제2회 디지털 포렌식 전문가 2급 자격시험

응시번호 :
성명 :

제2회 디지털 포렌식 전문가 2급 필기 시험

컴퓨터 구조와 디지털 저장매체

1. 32비트의 2의 보수법으로 표시된 다음 수의 십진수 값은 얼마인가?

$1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1100_2$

가. 2
나. -2
다. 4
라. -4

2. 어떤 장치가 다른 장치의 일을 잠시 중단시키고 자신의 상태 변화를 알려 주는 것을 무엇이라 하는가?

가. 인터럽트(interrupt)
나. 점프(jump)
다. 스위치(switch)
라. 서비스(service)

3. 프로세서 내부에 있는 레지스터 중의 하나로서, 다음에 실행될 명령어의 주소를 가지고 있는 것을 무엇이라 하는가?

가. ALU(Arithmetic-logic Unit)
나. SP(Stack Pointer)
다. CPU(Central Processing Unit)
라. PC(Program Counter)

4. 스레드(thread)에 대한 설명 중 옳지 않은 것은?

가. 스레드는 CPU 사용의 기본 단위이다.
나. 스레드는 스레드 ID, 프로그램 카운터, 레지스터 집합, 스택으로 구성된다.
다. 스레드는 같은 프로세스에 속한 다른 스레드와 운영체제 자원들을 공유하지 않는다.
라. 프로세스가 다수의 제어 스레드를 가진다면, 프로세스는 동시에 하나 이상의 작업들을 수행할 수 있다.

5. 다음 중 하드디스크 여러 개를 동시에 연결하여 동일한 데이터를 다른 위치에 중복하여 저장하는 것을 무엇이라 하는가?

가. 백업(backup)
나. RAID(redundant array of independent disks)
다. 버퍼(buffer)
라. 불량섹터(bad sector)

6. 다음 중 컴퓨터와 하드디스크를 연결하는 방식으로 옳지 않은 것은?

가. SATA
나. PATA
다. CDMA
라. IDE

7. 아래의 내용은 조사에 필요한 ATA(AT Attachment)에 대한 주요 명세이다. 괄호 안에 들어갈 내용으로 옳은 것은?

*ATA-1 : 1994년에 처음 발표. CHS와 28비트 LBA 주소 지원 *ATA-3 : 1997년에 발표. 신뢰성과 보안 요소 추가 *ATA/ATAPI-4 : 1998년에 발표. 이동식 매체 명세 정의 *ATA/ATAPI-6 : 2002년에 발표. ( ) 비트 LBA 주소 추가

가. 32
나. 40
다. 48
라. 64

8. 다음 중 USB 드라이브로 많이 쓰이는 플래시 메모리에 대한 설명으로 옳지 않은 것은?

가. 기본적으로 비휘발성 메모리이기 때문에 ROM과

같이 기록된 정보를 전원 없는 상태에서 보존하는 ROM의 역할을 할 수 있다.

나. 기억 단위가 섹터로 분할되어 포맷되는 디스크형 보조기억 장치와 구조가 유사하다.

다. 기계적인 운동부분이 없어 하드디스크에 비해 전력소모도 매우 적다.

라. 램 대용으로 사용할 수 있다.

9. 다음에서 설명하는 이것은 무엇인가?

- 이것은 데이터를 저장할 수 있는 디스크의 특별한 영역이고, 일반인들은 이것을 볼 수 없다. 이 영역의 크기는 ATA 명령으로 설정이 가능하고, 기본값으로 0이 설정된 경우가 많다. - 이것은 ATA-4에서 추가되었고, 사용자가 하드디스크 내용을 포맷하거나 삭제했을 때 지워지지 않는 데이터를 저장한다. - 이것은 디스크 끝에 있고 하드디스크 재설정에 의해서만 접근이 가능하다.

