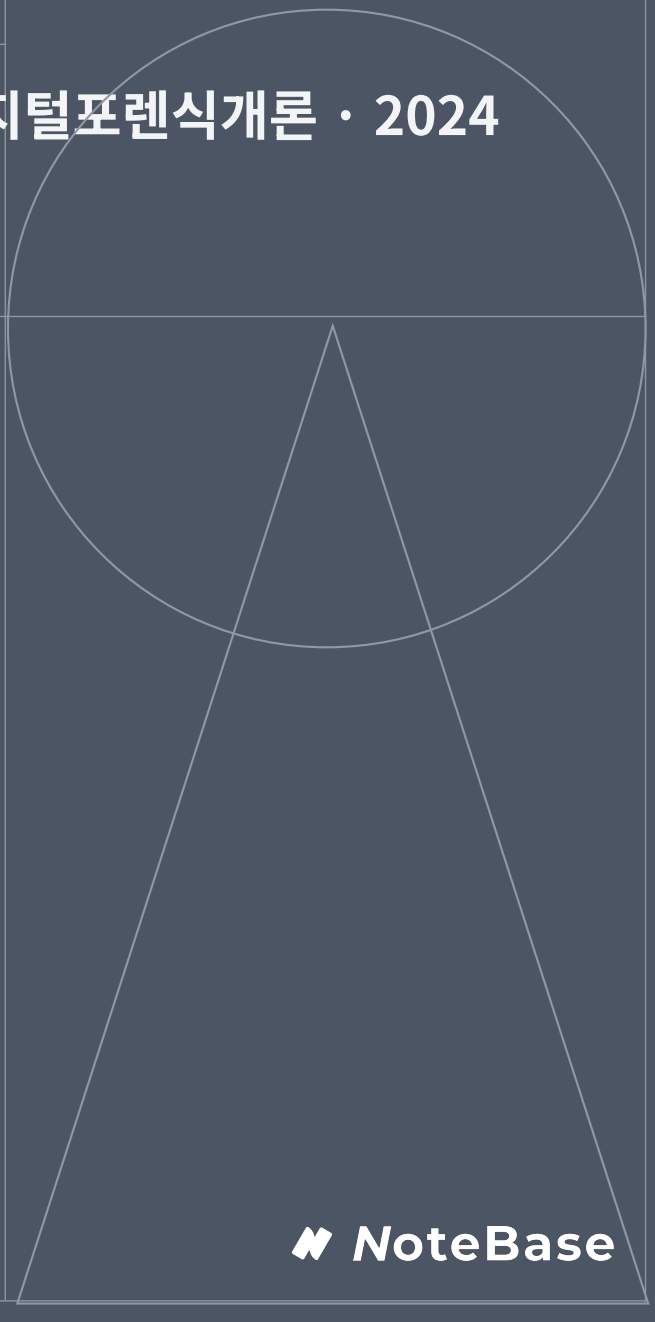
기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2024



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2024

공무원/경찰/경력채용 · 디지털포렌식개론 · 2024

문 1. 다음은 증거능력의 일반적 사항에 관한 설명이다. ㉠에 해당하는 용어로 가장 적절한 것은?

(㉠)는 사실인정의 기초가 되는 경험 사실에 대하여 경험자가 직접 법원에 진술하지 않고 '다른 사람을 통해서' 또는 '조서', '진술조서', '녹음테이프' 등을 통하여 법원에 제출하는 증거 또는 사람의 법정외 진술에 관한 증거로서 그 진술의 내용이 진실함을 증명하기 위하여 제출되는 것을 의미한다.

① 전자적 증거

② 진술서

③ 전문증거

④ 진술녹취서

정답 3번

공통 해설

전문증거는 법정 밖에서 한 진술을 다른 사람의 진술이나 조서·녹음 등을 통해 전달하여 **그 진술 내용의 진실성을 증명하려는 증거**이다. 진술의 존재 자체가 증명 대상인 경우와 구별된다.

타인의 진술을 내용으로 하는 진술이 전문증거인지 여부는 요증사실과의 관계에서 정하여지는바, 원진술의 내용인 사실이 요증사실인 경우에는 전문증거이나, 원진술의 존재 자체가 요증사실인 경우에는 본래증거이지 전문증거가 아니다(대법원 2008. 11. 13. 선고 2008도8007 판결 등 참조). (대법원 2012. 7. 26. 선고 2012도2937 판결)

NoteBase

문 2. 디지털포렌식 과정에서 원본의 무결성을 검증하기 위하여 사용하는 것으로 가장 적절한 것은?

① 시그니처(signature)

② 해시값(hash value)

③ 아티팩트(artifact)

④ 스테가노그래피(steganography)

정답 2번

간단한 해설

원본과 비교 대상의 같은 데이터 범위에 동일한 해시 알고리즘을 적용하고 **해시값을 대조**하여 변경 여부를 확인한다. 값이 달라지면 두 데이터는 동일하지 않다.

핵심 풀이

무결성은 디지털 증거의 내용이 수집·보관·분석 과정에서 변경되지 않았음을 뜻한다. 해시값은 데이터를 해시 함수에 입력하여 얻는 일정 길이의 요약값이다. 같은 범위의 데이터에 같은 알고리즘을 적용한 값을 비교하여 변경 여부를 확인하며, 충돌 저항성이 확보된 암호학적 해시를 사용한다.

원본에서 계산한 기준 해시값을 안전하게 보관하고, 복제본이나 이후 보관 자료의 해시값과 대조한다. 값이 다르면 데이터가 동일하지 않다는 뜻이다. 값의 일치는 동일성을 뒷받침하지만, 수집 전에 이미 잘못된 자료였는지나 누가 작성했는지까지 해시만으로 증명하지는 못한다.

