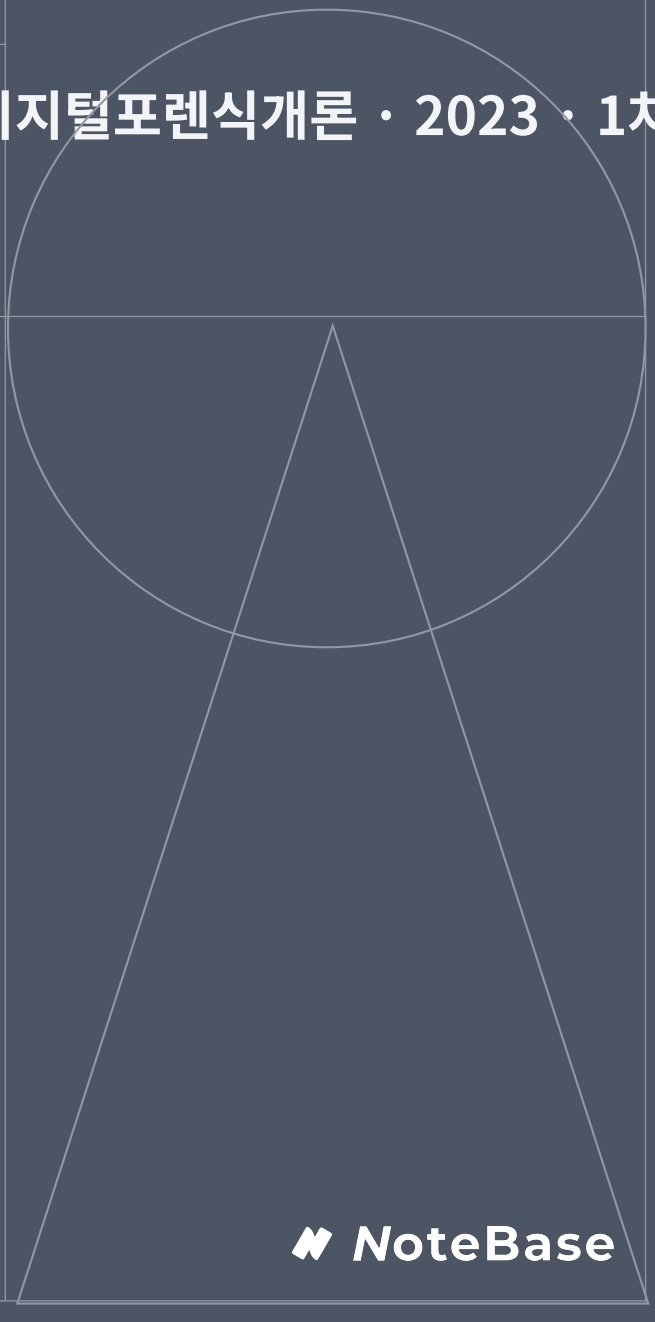
기출OX 해설집

공무원/경찰/공채(순경) · 디지털포렌식개론 · 2023 · 1차



NoteBase

기출OX 해설집

공무원/경찰/공채(순경) · 디지털포렌식개론 · 2023 · 1차

공무원/경찰/공채(순경) · 디지털포렌식개론 · 2023 · 1차

문 1. 다음은 자료 표현 단위를 오름차순으로 정렬한 것이다. 빈칸 ㉠과 ㉡에 들어갈 단위로 옳게 짝지어진 것은?

비트(bit) < (㉠) < 니블(nibble) < (㉡) < 워드(word)

① ㉠: 바이트(byte), ㉡: 쿼터(quarter)

② ㉠: 바이트(byte), ㉡: 더블워드(double word)

③ ㉠: 쿼터(quarter), ㉡: 바이트(byte)

④ ㉠: 쿼터(quarter), ㉡: 더블워드(double word)

정답 3번

출제 포인트

비트, 쿼터, 니블, 바이트, 워드의 크기 관계를 알고 빈칸에 알맞은 단위를 넣을 수 있는지를 묻는 문제이다.

핵심 개념

비트는 0 또는 1 하나를 나타내는 최소 정보 단위이다. 쿼터는 2비트, 니블은 4비트, 바이트는 8비트이다. 따라서 오름차순은 '비트 < 쿼터 < 니블 < 바이트 < 워드'가 된다. 더블워드는 워드 2개에 해당하므로 워드보다 큰 단위이다.

선지별 해설

① X — ㉠의 '바이트'와 ㉡의 '쿼터'가 모두 틀렸다. 바이트는 니블보다 크고, 쿼터는 니블보다 작다. 올바르게는 ㉠이 쿼터, ㉡이 바이트이다.
② X — ㉠의 '바이트'는 니블보다 작을 수 없고, ㉡의 '더블워드'는 워드보다 큰 단위이므로 두 위치가 모두 틀렸다. 올바르게는 ㉠이 쿼터, ㉡이 바이트이다.
③ O — 쿼터는 2비트이므로 비트와 니블 사이에 놓이고, 바이트는 8비트이므로 니블과 워드 사이에 놓인다.
④ X — ㉠의 '쿼터'는 맞지만 ㉡의 '더블워드'가 틀렸다. 더블워드는 워드보다 크므로 워드 앞의 빈칸에 올 수 없다. 올바르게는 ㉡이 바이트이다.

NoteBase

오답 포인트

‘쿼터’를 4비트로 착각하면 니블과 혼동하기 쉽다. 쿼터는 바이트의 4분의 1인 2비트이고, 니블은 바이트의 절반인 4비트이다. 또한 더블워드는 이름 그대로 워드 2개이므로 워드보다 앞에 올 수 없다.

다시 나오면 이렇게 판단

각 단위를 비트 수로 바꾸어 비교한다. 쿼터는 2비트, 니블은 4비트, 바이트는 8비트이며, 더블워드는 워드보다 크다는 관계를 적용한다.

암기 포인트

1비트 < 2비트 쿼터 < 4비트 니블 < 8비트 바이트 < 워드 < 더블워드이다.

NoteBase

문 2. 디지털 증거의 특성으로 가장 적절하지 않은 것은?

① 대량성

② 가시성

③ 초국경성

④ 변조의 용이성

정답 2번

출제 포인트

디지털 증거가 저장·표현·전송되는 방식에서 나타나는 특성을 구별하는 문제이다.

핵심 개념

디지털 증거는 디지털 형태로 저장되므로 대량으로 축적될 수 있고, 네트워크를 통해 국경을 넘어 존재할 수 있으며, 손쉽게 변경될 수 있다. 또한 그 자체를 사람이 바로 지각하기 어려워 장치와 소프트웨어를 이용해 사람이 인식할 수 있는 형태로 변환해야 하므로 비가시성을 가진다.

선지별 해설

① O — 대량성은 디지털 저장매체에 방대한 양의 정보가 저장·축적될 수 있다는 특성이다.
② X — 틀린 표현은 '가시성'이다. 디지털 증거는 그 자체를 사람이 직접 보거나 읽기 어려우므로, 올바르게는 '비가시성'이 디지털 증거의 특성이다.
③ O — 초국경성은 네트워크를 통해 디지털 정보가 여러 국가의 시스템이나 저장장소에 분산되거나 국경을 넘어 전송될 수 있다는 특성이다.
④ O — 변조의 용이성은 디지털 정보가 비교적 쉽게 수정·삭제될 수 있다는 특성으로, 무결성 확인이 중요해지는 이유이다.

오답 포인트

②의 '가시성'은 디지털 자료가 화면에 표시될 수 있다는 일상적 인상 때문에 그럴듯해 보인다. 그러나 화면에 보이는 것은 장치와 소프트웨어가 변환한 결과이며, 디지털 증거 자체의 특성은 비가시성이다.

다시 나오면 이렇게 판단

디지털 증거의 원래 저장 형태를 사람이 장치 없이 직접 인식할 수 있는지를 기준으로 판단한다. 별도의 장치와 변환 과정이 필요하므로 가시성이 아니라 비가시성이다.

암기 포인트

디지털 증거는 대량·초국경·변조 용이, 그리고 가시성이 아니라 비가시성이다.

NoteBase

문 3. 한글 2020 프로그램을 이용하여 암호화된 '경찰.hwp' 파일을 'C:\User\police\Desktop\'에 저장하는 과정에서 사용자의 개입 없이 운영체제가 생성하는 디지털 증거로 가장 적절한 것은?

① 파일 이름
② 파일 내용
③ 저장 시간
④ 문서 암호

정답 3번

출제 포인트

파일을 저장할 때 사용자가 직접 정하는 정보와 운영체제·파일시스템이 자동으로 기록하는 메타데이터를 구별하는 문제이다.

핵심 개념

파일시스템 메타데이터는 파일의 내용과 별도로 운영체제가 파일을 관리하기 위해 기록하는 정보이다. 파일의 생성·수정·접근 시각 같은 시간 정보는 저장 동작에 따라 시스템 시계를 바탕으로 자동 기록될 수 있다. 반면 파일 이름, 파일 내용, 문서 암호는 사용자가 지정하거나 입력한 정보이다.