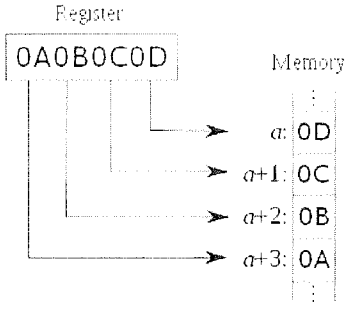
가. Unused Area

나. Hidden Sector

다. HPA

라. DCO

10. 디지털 데이터를 저장하기 위해서는 저장 장치 위치를 그 데이터에 할당할 필요가 있다. 아래의 그림은 4바이트 레지스터의 데이터를 메모리로 저장하는 형태를 보여주고 있는데, 어떤 엔디안(endian) 방식으로 저장하고 있는가?



가. Big endian

나. Middle endian

다. Small endian

라. Little endian

11. 다음 중 디지털 포렌식 관점에서 플래시 메모리를 조사할 때 확인해야 할 사항으로 옳지 않은 것은?

가. 플래시 메모리는 그 특징상 크기가 매우 작기 때문에 휴대성이 좋아 범죄자가 증거물을 쉽게 은닉할 수 있다.

나. 압수 · 수색 시 USB 메모리나 소형 메모리 카드를 숨길만한 장소까지 주의를 기울여 수색해야 하며, 수사 대상 시스템에서 메모리 카드의 사용 흔적이 있는지 파악해야 한다.

다. 하드 디스크와 같은 저장 매체와 마찬가지로 메모리 카드에 있는 데이터를 수집할 때에도 반드시 쓰기 방지 장치를 통해 데이터 기밀성을 유지해야 한다.

라. USB 메모리를 대상으로 데이터를 수집할 때에는 USB 메모리의 용량과 실제 디스크의 크기가 동일한 지를 확인하여 암호화 영역이나 숨겨진 영역이 존재하는지 점검해야 한다.

12. 스마트폰, PMP, 네비게이션과 같은 휴대용 단말기를 조사할 때의 유의 사항으로 옳지 않은 것은?

가. 내부에는 플래시 메모리가 내장되어 있으며, 평소 휴대폰을 사용하여 저장하는 정보는 대부분이 저장매체 안에 기록되므로 기기를 압수해서 조사해야 한다.

나. SIM(Subscriber Identity Module Card) 혹은 USIM(Universal Subscriber Identity Module Card) 메모리 카드를 장착하고 있으므로, 기기와 메모리 카드 각각을 분류해서 압수한다.

다. 스마트 폰의 경우에는 휴대폰과 같은 속성을 가지기 때문에 반드시 전자파를 차단해야 한다.

라. 네비게이션의 경우 데이터 저장은 외장 메모리에 의존하므로 SD카드만 확보하면 된다.

13. 다음 중 인터럽트 우선순위가 높은 것에서 낮은 순으로 옳게 나열된 것은?

가. 정전 > 기계적 오류 > 외부인터럽트 > 입출력인터럽트 > 프로그램 오류 > SVC

나. SVC > 정전 > 외부인터럽트 > 입출력인터럽트 > 프로그램 오류 > 기계적 오류

다. 정전 > 기계적 오류 > 입출력인터럽트 > 외부인터럽트 > 프로그램 오류 > SVC

라. 정전 > 기계적 오류 > 프로그램 오류 > 입출력인터럽트 > 외부인터럽트 > SVC

14. 다음 중 RAID 레벨에 대한 설명으로 옳지 않은 것은?

가. RAID 0에서 데이터는 모든 디스크에 분산되어 저장되며, 데이터 복구 기능이 없다.
나. RAID 1은 같은 데이터를 두 개의 디스크에 저장하며 데이터 복구가 가능하다.
다. RAID 3은 스트라이프를 사용하며, 패리티 저장을 위한 별도의 드라이브를 1개 사용한다.
라. RAID 4는 디스크마다 패리티 정보를 가진다.

15. 다음 중 비휘발성 메모리가 아닌 것은?

