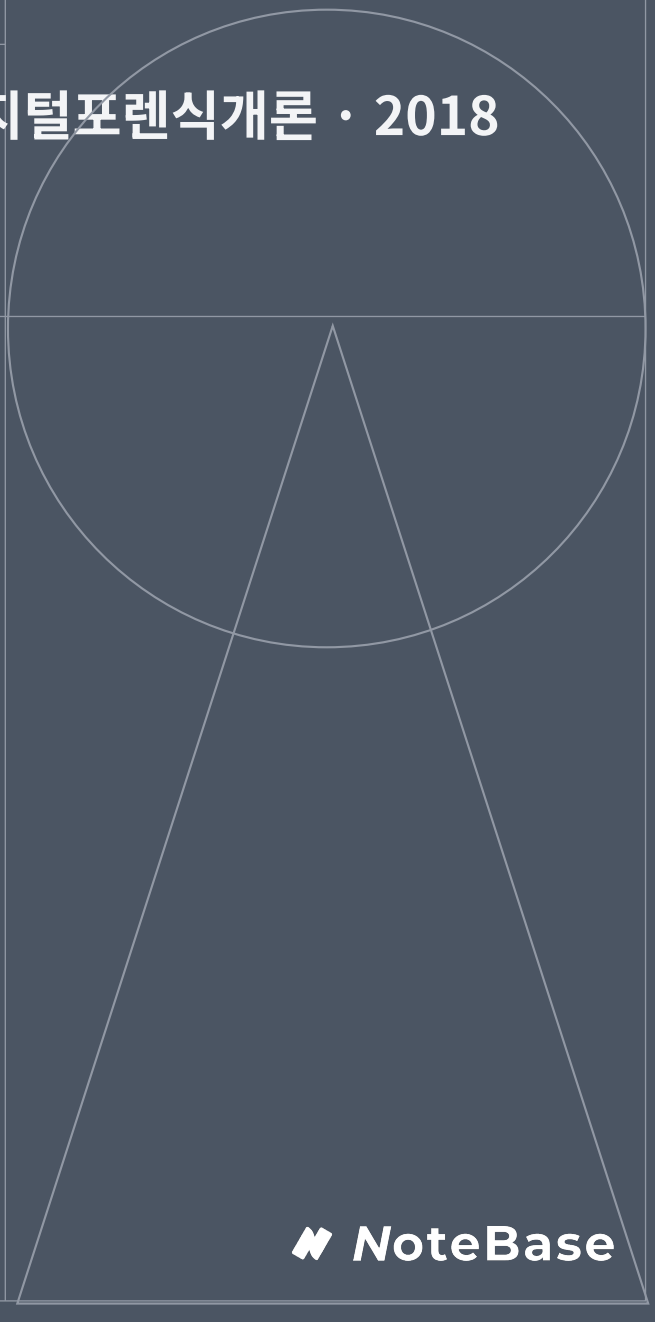
기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2018



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 디지털포렌식개론 · 2018

공무원/경찰/경력채용 · 디지털포렌식개론 · 2018

문 1. 디지털 포렌식 수행절차에 대한 순서가 가장 적절한 것은?

① 디지털포렌식보고서→증거수집→증거포장 및 이송→증거분석

② 증거수집→디지털포렌식보고서→증거포장 및 이송→증거분석

③ 증거수집→증거포장 및 이송→증거분석→디지털포렌식보고서

④ 증거수집→디지털포렌식보고서→증거분석→증거포장 및 이송

정답 3번

간단한 해설

증거를 먼저 확보하고 안전하게 포장·이송한 뒤 분석한다. 최종 디지털포렌식보고서는 **분석 결과를 근거로** 작성하므로 분석 뒤에 놓인다.

올바른 순서

증거수집 → 증거포장 및 이송 → 증거분석 → 디지털포렌식보고서

증거수집: 분석할 디지털 증거를 식별하고 필요한 데이터를 확보한다. 수집 당시의 상태와 취급 과정을 기록하고, 원본의 불필요한 변경을 방지하여 이후 분석의 기초를 마련한다.

증거포장 및 이송: 수집한 증거를 식별·봉인하고 손상이나 변조가 발생하지 않도록 보호하여 분석 장소로 옮긴다. 누가 언제 증거를 인계하고 인수했는지 기록하여 **증거 취급의 연속성**을 유지한다. 확보한 증거가 먼저 있어야 이를 포장·이송할 수 있다.

증거분석: 보호·이송된 증거에서 사건과 관련된 정보를 추출하고 해석한다. 가능한 경우 검증된 사본으로 분석하고 원본을 보존하며, 사용한 방법과 발견한 사실을 기록한다. 보고서의 결론은 이러한 분석 결과를 근거로 해야 한다.

디지털포렌식보고서: 수집·보존·분석 과정과 결과, 사용한 방법 및 해석의 한계를 정리한다. 최종 결과 보고서는 **분석이 이루어진 뒤** 작성한다. 다만 과정 기록 자체는 마지막에만 시작하는 것이 아니라 수집 단계부터 계속 남긴다.

NoteBase

문 2. 디지털 포렌식에서 저장 매체에 대한 복제를 수행할 때 가장 적절하지 않은 것은?

① 원본 디스크에 포렌식 도구인 쓰기방지 장치를 연결하고, 복제본을 생성한다.

② 원본 디스크의 저장 용량을 확인한 후, 원본 용량보다 더 많은 용량의 디스크를 사용하여 복제본을 생성한다.

③ 현장에서 원본 디스크에 대한 복제본을 생성 시, 원본과 복제본의 무결성을 입증하기 위하여, 해시 값을 생성하고, 원본과 복제본의 해시 값이 일치하는 것을 확인한다.

④ 원본 디스크를 인터넷 네트워크에 연결하여 복제본 디스크로 쉽게 복사하도록 하고, 네트워크 로그(log) 기록을 남기고 나서, 네트워크 접속을 차단한다.

정답 4번

간단한 해설

저장매체 복제에서는 **원본의 변경을 방지하고 복제 무결성을 검증**해야 한다. 단순히 복사를 쉽게 하려고 원본을 외부 인터넷에 연결하는 ④는 불필요한 변경 위험을 만든다.