선지별 해설

① X — 파일 이름은 사용자가 저장 과정에서 지정한 정보이다. '파일 이름'이 운영체제가 사용자의 개입 없이 생성한다는 부분이 틀렸으며, 올바르게는 사용자가 지정한 파일 식별 정보이다.
② X — 파일 내용은 사용자가 문서 프로그램에서 작성하거나 편집한 데이터이다. '파일 내용'이 운영체제가 자동 생성한다는 부분이 틀렸으며, 올바르게는 사용자가 입력한 문서 데이터이다.
③ O — 저장 시간은 파일을 저장할 때 운영체제·파일시스템이 시스템 시계를 바탕으로 파일의 시간 메타데이터에 자동 기록하는 정보이므로 가장 적절하다.
④ X — 문서 암호는 암호화 기능을 선택한 사용자가 설정하는 값이다. '문서 암호'가 운영체제에 의해 자동 생성된다는 부분이 틀렸으며, 올바르게는 사용자가 지정한 보안 정보이다.

오답 포인트

파일 안이나 파일 속성에 남아 있다는 사실만으로 모두 운영체제가 생성한 증거가 되는 것은 아니다. ① 파일 이름, ② 파일 내용, ④ 문서 암호는 저장 대상에 포함되지만 사용자의 의사와 입력이 반영된 정보이고, ③ 저장 시간은 저장 행위에 따라 시스템이 자동으로 남기는 메타데이터이다.

NoteBase

다시 나오면 이렇게 판단

각 정보가 '사용자가 정하거나 입력한 값'인지 '운영체제·파일시스템이 동작 과정에서 자동 기록한 값'인지로 나눈다. 생성·수정·접근 시각과 같은 타임스탬프는 후자에 해당한다.

암기 포인트

이름·내용·암호는 사용자 지정, 파일 시간은 시스템 자동 기록이다.

NoteBase

문 4. 디지털 증거가 최초 수집 시점으로부터 법정에 제출되기까지 변경 또는 훼손이 없어야 한다는 원칙으로 가장 적절한 것은?

① 신뢰성의 원칙
② 동일성의 원칙
③ 무결성의 원칙
④ 진정성의 원칙

정답 3번

출제 포인트

디지털 증거가 수집된 뒤 법정에 제출될 때까지 변경·훼손되지 않았음을 요구하는 무결성의 원칙을 다른 증거 원칙과 구별하는 문제이다.

핵심 개념

무결성의 원칙은 디지털 증거가 수집·보관·분석·이송·제출되는 전 과정에서 임의로 변경되거나 훼손되지 않아야 한다는 원칙이다. 해시값 비교와 적정한 증거 취급 기록은 이러한 무결성을 확인하는 대표적 수단이다. 신뢰성은 사용한 도구·절차와 그 결과를 믿을 수 있는지를, 동일성은 원본과 복제본 등 비교 대상이 서로 같은지를, 진정성은 제출된 자료가 주장하는 바로 그 증거인지를 중심으로 판단한다.

선지별 해설

① X — '신뢰성의 원칙'은 분석 도구와 절차가 신뢰할 수 있고 같은 조건에서 검증 가능한 결과를 내는지에 관한 원칙이다. 틀린 표현은 '신뢰성'이며, 수집 시점부터 제출 시점까지 변경·훼손이 없어야 한다는 설명은 '무결성의 원칙'이다.
② X — '동일성의 원칙'은 복제본이나 분석 대상이 원본과 동일한지를 확인하는 데 초점이 있다. 틀린 표현은 '동일성'이며, 증거 취급 전 과정에서 변경·훼손되지 않아야 한다는 원칙은 '무결성의 원칙'이다.
③ O — '무결성의 원칙'은 디지털 증거가 최초 수집 이후 법정 제출까지 변경되거나 훼손되지 않은 상태로 유지되어야 한다는 원칙이므로 제시된 설명과 일치한다.
④ X — '진정성의 원칙'은 제출된 자료가 주장하는 출처와 내용의 바로 그 증거임을 확인하는 데 초점이 있다. 틀린 표현은 '진정성'이며, 수집부터 제출까지 변경·훼손이 없어야 한다는 설명은 '무결성의 원칙'이다.

오답 포인트

②의 '동일성'은 원본과 복제본의 일치 여부를 떠올리게 하므로 ③의 '무결성'과 혼동하기 쉽다. 그러나 문장의 핵심이 '최초 수집 시점부터 법정 제출까지 변경 또는 훼손이 없음'이라는 전 과정의 상태 유지이므로 무결성을 선택한다.

NoteBase

다시 나오면 이렇게 판단

‘변경·훼손 없음’, ‘변조 방지’, ‘수집부터 제출까지 보존’이 핵심이면 무결성으로 판단한다. ‘도구·절차와 결과를 믿을 수 있음’은 신뢰성, ‘원본과 복제본이 같음’은 동일성, ‘주장된 바로 그 증거임’은 진정성으로 구별한다.

암기 포인트

무결성은 처음부터 법정까지 변경·훼손 없이 온전하게 유지되는 것이다.

NoteBase

문 5. 다음에서 설명하는 것으로 가장 적절한 것은?

‘디지털 지문’ 또는 ‘디지털 DNA’라고 불리며, 파일에 저장된 데이터의 한 비트만 변경되어도 다른 결괏값이 나오기 때문에 파일의 무결성을 입증할 때 사용한다.

① 해시값(hash value)
② 시그니처(signature)
③ 파일 이름(file name)
④ 파일 확장자(file extension)

정답 1번

출제 포인트

파일 데이터의 아주 작은 변화도 서로 다른 결괏값으로 나타내어 무결성을 확인하는 해시값의 개념을 묻는 문제이다.

핵심 개념

해시값은 파일의 데이터를 해시 함수에 입력하여 얻는 고정 길이의 결괏값이다. 원본과 사본의 해시값이 같으면 데이터가 변경되지 않았음을 확인하는 근거가 되며, 데이터가 한 비트만 달라져도 일반적으로 전혀 다른 해시값이 나온다.
파일 시그니처는 파일 내부의 특정 바이트 패턴으로 파일 형식을 식별하는 정보이고, 파일 이름은 사용자가 붙인 명칭이며, 파일 확장자는 파일 형식을 표시하기 위해 이름 끝에 붙이는 문자열이다.

선지별 해설

① O — 해시값은 파일 데이터로부터 계산되는 디지털 지문으로, 원본과 복제본의 동일성 및 파일의 무결성을 검증하는 데 사용한다.
② X — 틀린 표현은 ‘시그니처’이다. 파일 시그니처는 파일 내부의 고유한 바이트 패턴을 이용해 파일 형식을 식별하는 정보이며, 제시문처럼 파일의 한 비트 변화에 따라 달라지는 무결성 검증값은 해시값이다.
③ X — 틀린 표현은 ‘파일 이름’이다. 파일 이름은 파일을 구별하기 위해 붙인 명칭으로 데이터 내용이 그대로여도 바꿀 수 있으며, 파일 내용의 변경 여부를 검증하는 값은 해시값이다.
④ X — 틀린 표현은 ‘파일 확장자’이다. 파일 확장자는 파일 이름 끝에서 형식을 표시하는 문자열로 사용자가 임의로 변경할 수 있으며, 파일 자체의 무결성을 입증하는 값은 해시값이다.

오답 포인트

②의 ‘시그니처’도 디지털 포렌식에서 파일 식별에 활용되므로 해시값과 혼동하기 쉽다. 그러나 파일 형식을 식별하는 내부 패턴은 파일 시그니처이고, 파일 전체 데이터의 변경 여부를 비교하는 결괏값은 해시값이다.

NoteBase

다시 나오면 이렇게 판단

‘디지털 지문’, ‘한 비트만 바뀌어도 다른 결괏값’, ‘무결성 검증’이 함께 제시되면 해시값으로 판단한다. 파일 형식 식별은 시그니처, 사람이 붙이는 명칭은 파일 이름, 이름 끝의 형식 표시는 확장자로 구분한다.

암기 포인트

해시값은 내용의 동일성·무결성, 시그니처는 파일 형식 식별이다.

NoteBase

문 6. 다음은 디지털포렌식 조사 대상을 휘발성 정도에 따라 정렬한 것이다. 라이브 이미징(live imaging) 대상으로 옳게 짝지어진 것은?

㉠ 아카이브(archive) 매체에 있는 데이터
㉡ 원격에 위치한 로그(log) 데이터
㉢ 하드디스크에 있는 데이터
㉣ 주기억 장치에 있는 데이터
㉤ 라우팅 테이블, ARP 캐시 데이터
㉥ CPU 캐시 및 레지스터 데이터

① ㉠㉡㉢
② ㉡㉢㉣
③ ㉢㉣㉤
④ ㉣㉤㉥

정답 4번

출제 포인트

라이브 이미징의 대상이 되는 휘발성 데이터와 전원이 꺼져도 남는 비휘발성 데이터를 구분하는 문제이다.