가. EPROM
나. 플래시 메모리
다. DRAM
라. EEPROM

제2회 디지털 포렌식 전문가 2급 필기 시험

파일시스템과 운영체제

16. 다음 중 Active Directory에 대한 설명으로 옳지 않은 것은?

가. Windows 2000에서 소개된 이후로 Windows 기반 도메인의 핵심이다.
나. 컴퓨터의 그룹을 도메인으로 조직화시키는 표준 인터넷 서비스인 DNS를 사용한다.
다. Windows NT 4.0 도메인 컨트롤러를 Windows Server 2008과 함께 사용할 수 있다.
라. Active Directory는 네트워크에 연결된 Resource에 대하여 Single Sign-on을 제공한다.

17. 다음은 Windows Server 2008에서 사용하는 파일 및 폴더의 사용 권한에 대한 설명으로 옳지 않은 것은?

가. 기본적으로 접근 불가가 승인/거부되지 않았다면 접근이 거부된다.
나. 사용자의 권한은 속한 그룹의 권한에 우선한다.
다. 부모 폴더 사용 권한 설정 시 사용 권한의 상속을 폴더 내의 모든 파일과 하위 폴더에 강제할 수 있다.
라. 폴더에 파일을 생성할 때 해당 파일은 특정 사용 권한 설정을 상속 받는다.

18. 다음은 Windows Server 2008에서 실행되는 DNS 서버가 구동 될 때 수행하는 초기화 작업을 나열한 것이다. 옳지 않은 것은?

가. 파일이나 AD DS 저장소로부터 최상위 hints를 로드 한다.
나. AD DS에 저장된 것보다 파일에 저장된 모든 영역들을 로드한다.
다. 쿼리와 RPC에 대한 응답을 시작한다.
라. 초기화 작업과 동일한 쓰레드에서 AD DS에 저장되어 있는 영역들을 로드한다.

19. 다음 중 ext2 파일 시스템의 구성 요소에 해당되지 않는 것은?

가. Super Block : 블록의 크기, inode 개수 등의 주요 설정 정보들이 기록된다.
나. inode : 파일 객체가 저장되는 곳으로서 파일의 크기, 시간 정보, 권한 등의 정보를 기록하고 있다.
다. Group Descriptor Table : 그룹 안의 빈 블록 수 또는 inode 수 등의 Block group에 대한 descripti -on 정보를 기록하고 있다.
라. Journaling : 운용 중 시스템이 crash되었을 때 복구 메커니즘을 제공한다.

20. 다음 중 Windows의 Structured exception handling에 대한 설명으로 옳지 않은 것은?

가. S/W Exception 처리를 위한 전용 메커니즘이다.
나. Structured exception handling의 확장으로 Vector -ed exception handling이 있다.
다. Termination handling은 어떠한 코드가 실행된 후 반드시 실행되도록 하는 기능을 제공한다.
라. Exception이 발생하면 프로세서는 우선 실행을 멈추고 제어권을 시스템에 넘겨준다.

21. 다음 중 운영체제의 기능으로 옳지 않은 것은?

가. 프로세스 관리
나. 기억장치 관리

다. 파일 관리
라. 메일 관리

22. 다음 중 분산시스템(distributed system)의 특성으로 옳지 않은 것은?

가. 네트워크를 통하여 연결된 다수의 컴퓨터 시스템들로 구성된다.
나. 물리적인 공유 메모리(shared memory)를 사용한다.
다. 각 시스템들은 독립성(autonomy)을 가지며, 필요에 따라 공동의 작업을 위해 협력한다.
라. 은폐성(transparency)을 가지며, 사용자에게는 전체 시스템이 가상의 단일 시스템으로 보이도록 한다.

23. 다음 프로그램 상태 중 다중 스레드 프로세스의 스레드들 사이에 공유되는 것은?