선지별 해설

① O: 원본 매체와 복제 장비 사이에 **쓰기방지 장치**를 사용하면 복제 과정에서 원본으로 쓰기 명령이 전달되어 내용이 변경되는 위험을 줄일 수 있다. 장치의 정상 동작을 확인하고 원본은 보존하며, 분석은 복제본을 대상으로 수행하는 것이 원칙이다.

② O: 원본의 용량과 복제 방식에 필요한 공간을 확인하고 **충분한 용량의 대상 매체**를 준비해야 한다. 원본보다 큰 용량을 확보하는 것은 적절한 준비이다. 다만 디스크 간 복제에서는 충분한 실제 섹터 수가 중요하며, 항상 반드시 더 큰 명목 용량이어야만 가능한 것은 아니다. 이미지 파일 방식에서는 형식과 부가 정보 등에 필요한 저장 공간도 고려한다.

③ O: 원본과 복제한 **동일한 데이터 범위**에 같은 해시 알고리즘을 적용하여 값이 일치하는지 확인하고 기록하면 복제의 정확성과 무결성 검증에 도움이 된다. 더 큰 대상 디스크의 남는 영역이나 이미지 컨테이너의 헤더까지 포함한 전체 파일을 원본 데이터와 그대로 비교해서는 안 된다. 해시 일치만으로 모든 수집·보관 절차의 적정성까지 입증되는 것은 아니다.

④ X: 복사의 편의를 위해 원본 매체가 연결된 시스템을 **외부 인터넷에 불필요하게 노출**하면 원격 변경, 악성코드 동작, 자동 갱신 등으로 증거가 훼손될 수 있다. 접속 로그를 남겼다는 사정만으로 이러한 위험이 해소되지는 않는다. 통제된 환경에서 원본 쓰기를 차단하고 검증 가능한 방식으로 복제해야 한다. 이는 적절히 통제된 원격 수집 방식 자체를 모두 금지한다는 뜻은 아니다.

NoteBase

문 3. 디지털 포렌식에서 하드디스크 '쓰기방지 장치'로 가장 적절한 것은?

① HxD

② Tableau

③ StegoHunt

④ Intella

정답 2번

간단한 해설

쓰기방지 장치는 증거 하드디스크의 **원본 변경을 차단**하면서 데이터를 읽을 수 있게 한다. Tableau의 포렌식 브리지는 이 기능을 수행하는 하드웨어 장치이다.

핵심 풀이

쓰기방지 장치는 증거 하드디스크와 조사용 컴퓨터 사이에서 **쓰기 명령을 차단하고 읽기는 허용**한다. 증거를 복제·분석하는 과정에서 원본 데이터가 변경되는 것을 막아 무결성 보존을 돕는다.

Tableau의 포렌식 브리지는 이러한 하드웨어 쓰기방지 장치에 해당하므로 ②가 적절하다. 제품 이름만으로 모든 장비의 기능을 같다고 보는 것이 아니라, 증거 저장매체에 대한 쓰기를 차단하는 기능이 판단 기준이다.

HxD는 파일·디스크 등의 내용을 확인하고 편집하는 헥스 편집기이고,

StegoHunt는 스테가노그래피 탐지·분석 도구이다.

Intella는 수집한 전자정보를 처리·검색·검토하는 분석 도구로, 이 문항에서 묻는 하드웨어 쓰기방지 장치와 구별한다.

NoteBase

문 4. 컴퓨터 하드디스크의 이미징 기능을 수행하는 포렌식 도구로 가장 적절하지 않은 것은?

① dd
② WireShark
③ Adepto
④ LinEn

정답 2번

간단한 해설

Wireshark는 **네트워크 패킷 수집·분석** 도구이다. 저장매체를 이미지 파일로 복제하는 하드디스크 이미징 도구와는 목적과 처리 대상이 다르다.

개념 구분

디스크 이미징은 저장매체의 데이터를 이미지 파일로 복제하는 작업이다. **Wireshark는 네트워크 패킷을 수집·분석**하는 도구로, 하드디스크 자체의 이미지를 만드는 도구와 구별된다.

dd는 입력 데이터를 블록 단위로 읽어 출력에 복사하는 도구이다. 디스크 장치를 입력으로 지정해 원시 이미지 파일을 만들 수 있다.

Adepto는 dd 계열 도구를 그래픽 인터페이스로 이용하여 **포렌식 이미지 획득**을 수행하도록 돕는 도구이다.

LinEn은 리눅스 환경에서 사용하는 EnCase의 증거 획득 도구로, 디스크 이미지를 생성하는 데 쓰인다.

따라서 하드디스크 이미징 기능을 수행하는 도구로 적절하지 않은 것은 네트워크 분석 도구인 ② WireShark이다.

NoteBase

문 5. 디지털 포렌식 사본 이미지 생성에 사용되는 것으로 가장 적절한 것은?

① Live Search

② KFF(Known File Filter)

③ OS Artifacts

④ FTK Imager

정답 4번

간단한 해설

FTK Imager는 디지털 증거의 사본 이미지를 생성하는 도구이다. 검색 기능, 알려진 파일 필터, 운영체제 흔적과 구별한다.

핵심 풀이

포렌식 사본 이미지 생성은 저장매체의 데이터를 수집하여 **분석용 이미지 파일로 확보**하는 작업이다. FTK Imager는 이 증거 수집·이미징 기능을 제공하는 도구이다. 원본 보존을 위해 적절한 쓰기 방지와 수집 절차를 적용하고, 해시값 등으로 복제 결과의 무결성을 검증한다.

① Live Search는 증거 데이터에서 문자열·패턴 등을 직접 찾는 **검색 기능**이다. 이미지 생성 도구의 명칭이 아니다.

② KFF는 알려진 파일의 해시 집합과 비교하여 파일을 식별·분류하는 **필터링 기능**이다. 분석 대상을 추리는 데 쓰이며, 사본 이미지 생성과는 목적이 다르다.

