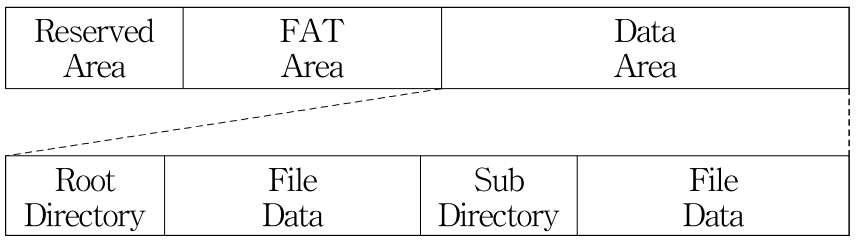
1. 디지털 증거의 특징에 관한 설명으로 가장 적절하지 **않은** 것은?
① 디지털 증거의 경우 해당 증거의 내용을 수사관의 지각으로 바로 인식할 수 없기 때문에 증거로 사용되기 위해서는 일정한 절차(가독화)를 거쳐야 하는 특징이 있다.
② 디지털 증거는 복제를 통해 원본과 동일한 사본을 만들 수 있으나 속성정보(메타데이터)가 변경되기 때문에 해시값도 변경된다.
③ 증거수집분석 등 일련의 취급과정에서 프로그램 조작자의 부주의로 인해 의도치 않게 증거물 파일의 내용이 쉽게 변경될 가능성이 높다.
④ 압수대상이 되는 디지털 증거는 단독으로 존재하기 보다는 사건과 관련 없는 개인적인 자료와 혼재되어 있는 경우가 많다.

2. 디지털 증거의 동일성·무결성·신뢰성에 관한 설명으로 가장 적절하지 **않은** 것은? (다툼이 있는 경우 판례에 의함)
① 무결성과 동일성, 신뢰성이 인정되지 않으면 증거능력이 부정되어 증거로 사용할 수 없다.
② 무결성은 디지털 증거가 수집 및 분석과정을 거쳐 법정에 제출되기까지 변경이나 훼손 없이 유지되어야 한다는 것을 의미한다.
③ 동일성과 무결성을 증명하는 방법은 원본과 해시값이 동일하다는 피압수자의 확인서면에 의해 증명할 수 있다.
④ 컴퓨터의 기계적 정확성, 프로그램의 신뢰성을 확보하되, 수사기밀 유지를 위하여 결과보고서에는 사용한 하드웨어 장비나 소프트웨어 도구를 기재해서는 안 된다.

3. 세계의 다양한 언어와 문자를 지원하는 국제코드 규약인 유니코드에서 가장 일반적으로 사용되며 영문은 1바이트, 한글은 3바이트로 표현하는 코드로 가장 적절한 것은?
① ASCII ② EBCDIC
③ BASE64 ④ UTF-8

4. 다음 그림에서 설명하는 구조를 사용하여 USB, 디지털카메라, 메모리카드에서 사용되는 파일시스템에 관한 설명으로 가장 적절하지 **않은** 것은?



① Boot 섹터는 파일시스템의 첫 번째 섹터에 위치한다.
② FAT Area는 클러스터의 할당 상태를 판단하며 백업용 FAT는 없다.
③ Data Area에는 실제 파일의 데이터가 존재한다.
④ Directory Entry는 파일과 디렉터리마다 할당된 데이터 구조체이며, 메타데이터가 포함된다.

5. 「디지털 증거의 처리 등에 관한 규칙」의 내용으로 옳지 **않은** 것은?
① 디지털 증거의 수집은 수사목적을 달성하는데 필요한 최소한의 범위에서 이루어져야 하며, 「형사소송법」 등 관계 법령에 따른 적법절차를 준수하여야 한다.
② 디지털 증거 처리의 각 단계에서 업무처리자 변동 등의 이력이 관리되어야 한다.
③ 증거분석관은 신속한 분석과 결과보고서의 신뢰성을 확보하기 위하여 분석의뢰물 원본을 대상으로 직접 분석하여야 한다.
④ 전자정보에 대한 압수·수색·검증영장을 신청하는 경우에는 혐의사실과의 관련성을 고려하여 압수·수색·검증할 전자정보의 범위 등을 명확히 하여야 한다.