가. 레지스터 값들
나. 힙 메모리
다. 전역 변수들
라. 스택 메모리

24. 다음 중 파일 시스템의 논리적 구조 중 루트(root) 디렉토리 밑에 여러 개의 하부 디렉토리를 갖는 구조는?

가. 평면 디렉토리 구조
나. 이단계 디렉토리 구조
다. 계층형 디렉토리 구조
라. 그래프 디렉토리 구조

25. Windows의 사용 권한 설정에 대한 설명으로 옳지 않은 것은?

가. NTFS 사용 권한을 표준화하기 위해 보안 템플릿과 그룹정책을 사용한다.
나. 사용권한이 설정된 파일을 복사하면 사용권한도 복사된다.
다. 사용자에게 필요한 최소한의 권한만을 설정한다.
라. 사용권한은 NTFS 파일 시스템에서만 설정할 수 있다.

26. Windows의 MMC(Microsoft Management Console)는 시스템을 관리하는데 중요한 관리도구이다. 다음 중 MMC에 대한 설명으로 옳지 않은 것은?

가. 모든 버전의 윈도우에서 제공된다.
나. MMC 자체로는 관리 기능이 없고 스냅인이라는 관리응용 프로그램을 관리한다.
다. MMC를 통해 여러 가지 작업관리를 동일한 인터페이스에서 할 수 있다.
라. MMC는 한 개 이상의 스냅인을 포함하는 콘솔이라는 관리 도구를 생성하고 관리한다.

27. Windows는 기본적으로 여러 가지의 로그를 제공한다. 다음 중 관리자가 시스템으로의 로그온 성공과 실패 내역을 보고자 할 때 참고해야 할 로그는?

가. 파일 복제 서비스 로그
나. 시스템 로그
다. DNS 로그
라. 보안 로그

28. 다음 중 리눅스의 디렉토리 구조에 대한 설명으로 옳지 않은 것은?

가. /　　: 최상위 디렉토리이고, 모든 디렉토리는 / 기준으로 생성됨
나. /dev : 시스템 장치 파일을 저장
다. /tmp : 임시로 파일이 저장되는 공간
라. /var : 사용자의 홈 디렉토리가 위치하여 사용자의 데이터를 저장

29. 리눅스 시스템에서 사용하는 로그 파일에 대한 내용으로 옳지 않은 것은?

가. lastlog : 사용자의 최근 로그인 시간에 대한 정보를 갖고 있다
나. wtmp : 파일이 생성되는 순간부터 사용자의 로그인과 로그아웃 정보를 갖고 있다.
다. secure : 로그인이 실패한 경우 이 파일에 저장된다.
라. messages : 로그인 기록부터 다바이스 정보, 시스템 설정오류, 파일 시스템 등의 정보를 갖고 있다.

30. Windows 시스템에서 운영되는 IIS(Internet Informa-tion Services) 웹서버에 대한 보안 고려 사항으로 옳지 않은 것은?

가. IIS에 포함된 모든 샘플 어플리케이션을 사용 안 함 또는 중지시킨다.
나. 상위 경로 사용 안함을 설정하여 인가되지 않은 디렉터리에 대한 열람을 금지시킨다.
다. 파일 종류에 따라 기본적인 ACL을 줄 수 있도록 서브 디렉터리에 나눠서 정리한다.
라. 가상 디렉터리에 존재하는 파일 중 script(.asp등) 파일은 Everyone 그룹에게 실행/쓰기 권한을 제거하고 읽기 권한만 부여한다.

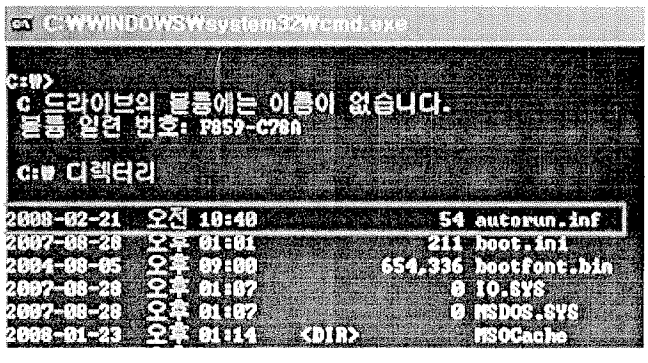
제2회 디지털 포렌식 전문가 2급 필기 시험

응용 프로그램과 네트워크의 이해

31. 윈도우 증거 수집 방법 중 시간확인 작업 시 중요도가 가장 낮은 항목은?