③ OS Artifacts는 운영체제 사용 과정에서 남는 **분석 대상 흔적**을 뜻한다. 로그·설정 정보 등에서 활동 단서를 찾는 개념이지 이미지 생성 도구가 아니다.

④ FTK Imager는 디스크 등 증거 원천의 데이터를 사본 이미지로 수집하고 확인하는 도구이므로 요구된 작업에 해당한다.

따라서 가장 적절한 것은 ④ FTK Imager이다.

NoteBase

문 6. 윈도우즈 PC의 압수·수색과정에서 발견된 'Thumbs.db'에 대한 설명으로 가장 적절하지 않은 것은?

① 사진이나 이미지에 관한 작은 그림이 포함된 파일 형태로 저장된다.

② Thumbs.db는 사용자가 직접 생성하며, 기본적으로 숨김 속성은 해제되어 있다.

③ 특정시간에 해당 파일을 열었다는 사실의 입증이 가능하다.

④ 사진이나 이미지를 삭제해도 Thumbs.db 파일이 남아 있을 수 있다.

정답 2번

간단한 해설

Thumbs.db는 이미지의 미리보기를 위해 **Windows가 자동 생성하는 숨김 캐시 파일**이다. 사용자가 직접 생성하며 기본 숨김 속성이 해제되어 있다는 설명은 잘못되었다.

선지별 해설

① O: Thumbs.db는 사진이나 이미지의 축소 미리보기인 **썸네일을 보관하는 캐시 파일**이다. 원본 이미지를 매번 처리하지 않고 미리보기를 표시하는 데 이용한다. Windows 버전과 저장 위치에 따라 캐시 방식은 달라질 수 있다.

② X: Thumbs.db는 일반적으로 사용자가 직접 만드는 파일이 아니라 **Windows가 자동으로 생성하는 숨김 파일**이다. 따라서 직접 생성한다는 설명과 기본적으로 숨김 속성이 해제되어 있다는 설명이 모두 잘못되었다.

③ O: 파일의 과거 존재·접근과 관련된 정황을 파악하고, 다른 기록과 함께 열람 사실을 입증하는 데 활용할 수 있다는 제한된 의미이다. 다만 썸네일은 자동 생성될 수 있으므로 **Thumbs.db만으로 특정 사용자의 실제 열람이나 정확한 열람 시각을 확정할 수는 없다**. 캐시에 있는 시각 정보도 해당 형식에서 무엇을 뜻하는지 확인하고 다른 흔적과 대조해야 한다.

④ O: 원본 사진이나 이미지를 삭제해도 캐시의 썸네일이 즉시 함께 삭제되는 것은 아니다. 따라서 남은 Thumbs.db에서 삭제 전 이미지의 흔적을 확인할 수 있다. 다만 캐시가 정리되거나 덮어써지면 남지 않을 수 있으며, 썸네일이 남았다는 사실이 원본 전체의 복원을 보장하지는 않는다.

NoteBase

문 7. 압수된 10개의 컴퓨터 하드 디스크를 10명의 포렌식 수사관이 증거분석하고 있다. 법정에서 증거 채택을 위하여 디지털 포렌식에서 지켜야 할 가장 적절한 사항은?

① Normal NAT

② 연계 보관성(Chain of custody)

③ 데이터 부하분산(Data load balancing)

④ 패킷 필터링(Packet filtering)

정답 2번

간단한 해설

여러 수사관이 증거를 분석할 때에는 **연계 보관성**을 유지하여 증거의 수집·보관·인계·분석 이력을 추적할 수 있어야 한다. 누가 언제 어떤 증거를 취급했는지를 연속적으로 기록하는 것이 핵심이다.

핵심 풀이

10개의 하드 디스크를 10명의 수사관이 나누어 분석하더라도, 각 증거가 수집부터 보관·인계·분석·제출까지 **누구의 관리하에 어떤 절차를 거쳤는지** 추적할 수 있어야 한다. 증거 식별번호, 취급자, 인계·인수 시각, 장소, 목적과 처리 내역 등을 연속적으로 기록하는 것이 연계 보관성이다. 담당자가 여러 명이라는 사실 자체가 문제인 것은 아니다.

① Normal NAT는 네트워크 주소를 변환하는 기능과 관련된다. 압수물의 취급·이동 이력을 입증하는 관리 원칙이 아니다.

② 연계 보관성(Chain of custody)은 **증거의 취급·보관·인계 이력을 연속적으로 관리**하는 것이다. 여러 수사관이 분석하는 상황에서 증거가 뒤바뀌거나 부적절하게 취급되지 않았음을 설명하는 근거가 된다. 해시 검증 등 무결성 확인과 함께 적용하되, 이것만으로 모든 법적 증거 채택 요건이 자동 충족되는 것은 아니다.

③ 데이터 부하분산은 작업이나 트래픽을 여러 자원에 나누는 기술이다. 분석 업무를 나누는 효율성과 증거 관리 이력의 신뢰성은 다른 문제이다.

④ 패킷 필터링은 네트워크 패킷을 조건에 따라 허용·차단하는 기능이다. 하드 디스크 증거의 인계·보관 이력을 유지하는 원칙과는 관계가 없다.

따라서 제시된 상황에서 가장 적절한 사항은 ② 연계 보관성이다.

NoteBase

문 8. 리눅스 운영체제에서 데이터를 수집하는 방법으로 가장 적절하지 않은 것은?

① 실행 중인 프로세스 정보를 획득하기 위하여 'ps -aux' 명령을 사용하였다.

② 현재 로그온 상태인 사용자를 확인하기 위하여 'who' 명령을 사용하였다.

③ IP 설정 정보를 확인하기 위하여 'ipconfig /all' 명령을 사용하였다.

④ ARP 정보를 확인하기 위하여 'arp -a' 명령을 사용하였다.

정답 3번

간단한 해설

ipconfig /all은 Windows 명령이므로 리눅스에서의 IP 설정 확인 방법으로 제시한 ③이 적절하지 않다. 리눅스에서는 ip addr show 등을 사용한다.