시그니처는 파일 형식 등을 식별하는 특징적인 패턴을 뜻할 수 있어 파일 전체의 무결성 비교값과는 다르다. 전자서명이라는 별도 의미의 signature는 무결성과 인증에 활용될 수 있지만, 이 문항의 원본 대조에 직접 쓰는 값은 해시값이다. 아티팩트는 시스템·사용자 활동이 남긴 흔적이며, 스테가노그래피는 다른 데이터에 정보를 숨기는 기법이다.

따라서 원본의 무결성 검증에 가장 적절한 것은 ② 해시값이다.

NoteBase

문 3. 디지털포렌식 절차 중 증거의 수집 및 보관에 관한 설명으로 가장 적절하지 않은 것은?

① 수집대상 시스템이 온라인 상태라면 휘발성 데이터를 가장 먼저 수집한다.

② 영장의 내용에 있는 범위 내에서 하드웨어, 소프트웨어, 모바일 기기, 보조기억장치 등을 적법한 절차에 의하여 수집한다.

③ 압수·수색의 종료는 압수·수색영장의 집행을 통하여 현장에서 획득한 압수물의 목록을 작성하여 소유자, 소지자, 보관자, 기타 이에 준할 자에게 교부함으로써 종료한다.

④ 모바일 기기의 잠금 패턴·암호를 확보하지 못한 경우에는 예외 없이 전원을 끄고 전파차단을 위한 조치를 한다.

정답 4번

①

휘발성 데이터는 전원을 끄거나 시간이 지나면 소실·변경될 수 있으므로, 가동 중인 시스템에서는 **비휘발성 데이터보다 휘발성 데이터를 먼저 수집**한다.

②

디지털 증거도 **영장에 특정된 압수·수색 대상과 범위 안에서 적법한 절차로 수집**해야 한다. 사건과 관계가 있다고 인정되는 기기·정보저장매체·전자정보 등이 수집 대상이 된다.

형사소송법 제114조(영장의 방식)
①압수 · 수색영장에는 다음 각 호의 사항을 기재하고 재판장이나 수명법관이 서명날인하여야 한다. 다만, 압수 · 수색할 물건이 전기통신에 관한 것인 경우에는 작성기간을 기재하여야 한다. <개정 2011.7.18, 2020.12.8>
3. 압수할 물건
4. 수색할 장소 · 신체 · 물건

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

④

전원을 끄면 재부팅 시 잠금·인증이 요구되어 증거 수집이 어려워질 수 있으므로, **잠금정보를 확보하지 못했다고 무조건 전원을 끄지 않는다**. 기기의 상태를 고려하여 전원을 유지하면서 전파차단 용기 등을 이용해 통신을 차단할 수 있다.

NoteBase

문 4. 전자적 증거(디지털 증거)로서 인정받기 위한 선결 요건으로 가장 적절하지 않은 것은?

① 수집과 법정 제출의 모든 과정에서 변경이나 훼손의 인위적인 조작이 없어야 한다는 동일성, 무결성 요건

② 범죄 관련 전자적 형태로 기록된 데이터를 압수, 수색하는 경우에 디지털포렌식에 전문적인 기술, 지식과 경험을 가진 전문가에 의해서 이루어져야 한다는 전문성 요건

③ 디지털포렌식에 사용되는 도구나 프로그램은 오류의 가능성이 전혀 없거나 무시할 정도로 극소한 것이어야 한다는 신뢰성과 정확성 요건

④ 포렌식 전용의 고성능 컴퓨터를 사용하는 가용성과 수집된 대용량 데이터 전송을 위한 네트워크 접속의 공유성 요건

정답 4번

①

디지털 증거는 수집부터 법정 제출까지 **내용이 변경·훼손되지 않는 무결성**과 **원본·복제본·출력물 사이의 동일성**이 확보되어야 한다.

(1) 압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 할 것인데, 그 동일성을 인정하기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보되어야 하고 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 '하드카피'·'이미징'한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 '하드카피'·'이미징'한 매체 사이에 자료의 동일성도 인정되어야 한다. (대법원 2007. 12. 13. 선고 2007도7257 판결)

NoteBase

②

디지털 증거를 압수·수색할 때에는 **디지털포렌식에 관한 전문적인 기술·지식·경험을 갖춘 전문가가 전자정보를 수집·처리해야 한다**. 이는 처리 과정의 오류나 변형을 막아 원본과의 동일성과 증거의 신뢰성을 확보하기 위한 전문성 요건이다.

전자적 증거의 분석 및 관리 규정 제7조(전자적 증거의 신뢰성 유지) 전자적 증거는 디지털포렌식 분석관이 신뢰할 수 있는 도구와 방법으로 관리 · 분석하여야 한다.

전자적 증거의 분석 및 관리 규정 제9조(디지털포렌식 분석관의 자격) 디지털포렌식 분석관은 다음 각 호의 어느 하나에 해당하는 자격요건을 갖춘 자 중에서 임명한다. 1. 공소청 디지털포렌식시스템담당관(이하 "담당관")이 실시하는 디지털포렌식 전문가 과정 또는 이에 준하는 전문교육 과정을 이수한 사람 2. 국내 · 외 공공기관, 전문교육기관 등에서 컴퓨터, 정보통신, 정보보호, 디지털포렌식 또는 그 밖의 관련 교육과정을 이수한 자로서 디지털포렌식 관련 지식이 충분하다고 인정되는 사람 3. 그 밖에 제1, 2호에 준하는 디지털포렌식 관련 전문지식을 갖춘 것으로 인정되는 사람

(1) 압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 할 것인데, 그 동일성을 인정하기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보되어야 하고 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 '하드카피'·'이미징'한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 '하드카피'·'이미징'한 매체 사이에 자료의 동일성도 인정되어야 한다. 나아가 법원 감정을 통해 디지털 저장매체 원본 혹은 '하드카피'·'이미징'한 매체에 저장된 내용과 출력된 문건의 동일성을 확인하는 과정에서 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다. (대법원 2007. 12. 13. 선고 2007도7257 판결)

③

증거 처리에 사용한 **장비의 기계적 정확성과 프로그램의 신뢰성**이 담보되어야 한다. 오류가 없거나 무시할 정도로 작아야 분석 결과를 신뢰할 수 있다.

