호 해시를 저장하는 대표적인 하이브는 **SAM**이다. SECURITY는 보안 정책과 인증 관련 정보를 보관하는 영역으로 구분한다.

선지별 해설

① O: SAM은 로컬 사용자와 그룹, 계정의 인증 정보를 관리한다. 기본적으로 SYSTEM 권한으로 보호되는 영역이므로 일반 사용자가 직접 읽는 레지스트리 영역과 구별된다. 여기서 시스템 계정만 접근한다는 설명은 기본 접근 통제를 뜻하며, 관리자에 의한 권한 변경이나 오프라인 분석까지 불가능하다는 뜻은 아니다.

② O: HARDWARE에는 하드웨어 구성과 장치·드라이버의 매핑 정보가 있다. DEVICEMAP 등의 하위 키로 관련 정보를 관리하며, 부팅할 때 다시 구성되는 휘발성 영역이므로 디스크에 지속적으로 저장되는 일반 하이브 파일과는 구별된다.

③ O: SYSTEM은 드라이버와 서비스, 제어 집합 등 **부팅과 시스템 동작에 필요한 구성 정보**를 보관한다. 따라서 시스템 전반의 시작 환경과 설정을 분석할 때 확인하는 영역이다.

④ X: 하이브의 대표 기능을 구분하는 문맥에서 **로컬 계정의 암호 해시는 SAM**에 저장된다. SECURITY는 보안 정책과 인증 관련 정보를 관리하므로, 이를 로컬 계정 암호 해시의 저장소로 설명한 부분이 가장 적절하지 않다. 다만 SECURITY에는 도메인 로그온의 캐시 검증값 등 해시 기반 정보가 존재할 수 있다. 따라서 SECURITY에 암호와 관련된 해시 정보가 전혀 없다는 뜻으로 일반화해서는 안 된다.

NoteBase

문 15. 디지털 포렌식과 관련된 설명으로 가장 적절하지 않은 것은?

① 비트락커(BitLocker)가 설치된 PC가 로그온 상태라면 비트락커 해제를 위한 공격을 하지 않고도 데이터를 복원할 수 있다.

② 트루크립트(TrueCrypt)는 실시간 암호화 기능을 제공한다.

③ 윈도우 PC에서 빠른 포맷(Format)을 사용한 후에는 증거 데이터를 복원할 수 없다.

④ 스테가노그래피(Steganography)를 이용하여 사진이나 동영상 같은 파일에 메시지나 데이터를 숨길 수 있다.

정답 3번

간단한 해설

빠른 포맷은 기존 데이터 영역 전체를 확실하게 지우는 것과 다르므로 **남아 있는 데이터의 복구 가능성**이 있다. 다만 저장장치와 이후 사용 상태에 따라 복구 여부는 달라진다.

선지별 해설

① O. 정상적으로 부팅·로그온하여 대상 BitLocker 볼륨이 잠금 해제된 상태라면 운영체제가 데이터를 투명하게 복호화하므로 **암호를 공격하지 않고도 접근 가능한 데이터를 수집**할 수 있다. 다만 로그인만으로 별도로 잠긴 모든 데이터 볼륨까지 열리거나, 삭제 데이터의 복구가 보장되는 것은 아니다.

② O. TrueCrypt는 파일을 읽거나 쓸 때 **실시간으로 복호화·암호화**하는 온더플라이 방식을 제공한다. 사용자는 마운트된 볼륨을 통해 데이터를 이용하고, 저장 매체에는 암호화된 형태로 기록된다.

③ X. 빠른 포맷은 파일시스템 관리 정보를 초기화하는 것이므로 **기존 데이터가 남아 복구될 가능성**이 있다. 따라서 빠른 포맷만으로 증거 데이터를 절대로 복원할 수 없다고 단정할 수 없다. 다만 덮어쓰기, SSD의 TRIM·내부 정리 등으로 실제 복구가 어려워질 수 있으므로 항상 복구 가능하다는 뜻도 아니다.