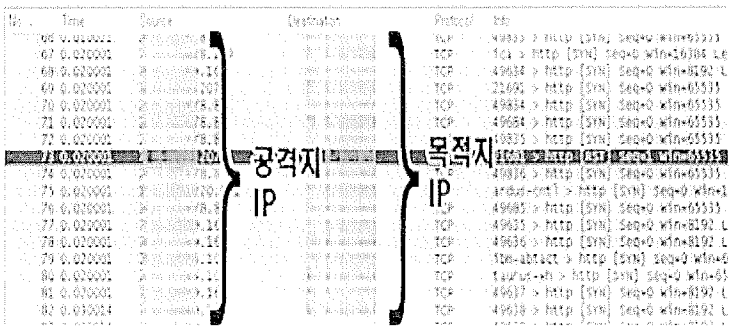
가. 점검 시간 (Checked Time)
나. 변경 시간 (Modified Time)
다. 접근 시간 (Accessed Time)
라. 생성 시간 (Created Time)

32. 아래 그림을 보고 디렉토리 내부의 숨김 속성을 확인할 수 있는 명령어 및 옵션으로 옳은 것은?



가. dir /A:D
나. dir /A:H
다. dir /O:D
라. dir /O:H

33. 아래 그림을 보고 어떤 분산서비스(DDoS)공격의 모습 인지 선택하시오.



가. CC Attack
나. UDP Flooding
다. ICMP Flooding
라. HTTP Flooding

34. 침해사고가 발생한 컴퓨터(PC)를 조사하는 과정에서 전자우편(E-mail)의 실제 발신정보를 분석하는데 가장 필요한 것은?

가. WHOIS 정보
나. 전자우편 헤더 정보
다. 전자우편 계정과 비밀번호
라. 방화벽 로그

35. 와이어샤크(WireShark) 프로그램을 이용하여 POP3 트레픽을 점검하려고 한다. 디지털포렌식 조사관은 어떤 포트를 검색해야 하는가?

가. 143
나. 25
다. 110
라. 125

36. 네트워크 명령어 중 현재 사용 중인 TCP, UDP 및 세션 정보를 알 수 있는 명령어는 무엇인가?

가. netstat
나. net share
다. ipconfig
라. arp

37. 다음 중 Internet Explorer의 Cookie, Temporary Int-ernet Files 등에 대하여 해당 파일에 대한 URL, Hit수, 실제 파일에 대한 mapping 정보 등의 정보를 저장하고 있는 별도의 파일이 존재한다. 이 파일명은 무엇인가?

가. index.dat
나. history.dat
다. IE.dat
라. ieinfo.reg

38. Windows XP 폴더구조(C:\Windows)에서 Windows 실행에 핵심이 되는 DLL, Drive 정보가 저장되어 있는 폴더명은 무엇인가?

가. Downloaded Program Files
나. system
다. Repair
라. system32

39. 방화벽(Firewall)에 대한 설명으로 옳지 않은 것은?

가. 패킷필터링 게이트웨이, 프록시 서버 두 가지 종류로 나눌 수 있다.
나. 미리 정해놓은 정책을 통해 허용된 IP 주소, 포트의 패킷만을 통과시키고 허용되지 않은 패킷은 차단한다.
다. 베스천 호스트는 보호하고자 하는 네트워크의 내부에 존재하여 보호할 네트워크에 대한 액세스 권한을 관리한다.
라. 이중 네트워크 호스트 구조의 방화벽 시스템은 라우팅 기능을 가지고 있지 않다.