나아가 법원 감정을 통해 디지털 저장매체 원본 혹은 '하드카피'·'이미징'한 매체에 저장된 내용과 출력된 문건의 동일성을 확인하는 과정에서 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다. (대법원 2007. 12. 13. 선고 2007도7257 판결)

NoteBase

④

고성능 컴퓨터 사용이나 네트워크 공유는 처리 환경에 관한 사항으로 **디지털 증거 인정의 선결 요건이 아니다**. 필요한 것은 동일성·무결성, 처리자의 전문성, 장비·프로그램의 신뢰성과 정확성이다.

(1) 압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 할 것인데, 그 동일성을 인정하기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보되어야 하고 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 '하드카피'·'이미징'한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 '하드카피'·'이미징'한 매체 사이에 자료의 동일성도 인정되어야 한다. 나아가 법원 감정을 통해 디지털 저장매체 원본 혹은 '하드카피'·'이미징'한 매체에 저장된 내용과 출력된 문건의 동일성을 확인하는 과정에서 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다. (대법원 2007. 12. 13. 선고 2007도7257 판결)

NoteBase

문 5. 윈도우(Windows) 시스템에서 프로그램의 실행 흔적을 찾기 위하여 확인해야 할 아티팩트(artifact) 중에서 프리패치(prefetch)에 관한 설명으로 가장 적절하지 않은 것은?

① 프로그램의 실행에 필요한 시스템 자원을 파일에 미리 저장해 놓은 것이다.

② 프리패치 파일의 시그니처는 ‘PRSG’이다.

③ 파일 시스템 분석에서 찾을 수 없는 파일의 실행 여부를 입증할 수 있다.

④ 레지스트리 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters에서 프리패치 설정이 가능하다.

정답 2번

간단한 해설

프리패치의 비압축 내부 구조를 식별하는 시그니처는 **'SCCA'**이다. 'PRSG'라는 설명은 이 식별자를 잘못 제시한 것이다.

선지별 해설

① O: 프리패치는 프로그램 시작 때 사용되는 파일·디렉터리 등 자원 접근 정보를 기록하여 이후 실행 시 필요한 데이터를 효율적으로 읽도록 돕는다. 자원 전체를 복제해 보관한다는 뜻이 아니라 **시작에 필요한 접근 정보를 저장**하는 실행 최적화 기능이다.

② X: 일반적인 비압축 프리패치 구조의 시그니처는 **'SCCA'**이지 'PRSG'가 아니다. 일부 Windows 버전의 압축된 프리패치 파일은 바깥쪽 압축 헤더가 있으므로, 원시 파일 첫 바이트와 압축 해제된 내부 구조의 식별자를 구별해야 한다.

③ O: 프로그램 파일이 삭제되어 현재 파일시스템에서 찾기 어려워도, 남아 있는 프리패치의 실행 파일명·실행 시각·실행 횟수 등의 정보로 **과거 실행 흔적**을 확인할 수 있다. 다만 기록의 생성 조건과 다른 아티팩트를 함께 살펴야 하며 특정 사용자의 의도까지 단독으로 확정하는 자료는 아니다.

④ O: 제시된 레지스트리의 PrefetchParameters 키는 프리패치 동작을 제어하는 설정 위치이다. EnablePrefetcher 같은 값을 통해 응용프로그램·부팅 프리패치 사용 여부를 설정하는 구조이다.

NoteBase

문 6. 디지털포렌식 도구인 Encase에 관한 설명으로 가장 적절하지 않은 것은?

① 통합 포렌식 도구로서 쓰기 방지기능을 지원하며 보고서 출력을 제공한다.

② 레지스트리 분석, 이벤트 로그 분석, 파일 시그니처 분류 등이 가능하다.

③ FAT, NTFS 등의 분석이 가능하며 삭제 파일 복구, 키워드 검색이 가능하다.

④ 텍스트 기반 UI로 구성되어 윈도우 운영체제에서 사용할 수 없다.

정답 4번

간단한 해설

EnCase는 **Windows에서 GUI로 증거를 수집·분석·보고**하는 통합 포렌식 도구이다. Windows에서 사용할 수 없다는 설명을 바로잡아야 한다.

선지별 해설

① O: EnCase는 증거 수집·분석·보고를 지원하는 **통합 포렌식 도구**이다. 쓰기 방지 기능이나 장비를 활용해 원본 변경을 막는 수집 환경을 구성하고, 분석 결과를 보고서로 정리할 수 있다. 프로그램 실행만으로 모든 연결 매체의 쓰기 방지가 보장되지는 않으며, 실제 보호 여부는 설정과 연결 상태에 따라 달라진다.

② O: **레지스트리·이벤트 로그 등 운영체제 아티팩트**를 분석하고 파일 시그니처를 이용해 파일 형식을 식별·분류하는 작업을 지원한다. 확장자와 실제 파일 형식이 일치하는지도 조사할 수 있다.

③ O: FAT·NTFS 같은 **파일시스템 구조를 해석**하여 파일을 조사하고, 삭제 파일 복구와 키워드 검색을 수행할 수 있다. 삭제 데이터가 덮어써졌는지 등 상태에 따라 복구 가능성이 달라지므로 모든 삭제 파일의 완전 복구를 보장하는 것은 아니다.

④ X: EnCase는 **Windows에서 그래픽 사용자 인터페이스를 제공**하는 포렌식 도구이다. 텍스트 기반 UI이므로 Windows에서 사용할 수 없다는 설명은 틀리다. 분석 대상 매체의 파일시스템과 분석 도구를 실행하는 운영체제는 별도로 구별해야 한다.

NoteBase

문 7. 썸네일(thumbnail)에 관한 설명으로 가장 적절하지 않은 것은?

① 윈도우(Windows) 등의 운영체제에서 자동으로 생성되는 증거이다.

② 각종 파일의 아이콘에 대해서도 썸네일이 생성된다.