④ O. 스테가노그래피는 사진·동영상 등의 매체 안에 메시지나 데이터를 넣어 **숨긴 정보의 존재를 드러내지 않으려는** 기법이다. 정보 내용을 읽기 어렵게 하는 암호화와는 구별되며, 두 방법을 함께 사용할 수도 있다.

따라서 빠른 포맷 후의 복구 가능성을 전면 부정한 ③이 가장 적절하지 않다.

NoteBase

문 16. 디지털 증거 수집을 위해 사용되는 다음의 디스크 이미징 툴 중, 이미징 소프트웨어로 가장 적절하지 않은 것은?

① SuperImager
② Forensic ToolKit
③ EnCase
④ ProDiscover

정답 1번

간단한 해설

SuperImager는 디스크 이미징을 수행하는 **독립형 하드웨어 장비**이다. 이미징 기능이 없어서가 아니라, 소프트웨어 도구와 구분되는 전용 장비이므로 해당 분류에 맞지 않는다.

개념 구분

디스크 이미징은 저장매체의 데이터를 복제하여 분석용 이미지로 확보하는 작업이다. 이 문항은 이미징 가능 여부가 아니라 **전용 하드웨어 장비와 소프트웨어의 구분**을 묻는다.

SuperImager는 저장매체를 직접 연결하여 이미징하는 독립형 포렌식 장비이다. 내부에서 소프트웨어를 실행하더라도 제품 자체는 전용 하드웨어 기반의 이미저로 분류한다.

Forensic ToolKit(FTK)은 포렌식 소프트웨어 계열이며, 이미지 획득에는 FTK Imager가 대표적으로 사용된다. EnCase와 ProDiscover도 증거 수집·이미징과 분석에 사용되는 소프트웨어 도구이다.

따라서 이미징 소프트웨어라는 분류에 가장 적절하지 않은 것은 전용 장비인 ① SuperImager이다. 이는 SuperImager가 디지털 증거 수집에 부적합하다는 뜻이 아니다.

NoteBase

문 17. 윈도우의 NTFS 파일 시스템에는 다수의 메타 데이터 파일(Meta Data File)이 사용된다. 볼륨 내의 클러스터 할당 상태 정보를 관리하는 파일로서 가장 알맞은 것은?

① $MFT
② $Bitmap
③ $AttrDef
④ $LogFile

정답 2번

간단한 해설

NTFS 볼륨 내 클러스터의 할당·비할당 상태를 비트로 관리하는 메타데이터 파일은 ② **$Bitmap**이다.

핵심 풀이

NTFS에서 볼륨의 클러스터별 사용 여부를 나타내는 메타데이터 파일은 **$Bitmap**이다. 각 비트가 클러스터의 할당 상태에 대응하며, 일반적으로 1은 할당됨, 0은 비할당 상태를 나타낸다. 따라서 정답은 ②이다.

$MFT는 파일과 디렉터리의 레코드 및 속성 정보를 관리하는 마스터 파일 테이블이다.

$AttrDef는 NTFS에서 사용하는 속성의 종류와 정의를 보관하며,

$LogFile은 파일시스템 메타데이터 변경의 복구를 위한 트랜잭션 로그를 관리한다.

이들은 볼륨 전체의 클러스터 할당 상태를 표시하는 $Bitmap과 역할이 다르다.

비할당 상태가 데이터의 완전한 소거를 뜻하지는 않는다. 파일 삭제 등으로 클러스터가 비할당으로 표시되어도, 해당 영역이 덮어써지거나 장치의 정리 동작 등으로 소거되기 전에는 잔존 데이터가 남을 수 있다. 따라서 할당 상태와 실제 바이트의 잔존 여부는 구별해야 한다.

NoteBase

문 18. 이메일이나 첨부파일로 기업의 핵심기술이 외부로 유출될 수 있으므로 이메일 분석은 중요한 요소이다. 다음 내용 중 ㉠, ㉡, ㉢, ㉣에 들어가는 용어의 순서대로 가장 적절한 것은?