선지별 해설

① O: **ps**는 현재 프로세스의 정보를 출력하므로 실행 중인 프로세스 조사에 사용한다. 다만 원문의 ps -aux는 BSD식과 UNIX식 옵션이 섞여 사용자 x의 존재 등에 따라 해석이 달라질 수 있는 비권장 표기이다. 전체 프로세스를 사용자 중심 형식으로 확인하려는 의도에는 **ps aux**처럼 하이픈 없는 BSD식 표기를 사용하는 것이 명확하다.

② O: **who**는 현재 로그인한 사용자와 터미널, 로그인 시각 등의 정보를 확인하는 명령이다. 현재 접속 상태를 파악할 때 사용하며, 과거 전체 로그인 이력을 조회하는 것과는 구별한다.

③ X: **ipconfig /all은 Windows의 네트워크 설정 확인 명령**이다. 일반적인 리눅스 환경에서 IP 주소를 확인하려면 **ip addr show**를 사용하고, 라우팅 정보는 ip route로 확인할 수 있다. 구형 도구가 설치된 환경에서는 ifconfig -a도 사용할 수 있다.

④ O: **arp -a**는 시스템의 ARP 캐시 항목을 표시하여 IPv4 주소와 MAC 주소의 대응을 확인하는 데 사용한다. net-tools의 arp 명령이 설치되어 있어야 하며, 현대 리눅스에서는 ip neigh show로 이웃 캐시를 확인할 수도 있다.

NoteBase

문 9. 디지털 포렌식 증거 수집에 대한 설명으로 가장 적절한 것은?

① 정보저장매체 또는 전자정보를 수집할 때부터 법정에 증거로 제출할 때까지, 변경 또는 훼손되지 않도록 무결성을 유지하여야 하고 그 과정을 기록하여 수사기록에 첨부하여야 한다.

② 증거 획득과정에서 증거로 판단되는 디지털 파일은 데이터 이미지 절차나 원본 데이터의 무결성 유지에 앞서, 현장에서 사용자가 직접 클릭하여 확인한다.

③ 디지털 증거의 획득 시에 오류가 생겨도, 제3의 전문가를 통해 정당한 증거로 입증 받을 수 있다.

④ 디지털 증거에 대한 증거분석은 증거 획득과정에서 원본 이미지와 사본 이미지를 모두 실행하여 인터넷 네트워크에 접속하고, 즉시 원본과 사본의 이미지의 실행 결과가 일치하는지를 확인해야 한다.

정답 1번

간단한 해설

디지털 증거는 수집부터 법정 제출까지 **무결성을 유지**하고 취급 과정을 기록해야 한다. 원본을 직접 실행하거나 인터넷에 연결하는 방식은 증거를 변경할 위험이 있다.

선지별 해설

① O: 디지털 증거는 복제·변경이 쉬우므로 수집부터 제출까지 **무결성**을 유지해야 한다. 수집·보관·이관·분석 과정과 담당자를 기록하면 증거가 어떤 경로로 관리되었는지 추적할 수 있으며, 이러한 기록은 수사기록에 첨부하여 증거의 신뢰성을 뒷받침한다.

② X: 원본 파일을 직접 클릭하거나 실행하면 접근 시각, 로그 등 관련 데이터가 바뀔 수 있다. 무결성 보호보다 내용 확인을 앞세우지 말고, 원본을 보호하면서 적절한 방법으로 증거를 획득한 뒤 **검증된 사본을 분석**해야 한다.

③ X: 제3의 전문가가 관여한다고 획득 과정의 오류가 자동으로 해소되는 것은 아니다. 오류의 내용과 영향을 기록하고 원본과의 동일성·무결성 및 수집 과정의 신뢰성을 검토해야 하며, 전문가의 확인만으로 정당한 증거임이 보장된다고 할 수 없다.

④ X: 원본과 사본을 모두 실행해 인터넷에 연결하면 데이터 변경이나 외부 간섭이 발생할 수 있다. 원본은 보존하고 필요한 분석은 통제된 환경의 사본에서 수행하며, 복제의 정확성은 **해시값 대조 등으로 확인**한다. 인터넷 연결 후 실행 결과가 같다는 것만으로 이미지의 동일성이 입증되지는 않는다.

NoteBase

문 10. 텍스트 문서 name.txt를 name.hwp로 확장자만 수정하였다. 파일의 확장자에 상관없이 name.txt 파일의 본래 유형을 찾으려 할 때, 사용하는 방법으로 가장 적절한 것은?

① 인덱스(Index) 검색

② 시그니처(Signature) 분석

③ 슬랙(Slack) 검색

④ 타임 라인(Time line) 분석

정답 2번

간단한 해설

확장자만 바꾸어도 **파일 내부 형식은 그대로** 남는다. 시그니처 등 내용 기반의 특징을 조사해 표시된 확장자와 실제 유형의 불일치를 판단한다.

핵심 풀이

파일의 확장자를 .txt에서 .hwp로 바꾸어도 **파일 내부의 바이트와 형식은 변하지 않는다**. 이름이 아니라 내부의 식별 패턴과 구조를 조사하는 방법이므로, 제시된 방법 중에는 ② 시그니처 분석이 가장 적절하다.

일반적으로 시그니처 분석은 헤더 등 특정 위치의 매직 넘버나 고유 패턴을 알려진 형식과 비교한다. 다만 **일반 텍스트 파일에 공통된 고유 헤더가 반드시 있는 것은 아니다**. 이 사례에서는 문자 인코딩과 내용의 특징도 살펴 텍스트인지 판단하고, 확장자가 나타내는 형식과 일치하는지 검토해야 한다.

인덱스 검색은 미리 만든 색인을 이용해 단어 등을 찾고,

슬랙 검색은 파일의 실제 끝과 할당 공간 끝 사이 등에 남은 데이터를 조사한다.

타임 라인 분석은 시각 정보를 종합해 사건의 흐름을 재구성하는 것이므로, 확장자가 바뀐 파일의 유형 식별과 목적이 다르다.

NoteBase

문 11. 사이버범죄에 이용되고 있는 PC의 임시기억장소에 기억된 휘발성 증거를 압수·수색하는 방법으로 가장 적절한 것은?