③ 원본 파일이 삭제되면 관련 썸네일은 삭제된다.

④ 썸네일 캐시는 원본 이미지에 대한 작은 그림을 저장하고 있어 '미리보기'를 가능하게 한다.

정답 3번

간단한 해설

원본 파일을 삭제해도 썸네일 캐시는 남을 수 있다. 썸네일은 별도로 저장된 미리보기 이미지이므로 삭제된 원본의 내용을 추정하는 단서가 될 수 있다.

선지별 해설

① O. 썸네일은 윈도우 탐색기 등이 파일을 표시하는 과정에서 **자동으로 생성·캐시할 수 있는 흔적**이다. 사용자가 별도로 증거를 만들지 않아도 남을 수 있지만, 실제 생성 여부는 보기 설정과 파일 형식 지원 등에 따라 달라진다.

② O. 파일의 아이콘 표시 영역에서 사진뿐 아니라 문서·동영상 등 **여러 파일 형식의 미리보기 썸네일**을 사용할 수 있다는 취지이다. 다만 일반 아이콘과 내용 기반 썸네일은 구별되며, 모든 아이콘 그림 자체가 반드시 썸네일로 변환·저장된다는 의미는 아니다. 지원하는 처리기와 표시 설정이 필요하다.

③ X. **원본 삭제와 썸네일 캐시 삭제는 별개**이다. 원본 파일이 지워져도 캐시에 미리보기 이미지가 남을 수 있으므로, 원본을 삭제하면 관련 썸네일도 함께 삭제된다고 단정할 수 없다. 다만 캐시 정리·교체 등에 의해 나중에 없어질 수 있어 영구 보존을 뜻하지도 않는다.

④ O. 썸네일 캐시는 원본을 축소한 **작은 미리보기 이미지**를 보관하여 빠른 표시를 돕는다. 남은 썸네일은 원본 내용의 단서가 될 수 있지만 축소·변환된 자료이므로 원본 파일 전체와 동일한 것은 아니다.

따라서 가장 적절하지 않은 것은 원본 삭제 시 썸네일도 삭제된다고 단정한 ③이다.

NoteBase

문 8. 정보 은닉(information hiding) 방법에 관한 설명으로 가장 적절한 것은?

① 워터마킹(watermarking)은 스테고 키(stego key)를 사용하는 방법이다.

② 핑거프린팅(fingerprinting)은 원본에 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 방법이다.

③ 애너니머티(anonymity)는 사용자를 명확히 구분하기 위한 방법이다.

④ 스테가노그래피(steganography)에서 커버 데이터(cover data)의 크기는 메시지 데이터(message data)의 크기보다 반드시 작아야 한다.

정답 2번

출제 포인트

정보 은닉 기법을 소유권 표시, 구매자 추적, 신원 은닉, 메시지 존재 은닉으로 구분하는 문제이다.

핵심 개념

워터마킹은 소유권·저작권 표식을, 핑거프린팅은 구매자별 식별 정보를 콘텐츠에 삽입하는 기법이다. 애너니머티는 신원을 감추는 익명성이다. 스테가노그래피는 커버 데이터에 메시지를 숨겨 존재를 감추는 기법이다. 스테고 키는 은닉·검출·복원을 제어한다.

선지별 해설

O/X는 가장 적절한 선지를 고르는 선택 판단이다.
① X: 워터마킹에서도 키를 사용할 수 있어 키 사용 자체는 틀린 사실이 아니다. 다만 “스테고 키를 사용하는 방법”만으로는 고유 목적을 구분하지 못한다. 더 정확하게는 콘텐츠에 소유권·저작권 표식을 삽입하는 방법이다.
② O: 구매자별 식별 정보를 삽입하면 불법 복제본에서 이를 검출하여 유출된 사본의 구매자를 추적할 수 있다. “최초의 배포자”는 이 문맥에서 불법 유출의 출처가 된 구매자를 뜻한다.
③ X: “사용자를 명확히 구분”한다는 표현은 익명성의 목적과 반대이다. 애너니머티는 사용자의 실제 신원을 감추는 방법이다.
④ X: 커버 데이터가 메시지보다 “반드시 작아야 한다”는 조건은 없다. 커버 데이터에는 충분한 은닉 용량이 필요하며, 일반적으로 작은 메시지를 더 큰 커버 데이터에 숨긴다.

오답 포인트

①의 키 사용은 공통 구현 요소이므로 목적을 구체적으로 설명한 ②보다 적절성이 낮다. ④는 메시지를 담는 매체와 메시지의 크기 관계를 뒤집었다.

NoteBase

다시 나오면 이렇게 판단

기법의 공통 구현 요소보다 고유 목적을 기준으로 판단한다. 구매자마다 다른 정보를 삽입하여 유출을 추적한다면 핑거프린팅이다.

암기 포인트

워터마킹은 소유자 표시, 핑거프린팅은 구매자 추적, 애너니머티는 신원 은닉, 스테가노그래피는 존재 은닉이다.

NoteBase

문 9. 슬랙 공간(slack space)에 관한 설명으로 가장 적절하지 않은 것은?

① 램 슬랙(ram slack)은 0x00의 값으로 채워진다.

② 드라이브 슬랙(drive slack)은 슬랙 공간에 이전 데이터가 그대로 남아있다.

③ 파일 시스템 슬랙(file system slack)은 섹터에 남은 비할당 영역이다.

④ 볼륨 슬랙(volume slack)은 파티션으로 분리하고 남은 공간이다.

정답 3번

간단한 해설

파일 시스템 슬랙은 **볼륨 크기와 파일 시스템의 할당 공간 사이에서 남는 영역**이다. 파일의 끝에서 마지막 섹터의 끝까지 남는 부분인 램 슬랙과 구별해야 한다.

선지별 해설

① O: 램 슬랙은 파일의 논리적 끝에서 마지막 사용 섹터의 끝까지 남는 공간이다. 일반적인 현대 운영체제에서는 섹터 단위로 파일을 기록하면서 이 빈 부분을 **0x00으로 채운다**. 다만 일부 구형 운영체제에서는 RAM의 잔여 내용이 기록되기도 했으므로, 모든 운영체제에 예외 없이 성립하는 설명으로 일반화하지 않는다.