핵심 개념

라이브 이미징은 시스템이 작동 중인 상태에서만 확보할 수 있거나 시간이 지나면서 빠르게 변하는 데이터를 수집하는 방식이다. 주기억 장치의 데이터, 라우팅 테이블·ARP 캐시, CPU 캐시·레지스터는 대표적인 휘발성 데이터이다. 반면 하드디스크, 원격 로그, 아카이브 매체의 데이터는 전원이 차단되어도 상대적으로 오래 남으므로 일반적인 라이브 이미징의 핵심 대상이 아니다.

선지별 해설

① X — ㉠ 아카이브 데이터, ㉡ 원격 로그 데이터, ㉢ 하드디스크 데이터는 모두 비휘발성 저장 데이터에 해당한다. 틀린 묶음 ㉠㉡㉢은 라이브 이미징 대상인 ㉣㉤㉥으로 고쳐야 한다.
② X — ㉣ 주기억 장치 데이터는 라이브 이미징 대상이지만, ㉡ 원격 로그와 ㉢ 하드디스크 데이터는 비휘발성이다. 틀린 묶음 ㉡㉢㉣은 ㉣㉤㉥으로 고쳐야 한다.
③ X — ㉣ 주기억 장치와 ㉤ 라우팅 테이블·ARP 캐시는 휘발성 데이터이지만, ㉢ 하드디스크 데이터는 비휘발성이다. ㉢ 대신 가장 휘발성이 높은 ㉥ CPU 캐시·레지스터를 포함하여 ㉣㉤㉥으로 고쳐야 한다.
④ O — ㉣ 주기억 장치, ㉤ 라우팅 테이블·ARP 캐시, ㉥ CPU 캐시·레지스터는 시스템 종료나 시간 경과로 소실·변경될 수 있으므로 작동 중 우선 수집하는 라이브 이미징 대상이다.

NoteBase

오답 포인트

ⓒ 하드디스크도 디지털포렌식의 중요한 조사 대상이어서 라이브 이미징 대상과 혼동하기 쉽다. 그러나 이 문항은 모든 포렌식 대상이 아니라 전원이 켜진 상태에서 확보해야 하는 휘발성 데이터를 묻는다.

다시 나오면 이렇게 판단

전원이 꺼지거나 시스템 상태가 바뀌면 사라지는지를 기준으로 판단한다. CPU 캐시·레지스터, 네트워크 상태 정보, 주기억 장치는 라이브 상태에서 우선 수집하고, 디스크·원격 로그·아카이브는 상대적으로 비휘발성인 저장 데이터로 구분한다.

암기 포인트

라이브 이미징은 레지스터·캐시, 네트워크 상태, 메모리처럼 사라지기 쉬운 데이터부터 확보한다.

NoteBase

문 7. 다음에서 설명하는 디지털포렌식 작업으로 옳게 짝지어진 것은?

분석대상 하드디스크(hard disk)에 대한 완전 복사본(comprehensive copy)을 생성하여 다른 하드디스크에 동일한 구조로 저장하는 작업으로, 이 두 개 하드디스크의 물리적 섹터에 동일한 데이터 분포를 보존할 수 있다. 이를 통해 원본 하드디스크의 훼손 없이 비할당 영역까지 조사 및 포렌식 분석이 가능하다.

① Disk imaging, disk cloning

② Disk imaging, disk partitioning

③ Disk data copying, disk cloning

④ Disk data copying, disk partitioning

정답 1번

출제 포인트

완전 복사본을 만드는 디스크 이미징과 그 복사 내용을 다른 디스크에 동일한 구조로 재현하는 디스크 클로닝을 구별하는 문제이다.

핵심 개념

Disk imaging은 원본 저장매체의 물리적 섹터를 빠짐없이 읽어 이미지 형태의 완전 복사본을 만드는 작업이다. 비할당 영역과 삭제 데이터의 흔적까지 보존할 수 있다.
Disk cloning은 원본 디스크의 섹터별 내용을 다른 디스크에 직접 복제하여 원본과 같은 구조와 데이터 배치를 재현하는 작업이다.
Disk data copying은 일반적인 파일·데이터 복사로, 물리적 섹터 전체와 비할당 영역의 보존을 보장하지 않는다. Disk partitioning은 하나의 디스크 공간을 여러 논리 영역으로 나누는 작업이다.

선지별 해설

① O — 완전 복사본을 생성하는 것은 Disk imaging이고, 이를 다른 하드디스크에 동일한 구조로 재현하는 것은 Disk cloning이다. 두 작업 모두 물리적 섹터 수준의 보존이라는 제시문의 핵심과 맞는다.
② X — 틀린 표현은 두 번째의 ‘disk partitioning’이다. 디스크 공간을 구획하는 작업이 아니라 다른 디스크에 동일한 구조로 복제하는 작업이므로 ‘disk cloning’이 맞다.
③ X — 틀린 표현은 첫 번째의 ‘disk data copying’이다. 일반적인 데이터 복사가 아니라 비할당 영역까지 포함한 완전 복사본을 생성하므로 ‘disk imaging’이 맞다. 두 번째의 ‘disk cloning’은 옳다.
④ X — ‘disk data copying’과 ‘disk partitioning’이 모두 제시문의 작업과 다르다. 올바른 짝은 완전 복사본 생성에 해당하는 ‘disk imaging’과 다른 디스크에 동일 구조로 복제하는 ‘disk cloning’이다.

NoteBase

오답 포인트

‘copy’라는 일상적 표현 때문에 Disk data copying을 고르기 쉽지만, 제시문의 ‘물리적 섹터’, ‘비할당 영역’, ‘완전 복사본’은 단순 파일 복사가 아니라 Disk imaging을 가리킨다. 또한 다른 하드디스크에 동일한 구조로 저장한다는 표현은 공간을 나누는 partitioning이 아니라 cloning의 단서이다.

다시 나오면 이렇게 판단

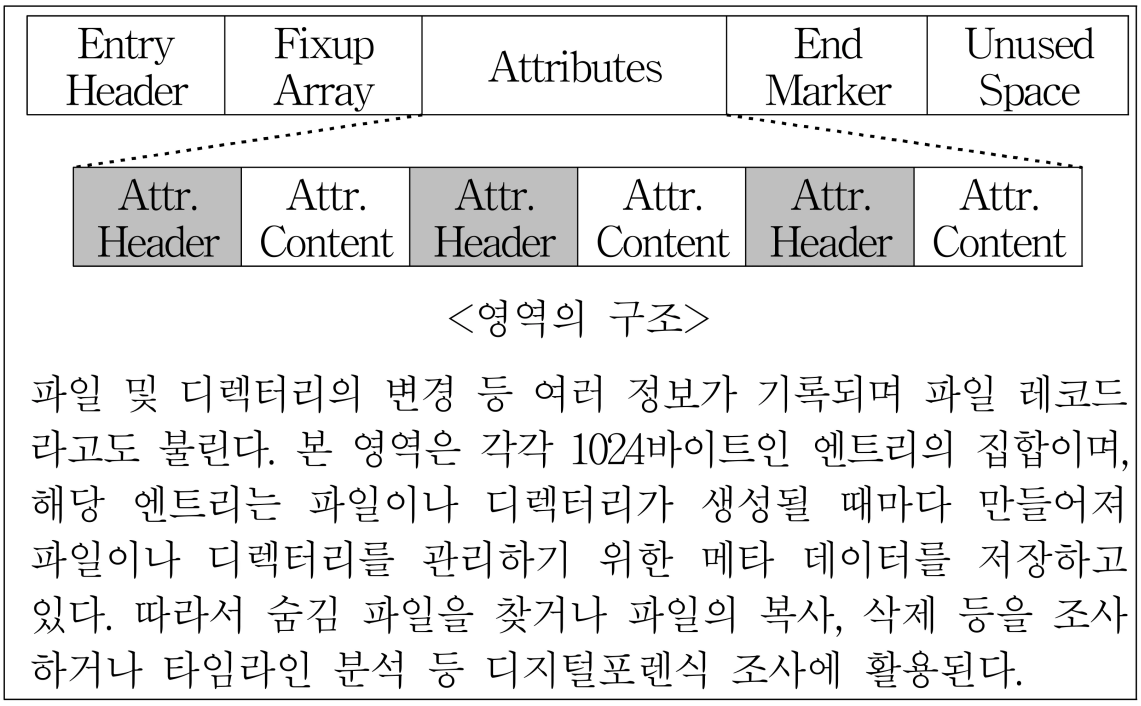
비할당 영역을 포함한 섹터 단위 완전 복사본이면 imaging, 그 내용을 다른 물리 디스크에 원본과 같은 구조로 재현하면 cloning, 디스크 공간을 구획하면 partitioning으로 판단한다.

암기 포인트

이미지 파일을 만드는 것은 imaging, 디스크를 디스크로 복제하는 것은 cloning, 공간을 나누는 것은 partitioning이다.