6. 디스크를 병렬처리하여 성능과 안전성을 향상시키는 저장 방식인 RAID(Redundant Array of Inexpensive Disks)에 관한 설명으로 가장 적절하지 **않은** 것은?

	레벨	특징
①	RAID 0	병렬기록, 스트라이핑 모드
②	RAID 1	중복기록, 미러링 모드
③	RAID 3	패리티 정보기반 병렬 분산 저장
④	RAID 5	최소한 2개 이상의 디스크 필요

7. SSD(Solid State Drive)에 관한 설명 중 옳고 그름의 표시(O, X)가 바르게 된 것은?

> ㉠ 비휘발성으로 전원이 없어도 데이터 저장 상태를 유지할 수 있다.
> ㉡ HDD와 비교하면 작동 시 소음이 없으며 전력 소모가 많은 대용량 플래시 메모리이다.
> ㉢ 임의접근 방법을 사용하므로 데이터 입·출력을 저속으로 수행할 수 있다.
> ㉣ HDD와 비교하면 외부의 충격, 진동, 자성에 강하여 데이터 손실의 가능성이 낮다.

① ㉠(O) ㉡(X) ㉢(X) ㉣(X) ② ㉠(X) ㉡(X) ㉢(O) ㉣(X)
③ ㉠(O) ㉡(O) ㉢(X) ㉣(X) ④ ㉠(O) ㉡(X) ㉢(X) ㉣(O)

8. 디지털 증거의 압수·수색·검증에 관한 설명으로 가장 적절하지 **않은** 것은? (다툼이 있는 경우 판례에 의함)
① 전자정보 압수는 원칙적으로 범죄 혐의사실과 관련된 전자정보에 한하여 문서로 출력하거나 휴대한 정보저장매체에 해당 전자정보만을 복제하는 방식으로 하여야 한다.
② 정보저장매체 원본을 압수·수색·검증현장에서 수사기관 사무실 등으로 반출한 경우에는 피압수자에게 참여권을 보장하여야 한다.
③ 압수된 정보의 상세목록에는 정보의 파일 명세가 특정되어 있어야 하고, 서면으로 교부하거나 압수한 전자정보를 전자파일 형태로 복사해 주는 방식으로도 교부할 수 있다.
④ 압수·수색·검증현장에서 정보저장매체 원본을 반출한 경우에는 수사 종결 때까지 원본을 증거물 보관실에 보관한 후, 반환하여야 한다.

9. 다음 전자정보 중 전문증거에 해당하는지 확인해 볼 필요가 있는 증거를 모두 고른 것은?

> ㉠ 운영체제 이벤트 로그기록 ㉡ 웹 히스토리
> ㉢ 사용자 작성의 문서파일 ㉣ 송·수신된 이메일 내용
> ㉤ 방화벽 로그

① ㉠㉡ ② ㉡㉢ ③ ㉢㉣ ④ ㉣㉤

10. 하나의 클러스터보다 작은 데이터가 저장될 때 클러스터 일부만 사용되고 나머지 공간은 사용되지 않는다. 이 공간을 분석하는 기술로 가장 적절한 것은?
① 윈도우(windows) 레지스트리 분석
② 타임라인(timeline) 분석
③ 슬랙(slack) 분석
④ 파일 시그니처(signature) 분석

11. 다음 설명 중 ㉠과 ㉡에 해당하는 모바일포렌식 용어가 올바르게 짝지어진 것은?

> 최근 가장 중요한 수사 분야인 모바일포렌식에서는 ㉠스마트폰 단말기 고유정보와 ㉡가입자 고유정보를 파악할 수 있는 15자리로 구성된 2가지 모듈을 사용한다.

① ㉠ IMEI ㉡ MEID ② ㉠ IMEI ㉡ IMSI
③ ㉠ IDEN ㉡ IMSI ④ ㉠ MCC ㉡ ICCID

12. 네트워크 침해사고 관련 증거 확보방식 중 패킷 캡처에 활용되는 장비와 애플리케이션에 관한 설명으로 적절하지 **않은** 것은?

① FTK imager : 네트워크 트래픽 캡처의 메모리 이미징을 수행한다.
② 네트워크 탭 : 손상된 호스트와 스위치를 인라인하여 패킷 캡처를 수행한다.
③ tcpdump : root 권한으로 실행되면서 네트워크 트래픽을 모니터링한다.
④ wireshark : GUI 기반 도구로 패킷 캡처와 분석을 수행한다.