② O: 드라이브 슬랙은 마지막 사용 섹터 다음부터 파일에 할당된 클러스터의 끝까지 남는 공간이다. 새 파일의 내용이 기록되지 않은 섹터이므로 **이전에 기록된 데이터가 덮어써지지 않고 남을 수 있다**. 슬랙을 별도로 지우지 않았다면 삭제 파일의 흔적을 찾는 자료가 된다.

③ X: 파일 시스템 슬랙은 개별 섹터의 남는 부분이 아니라, **볼륨 크기와 파일 시스템이 할당 단위로 사용하는 공간의 차이**에서 발생하는 영역이다. 파일의 끝에서 마지막 섹터의 끝까지 남는 공간은 램 슬랙에 해당한다.

④ O: 이 문항의 용어 구분에서 볼륨 슬랙은 디스크 전체 공간 중 **파티션으로 할당하고 남은 공간**을 뜻한다. 파일 내부의 여유 공간이나 클러스터 내부의 잔여 영역과 달리, 파티션 할당 범위 밖에 있다는 점으로 구별한다.

NoteBase

문 10. 파일 카빙(file carving)에 관한 설명으로 가장 적절한 것은?

① 저장 매체의 '비할당 영역'에서 파일을 복구하는 방법이다.

② 파일의 메타 데이터 정보를 이용한다.

③ 시그니처 기반 카빙은 '헤더 시그니처'가 존재하지 않을 경우에 사용할 수 있는 방법이다.

④ 파일 구조체 카빙에서는 램 슬랙의 정보를 이용하여 카빙한다.

정답 1번

간단한 해설

파일 카빙은 파일시스템의 연결 정보가 없어도 **남아 있는 데이터의 시그니처·내부 구조**를 찾아 파일을 복구하는 방식이다. 따라서 삭제 후 비할당 영역에 남은 파일 내용도 복구 대상이 될 수 있다.

선지별 해설

① O: 파일 카빙은 저장매체의 데이터 내용에서 파일의 특징을 찾아 복구하는 방법이다. 삭제로 파일시스템 연결 정보가 사라져도 **비할당 영역에 내용이 남아 있으면** 복구를 시도할 수 있다. 다만 비할당 영역에만 한정되는 기술은 아니며 덮어쓴 데이터를 되살리는 것은 아니다.

② X: 파일 카빙은 파일명·디렉터리 항목·할당 정보 등 **파일시스템 메타데이터에 의존하지 않고** 파일 내용의 특징을 분석한다. 이러한 메타데이터를 이용하여 파일 위치를 추적하는 복구와 구별된다. 파일 형식 내부의 길이 필드나 구조 정보는 카빙에 활용할 수 있다.

③ X: 기본적인 시그니처 기반 카빙은 **헤더 등 알려진 식별 패턴을 찾아** 파일 시작과 경계를 판단한다. 헤더 시그니처가 없을 때 사용하는 방식이라고 정의할 수 없다. 헤더가 훼손되면 단순 헤더 탐색은 어려워지고 다른 구조적 단서 등이 필요하다.

④ X: 파일 구조체 카빙은 파일 형식의 내부 구조·길이·블록 관계 등을 분석하여 유효한 파일을 구성한다. 램 슬랙은 파일의 논리적 끝부터 해당 섹터 끝까지의 여유 공간을 가리키며, **파일 형식의 내부 구조 자체가 아니다**. 램 슬랙을 이용하는 것이 구조체 카빙의 정의는 아니다.

NoteBase

문 11. RAID(Redundant Array of Inexpensive Disks)는 여러 개의 디스크를 연결하여 하나의 대용량 디스크처럼 사용하는 기술이다. 오류 검출과 수정에 패리티를 사용하지 않는 방식으로 가장 적절한 것은?

① RAID 0, RAID 1

② RAID 2, RAID 3

③ RAID 3, RAID 4

④ RAID 4, RAID 5

정답 1번

간단한 해설

RAID 0은 패리티 없는 스트라이핑, RAID 1은 패리티 대신 복사본을 두는 미러링이다. 패리티 미사용과 장애 복구 능력의 유무는 구별해야 한다.

개념 구분

판단 기준은 **데이터를 분산하는지보다 패리티 정보를 저장하는지**이다. 스트라이핑은 저장 배치 방식이고, 패리티는 장애 시 데이터를 재구성하기 위한 중복 정보이므로 둘을 같은 개념으로 보아서는 안 된다.

RAID 0은 데이터를 여러 디스크에 나누어 저장하는 **패리티 없는 스트라이핑**이다. 중복 복사본도 두지 않아 한 디스크의 장애로 배열의 데이터를 잃을 수 있다. 패리티를 사용하지 않는다는 사실이 오류 복구 능력이 있다는 뜻은 아니다.

RAID 1은 같은 데이터를 다른 디스크에 복제하는 **미러링**이다. 별도의 패리티를 계산하는 대신 복사본으로 중복성을 확보하므로 패리티 미사용 방식에 해당한다.

RAID 2는 해밍 코드의 검사 비트로 오류 정정 정보를 두는 방식이며, RAID 3·4는 전용 패리티 디스크를, RAID 5는 분산 패리티를 사용한다. 따라서 이들이 들어간 나머지 조합은 두 방식 모두 패리티를 사용하지 않는다는 조건에 맞지 않는다.

따라서 패리티를 사용하지 않는 RAID 0과 RAID 1을 묶은 ①이 정답이다.

NoteBase

문 12. 다음은 기억장치의 특성에 관한 설명이다. ㉠에 해당하는 장치로 가장 적절한 것은?