NoteBase

문 8. 다음에서 설명하는 영역을 사용하는 운영체제로 가장 적절한 것은?



<영역의 구조>

파일 및 디렉터리의 변경 등 여러 정보가 기록되며 파일 레코드라고도 불린다. 본 영역은 각각 1024바이트인 엔트리의 집합이며, 해당 엔트리는 파일이나 디렉터리가 생성될 때마다 만들어져 파일이나 디렉터리를 관리하기 위한 메타 데이터를 저장하고 있다. 따라서 숨김 파일을 찾거나 파일의 복사, 삭제 등을 조사하거나 타임라인 분석 등 디지털포렌식 조사에 활용된다.

① OS X

② Linux

③ Android

④ Windows

정답 4번

출제 포인트

도식의 1024바이트 엔트리, 속성 헤더와 속성 내용의 반복, 종료 표식은 NTFS의 MFT(Master File Table) 레코드 구조를 나타낸다. NTFS를 기본적으로 사용하는 운영체제를 식별하는 문제이다.

NoteBase

선지별 해설

① X — OS X라는 연결이 틀리다. OS X의 대표적인 기본 파일 시스템은 HFS+이며, 이후에는 APFS를 사용한다. 제시된 구조는 OS X의 기본 파일 시스템 영역이 아니라 NTFS의 MFT이다.
② X — Linux라는 연결이 틀리다. Linux에서는 ext 계열 파일 시스템의 inode 등이 파일 메타데이터를 관리한다. 제시된 구조는 Linux 고유의 inode 구조가 아니라 NTFS의 MFT이다.
③ X — Android라는 연결이 틀리다. Android는 Linux 커널을 기반으로 하며 저장장치에 ext4나 F2FS 등을 주로 사용한다. 제시된 구조는 Android의 대표적인 파일 시스템 영역이 아니라 NTFS의 MFT이다.
④ O — Windows는 NTFS를 사용하며, NTFS의 MFT는 각 파일과 디렉터리에 관한 메타데이터를 레코드 단위로 저장한다. 도식의 엔트리 헤더, 속성 배열, 종료 표식과 설명의 1024바이트 엔트리가 이에 해당한다.

오답 포인트

파일과 디렉터리의 메타데이터를 저장한다는 일반적 설명만 보고 inode와 혼동하기 쉽다. 이 문항에서는 1024바이트 MFT 엔트리와 속성의 반복 구조가 NTFS를 특정하는 결정적 단서이다.

다시 나오면 이렇게 판단

MFT, 1024바이트 파일 레코드, 속성 헤더·속성 내용의 반복이 제시되면 NTFS를 떠올리고 Windows와 연결한다. inode는 Linux의 ext 계열, APFS는 macOS, F2FS는 Android 계열의 대표 단서로 구분한다.

암기 포인트

MFT → NTFS → Windows로 연결한다.

NoteBase

문 9. 다음에서 설명하는 디스크 브라우징(disk browsing) 도구로 가장 적절하지 않은 것은?

저장매체 또는 하드디스크 이미지의 내부 구조와 파일 시스템을 확인할 수 있으며, 파일 시스템 내부에 존재하는 파일에 대응하는 응용 프로그램의 별도 구동 없이 쉽고 빠른 분석을 지원하는 기법을 디스크 브라우징 기술이라 한다. 디스크 브라우징 기술은 사용자가 복제한 이미지를 수동으로 마운팅(mounting)하여 열람할 필요가 없으므로 분석 시간을 단축할 수 있는 장점이 있다.

① Falcon

② EnCase

③ X-Ways Forensics

④ FTK(Forensic Tool Kit)

정답 1번

출제 포인트

디지털 포렌식 도구를 증거 저장매체의 이미지를 만드는 이미징·복제 도구와, 확보한 이미지의 파일 시스템 및 파일을 살펴보는 디스크 브라우징 도구로 구분하는 문제이다.

핵심 개념

디스크 브라우징은 포렌식 이미지나 저장매체의 파티션·파일 시스템 구조를 해석하여 파일과 메타데이터를 탐색·분석하는 기술이다. 반면 이미징·복제는 원본 저장매체의 데이터를 분석용 사본으로 획득하는 단계이다. 이 문항에서는 EnCase, X-Ways Forensics, FTK가 디스크 브라우징 기능을 제공하고, Falcon은 저장매체 이미징·복제 용도의 도구로 구분된다.

선지별 해설

① X — Falcon은 저장매체의 데이터를 포렌식 이미지로 획득하거나 복제하는 용도의 도구로 분류되므로, 확보된 이미지의 파일 시스템과 파일을 탐색하는 디스크 브라우징 도구로 보기 어렵다. 틀린 분류는 'Falcon은 디스크 브라우징 도구이다'이며, 올바르게는 'Falcon은 저장매체 이미징·복제 도구이다'이다.
② O — EnCase는 증거 이미지 등을 불러와 파티션과 파일 시스템 구조를 해석하고 내부 파일을 탐색·분석할 수 있는 대표적인 디지털 포렌식 분석 도구이다.
③ O — X-Ways Forensics는 디스크 이미지와 파일 시스템을 열어 파일, 폴더, 메타데이터 및 삭제 흔적 등을 조사할 수 있으므로 디스크 브라우징 도구에 해당한다.
④ O — FTK는 증거 이미지의 파일 시스템을 분석하고 파일 트리 탐색, 검색 및 파일 검토 기능을 제공하므로 디스크 브라우징 도구에 해당한다.

NoteBase

오답 포인트

Falcon도 디지털 포렌식 분야에서 사용하는 제품이므로 분석 도구로 혼동하기 쉽다. 그러나 이 문항의 구분 기준은 포렌식 도구인지 여부가 아니라, 저장매체를 복제하는 획득 단계의 도구인지 확보된 이미지 내부를 탐색하는 분석 단계의 도구인지이다.

다시 나오면 이렇게 판단

도구의 주된 기능이 원본 매체에서 이미지를 생성하는 것이면 이미징·복제 도구로, 이미지의 파티션·파일 시스템·파일을 열어 조사하는 것이면 디스크 브라우징 도구로 판단한다.

암기 포인트

Falcon은 획득·복제, EnCase·X-Ways Forensics·FTK는 이미지 내부 탐색·분석으로 구분한다.

NoteBase

문 10. 운영체제 구동을 위한 부팅(booting) 정보가 저장된 하드디스크의 영역으로 가장 적절한 것은?

① Boot sector

② Data sector

③ Root directory

④ MBR(Master Boot Record)

정답 4번

출제 포인트

이 문제는 하드디스크의 부팅 과정에서 MBR, 파티션의 부트 섹터, 데이터 영역, 루트 디렉터리가 맡는 역할을 구별하는 문제이다.

핵심 개념

MBR(Master Boot Record)은 하드디스크의 첫 번째 물리 섹터에 위치하며, 부팅에 사용되는 코드와 파티션 정보를 담는 영역이다. 전통적인 BIOS 방식에서는 MBR의 부트 코드가 실행되어 부팅 가능한 파티션의 다음 부팅 단계로 제어를 넘긴다.
MBR은 디스크 전체의 시작 지점, 부트 섹터는 일반적으로 개별 파티션 또는 볼륨의 시작 지점이라는 차이가 핵심이다.

선지별 해설

① X — 틀린 표현은 'Boot sector'이다. 부트 섹터는 일반적으로 개별 파티션 또는 볼륨의 시작 부분에서 그 볼륨의 부팅 정보와 파일시스템 정보를 담는다. 이 문항에서 묻는 하드디스크 전체의 최초 부팅 정보 영역은 MBR이다.
② X — 틀린 표현은 'Data sector'이다. 데이터 섹터는 파일의 실제 내용 등 사용자 데이터를 저장하는 영역이다. 부팅 코드와 파티션 정보를 저장하는 영역은 MBR이다.
③ X — 틀린 표현은 'Root directory'이다. 루트 디렉터리는 파일명, 속성, 시작 위치 등 파일과 하위 디렉터리의 항목을 관리하는 최상위 디렉터리 영역이다. 디스크 부팅 정보를 저장하는 영역은 MBR이다.
④ O — MBR은 Master Boot Record의 약자로, 하드디스크의 첫 번째 물리 섹터에 있으며 부팅 코드와 파티션 정보를 담으므로 가장 적절하다.

오답 포인트

①의 'Boot sector'도 부팅 관련 정보를 담기 때문에 혼동하기 쉽다. 그러나 디스크 전체의 시작 영역을 묻는 경우에는 MBR을, 개별 파티션이나 볼륨의 시작 영역을 묻는 경우에는 부트 섹터를 대응시킨다.

NoteBase

다시 나오면 이렇게 판단

문제에서 '하드디스크의 첫 영역·파티션 정보·최초 부팅 코드'를 묻는지 확인하면 MBR로 판단한다. '개별 볼륨의 시작·파일시스템 정보'를 묻는다면 부트 섹터와 구별한다.

암기 포인트

디스크 전체의 출발점은 MBR, 파티션·볼륨의 출발점은 부트 섹터이다.