① PC 종료와 함께 삭제되는 휘발성 정보를 우선적으로 획득하기 위하여, 인터넷 네트워크 접속 정보, 프로세스 정보 등 임시기억장소에 기록되는 정보 자료를 확보하고 범죄관련 화면과 실행 프로그램에 대한 현장 사진의 확보 및 사용자의 진술을 확보하고, 저장매체를 압수·수색한다.

② PC를 인터넷 네트워크를 통한 외부 접속을 실시하여, 저장매체에 대한 출력, 복제를 수행한다.

③ PC 전원을 우선 끄고 저장매체 자체를 압수하는 방식을 고려하여 가까운 장소에서 편리한 도구로 증거를 분석한다.

④ PC의 디스크에 대한 복제를 수행하여 휘발성 정보를 수집한다.

정답 1번

간단한 해설

휘발성 정보는 전원 종료로 사라질 수 있으므로 **종료 전에 현재 상태를 기록하고 수집**하는 것이 핵심이다. 디스크 복제만으로 현재 메모리나 네트워크 접속 상태가 모두 확보되는 것은 아니다.

선지별 해설

① O. 휘발성 증거를 확보하려는 상황에서는 **전원 종료 전에** 현재 네트워크 접속·프로세스·메모리 등 쉽게 사라지는 정보를 우선 수집해야 한다. 화면과 실행 프로그램의 현장 사진, 사용자 진술은 당시 상태를 보완하는 자료가 된다. 이후 저장매체의 증거도 확보한다. 수집 자체가 시스템 상태를 바꿀 수 있으므로 검증된 도구를 사용하고 조치·시각·변경 사항을 기록해야 하며, 법적 권한과 범위를 준수해야 한다.

② X. 휘발성 정보 보존을 위해 불필요한 **외부 네트워크 접속을 새로 수행**하는 것은 적절하지 않다. 접속·프로세스·로그 상태가 바뀌고 원격 조작 위험도 생길 수 있다. 현 상태를 기록하고 안전한 수집 경로를 판단해야 하며, 저장매체의 출력·복제만으로 휘발성 정보가 확보되는 것도 아니다.

③ X. **전원을 먼저 끄면 메모리의 휘발성 정보가 소실**될 수 있다. 이 문제처럼 휘발성 증거가 목적일 때에는 이를 확보하기 전에 일률적으로 종료해서는 안 된다. 분석 장소나 도구도 가까움·편리함이 아니라 증거 보존, 도구 검증 및 절차의 신뢰성을 기준으로 정해야 한다.

④ X. **디스크 복제와 메모리 수집은 다르다.** 디스크 이미지는 저장매체의 데이터를 복제하는 것이며 현재 RAM 전체나 실시간 접속 상태를 그대로 수집하는 방법이 아니다. 페이지파일 등에 메모리 일부 흔적이 남을 수 있어도 별도의 휘발성 정보 수집을 대체하지 못한다.

따라서 제시된 휘발성 증거 수집 상황에서 가장 적절한 방법은 ①이다.

NoteBase

문 12. 디지털 포렌식에서 삭제된 파일의 복구와 관련된 설명으로 가장 적절하지 않은 것은?

① 파일을 삭제할 경우 메타정보와 실제 파일 내용을 초기화하지 않고, 단순히 메타정보의 특정 플래그만 변경시킨다.

② 파일 카빙(Carving)은 파일의 메타정보를 이용하여 삭제된 파일을 복구한다.

③ FAT 파일시스템에서 파일이 삭제될 경우 해당파일 Directory Entry의 오프셋 0x00 값이 삭제를 나타내는 0xE5로 변경된다.

④ 삭제 표시된 Directory Entry에 파일 크기와 시작 클러스터 정보를 이용하여 파일을 복구할 수 있다.

정답 2번

간단한 해설

파일 카빙은 **파일 내용의 시그니처나 구조**를 분석하는 복구 방식이다. 파일시스템의 메타정보를 이용하는 복구 방식으로 설명하면 두 방법을 혼동한 것이다.

선지별 해설

① O: 일반적인 논리적 삭제가 파일 내용을 곧바로 모두 지우는 것은 아니라는 취지의 설명이다. 다만 **특정 플래그만 바뀐다는 표현은 교육적인 단순화**이며, 실제로 변경되는 메타데이터는 파일시스템에 따라 다르다. FAT에서는 디렉터리의 삭제 표시 외에 할당 체인 정보도 해제될 수 있으므로 모든 삭제가 플래그 하나만 변경하는 것은 아니다.

② X: **파일 카빙은 파일시스템의 메타정보가 아니라 파일 내용과 형식의 특징**을 바탕으로 파일을 찾아 복구하는 방법이다. 예를 들어 시그니처, 헤더·푸터, 내부 구조를 분석한다. 디렉터리나 할당 정보에 의존하는 복구와 구별된다.

③ O: 전통적인 FAT 파일시스템에서는 디렉터리 엔트리의 첫 바이트, 즉 **오프셋 0x00을 0xE5**로 표시하여 삭제되어 사용 가능한 엔트리임을 나타낸다. 이 표시 자체가 파일 데이터 영역까지 모두 지웠다는 뜻은 아니다.

④ O: 삭제된 디렉터리 엔트리에 남은 **파일 크기와 시작 클러스터**는 복구에 활용할 수 있다. 다만 데이터가 남아 있어야 하며, 조각난 파일에서 연결 정보가 사라졌거나 덮어쓰기·TRIM 등의 영향이 있으면 복구가 어렵거나 불가능할 수 있다. 해당 정보가 있다는 것만으로 완전한 복구가 보장되지는 않는다.

NoteBase

문 13. 아래 (㉠)에 들어갈 용어로 가장 적절한 것은?

윈도우즈 운영체제에서 (㉠)는(은), 파일의 앞부분(header)과 마지막부분(footer)에 있는 파일 고유의 정보이다. 응용 프로그램에서 생성한 파일임을 인식할 수 있도록 파일 내부의 특정위치에 있는 몇 바이트가 항상 동일한데, 이러한 고정 값을 (㉠)(이)라고 한다. 이러한 (㉠)도 의도적으로 변경할 수 있지만 확장자의 변경에 비해서 용이하지 않다.