(㉠)은 CPU 또는 GPU와 같은 처리장치와 연결되어 고해상도 그래픽 데이터, 데이터 센터, AI, 머신러닝, 슈퍼컴퓨팅 등의 응용 분야에서 대량의 데이터 처리와 고속 데이터 전송을 가능하게 함으로써 메모리와 처리장치 간의 병목현상을 최소화한다. (㉠)의 대역폭은 기존 DDR 메모리와 비교하여 매우 높아 다양한 데이터 집약적 작업에서 뛰어난 성능을 발휘한다.

① EPROM

② Mask ROM

③ HBM

④ SRAM

정답 3번

간단한 해설

처리장치에 대량의 데이터를 고속으로 공급해 병목을 줄이는 고대역폭 메모리는 **HBM**이다. 여러 DRAM 다이의 적층과 넓은 병렬 연결이 핵심이다.

빈칸별 해설

㉠은 **HBM(High Bandwidth Memory, 고대역폭 메모리)**이다. 여러 DRAM 다이를 적층하고 많은 데이터 신호를 병렬로 전달하는 구조로 높은 대역폭을 확보한다. CPU·GPU 등 처리장치에 대량의 데이터를 공급하여 데이터 전송 병목을 줄인다는 단서가 핵심이다.

대역폭은 단위 시간에 전달할 수 있는 데이터의 양이므로, AI 연산이나 고성능 그래픽처럼 많은 데이터를 주고받는 작업에서 중요하다. HBM의 높은 대역폭을 모든 작업에서 지연시간까지 항상 더 짧다는 뜻으로 해석해서는 안 된다.

EPROM은 자외선으로 지운 뒤 다시 기록할 수 있는 비휘발성 ROM이고, Mask ROM은 제조 과정에서 내용을 정하는 ROM이다. SRAM은 빠른 접근에 적합하여 캐시 등에 쓰이지만, 제시문이 강조한 **적층 DRAM 기반의 대량 병렬 전송용 메모리**를 가리키는 명칭은 HBM이다. 따라서 ㉠에 대응하는 선택지는 ③이다.

NoteBase

문 13. 윈도우(Windows) 시스템 포렌식과 관련하여 계정정보와 비밀번호 등의 사용자 보안을 관리하는 파일로 가장 적절한 것은?

① SAM

② DMA

③ SID

④ Built-In Account

정답 1번

간단한 해설

Windows의 **SAM**은 로컬 계정 정보를 보관하는 보안 계정 데이터베이스이다. 비밀번호는 평문이 아니라 해시값 형태의 인증 정보로 저장된다.

핵심 풀이

SAM(Security Accounts Manager)은 Windows의 로컬 사용자·그룹 계정 정보를 보관하는 보안 계정 데이터베이스이다. 디스크에서는 SAM 레지스트리 하이브 파일로 저장되며, 사용자 이름과 계정 속성, 암호 인증에 필요한 정보 등을 확인하는 포렌식 분석 대상이 된다.

비밀번호 관련 정보가 있다는 것은 평문 비밀번호가 그대로 들어 있다는 뜻이 아니다. SAM에는 **비밀번호 자체가 아니라 해시값**이 저장된다. 또한 로컬 계정 데이터베이스이므로 도메인의 모든 사용자 계정 정보를 저장하는 파일과 동일시해서는 안 된다.

DMA(Direct Memory Access)는 장치가 메모리와 데이터를 직접 주고받는 방식으로, 계정 관리 파일이 아니다. SID(Security Identifier)는 사용자·그룹 등 보안 주체를 구별하는 식별자이다. Built-In Account는 Administrator나 Guest처럼 기본 제공되는 계정을 가리키며, 계정 정보 저장 파일의 명칭이 아니다.

따라서 사용자 계정과 비밀번호 관련 보안 정보를 관리하는 파일에 해당하는 것은 ① SAM이다.

NoteBase

문 14. 이메일은 디지털포렌식에서 중요한 증거가 된다. 디지털 포렌식 분석관이 메일 헤더에서 수집할 수 없는 자료로 가장 적절한 것은?

① 메일 서버 정보

② 발신자 IP주소

③ 메일 전송 경로에 있는 라우터 정보

④ 이메일 관련 날짜, 시간 정보

정답 3번

간단한 해설

메일 헤더에는 **메일 서버·접속 IP·날짜와 시간**의 단서가 남을 수 있다. 그러나 패킷이 거친 **중간 라우터 경로**까지 일반적으로 기록되지는 않는다.

핵심 풀이

메일 헤더의 **Received 필드**에는 메시지를 전달·수신한 메일 서버의 이름, 접속 상대의 IP 주소, 처리 시각 등의 정보가 기록될 수 있다. Date 필드에도 메시지 작성자가 전송 준비를 마쳤다고 표시한 날짜·시간이 담긴다.
따라서 메일 서버와 IP 주소 및 시간 정보는 헤더 분석 대상이다.

다만 헤더에 나타난 IP가 언제나 실제 발신자의 개인 단말 IP라는 뜻은 아니다. 웹메일·중계 서버를 거치면 서버 주소만 보일 수 있고 일부 필드는 위조될 수 있으므로 **신뢰할 수 있는 서버의 기록과 교차 검증**해야 한다.

메일 서버 사이에서 패킷을 전달한 **중간 라우터들의 경로**는 일반적인 메일 헤더에 나열되지 않는다. Received에 보이는 메일 중계 서버 경로와 IP 계층의 라우터 경로는 서로 다르다.

따라서 일반적인 메일 헤더만으로 수집하기 어려운 자료는 ③ 메일 전송 경로에 있는 라우터 정보이다.

NoteBase

문 15. 다음은 전자적 증거(디지털 증거) 분석 기술에 관한 설명이다. ㉠에 들어갈 용어로 가장 적절한 것은?

(㉠)은 시스템 정보, 시간 정보, 마지막으로 로그인한 사용자, 서비스 및 드라이버 목록, USB 이동식 저장장치 정보 등을 확인할 때 사용하는 방법이다.