이메일 파일은 자체적인 포맷을 기반으로 한 Lotus Notes의 (㉠), Outlook의 PST와 (㉡), Outlook Express의 (㉢) 등이 있으며 MIME 형식을 기반으로 한 Mozilla Thunderbird의 MBOX, 다수의 웹 메일, Live Mail의 (㉣) 등이 존재한다.

① NSF - OST - DBX - EML
② OST - DBX - EML - NSF
③ EML - OST - DBX - NSF
④ NSF - DBX - OST - EML

정답 1번

간단한 해설

Lotus Notes는 NSF, Outlook의 오프라인 파일은 OST이다. Outlook Express의 DBX와 Live Mail의 개별 메시지 파일인 EML을 구별하면 빈칸의 대응을 정할 수 있다.

빈칸별 해설

㉠ NSF: Lotus Notes는 메일 등 문서를 **NSF 데이터베이스**에 저장한다. 따라서 Notes의 자체 저장 형식을 묻는 빈칸에는 NSF가 들어간다.

㉡ OST: Outlook은 PST와 함께 **오프라인 Outlook 데이터 파일인 OST**를 사용한다. OST는 서버 사서함 내용을 로컬에 동기화하여 오프라인에서도 이용하도록 하는 데 쓰인다.

㉢ DBX: Outlook Express에서 메일 폴더의 메시지를 저장하는 대표적인 형식은 **DBX**이다. Outlook의 PST·OST와 Outlook Express의 DBX를 구별해야 한다.

㉣ EML: Windows Live Mail은 개별 이메일 메시지를 **EML 파일**로 저장한다. EML은 메시지 헤더와 본문을 담고 MIME 구조로 첨부파일 등을 표현할 수 있다. 지문에서 함께 언급한 MBOX는 여러 메시지를 하나의 사서함 파일로 묶는 방식으로, 개별 메시지 파일인 EML과 구별된다.

따라서 ㉠~㉣은 NSF - OST - DBX - EML이며, 이 대응을 제시한 선택지는 ①이다.

NoteBase

문 19. 윈도우 PC의 디지털 증거 분석을 위해 프리패치(Prefetch)를 확인하려고 한다. 프리패치와 관련된 내용으로 가장 적절하지 않은 것은?

① 부트 프리패칭과 응용프로그램 프리패칭으로 구분할 수 있다.

② 특정 응용프로그램 이름과 실행 횟수를 파악할 수 있다.

③ 프리패치 파일에서 파일시스템 시간 정보(생성, 마지막 접근 시간 등) 획득을 통해 통합 타임라인 분석이 가능하다.

④ 프리패치는 시스템 복원을 목적으로 실행파일의 정보를 시스템에 저장하는 것이다.

정답 4번

간단한 해설

프리패치는 **부팅과 응용프로그램 시작 속도를 높이는 기능**으로, 시스템 복원을 위한 기능이 아니다. 그 과정에서 남은 실행파일·실행 횟수·시각 정보가 디지털 증거 분석에 활용된다.

선지별 해설

① O: 프리패칭은 부팅 때 필요한 데이터를 미리 읽는 부트 프리패칭과 응용프로그램 시작에 필요한 데이터를 미리 읽는 응용프로그램 프리패칭으로 구분할 수 있다. 과거의 접근 양상을 이용하여 이후 시작 과정의 디스크 입출력 대기를 줄인다.

② O: 응용프로그램 프리패치에는 실행파일 이름과 실행 횟수 등의 정보가 남아 프로그램 실행 흔적을 파악하는 데 활용된다. 다만 기록 삭제·재생성이나 기능 비활성화의 영향을 받으므로, **남아 있는 실행 횟수를 전체 사용 이력과 동일시하지 않는다**.