NoteBase

문 11. NTFS(New Technology File System)에서 파일이나 디렉터리를 관리하기 위한 메타 데이터를 저장한 테이블로 가장 적절한 것은?

① $MFT
② $Bitmap
③ $LogFile
④ $Volume

정답 1번

출제 포인트

NTFS의 주요 메타데이터 파일이 각각 어떤 정보를 관리하는지 구별하는 문제이다.

핵심 개념

$MFT(Master File Table)는 NTFS 볼륨에 존재하는 모든 파일과 디렉터리의 메타데이터 레코드를 저장하는 핵심 테이블이다. 파일명, 시간 정보, 속성, 데이터 위치 등 파일 시스템이 객체를 관리하는 데 필요한 정보가 기록된다.
$Bitmap은 클러스터의 할당 여부를, $LogFile은 메타데이터 변경 작업의 로그를, $Volume은 볼륨 자체의 정보를 관리한다.

선지별 해설

① O — $MFT는 NTFS에서 각 파일과 디렉터리에 대응하는 레코드를 두고 그 메타데이터를 저장하는 테이블이다.
② X — $Bitmap은 파일·디렉터리의 메타데이터 테이블이 아니다. 틀린 선택지 $Bitmap → 올바르게는 볼륨의 각 클러스터가 사용 중인지 비어 있는지를 비트 단위로 나타내는 메타데이터 파일이다.
③ X — $LogFile은 파일·디렉터리의 메타데이터 테이블이 아니다. 틀린 선택지 $LogFile → 올바르게는 NTFS 메타데이터 변경 작업을 기록하여 장애 발생 시 파일 시스템의 일관성을 복구하는 데 쓰이는 트랜잭션 로그 파일이다.
④ X — $Volume은 파일·디렉터리의 메타데이터 테이블이 아니다. 틀린 선택지 $Volume → 올바르게는 NTFS 버전과 볼륨 상태 플래그 등 볼륨 자체의 정보를 저장하는 메타데이터 파일이다.

오답 포인트

네 항목이 모두 NTFS의 특수 메타데이터 파일이라는 점이 함정이다. 질문은 메타데이터 파일의 존재 여부가 아니라 파일과 디렉터리별 관리 레코드를 모아 둔 테이블을 묻고 있으므로 $MFT가 정답이다.

NoteBase

다시 나오면 이렇게 판단

파일·디렉터리별 정보는 $MFT, 클러스터 사용 현황은 $Bitmap, 변경 작업 기록은 $LogFile, 볼륨 자체 정보는 $Volume으로 구분한다.

암기 포인트

$MFT는 파일 목록의 중심, $Bitmap은 공간 지도, $LogFile은 변경 기록, $Volume은 볼륨 정보이다.

NoteBase

문 12. 다음 디지털포렌식 분석에 활용되는 Windows의 파일로 가장 적절한 것은?

응용 프로그램의 실행에 필요한 시스템 자원 정보를 파일에 저장해 놓음으로써, 이 같은 정보를 활용하여 프로그램 실행 속도를 높일 수 있다. 따라서, 자원 정보는 실행 프로그램에 대한 프로그램 이름, 경로 정보, 수행 횟수, 실행 시 참조한 파일 등을 포함하고 있으므로, 디지털포렌식 분석을 통해 증거로 활용될 수 있다.

① 캐시(cache)

② 쉘백(shellbag)

③ 프리패치(prefetch)

④ 볼륨쉐도우(volume shadow)

정답 3번

출제 포인트

응용 프로그램 실행을 빠르게 하기 위해 실행 관련 자원 정보를 저장하며, 포렌식 분석에서 프로그램명·경로·실행 횟수·참조 파일 등을 확인할 수 있는 Windows 아티팩트를 구별하는 문제이다.

핵심 개념

프리패치(prefetch)는 Windows가 응용 프로그램의 실행 속도를 높이기 위해 실행 과정에서 필요한 파일 등의 정보를 미리 기록해 두는 기능이자 그 기록 파일이다. 프리패치 파일에는 실행 파일 정보, 실행 횟수, 최근 실행 시각, 실행 시 참조한 파일과 디렉터리 등의 흔적이 남을 수 있어 프로그램 실행 여부와 사용 정황을 분석하는 데 활용된다.
캐시는 자주 사용하는 데이터에 빠르게 접근하도록 임시 저장하는 영역이고, 쉘백은 사용자가 탐색한 폴더의 흔적을 담는 레지스트리 아티팩트이며, 볼륨 쉐도우는 특정 시점의 볼륨 데이터를 복사해 둔 스냅숏이다.

NoteBase

선지별 해설

① X — 캐시(cache)는 자주 사용하는 데이터나 처리 결과를 임시 저장하여 접근 속도를 높이는 일반적인 저장 방식이다. 제시문처럼 프로그램 실행에 참조된 파일과 실행 횟수 등을 기록하는 Windows 실행 아티팩트라는 부분이 틀렸으며, 올바른 개념은 프리패치이다.
② X — 쉘백(shellbag)은 Windows 탐색기에서 사용자가 열어 본 폴더의 경로와 표시 관련 흔적 등을 레지스트리에 남기는 아티팩트이다. 프로그램 실행 속도를 높이기 위한 자원 정보 파일이라는 부분이 틀렸으며, 올바른 개념은 프리패치이다.
③ O — 프리패치(prefetch)는 응용 프로그램 실행에 필요한 정보를 파일에 기록하여 이후 실행을 빠르게 하고, 실행 파일 정보·실행 횟수·최근 실행 시각·참조 파일 등의 흔적을 남길 수 있으므로 제시문에 가장 적절하다.
④ X — 볼륨 쉐도우(volume shadow)는 특정 시점의 볼륨 상태를 보존한 스냅숏으로, 삭제·변경 전 파일이나 과거 상태를 복원·분석하는 데 활용된다. 프로그램별 실행 자원 정보와 실행 횟수를 기록하는 파일이라는 부분이 틀렸으며, 올바른 개념은 프리패치이다.

오답 포인트

① 캐시도 속도 향상을 목적으로 하므로 혼동하기 쉽다. 그러나 제시문의 결정적 단서는 프로그램 실행 정보와 실행 횟수, 실행 시 참조한 파일까지 남는다는 점이며, 이는 프리패치의 특징이다.

다시 나오면 이렇게 판단

프로그램 실행 가속과 실행 횟수·참조 파일이 함께 제시되면 프리패치로 판단한다. 폴더 탐색 흔적은 쉘백, 특정 시점의 과거 파일 복원은 볼륨 쉐도우, 일반적인 임시 데이터 저장은 캐시로 구별한다.

암기 포인트

프리패치는 프로그램 실행 흔적, 쉘백은 폴더 탐색 흔적, 볼륨 쉐도우는 과거 시점의 스냅숏이다.

NoteBase

문 13. 크롬 웹 브라우저(chrome web browser)가 기록하는 정보와 이를 저장하는 데이터베이스가 옳게 짝지어진 것은?

① 정보: 웹 서버에 접근한 사용자에 대한 정보, 데이터베이스: history data

② 정보: 방문한 URL의 접근 횟수에 따른 순위, 데이터베이스: top sites

③ 정보: 자동 완성 폼 채우기 기능에 사용된 정보, 데이터베이스: login data

④ 정보: 브라우저 상단에 방문 사이트 아이콘 정보, 데이터베이스: web data

정답 2번

출제 포인트

크롬이 생성하는 주요 데이터베이스 파일과 그 파일에 저장되는 웹 사용 흔적의 대응 관계를 묻는 문제이다.

핵심 개념

History는 방문 URL과 방문 기록을, Top Sites는 자주 방문한 사이트의 순위 정보를 저장한다. Login Data는 저장된 로그인 자격 증명을, Web Data는 자동 완성에 이용되는 폼 정보를 저장하며, Favicons는 사이트 아이콘 정보를 저장한다.

NoteBase

선지별 해설

① X
History 데이터베이스는 방문한 URL, 제목, 방문 시각·횟수 등의 브라우징 기록을 저장한다. 틀린 표현은 '웹 서버에 접근한 사용자에 대한 정보 → history data'이며, 이러한 사용자 상태 정보는 쿠키와 관련되고 History에는 방문 이력이 저장된다.

② O
Top Sites 데이터베이스에는 방문 빈도 등을 바탕으로 한 자주 방문한 URL의 순위 정보가 저장된다. 따라서 '방문한 URL의 접근 횟수에 따른 순위 → top sites'의 대응은 옳다.

③ X
자동 완성 폼 채우기에 사용된 정보는 Web Data 데이터베이스에 저장된다. 틀린 표현은 '자동 완성 폼 채우기 정보 → login data'이며, 올바르게는 '자동 완성 폼 채우기 정보 → web data'이다. Login Data는 저장된 로그인 아이디와 비밀번호 등 로그인 자격 증명에 관한 정보를 저장한다.