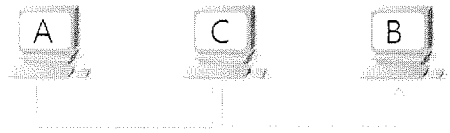
40. HTTP Protocol을 분석하여 XSS, SQL Injection, Restrict URL Access 등의 침해에 대한 탐지 및 차단 기능을 수행하는 보안 프로그램은 무엇인가?

가. Web Vulnerability Scanner
나. HTTPS
다. Web Application Firewall
라. Network Virus Wall

41. 이메일 클라이언트가 저장하는 파일 형태가 아닌 것은?

가. OCX
나. PST
다. DBX
라. EML

42. 다음에서 설명하고 있는 공격 방법은 무엇인가?



C가 A와 B의 사이에서 통신을 감시하고 있다가 A가 B의 MAC 주소를 물어 왔을때 C가 B대신 C의 MAC 주소를 가르쳐 주어 A는 C가 B인줄 알고 C에게 메시지를 보낸다.

가. MAC Flooding
나. ARP Spoofing
다. Denial of Service
라. Race Condition

43. Windows XP에서 thumbs.db에 미리 보기 정보가 기록되지 않는 파일형식은?

가. JPG
나. GIF
다. MP3
라. BMP

44. 다음 중 OSI 7 layer의 응용 계층 프로토콜이 아닌 것은?

가. SMTP - Simple Mail Transfer Protocol
나. SNMP - Simple Network Management Protocol
다. ICMP - Internet Control Message Protocol
라. FTP - File Transfer Protocol

45. 다음 중 무선(Wireless LAN - Wi-Fi) 규격에 해당하는 것은?

가. IEEE 1394
나. IEEE 802.11
다. IEEE 802.15.1
라. IEEE 802.15.4

제2회 디지털 포렌식 전문가 2급 필기 시험

데이터베이스

46. 트랜잭션(transaction)이 준수해야 하는 특성들에 대한 설명 중 옳지 않은 것은?

가. 원자성(atomicity) : 트랜잭션의 모든 연산들을 완전히 수행하거나 혹은 전혀 수행하지 않아야 한다.
나. 일관성(consistency) : 트랜잭션 수행 전의 값이 정확한 값을 가졌다면, 트랜잭션 수행 중간에도 항상 정확한 값이 유지되도록 보장해야 한다.
다. 고립성(isolation)) : 수행 중인 각 트랜잭션이 갱신한 데이터 항목의 값들을 자신이 완료할 때까지, 다른 트랜잭션들에게 보이지 않도록 한다.
라. 지속성(durability) : 트랜잭션이 성공적으로 완료되면 수행 중에 변경한 값들은 데이터 손실 없이 최종적으로 데이터베이스에 반영이 되어야 한다.

47. 두 개의 릴레이션(relation)들 사이에 참조 무결성(referential integrity)이 위반 되었는지를 검증하기 위해 SQL 트리거(trigger) 연산이 사용된다. 다음 중 검증을 할 필요가 없는 연산은?

가. CASCADE ON DELETE
나. SET NULL ON DELETE
다. CASCADE ON INSERT
라. SET DEFAULT ON UPDATE

48. 두 개의 릴레이션 R1과 R2를 조인(join) 연산을 수행한 결과에서 생성될 수 있는 튜플(들)의 최소 개수와 최대 개수는 각각 얼마인가? 여기서 R1의 튜플 개수는 100개, R2의 튜플 개수는 50개로 가정한다.

가. 최소 : 1개, 최대 : 150개
나. 최소 : 0개, 최대 : 150개
다. 최소 : 1개, 최대 : 5,000개
라. 최소 : 0개, 최대 : 5,000개

49. 다음의 관계형 대수 질의 표현과 동등하게 표현한 SQL 명령문은 어느 것인가? (단, π는 프로젝트, σ는 셀렉트, X는 카티션 프로덕트 연산자를 의미한다.)