① 슬랙(slack) 분석
② 시그니처(signature) 분석
③ 레지스트리(registry) 분석
④ 해시(hash) 분석

정답 3번

간단한 해설

시스템·사용자 설정과 서비스, 드라이버, USB 장치의 흔적은 **Windows 레지스트리**에 남을 수 있다. 이를 해석하여 시스템 구성과 사용 이력을 확인하는 방법이 레지스트리 분석이다.

빈칸별 해설

㉠은 레지스트리 분석이다. Windows 레지스트리는 운영체제·사용자·프로그램의 설정을 계층적으로 저장하는 데이터베이스이다. 시스템 설정과 시간 관련 정보, 사용자 로그인 관련 흔적, 등록된 서비스·드라이버, 연결된 USB 저장장치의 식별 정보 등이 여러 키와 값에 남을 수 있으므로 **시스템 구성과 사용 흔적을 함께 확인**하는 데 활용한다.

슬랙 분석은 파일의 논리적 끝과 할당 공간 사이 등에 남은 여유 영역의 데이터를 조사한다.

시그니처 분석은 파일의 고유 바이트 패턴으로 형식을 식별하고,

해시 분석은 내용에서 계산한 값으로 무결성이나 알려진 파일과의 일치 여부를 확인한다. 이들은 지문처럼 다양한 Windows 설정·장치·사용자 정보를 모아 확인하는 레지스트리 분석과 목적이 다르다.

따라서 ㉠에 들어가는 용어는 ③ 레지스트리 분석이다.

NoteBase

문 16. 유닉스(Unix) 운영체제에서 파일의 사용 접근 권한에 관한 설명으로 가장 적절한 것은?

① -rw-rw-rw- : 소유자, 소유자 그룹 구성원, 기타 사용자 모두 파일 읽기, 실행만 가능

② -rwxrw-r-- : 소유자는 파일 읽기, 쓰기, 실행 가능, 소유자 그룹 구성원은 파일 읽기, 쓰기 가능, 기타 사용자는 파일 읽기만 가능

③ -rwxrwxrwx : 소유자, 소유자 그룹 구성원, 기타 사용자 모두 파일 실행만 가능

④ -rwx------ : 소유자, 소유자 그룹 구성원, 기타 사용자 모두 파일 읽기, 쓰기, 실행 가능

정답 2번

간단한 해설

파일 유형 표시 뒤의 권한은 **소유자·그룹·기타 사용자 순서로 세 자리씩** 읽는다. r은 읽기, w는 쓰기, x는 실행이며 -는 해당 권한이 없다는 표시이다.

선지별 해설

① X: 맨 앞의 -는 일반 파일을 나타내고, 뒤의 아홉 자리는 **소유자·그룹·기타 사용자 순서로 세 자리씩** 읽는다. rw-는 읽기(r)와 쓰기(w)만 허용하고 실행(x)은 허용하지 않으므로, 모두 읽기·실행만 가능하다는 해석은 틀리다.

② O: 권한을 rwx / rw- / r--로 나누면 **소유자는 읽기·쓰기·실행, 그룹은 읽기·쓰기, 기타 사용자는 읽기**에 해당한다. 각 세 자리의 r·w·x가 해당 권한을 나타내고 -는 그 자리에 권한이 없음을 뜻하므로 설명과 일치한다.

③ X: rwx / rwx / rwx는 세 사용자 구분 모두에게 **읽기·쓰기·실행 권한**을 부여한 것이다. 실행만 허용하려면 각 묶음이 --x여야 하므로 rwx를 실행 전용으로 해석하면 안 된다.

④ X: rwx / --- / ---는 **소유자에게만 읽기·쓰기·실행 권한**이 있고 그룹과 기타 사용자에게는 이 기본 모드 비트의 권한이 없는 상태이다. 모두에게 권한을 부여한 경우와 반대이다.

NoteBase

문 17. 운영체제에서 현재 실행 중인 프로그램을 의미하는 용어로 가장 적절한 것은?

① 프로세스(process)

② 세마포어(semaphore)

③ 문맥교환(context switching)

④ 로더(loader)

정답 1번

간단한 해설

운영체제가 관리하는 **실행 중인 프로그램의 인스턴스**는 프로세스이므로 ①이다. 프로그램 파일 자체와 그 실행 상태·자원을 가진 프로세스를 구별한다.

핵심 풀이

프로세스는 실행 중인 프로그램의 인스턴스를 뜻하므로 정답은 ①이다. 저장장치의 프로그램 파일이 정적인 명령어 집합이라면, 프로세스는 그 프로그램의 실행을 위해 운영체제가 관리하는 메모리·자원·실행 상태를 갖는다.

세마포어는 공유 자원의 사용이나 실행 순서를 조절하는 동기화 수단이고,

문맥교환은 실행을 전환할 때 기존 실행 상태를 저장하고 다른 실행 상태를 복원하는 동작이다.

로더는 프로그램을 메모리에 적재하고 실행 준비를 돕는 기능이므로, 어느 것도 실행 중인 프로그램 자체를 가리키지 않는다.

프로세스가 존재한다고 해서 그 순간 계속 CPU를 점유한다는 뜻은 아니다. 스케줄링에 따라 준비·대기 상태에 있을 수 있으며, 실제 실행 흐름은 프로세스 안의 **스레드**로 이루어질 수 있다.

NoteBase

문 18. NTFS 파일 시스템의 MFT(Master File Table)는 다수의 MFT 엔트리로 구성된다. MFT 엔트리 구조에 관한 설명으로 가장 적절하지 않은 것은?

① MFT 엔트리에는 하나의 파일 또는 디렉터리에 대한 정보가 저장된다.

② MFT 엔트리의 시작을 표시하기 위하여 MFT 엔트리 시그니처로 “FILE”을 사용한다.

③ 일반적으로 파일은 $STANDARD_INFORMATION, $FILE_NAME, $DATA 속성을 가진다.

④ MFT 엔트리의 마지막을 표시하기 위하여 Fixup Array를 사용한다.