④ X
방문 사이트의 아이콘인 파비콘 정보는 Favicons 데이터베이스에 저장된다. 틀린 표현은 '방문 사이트 아이콘 정보 → web data'이며, 올바르게는 '방문 사이트 아이콘 정보 → favicons'이다. Web Data는 자동 완성 폼 정보 등을 저장한다.

오답 포인트

③과 ④는 Web Data의 저장 대상을 서로 다른 데이터베이스의 기능과 바꾸어 놓은 선지이다. 특히 파일 이름만 보고 Login Data에 자동 완성 정보까지 모두 들어간다고 판단하면 틀리기 쉽다.

다시 나오면 이렇게 판단

데이터베이스 이름을 저장 대상과 직접 연결한다. 방문 이력은 History, 자주 방문한 사이트 순위는 Top Sites, 로그인 자격 증명은 Login Data, 자동 완성 폼은 Web Data, 사이트 아이콘은 Favicons로 구분한다.

암기 포인트

History는 방문 기록, Top Sites는 자주 방문한 사이트, Login Data는 로그인 정보, Web Data는 자동 완성, Favicons는 사이트 아이콘이다.

NoteBase

문 14. 다음에서 설명하는 디지털포렌식 작업으로 가장 적절한 것은?

· 메타 데이터 없이 컴퓨터 파일 조각들을 재조립한다.
· 저장매체의 비할당 공간에 존재하는 파일을 활용한다.
· 삭제 또는 숨김 파일 분석을 위한 복구과정의 일부이다.

① 파일 카빙(file carving)
② 파일 뷰잉(file viewing)
③ 디스크 브라우징(disk browsing)
④ 디스크 조각 모음(disk defragmentation)

정답 1번

출제 포인트

이 문제는 파일시스템의 메타데이터 없이 비할당 공간 등에서 파일의 내용과 고유한 구조를 찾아 복구하는 파일 카빙의 개념을 묻는다.

핵심 개념

파일 카빙은 파일명, 디렉터리 정보, 할당 정보 같은 파일시스템 메타데이터에 의존하지 않고 파일의 헤더·푸터 등 내용상의 특징을 이용하여 파일 조각을 식별하고 복구하는 기법이다. 삭제된 파일의 데이터가 남아 있을 수 있는 비할당 공간을 분석할 때 활용된다.
파일 뷰잉은 파일의 내용을 열어 확인하는 작업이고, 디스크 브라우징은 파일시스템의 디렉터리와 파일 구조를 탐색하는 작업이다. 디스크 조각 모음은 흩어진 할당 파일 조각을 재배치하여 저장 상태를 정리하는 작업이다.

선지별 해설

① O — 메타데이터 없이 파일의 내용과 구조를 바탕으로 조각을 재조립하고, 비할당 공간에서 삭제·숨김 파일의 흔적을 복구하는 작업은 파일 카빙이다.
② X — 틀린 표현은 '파일 뷰잉'이다. 파일 뷰잉은 이미 식별된 파일의 내용을 열어 확인하는 작업이며, 제시문처럼 비할당 공간의 파일 조각을 복구하는 작업은 파일 카빙이다.
③ X — 틀린 표현은 '디스크 브라우징'이다. 디스크 브라우징은 디스크의 파일시스템 구조와 파일·폴더를 탐색하는 작업이며, 메타데이터 없이 파일 조각을 재구성하는 작업은 파일 카빙이다.
④ X — 틀린 표현은 '디스크 조각 모음'이다. 디스크 조각 모음은 할당된 파일의 흩어진 조각을 재배치하여 연속적으로 정리하는 작업이며, 삭제된 파일을 비할당 공간에서 복구하는 작업은 파일 카빙이다.

NoteBase

오답 포인트

제시문의 ‘파일 조각 재조립’만 보고 디스크 조각 모음을 고르기 쉽다. 그러나 ‘메타데이터 없이’, ‘비할당 공간’, ‘삭제 또는 숨김 파일 복구’가 함께 제시되면 저장 성능을 위한 조각 모음이 아니라 포렌식 복구 기법인 파일 카빙을 뜻한다.

다시 나오면 이렇게 판단

파일시스템 메타데이터가 없거나 손상된 상태에서 파일의 고유한 내용·구조를 이용해 비할당 공간의 데이터를 복구한다면 파일 카빙으로 판단한다. 단순 열람은 파일 뷰잉, 구조 탐색은 디스크 브라우징, 할당 파일의 재배치는 디스크 조각 모음으로 구분한다.

암기 포인트

메타데이터 없이 비할당 공간에서 파일 흔적을 복구하면 파일 카빙이다.

NoteBase

문 15. 다음에서 설명하는 용어로 가장 적절한 것은?

파일의 헤더(header) 또는 푸터(footer)에 있는 파일의 고유 정보이다. 예를 들어 JPG 형식의 이미지 파일은 헤더에 'FF D8'이라는 문자열이 존재한다. 따라서, 파일의 확장자를 임의로 변경하더라도 이 같은 정보를 활용한다면 해당 파일의 변경 전 형식을 확인할 수 있다.

① 클러스터(cluster)
② 아카이브(archive)
③ 시그니처(signature)
④ 스왑공간(swap space)

정답 3번

출제 포인트

파일의 헤더나 푸터에 기록된 고유한 바이트 패턴으로 원래 파일 형식을 식별하는 개념을 묻는 문제이다.

핵심 개념

파일 시그니처는 특정 파일 형식을 식별할 수 있도록 파일의 헤더나 푸터에 나타나는 고유한 바이트 패턴이다. 파일 확장자가 바뀌어도 내부의 시그니처를 확인하면 실제 파일 형식을 판별할 수 있다. 예를 들어 JPEG 파일의 시작 부분에는 일반적으로 16진수 바이트 FF D8이 나타난다.
클러스터는 저장장치에서 파일에 공간을 할당하는 단위이고, 아카이브는 여러 파일을 보관하거나 하나로 묶은 자료이며, 스왑 공간은 주기억장치가 부족할 때 보조기억장치의 일부를 임시 메모리처럼 사용하는 영역이다.

선지별 해설

① X — 클러스터는 파일 시스템이 파일 저장 공간을 할당하는 단위이다. 틀린 표현은 '클러스터'이며, 제시문의 용어는 '파일 시그니처'이다.
② X — 아카이브는 여러 파일을 보관하거나 하나의 묶음으로 만든 자료를 뜻한다. 틀린 표현은 '아카이브'이며, 파일 내부의 고유 바이트 패턴은 '파일 시그니처'이다.
③ O — 시그니처는 파일의 헤더 또는 푸터에 나타나는 고유한 바이트 패턴이다. 확장자가 임의로 변경되어도 이를 이용해 실제 파일 형식을 확인할 수 있으므로 제시문과 일치한다.
④ X — 스왑 공간은 주기억장치가 부족할 때 보조기억장치의 일부를 메모리처럼 사용하는 영역이다. 틀린 표현은 '스왑 공간'이며, 제시문의 용어는 '파일 시그니처'이다.

오답 포인트

'파일의 고유 정보'라는 표현만 보고 저장 단위인 클러스터나 보관 자료인 아카이브를 고르기 쉽다. 그러나 확장자를 바꿔도 헤더·푸터의 바이트 패턴으로 파일 형식을 식별한다는 단서가 시그니처를 직접 가리킨다.

NoteBase

다시 나오면 이렇게 판단

헤더·푸터, 고유 바이트 패턴, 확장자 변경 후 원래 형식 식별이라는 단서가 함께 나오면 파일 시그니처로 판단한다.

암기 포인트

확장자는 이름표이고, 시그니처는 파일 내부의 형식 표지이다.

NoteBase

문 16. Windows 10의 레지스트리(registry)에 저장된 USB 연결 흔적 정보에 관한 설명으로 가장 적절하지 않은 것은?

① MountedDevices 키(key)의 일부에 드라이브 문자(drive letter)가 저장된다.

② USB 사용자별 고유한 값이 고유 인스턴스(unique instance) ID에 저장된다.

③ 제조사, 제품명 그리고 버전정보는 장치 클래스(device class) ID에 저장된다.

④ 드라이브로 인식된 USB 장치에 대한 정보는 USBStor의 하위 키로 저장된다.

정답 2번

출제 포인트

Windows 10 레지스트리에 남는 USB 저장장치 흔적에서 MountedDevices, USBSTOR의 장치 클래스 ID, 고유 인스턴스 ID가 각각 무엇을 나타내는지 구분하는 문제이다.

핵심 개념

MountedDevices는 볼륨 식별 정보와 할당된 드라이브 문자의 대응 관계를 남긴다. USBSTOR 아래의 장치 클래스 ID에는 제조사, 제품명, 버전 정보가 포함되고, 그 아래의 고유 인스턴스 ID는 개별 USB 장치 인스턴스를 식별하는 값으로 보통 장치의 일련번호를 바탕으로 형성된다.