① 레지스트리(Registry)

② 파일 확장자(File extension)

③ 파일 이름(File name)

④ 파일 시그니처(File signature)

정답 4번

간단한 해설

파일 내부의 특정 위치에 있는 고정된 바이트 패턴으로 형식을 식별하는 정보는 **파일 시그니처**이다. 따라서 ㉠에 들어갈 용어는 ④이다.

핵심 풀이

㉠은 **파일 시그니처**이다. 파일 내부의 특정 위치에 나타나는 일정한 바이트 패턴은 파일 형식을 식별하는 단서로 쓰인다. 따라서 파일 내부의 고정 값이라는 설명에 맞는 용어는 ④이다. 여기서 시그니처는 전자서명이나 파일 전체의 해시 값을 뜻하지 않는다.

파일 확장자와 파일 이름은 파일을 부르는 이름의 일부로서 사용자가 바꿀 수 있다. 이름이나 확장자를 변경해도 파일 내부 형식까지 자동으로 달라지는 것은 아니므로, 포렌식 분석에서는 확장자와 내부 시그니처가 일치하는지도 확인한다.

레지스트리는 Windows의 시스템·사용자·응용프로그램 설정 등을 보관하는 데이터베이스로, 제시된 파일 내부 고정 패턴과 다르다.

헤더나 푸터는 시그니처가 나타날 수 있는 위치의 예이다. **모든 형식에 헤더와 푸터가 모두 있는 것은 아니며**, 시그니처도 위조·변경될 수 있다. 따라서 몇 바이트가 일치한다는 사실만으로 파일의 정상성이나 무결성을 확정하지 않고, 내부 구조 등 추가 정보를 함께 검토한다.

NoteBase

문 14. 인터넷 네트워크에 접속한 윈도우즈 운영체제에서, 디지털 포렌식 수사관이 인터넷 접속 정보를 수집할 경우에, 필요한 항목으로 가장 적절하지 않은 것은?

① Temporary internet files

② Cookie

③ ProcessExplorer

④ Web history

정답 3번

간단한 해설

ProcessExplorer는 **실행 중인 프로세스를 조사하는 도구**이지, 브라우저가 남긴 접속 이력 자료가 아니다. 임시 인터넷 파일·쿠키·웹 방문 이력은 인터넷 이용 흔적을 확인할 수 있는 자료이다.

개념 구분

Temporary internet files는 브라우저가 웹페이지의 이미지·문서 등의 내용을 임시로 저장한 **캐시**이다. 남아 있는 파일과 관련 정보를 통해 접속한 웹사이트나 열람 내용의 단서를 얻을 수 있다.

Cookie는 웹사이트가 브라우저에 저장하는 작은 데이터로, 사이트 식별과 세션·환경설정 등의 정보를 담을 수 있다. 해당 사이트와의 이용 관계를 살피는 자료가 되지만, 쿠키 하나만으로 구체적인 모든 방문 행위가 입증되는 것은 아니다.

ProcessExplorer는 현재 실행 중인 **프로세스·핸들·DLL 등을 조사하는 도구**이다. 시스템 조사에 활용될 수는 있으나, 나머지 항목처럼 브라우저의 과거 인터넷 이용 흔적이 저장된 자료 자체는 아니다.

Web history는 방문한 웹페이지의 주소와 방문 시각 등 **웹 방문 이력**을 제공하여 인터넷 접속 경위를 파악하는 데 쓰인다.

따라서 인터넷 접속 정보를 수집할 자료 항목으로 가장 적절하지 않은 것은 분석 도구 이름인 ③ ProcessExplorer이다.

NoteBase

문 15. 아래 (㉠)에 들어갈 용어로 가장 적절한 것은?

윈도우즈 운영체제에서 (㉠)는 부팅과정에서부터 로그인, 서비스 실행, 응용프로그램 실행, 사용자 행위 등 윈도우즈 운영체제의 거의 모든 활동에 관여한다. 특히 원격 접속 흔적, 드라이브 연결 흔적, 저장매체 사용 흔적 등의 정보를 이용하여 추가적인 포렌식 분석 대상을 선별하는데 활용할 수 있다.

① 레지스트리(Registry)

② 웹 히스토리(Web history)

③ 프로퍼티 리스트(Property list)

④ 메타 데이터(Meta data)

정답 1번

간단한 해설

Windows의 사용자·서비스·장치 설정을 관리하는 **레지스트리**에는 포렌식에 활용할 흔적도 남을 수 있다. 시스템 설정과 연결 장치 등의 정보를 바탕으로 추가 분석 대상을 찾는다.

핵심 풀이

㉠은 ① **레지스트리**이다. Windows와 응용프로그램이 사용하는 설정 정보를 키와 값으로 관리하는 계층형 데이터베이스로, 사용자 프로필·서비스·하드웨어 등 운영체제의 다양한 구성에 관여한다.

포렌식에서는 레지스트리에 남은 장치 연결 정보나 사용자·응용프로그램 관련 흔적을 조사하여 추가 분석할 저장매체와 대상 등을 찾을 수 있다. 다만 레지스트리가 **모든 행위를 빠짐없이 기록하는 로그라는 뜻은 아니며**, 남는 정보는 운영체제 버전과 설정 등에 따라 달라지므로 다른 흔적과 종합해야 한다.

웹 히스토리는 웹 이용 내역이고,

프로퍼티 리스트는 Apple 운영체제 등에서 설정·속성 정보를 저장하는 데 쓰이는 형식이다.

메타데이터는 데이터를 설명하는 정보라는 일반 개념으로, 제시문의 Windows 구성 데이터베이스를 특정하는 명칭은 아니다.

NoteBase

문 16. 디지털 포렌식 증거 분석에 활용하는, 디스크 브라우징(Disk Browsing) 기술의 설명으로 가장 적절한 것은?

① 디스크 파일 또는 저장매체 전체를 대상으로 특정 키워드인 파일이름, 속성, 내부 문자열, 코드 값, 시그니처를 쉽게 찾는 기술이다.

② 프로그램 정보와 네트워크 시스템 정보에 대한 레지스트리의 기록을 분석한다.