정답 4번

간단한 해설

Fixup Array는 **다중 섹터 레코드의 일관성 검사**에 사용하는 구조이다. MFT 엔트리나 속성 목록의 마지막을 표시하는 종료 표식과는 역할이 다르다.

선지별 해설

① O: MFT는 NTFS의 파일·디렉터리 정보를 파일 레코드 형태로 관리한다. 하나의 MFT 엔트리는 **특정 파일 또는 디렉터리의 속성 정보**를 담는다. 속성이 많아 한 엔트리에 들어가지 않으면 확장 엔트리를 사용할 수도 있으므로, 한 파일이 반드시 한 엔트리만 차지한다는 뜻은 아니다.

② O: 정상적인 MFT 파일 레코드의 헤더는 **'FILE' 시그니처**로 식별된다. 분석할 때 이 값과 레코드 구조를 함께 확인하여 MFT 엔트리를 판독한다.

③ O: 일반적인 파일에는 시간·플래그 등의 기본 정보를 담는 $STANDARD_INFORMATION, 이름과 부모 디렉터리 참조 등을 담는 $FILE_NAME, 실제 파일 내용을 나타내는 $DATA 속성이 있다. $DATA는 크기 등에 따라 레코드 내부에 상주하거나 외부 클러스터를 참조할 수 있다.

④ X: Fixup Array는 여러 섹터에 걸친 레코드의 **불완전한 쓰기나 손상을 탐지**하기 위한 Update Sequence Array이다. 각 섹터 끝의 대체 값과 보존된 원래 값을 이용해 일관성을 검사·복원하며, 엔트리의 끝을 표시하는 표식이 아니다. 속성 목록의 끝에는 통상 0xFFFFFFFF 종료 표식이 사용된다.

NoteBase

문 19. 윈도우(Windows) 시스템의 이벤트 로그(event log)에 기록된 내용으로 가장 적절하지 않은 것은?

① 시스템 로그(system log) - 부팅 시 발생하는 시스템 구성 요소의 로드 오류와 관련된 이벤트

② 보안 로그(security log) - 파일 생성, 접근, 삭제 등의 리소스 사용과 관련된 이벤트

③ 응용 로그(application log) - 응용 프로그램이 기록한 다양한 이벤트

④ 전달된 이벤트 로그(forwarded events log) - 응용 프로그램 설치와 관련된 이벤트

정답 4번

간단한 해설

전달된 이벤트 로그는 설치 여부가 아니라 **다른 컴퓨터에서 이벤트를 전달받았다는 점**으로 구분한다. 따라서 응용 프로그램 설치 이벤트를 저장하는 로그로 정의하는 것은 부적절하다.

선지별 해설

① O: 시스템 로그는 Windows 시스템 구성 요소가 기록하는 이벤트를 담는다. 부팅 과정에서 드라이버나 서비스 등 구성 요소를 불러오지 못한 오류는 시스템 작동과 관련된 기록이므로 이에 해당한다.

② O: 보안 로그는 로그온이나 개체 접근 등 보안 감사 이벤트를 기록한다. 파일 생성·접근·삭제 같은 자원 사용도 **감사 정책과 대상의 감사 설정이 충족되면** 기록할 수 있다. 모든 파일 작업이 설정 없이 자동 기록된다는 뜻은 아니다.

③ O: 응용 로그는 응용 프로그램이 기록하는 오류·경고·정보 등의 이벤트를 담는다. 프로그램 실행 중 발생한 오류나 프로그램이 정의한 상태 변화 등이 기록 대상이다.

④ X: 전달된 이벤트 로그는 **다른 컴퓨터에서 전달받은 이벤트**를 저장하는 로그이다. 응용 프로그램 설치 이벤트만을 뜻하는 분류가 아니다. 설치 관련 기록은 설치 방식과 이벤트 공급자에 따라 응용 로그나 설치 관련 채널 등에 남을 수 있으며, 그러한 이벤트도 전송 설정에 따라 전달될 수 있다.

NoteBase

문 20. NTFS 파일 시스템에서 사용하는 메타 데이터 파일(meta data file)에 관한 설명으로 가장 적절하지 않은 것은?

① $LogFile은 볼륨에서 사용되는 여러 속성에 관한 정보를 저장한다.

② $MFTMirr는 MFT 엔트리의 복사본을 저장한다.

③ $Bitmap은 볼륨의 클러스터 할당 상태를 저장한다.

④ $UsnJrnl은 파일이나 디렉터리 변경 사항에 관한 정보를 저장한다.

정답 1번

간단한 해설

$LogFile은 NTFS의 트랜잭션 로그**이며, 속성 정의 정보를 관리하는 파일은 **$AttrDef이다. 메타데이터 파일의 이름과 고유 역할을 구별해야 한다.

선지별 해설

① X. **$LogFile은 트랜잭션 로그**로, NTFS 메타데이터 변경 작업과 장애 복구에 관련된 기록을 보관한다. 볼륨에서 사용하는 속성의 정의를 관리하는 파일은 **$AttrDef**이므로 두 역할을 혼동한 설명이다.

② O. **$MFTMirr는 MFT의 핵심 초기 엔트리 복사본**을 보관한다. 일반적으로 첫 4개 레코드를 복제하는 것으로 설명되며, MFT 전체와 모든 파일 내용을 통째로 백업하는 파일이라는 뜻은 아니다.

③ O. **$Bitmap은 클러스터 할당 여부**를 비트맵으로 관리한다. 각 클러스터가 사용 중인지 비어 있는지를 나타내므로 볼륨의 공간 할당 상태를 확인하는 데 이용된다.

④ O. **$UsnJrnl은 파일·디렉터리 변경 기록**을 보관하는 USN 변경 저널이다. 생성·삭제·수정 등의 사실과 변경 종류를 조사할 수 있지만, 변경 전후의 파일 내용 전체를 저장하여 모든 변경을 되돌릴 수 있는 백업은 아니다.

따라서 가장 적절하지 않은 것은 $LogFile을 속성 정의 정보 파일처럼 설명한 ①이다.

NoteBase