선지별 해설

① O — MountedDevices 키에는 드라이브 문자와 볼륨 식별 정보의 대응 흔적이 저장되므로 연결된 볼륨에 할당된 드라이브 문자를 확인할 수 있다.
② X — 틀린 표현은 ‘USB 사용자별 고유한 값’이다. 고유 인스턴스 ID는 사용자별 식별값이 아니라 개별 USB 장치 인스턴스를 구분하는 값이며, 올바르게는 ‘USB 장치별 고유한 식별값이 고유 인스턴스 ID에 저장된다’라고 해야 한다.
③ O — USBSTOR의 장치 클래스 ID에는 제조사, 제품명, 버전 정보를 나타내는 항목이 결합되어 저장된다.
④ O — Windows가 저장장치로 인식한 USB 장치의 식별 정보는 USBSTOR 키 아래의 하위 키들에 저장된다.

오답 포인트

②의 ‘고유’라는 말만 보고 맞다고 판단하기 쉽다. 고유 인스턴스 ID의 구분 대상은 사용자가 아니라 USB 장치 인스턴스라는 점이 함정이다.

다시 나오면 이렇게 판단

드라이브 문자 대응은 MountedDevices, 장치의 제조사·제품명·버전은 USBSTOR의 장치 클래스 ID, 개별 장치 식별값은 고유 인스턴스 ID로 대응시킨다. 사용자별 정보라고 표현하면 장치별 식별 정보와 혼동한 것인지 확인한다.

NoteBase

암기 포인트

MountedDevices는 드라이브 문자, 장치 클래스 ID는 제품 정보, 고유 인스턴스 ID는 장치별 식별값이다.

NoteBase

문 17. 다음은 SSD 저장장치에 관한 설명이다. 빈칸 ㉠과 ㉡에 들어갈 용어로 옳게 짝지어진 것은?

SSD는 플래시 메모리의 장점을 활용하여 개발된 대용량 플래시 메모리 저장장치이다. 랩탑(laptop) 컴퓨터나 태블릿(tablet) PC 등 부피가 작은 디지털 기기에 많이 활용되고 있는데 SSD는 삭제된 데이터의 공간을 미리 비움으로써, 쓰기 속도 저하를 완화시켜 주는 (㉠) 또는 (㉡) 기능이 사용되고 있어 기존 하드디스크와 달리 운영체제의 기능 또는 이미징 작업에 의해 비할당 영역의 데이터가 변형될 수 있다.

① ㉠: Trim, ㉡: buffer memory

② ㉠: Trim, ㉡: garbage collection

③ ㉠: Virtual memory, ㉡: garbage collection

④ ㉠: Virtual memory, ㉡: buffer memory

정답 2번

출제 포인트

SSD에서 삭제된 데이터가 차지하던 영역을 쓰기 가능한 상태로 준비하는 TRIM과 가비지 컬렉션의 기능을 구별하는 문제이다.

핵심 개념

TRIM: 운영체제가 파일 삭제 등으로 더 이상 사용하지 않는 논리 블록을 SSD에 알려 주는 기능이다. SSD는 이 정보를 바탕으로 해당 데이터를 이후 정리 대상으로 처리할 수 있다.
가비지 컬렉션(garbage collection): SSD 컨트롤러가 유효한 페이지를 모아 옮기고 불필요한 페이지가 포함된 블록을 지워, 새 데이터를 쓸 수 있는 빈 블록을 확보하는 내부 정리 작업이다.
버퍼 메모리는 입출력 속도 차이를 완화하기 위해 데이터를 일시 저장하는 공간이고, 가상 메모리는 저장장치 일부를 활용하여 주기억장치의 주소 공간을 보조하는 기법이다. 둘 다 삭제된 SSD 영역을 정리하는 기능을 뜻하지 않는다.

NoteBase

선지별 해설

① X — ㉠의 TRIM은 맞지만 ㉡의 buffer memory가 틀리다. 버퍼 메모리는 데이터를 임시 보관하는 공간이므로 삭제된 플래시 페이지를 정리하지 않는다. 올바르게는 '㉠: TRIM, ㉡: garbage collection'이다.
② O — TRIM은 운영체제가 미사용 논리 블록을 SSD에 알리고, 가비지 컬렉션은 SSD 내부에서 유효 데이터를 재배치한 뒤 불필요한 블록을 지워 쓰기 가능한 공간을 확보한다. 두 기능 모두 지문이 설명한 SSD의 삭제 영역 사전 정리와 관련된다.
③ X — ㉡의 garbage collection은 맞지만 ㉠의 Virtual memory가 틀리다. 가상 메모리는 주기억장치의 주소 공간을 보조하는 기법으로 SSD의 삭제 영역을 알리는 기능이 아니다. 올바르게는 '㉠: TRIM, ㉡: garbage collection'이다.
④ X — Virtual memory와 buffer memory는 모두 SSD의 삭제 영역을 정리하는 기능이 아니다. 올바르게는 '㉠: TRIM, ㉡: garbage collection'이다.

오답 포인트

SSD가 메모리 기반 저장장치라는 점 때문에 buffer memory나 Virtual memory를 고르기 쉽다. 그러나 문제의 핵심 표현은 '삭제된 데이터의 공간을 미리 비움'이며, 이에 대응하는 용어는 미사용 영역을 알리는 TRIM과 내부적으로 블록을 정리하는 가비지 컬렉션이다.

다시 나오면 이렇게 판단

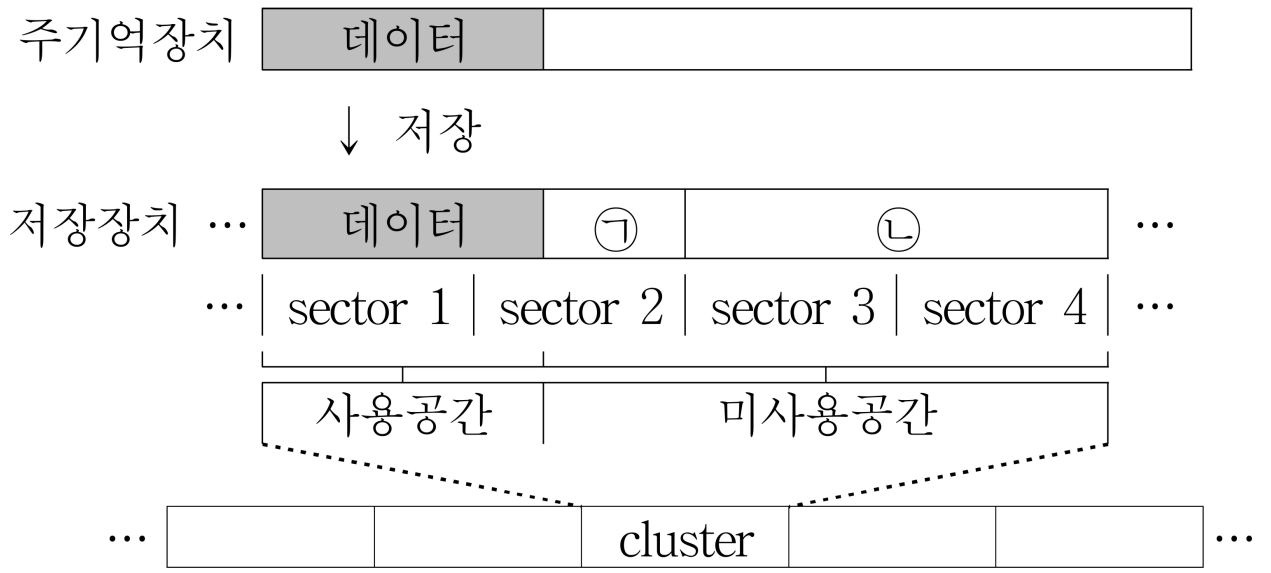
운영체제가 SSD에 삭제·미사용 영역을 알려 주는 기능이면 TRIM, SSD 컨트롤러가 유효 데이터를 모으고 블록을 지워 빈 공간을 만드는 작업이면 가비지 컬렉션으로 판단한다. 임시 저장은 버퍼 메모리, 주기억장치 보조는 가상 메모리로 구별한다.

암기 포인트

TRIM은 '미사용 영역 알림', 가비지 컬렉션은 'SSD 내부 블록 정리'이다.

NoteBase

문 18. 다음은 주기억장치와 저장장치에 관한 구조이다. 빈칸 ㉠과 ㉡에 발생한 슬랙(slack)들을 합친 슬랙으로 가장 적절한 것은?



① 볼륨 슬랙

② 파일 슬랙

③ 드라이브 슬랙

④ 파일 시스템 슬랙

정답 2번

출제 포인트

파일의 논리적 끝부터 그 파일에 할당된 마지막 클러스터의 끝까지 남는 공간이 파일 슬랙이며, 도식의 ㉠과 ㉡이 이 범위를 이룬다.

NoteBase

선지별 해설

① X
볼륨 슬랙은 파일 하나에 할당된 클러스터 내부의 빈 공간이 아니라 파일 시스템의 끝과 이를 담은 볼륨의 끝 사이에 남는 공간이다. 따라서 ㉠과 ㉡의 합은 볼륨 슬랙이 아니라 파일 슬랙이다.