③ 디스크 파일 또는 저장매체에 저장된 파일의 시간정보, 내부 메타 데이터의 시간정보를 분석하는 기술이다.

④ 저장매체 또는 디스크 이미지의 내부 구조와 파일 시스템을 확인하고, 파일시스템 내부에 존재하는 파일에 대응되는 응용 프로그램의 구동 없이 쉽고 빠르게 분석할 수 있도록 하는 기법이다.

정답 4번

간단한 해설

디스크 브라우징은 **저장매체·이미지의 구조와 파일시스템을 탐색**하여 파일 및 관련 정보를 확인하는 기법이다. 검색, 레지스트리 분석, 시간정보 분석과 초점이 다르다.

개념 구분

디스크 브라우징은 저장매체나 이미지의 **파일시스템 구조를 해석하여 탐색**하고 파일과 관련 정보를 확인하는 기능이다. 특정 정보를 검색하거나 시간 흐름을 재구성하는 작업과 구별하여, 증거 매체의 구조와 내용을 살펴보는 데 초점을 둔다.

① 파일명·속성·문자열·코드 값·시그니처 등 조건에 맞는 정보를 찾는 것은 **검색** 기능의 설명이다. 브라우징 도구에 검색 기능이 함께 있어도, 이 설명만으로 디스크 브라우징 자체를 정의한 것은 아니다.

② 프로그램 및 네트워크·시스템 설정 관련 레지스트리 기록을 살펴보는 것은 **레지스트리 분석**이다. 운영체제 설정과 사용 흔적을 해석하는 특정 분석 영역이다.

③ 파일 시간정보와 내부 메타데이터의 시간을 비교·해석하는 것은 **시간정보·타임라인 분석**에 해당한다. 사건의 시간적 흐름을 파악하는 데 활용하며, 단순한 디스크 구조 탐색과 목적이 다르다.

④ 저장매체·디스크 이미지의 구조와 파일시스템을 확인하고 파일 내용을 살펴보는 것이 **디스크 브라우징**이다. 포렌식 도구의 뷰어·해석 기능을 이용하면 지원되는 파일을 원래의 응용 프로그램으로 실행하지 않고도 확인할 수 있다. 다만 모든 파일 형식을 지원하거나 암호화·손상된 내용까지 자동으로 해석한다는 뜻은 아니다.

따라서 디스크 브라우징을 가장 적절하게 설명한 것은 ④이다.

NoteBase

문 17. 디지털 포렌식에서 해시 함수(Hash Function)에 대한 설명으로 가장 적절하지 않은 것은?

① MD5, SHA-1 등의 해시 함수가 사용되고 있다.

② 디지털 데이터의 위조·변조 문제를 검증하는 수단이다.

③ 파일의 무결성을 검증할 때, 파일의 이름이 바뀌면 해시 값도 바뀐다.

④ 디지털 데이터의 크기에 상관없이, 일정한 길이의 비트열(Bit stream)로 변환되어 해시 값을 산정한다.

정답 3번

간단한 해설

일반적인 파일 해시는 **파일 내용**으로 계산한다. 내용의 바이트열이 같다면 이름만 바꾸어도 해시값은 그대로이다.

선지별 해설

① O: MD5와 SHA-1은 디지털 포렌식에서 파일의 해시값 산정에 사용되어 온 해시 함수이다. 다만 사용 이력이 있다는 사실과 공격에 안전하다는 평가는 다르며, 두 함수는 충돌 취약성이 알려져 있어 **공격에 대한 무결성 보호**에는 더 안전한 해시 함수를 선택해야 한다.

② O: 신뢰할 수 있게 보관한 기준 해시값과 현재 데이터의 해시값을 같은 알고리즘으로 비교하면 **내용의 변경 여부**를 점검할 수 있다. 값이 다르면 입력 데이터가 달라졌음을 알 수 있으므로 위조·변조 검증 수단으로 활용된다. 다만 해시만으로 변경 주체나 변경 원인까지 알 수 있는 것은 아니다.

③ X: 일반적인 파일 해시는 **파일 내용의 바이트열**을 입력으로 계산한다. 내용이 그대로라면 파일 이름만 바뀌어도 해시값은 변하지 않는다. 파일명까지 포함한 별도 자료나 디스크 전체 이미지를 해싱하는 경우와 파일 내용 자체의 해싱을 구별해야 한다.

④ O: MD5나 SHA-1과 같은 고정 출력 길이 해시 함수는 입력 데이터의 크기가 달라도 정해진 길이의 해시값을 만든다. MD5는 128비트, SHA-1은 160비트이며, **출력 길이는 사용하는 알고리즘**에 의해 정해진다.

NoteBase

문 18. 디지털 포렌식에서 증거 관련 보고서를 작성하는 방법에 대한 설명으로 가장 적절하지 않은 것은?

① 포렌식 수사관은 분석 과정에서 이용한 분석도구, 분석을 수행한 절차, 그리고 분석 결과를 포렌식 보고서에 명확하게 기록해야 한다.

② 포렌식 보고서의 분석 결과를 증거 자료로 인정받기 위해서는, 보고서의 분석 결과를 재현하였을 경우에도 완벽히 일치하여야 한다.

③ 포렌식 분석에 활용되는 증거수집 기술과 방법이 이미 증거 추출 과정에서 사용되었으므로, 보고서에는 증거수집 도구만 기록해도 된다.

④ 포렌식 보고서는 증거 분석에 대한 사실관계를 상세하고 객관적으로 기록해야 한다.

정답 3번

간단한 해설

보고서에는 수집·분석 도구뿐 아니라 **사용한 기술·방법, 수행 절차와 결과**도 기록해야 한다. 이미 증거 추출에 사용했다는 이유로 방법과 절차를 생략할 수 없으므로 ③이 가장 적절하지 않다.

선지별 해설

① (O) 분석 결과를 검토할 수 있도록 **사용한 도구, 수행 절차, 결과를 함께 기록**해야 한다. 도구의 버전이나 주요 설정 등 결과에 영향을 주는 조건도 남겨야 다른 분석자가 무엇을 어떻게 확인했는지 추적할 수 있다.