③ O: 프리패치 파일 자체의 생성·수정·접근 시각 같은 파일시스템 메타데이터와 프리패치 내부의 실행 시각을 다른 증거의 시각과 함께 대조하여 통합 타임라인을 구성할 수 있다. **파일시스템 시각과 내부 실행 시각은 서로 다른 정보**이며, 마지막 접근 시각은 운영체제의 갱신 정책이나 수집·접근의 영향을 받을 수 있어 곧바로 실행 시각으로 단정하지 않는다.

④ X: 프리패치는 **부팅과 응용프로그램 시작 속도를 높이기 위한 성능 최적화 기능**이다. 실행에 필요한 데이터의 접근 양상을 기록하고 이를 다음 실행에서 미리 읽는 데 이용한다. 과거 시스템 상태로 되돌리는 시스템 복원이 목적이 아니다. 포렌식에서는 성능 최적화를 위해 남은 기록을 실행 흔적의 단서로 활용한다.

NoteBase

문 20. 데이터베이스 포렌식으로 가장 적절하지 않은 것은?

① 데이터베이스 서버가 RAID로 구성되어 있는 경우에는 서버 운영을 정지시키고 RAID가 구성되어 있는 상태에서 EnCase나 DD로 이미지 파일을 추출하는 방법으로 데이터베이스의 데이터를 획득할 수 있다.

② 관계형 데이터베이스의 개체 무결성은 두 개의 릴레이션들 간에 명시되는 제약조건이며 올바른 연결을 보장하기 위한 제약조건으로 외래키와 기본키와의 관련으로 표현된다.

③ 데이터베이스 분석도구에는 SQLite Expert, Exchange EDB Viewer, EseDbViewer, Oxygen SQLite Viewer 등이 있다.

④ 데이터베이스 백업은 사실을 확인하는 데 중요한 자료가 될 수 있으며 특히 데이터베이스에서 특정의 레코드를 삭제한 것으로 의심되는 경우에 그 효용가치가 높아진다.

정답 2번

간단한 해설

외래키와 참조 대상 키의 관계를 보장하는 것은 **참조 무결성**이다. 개체 무결성은 기본키의 유일성과 NULL 불허 등 개체 식별에 관한 제약이다.

선지별 해설

① O. 서버 운영을 정지하고 **RAID 구성을 유지하여 논리 볼륨을 인식**할 수 있는 환경에서 EnCase나 dd 등의 도구로 이미지를 획득하는 방법을 사용할 수 있다. RAID의 디스크 순서·구성 정보와 원본 무결성을 보존해야 하며, 모든 서버에서 반드시 운영을 중단해야 한다는 의미는 아니다.

② X. 외래키와 참조 대상 키의 연결을 보장하는 것은 **참조 무결성**이다. 개체 무결성은 한 릴레이션 안에서 각 튜플을 식별하는 기본키에 관한 것으로, 기본키 값은 유일하고 기본키를 구성하는 속성은 NULL일 수 없다. 두 무결성의 적용 대상을 구별해야 한다.

③ O. SQLite Expert와 Oxygen SQLite Viewer는 **SQLite 데이터베이스의 구조·레코드 확인** 등에 활용된다. Exchange EDB Viewer는 Exchange 데이터베이스를, EseDbViewer는 ESE 데이터베이스를 살펴보는 도구이므로 데이터베이스 형식에 맞추어 선택한다. 모든 도구가 모든 형식이나 삭제 레코드 복구를 동일하게 지원하는 것은 아니다.

④ O. 삭제 전 시점의 백업에 해당 레코드가 남아 있다면 현재 데이터베이스와 비교하여 **과거 레코드의 존재와 내용**을 확인할 수 있다. 따라서 삭제가 의심될 때 백업은 유용한 대조 자료이다. 다만 백업 시점을 확인해야 하며, 백업만으로 삭제 시각이나 행위자까지 자동으로 확정되는 것은 아니다.

따라서 참조 무결성을 개체 무결성으로 잘못 설명한 ②가 가장 적절하지 않다.

NoteBase