② O
㉠은 파일 데이터의 논리적 끝부터 해당 섹터의 끝까지 남는 RAM 슬랙이고, ㉡은 그 뒤부터 할당된 클러스터의 끝까지 남는 드라이브 슬랙이다. 두 영역을 합치면 파일의 논리적 끝부터 마지막 할당 클러스터의 끝까지이므로 파일 슬랙이다.

③ X
드라이브 슬랙은 ㉠과 ㉡ 전체가 아니라 파일의 마지막 데이터가 들어 있는 섹터 다음부터 할당 클러스터의 끝까지인 ㉡에 해당한다. 따라서 ㉠과 ㉡의 합은 드라이브 슬랙이 아니라 파일 슬랙이다.

④ X
파일 시스템 슬랙은 파일 시스템의 할당 단위로 사용할 수 없어 파일 시스템 끝부분에 남는 공간을 가리키며, 개별 파일의 마지막 할당 클러스터 내부에 생긴 ㉠과 ㉡의 합을 뜻하지 않는다. 올바른 명칭은 파일 슬랙이다.

오답 포인트

㉡만 보고 드라이브 슬랙을 고르거나, 저장장치에 남는 공간이라는 이유만으로 볼륨 슬랙·파일 시스템 슬랙과 혼동하기 쉽다. 이 문항은 ㉠과 ㉡을 합친 전체 범위를 묻고 있으므로 파일 슬랙으로 판단한다.

다시 나오면 이렇게 판단

파일의 논리적 끝에서 섹터 끝까지는 RAM 슬랙, 그 다음 섹터부터 마지막 할당 클러스터 끝까지는 드라이브 슬랙이며, 둘의 합은 파일 슬랙이다.

암기 포인트

파일 슬랙 = RAM 슬랙 + 드라이브 슬랙이다.

NoteBase

문 19. 다음 설명의 빈칸에 들어갈 기능으로 가장 적절한 것은?

Windows 10이 설치된 시스템을 디지털포렌식 분석하는 과정에서 디스크의 볼륨이 비워져 비할당 영역으로 표시될 수가 있다. 이 같은 경우, 사용하지 않거나 포맷이 되지 않은 빈 디스크로 판단해서는 안 되며, ( )이/가 설정되어 있는지를 추가로 조사해야 한다.

① 숨김 파일

② 코드 난독화

③ 해시(hash) 암호화

④ 비트락커(bitlocker) 암호화

정답 4번

출제 포인트

파일 시스템을 정상적으로 인식하지 못해 볼륨이 비어 있거나 비할당 영역처럼 보일 때, 전체 볼륨 암호화 기능인 BitLocker의 적용 여부를 확인할 수 있는지를 묻는 문제이다.

핵심 개념

BitLocker는 Windows에서 드라이브 전체를 암호화하는 기능이다. 분석 도구가 암호화된 볼륨을 해제하여 파일 시스템 구조를 읽지 못하면 해당 영역을 정상 볼륨으로 식별하지 못할 수 있으므로, 빈 디스크로 단정하기 전에 BitLocker 암호화 여부와 복구 키 확보 가능성을 확인해야 한다.
숨김 파일은 파일의 표시 속성, 코드 난독화는 코드의 분석 방해, 해시는 데이터의 동일성·무결성 확인과 관련되고, BitLocker만 디스크 볼륨 자체의 암호화와 직접 관련된다.

NoteBase

선지별 해설

① X — 숨김 파일은 특정 파일이 일반적인 목록에 나타나지 않도록 속성을 설정한 것이다. 디스크 볼륨 전체가 비할당 영역처럼 식별되는 원인이 아니다. 틀린 표현인 '숨김 파일'은 '비트락커(BitLocker) 암호화'로 고쳐야 한다.
② X — 코드 난독화는 프로그램 코드의 구조와 의미를 알아보기 어렵게 만드는 기법이다. 볼륨의 파일 시스템을 암호화하여 인식을 방해하는 기능이 아니다. 틀린 표현인 '코드 난독화'는 '비트락커(BitLocker) 암호화'로 고쳐야 한다.
③ X — 해시는 입력값으로부터 고정 길이의 해시값을 생성하는 단방향 처리로, 주로 데이터 동일성이나 무결성을 확인하는 데 사용한다. 볼륨을 복호화 가능한 형태로 암호화하는 기능이 아니므로 '해시 암호화'라는 표현은 적절하지 않다. 이 문맥에서는 '비트락커(BitLocker)를 이용한 볼륨 암호화'가 올바르다.
④ O — BitLocker는 드라이브 전체를 암호화한다. 암호화가 해제되지 않아 분석 도구가 파일 시스템을 인식하지 못하면 볼륨이 비어 있거나 비할당 영역처럼 보일 수 있으므로 BitLocker 설정 여부를 추가로 조사해야 한다.

오답 포인트

③의 '해시 암호화'와 ④의 'BitLocker 암호화'를 모두 보안 기술로만 묶어 생각하기 쉽다. 그러나 해시는 데이터의 동일성·무결성 확인에 쓰이는 단방향 처리이고, BitLocker는 드라이브의 내용을 복호화 없이는 읽지 못하게 하는 볼륨 암호화 기능이라는 차이가 있다.

다시 나오면 이렇게 판단

디스크나 볼륨 전체가 비어 있거나 파일 시스템을 인식하지 못한 것처럼 보인다는 단서가 나오면 먼저 전체 볼륨 암호화를 의심한다. Windows 환경에서 드라이브 전체 암호화와 연결되는 기능은 BitLocker이다.

암기 포인트

숨김은 표시 속성, 난독화는 코드 분석 방해, 해시는 무결성 확인, BitLocker는 볼륨 전체 암호화이다.

NoteBase

문 20. 하드디스크에 저장된 데이터를 복구할 수 없도록 완전히 삭제하는 안티포렌식(anti-forensic) 기법으로 가장 적절하지 않은 것은?

① 와이핑(wiping)
② 디가우징(degaussing)
③ 빠른 포맷(quick format)
④ 물리적 파쇄(micro-shredding)

정답 3번

출제 포인트

이 문제는 저장매체의 데이터를 실제로 제거하거나 복구가 어렵도록 만드는 기법과, 파일시스템 정보만 간단히 초기화하는 빠른 포맷을 구별하는 문제이다.

핵심 개념

와이핑은 저장 영역에 데이터를 덮어써서 기존 내용을 복구하기 어렵게 만드는 논리적 삭제 기법이다.
디가우징은 강한 자기장으로 자기식 저장매체의 자화 상태를 교란하는 기법이고, 물리적 파쇄는 매체 자체를 잘게 파괴하는 기법이다. 반면 빠른 포맷은 주로 파일시스템의 관리 정보만 새로 설정하므로 데이터 영역의 기존 내용이 남을 수 있다.

선지별 해설

① X — 와이핑은 데이터가 있던 저장 영역을 덮어쓰므로 복구 방지를 위한 완전 삭제 기법으로 적절하다. '완전 삭제 기법으로 적절하지 않다'가 아니라, 올바르게는 '논리적 완전 삭제 기법으로 적절하다'이다.
② X — 디가우징은 하드디스크의 자기 기록을 강한 자기장으로 교란하여 데이터를 읽기 어렵게 하므로 복구 방지 기법으로 적절하다. '완전 삭제 기법으로 적절하지 않다'가 아니라, 올바르게는 '자기식 저장매체의 데이터 제거 기법으로 적절하다'이다.
③ O — 빠른 포맷은 파일시스템의 관리 구조를 초기화할 뿐 데이터가 저장된 모든 영역을 덮어쓰지 않으므로, 포맷 직후에는 기존 데이터가 복구될 가능성이 있다. 따라서 복구할 수 없도록 완전히 삭제하는 기법으로 가장 적절하지 않다.
④ X — 물리적 파쇄는 저장매체 자체를 잘게 파괴하여 데이터 판독과 복구를 어렵게 하므로 완전 삭제 기법으로 적절하다. '완전 삭제 기법으로 적절하지 않다'가 아니라, 올바르게는 '물리적 매체 파괴를 통한 완전 삭제 기법으로 적절하다'이다.

오답 포인트

③의 '포맷'이라는 말 때문에 데이터까지 모두 지워진다고 생각하기 쉽다. 그러나 빠른 포맷은 저장 영역 전체를 덮어쓰는 작업이 아니므로, 와이핑과 같은 완전 삭제 기법으로 볼 수 없다.

NoteBase

다시 나오면 이렇게 판단

기법이 데이터 영역을 덮어쓰거나, 자기 기록을 제거하거나, 매체 자체를 파괴하는지를 확인한다. 파일 목록과 파일시스템 관리 정보만 초기화한다면 완전 삭제가 아니다.

암기 포인트

와이핑은 덮어쓰기, 디가우징은 자기장 제거, 파쇄는 물리적 파괴, 빠른 포맷은 관리 정보 초기화이다.

NoteBase