13. 다음 윈도우포렌식에 관한 설명에서 ㉠과 ㉡에 해당하는 것으로 가장 적절한 것은?

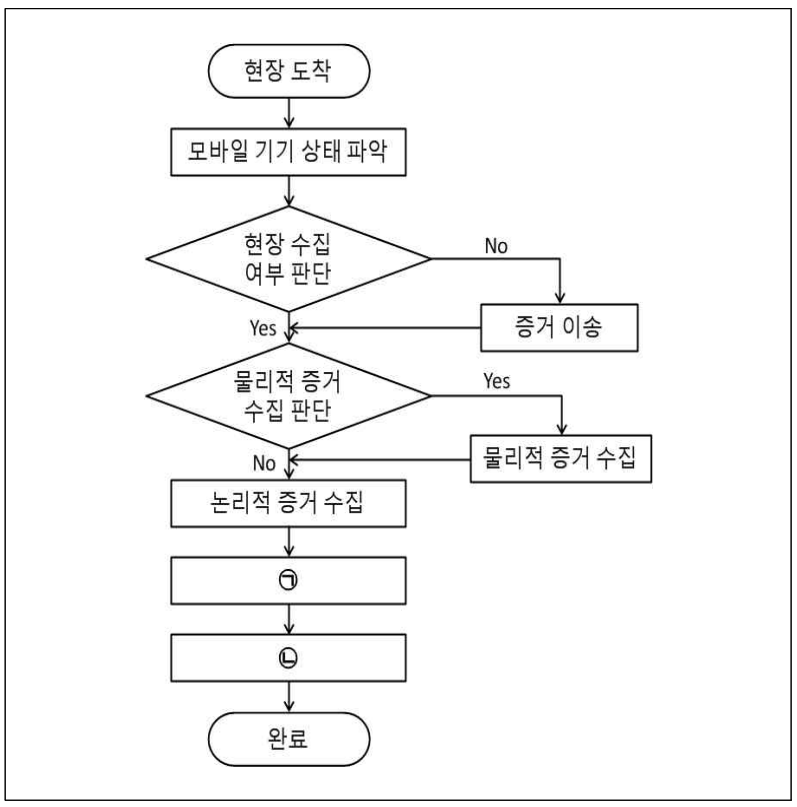
> 컴퓨터의 원본이미지가 삭제되어 복원하지 못한다고 하더라도 윈도우에서 미리보기를 선택하면 자동으로 생성되는 로딩속도가 빠른 ㉠소용량의 작은 미리보기용 이미지를 차선의 증거로 사용할 수 있다. 이 파일은 폴더 옵션에서 "보호된 운영체제 파일 숨기기" 항목의 체크 상태를 해제하여 볼 수 있으며, 이 파일의 존재를 통해 ㉡시스템에서 특정 시점에 원본 이미지가 존재하였다는 사실을 증명할 수 있다.

① ㉠ timeline ㉡ timeline cache
② ㉠ thumbnail ㉡ thumbnail cache
③ ㉠ metadata ㉡ metadata cache
④ ㉠ signature ㉡ signature cache

14. 디지털포렌식 도구에 관한 설명으로 가장 적절하지 **않은** 것은?

① Autopsy는 Windows와 Linux 파일시스템 내용분석은 가능하나 Android의 파일시스템 내용분석은 불가능하다.
② Encase는 포렌식 소프트웨어가 갖추어야 할 증거 보존 및 분석 기능을 갖춘 강력한 포렌식 도구이다.
③ TCT는 UNIX 계열 시스템에서 수행되는 강력한 포렌식 도구로 확장된 기능은 TCTUtils에서 제공한다.
④ BlackLight는 Mac, Windows, Android와 iOS에 대한 포렌식 도구이다.

15. 모바일포렌식 절차에 관한 흐름도에서 ㉠과 ㉡에 들어갈 단계로 가장 적절한 것은?



① ㉠ 분석 ㉡ 보존 ② ㉠ 분석 ㉡ 검사
③ ㉠ 분석 ㉡ 보고서 작성 ④ ㉠ 보존 ㉡ 보고서 작성

16. 디지털포렌식 이미지에 관한 설명 중 옳고 그름의 표시(O, X)가 바르게 된 것은?