② (O) 이는 분석 결과의 **재현성**을 요구하는 설명이다. 동일하게 보존된 증거에 같은 분석 조건과 절차를 적용하면 같은 사실적 결과를 확인할 수 있어야 한다. 여기서 일치란 분석 결과의 일치를 뜻하며, 보고서의 서식까지 같아야 한다는 뜻은 아니다. 또한 재현성만으로 모든 증거 인정 요건이 충족된다는 의미도 아니다.

③ (X) 증거수집 도구의 이름만 기록하는 것으로는 부족하다. 이미 추출 과정에 사용했더라도 **수집 기술·방법과 실제 수행 절차**를 기록해야 한다. 무엇을 어떤 조건에서 수집·분석했는지 남기지 않으면 결과의 신뢰성과 재현성을 검토하기 어렵다.

④ (O) 보고서는 증거에서 확인한 **사실관계를 상세하고 객관적으로** 기록해야 한다. 관찰한 사실과 분석자의 해석을 구분하고, 분석의 한계나 결론과 맞지 않는 결과도 빠뜨리지 않아야 한다.

NoteBase

문 19. 압수된 디지털 저장매체로부터 출력한 문건을 증거로 사용하기 위한 요건으로 가장 적절하지 않은 것은?(다툼이 있는 경우 판례에 의함).

① 디지털 저장매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 한다.

② 디지털 저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았음이 담보되어야 한다.

③ 디지털 저장매체 원본과 '하드카피' 또는 '이미징'한 매체를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다.

④ 원본 가용성은 증거능력의 요건에 해당하므로 포렌식 수사관이 그 존재에 대하여 가용성을 구체적으로 주장·증명해야 한다.

정답 4번

간단한 해설

출력물의 증거능력과 관련하여 요구되는 **원본 동일성은 검사가 구체적으로 주장·증명**해야 한다. 이를 원본 가용성에 관한 포렌식 수사관의 증명책임으로 설명한 것은 잘못이다.

선지별 해설

① O: 출력 문건을 증거로 사용하려면 **원본에 저장된 내용과 출력된 내용의 동일성**이 인정되어야 한다. 복사·출력 과정에서 내용이 편집되거나 바뀐 자료를 원본 그대로의 증거로 취급해서는 안 되기 때문이다.

② O: 원본과 출력물의 동일성을 인정하려면 **압수 때부터 출력 때까지 원본 내용이 변경되지 않았음**이 담보되어야 한다. 이는 수집·보관·분석 과정의 무결성에 관한 요구이다.

③ O: 원본 대신 하드카피나 이미징한 매체에서 출력한 경우에는 원본과 복제 매체 사이의 동일성도 확인해야 한다. 그 확인에 사용한 **장비의 정확성, 프로그램의 신뢰성, 작업자의 기술능력과 정확성**이 확보되어야 복제·처리 결과를 신뢰할 수 있다.

④ X: 판례가 증거능력의 요건으로 드는 것은 이 문맥에서 **원본 동일성**이며, 그 존재를 구체적으로 주장·증명할 주체는 **검사**이다. 원본 가용성을 포렌식 수사관이 주장·증명해야 한다는 설명은 요건과 증명 주체를 잘못 연결한다. 수사관의 증언이나 분석 결과는 동일성을 뒷받침하는 자료가 될 수 있지만, 그 때문에 소송상 증명책임의 주체가 수사관으로 바뀌지는 않는다.

NoteBase

문 20. 수사기관이 압수·수색 영장을 집행할 때의 설명으로 가장 적절하지 않은 것은?(다툼이 있는 경우 판례에 의함).

① 정보저장매체인 경우에는 영장 발부의 사유로 된 범죄 혐의사실과 관련 있는 정보의 범위를 정하여 출력하거나 복제하여 이를 제출받아야 하고, 피의자나 변호인에게 참여의 기회를 보장하여야 한다.

② 압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준할 자에게 교부하여야 한다.

③ 압수된 정보의 상세목록에는 정보의 파일 명세가 특정되어 있어야 하고, 수사기관은 이를 출력한 서면을 교부하거나 전자파일 형태로 복사해 주어야 한다. 단, 이메일을 전송하는 방식으로는 할 수 없다.

④ 법원은 압수·수색영장의 집행에 관하여 범죄 혐의사실과 관련 있는 정보의 탐색·복제·출력이 완료된 때에는 지체 없이 압수된 정보의 상세목록을 피의자 등에게 교부할 것을 정할 수 있다.

정답 3번

간단한 해설

압수된 전자정보의 상세목록은 파일 명세를 특정해야 하지만, **이메일로 전송하는 방식도 허용**된다. 서면 교부나 전자파일 복사만 가능한 것은 아니다.

선지별 해설

① O. 정보저장매체에 대한 압수·수색은 **영장에 기재된 혐의사실과 관련된 정보**를 범위로 삼아 출력·복제하는 방식으로 이루어져야 한다. 이 집행 과정에서 피의자나 변호인에게 참여 기회를 보장하여 절차를 확인하고 권리를 행사할 수 있게 해야 한다.

② O. 형사소송법 제129조 및 제219조에 따라 수사기관이 압수하면 **압수목록을 작성하여 교부**해야 한다. 소유자·소지자·보관자 등은 이를 통해 무엇이 압수되었는지 확인하고 압수처분에 대한 불복 등 권리를 행사할 수 있다.

③ X. 상세목록은 압수된 **개별 파일의 명세를 특정**해야 하지만, 교부 방법이 종이나 직접 파일 복사로만 제한되지는 않는다. 판례는 **이메일 전송도 가능**하다고 보므로, 이메일로는 할 수 없다는 단서가 잘못되었다.

④ O. 법원은 영장 집행 조건으로 관련 정보의 탐색·복제·출력이 끝나면 **지체 없이 상세목록을 교부**하도록 정할 수 있다. 이는 압수 범위를 확인시키고 권리행사를 보장하기 위한 절차이다.

따라서 가장 적절하지 않은 설명은 ③이다. 이 판단은 대법원 2018. 2. 8. 선고 2017도13263 판결의 법리에 따른다.

NoteBase