> ㉠ 포렌식 이미지는 증거로부터 동일하게 이미지화한 데이터이다.
> ㉡ 포렌식 이미지는 이미지 파일 자체에 대한 이름, 크기, 타임스탬프 및 이미지 자체에 포함된 기타 정보 등을 포함한다.
> ㉢ 포렌식 이미지는 섹터 0부터 접근 가능한 마지막 섹터의 하드디스크 섹터를 복사하지 않고 파일을 복사한다.
> ㉣ 포렌식 이미지를 만들기 위하여 사용하는 가장 오래된 도구는 Windows에서 사용하는 dd 유틸리티이다.

① ㉠(O) ㉡(O) ㉢(X) ㉣(X) ② ㉠(X) ㉡(X) ㉢(O) ㉣(O)
③ ㉠(O) ㉡(X) ㉢(X) ㉣(O) ④ ㉠(O) ㉡(X) ㉢(O) ㉣(X)

17. 컴퓨터에서 USB 사용 흔적과 프린터 출력 정보를 확인하고자 할 때 수집해야할 전자정보를 모두 고른 것은?

> ㉠ 레지스트리 ㉡ 쿠키(cookie) 정보
> ㉢ 웹 캐시(web cache) ㉣ $RECYCLE.BIN 폴더
> ㉤ 스풀(spool) 파일

① ㉠㉡ ② ㉢㉣ ③ ㉣㉤ ④ ㉠㉤

18. 디지털 증거 압수·수색·검증 과정에서 별도의 범죄혐의와 관련된 전자정보(별건 정보)를 우연히 발견한 경우 취해야 할 조치에 관한 설명으로 가장 적절하지 **않은** 것은?

① 별건 정보는 영장의 범위를 벗어나기 때문에 별건 범죄혐의와 관련된 추가 탐색은 중단하여야 한다.
② 적법한 탐색 과정에서 별건 정보를 발견한 경우에는 별도의 압수·수색·검증영장 없이 별건 정보를 압수할 수 있다.
③ 영장에 기재된 범죄 혐의사실과 관련된 전자정보 탐색은 진행할 수 있다.
④ 별건 정보에 대한 압수·수색절차에서도 피압수자에게 참여권을 보장하고 압수목록을 교부하여야 한다.

19. 다음 사례에 대한 증거수집 및 분석방법으로 가장 적절하지 **않은** 것은?

> A는 서울역 지하철에서 스마트폰으로 타인의 신체를 몰래 사진 촬영한 후, 자신의 컴퓨터에 저장하였다. A는 컴퓨터에 저장된 해당 사진파일을 인터넷 커뮤니티 사이트에 올리고 확장자명을 hwp로 변경·저장하였다. 사법경찰관 P는 A를 성폭력범죄의 처벌등에관한특례법 위반죄로 수사하면서 A의 컴퓨터에서 사진파일을 찾고 범죄사실을 증명하고자 한다.

① 해시(hash) 분석을 통해 인터넷 커뮤니티 사이트에 올려진 사진파일의 해시값과 동일한 파일을 찾는다.
② 시그니처(signature) 분석을 통해 확장자명이 변경된 파일을 찾는다.
③ 웹 브라우저에서 히스토리 정보를 통해 웹 사이트의 접속날짜, 시간, URL 등을 확인한다.
④ 메인 메모리(main memory) 분석을 통해 썸네일(thumbnail)과 삭제된 파일을 분석하고, IP기록을 확인한다.

20. 다음 사례에 관한 설명으로 가장 적절하지 **않은** 것은?

> 인천 국제공항 테러를 목적으로 A와 B는 X회사에서 서비스하는 컴퓨터 메신저를 통해 범행을 실시간으로 모의하고 있다. 사법경찰관 P는 이와 같은 첩보를 입수하고 A와 B의 메신저 아이디를 확인한 후, 관련 증거를 수집하고자 한다.

① A와 B의 대화 내용을 네트워크상에서 실시간 수집·확인하기 위해서는 압수·수색·검증영장을 발부 받아야 한다.
② 와이어샤크(wireshark) 포렌식 도구를 이용하여 패킷을 수집·분석할 수 있다.
③ 법원의 허가를 받아 A와 B의 통신사실 확인자료를 전기통신사업자에게 요청할 수 있다.
④ IP 패킷 헤더를 통해 A와 B가 사용하고 있는 IP 주소를 파악할 수 있다.