릴레이션 : 사원 (사번, 사원명, 봉급, 부서번호)
부서 (부서번호, 부서명)
관계형 대수 질의 :
봉급 (σ 부서번호 = 부서번호(σ 부서명 = 경리과(사원 X 부서))

가. SELECT 봉급 FROM 사원, 부서
WHERE (부서명 = '경리과') AND (부서번호 = 부서번호)
나. SELECT DISTINCT 봉급 FROM 사원, 부서
WHERE (부서번호 = 부서번호) AND (부서명 = '경리과')
다. SELECT DISTINCT 봉급 FROM 사원, 부서
WHERE (부서명 = '경리과') OR (부서번호 = 부서번호)
라. SELECT 봉급 FROM 사원, 부서
WHERE (부서명 = '경리과') OR (부서번호 = 부서번호)

50. 다음 문장의 각 괄호 안에 들어가는 용어로서 옳은 묶음은?

(①)는 트렌젝션의 원자성(atomicity)을, (②)는 트렌젝션의 지속성(durability)을 보장하기 위한 연산이다. 모든 트렌잭션은 모든 읽기/쓰기 연산에 대한 기록을 (③)에 저장해야 한다.

가. ① REDO ② UNDO ③ 로그(log)
나. ① UNDO ② REDO ③ 메타데이터(metadata)
다. ① REDO ② UNDO ③ 메타데이터(metadata)
라. ① UNDO ② REDO ③ 로그(log)

51. 다음의 릴레이션에서 밑줄 그은 속성이 주키(primary key)이고, '수강' 릴레이션은 '학생' 릴레이션과 '과목' 릴레이션을 참조한다고 가정한다. 다음 중 참조 무결성 검증을 위해 사용할 수 없는 명령어는?

학생(학번, 이름, 나이, 주소)
수강({학번, 과목번호}, 성적)
과목(과목번호, 과목명)

가. SET DEFAULT ON DELETE 과목
나. CASCADE ON DELETE 학생

다. SET NULL ON UPDATE 학생
라. CASCADE ON DELETE 과목

52. 데이터 항목 X와 Y의 초기값으로 각각 1000과 2000이 있다고 하자. 다음 트랜잭션 T의 수행에 대한 설명으로 옳은 것은?

```
T : Begin_Trans
    Read(X)
    X = X - 100
    Write(X)
    Read(Y)
    Y = Y + 100
    Abort
```

가. T가 abort한 후 X와 Y의 값은 각각 900과 2100이다.
나. T가 abort한 후 주기억장치와 디스크의 X와 Y의 값은 모두 서로 같다.
다. T가 수행했던 모든 연산들을 취소하여 X와 Y의 값을 각각 1000과 2000으로 복귀시켜야 한다.
라. T가 수행했던 일부 연산들을 취소하여 X와 Y의 값을 각각 900과 2000으로 복귀시켜야 한다.

53. 다음의 '사원' 릴레이션에서 발생하는 문제점으로 옳지 않은 것은? (단, 여기서 이 릴레이션의 주키(primary key)는 '사번'이라고 가정한다.)

사원(사번, 사원명, 사원주소, 부서번호, 부서명, 부서장)

가. 새로운 부서의 정보를 반영하는 경우, 만약 그 부서에 근무하는 사원이 아직 한 명도 정해지지 않았다면, 이 부서의 정보를 이 릴레이션에 삽입할 수 없다.
나. 각 사원이 단 하나의 부서에만 근무하는 경우, 만약 어떤 특정 부서를 이 릴레이션에서 삭제하는 경우, 그 부서에서 근무하는 사원의 정보도 함께 삭제된다.
다. 새로운 신입 사원의 정보를 반영하는 경우, 만약 그 사원이 근무하는 부서가 아직 정해지지 않았다면, 이 사원의 정보를 이 릴레이션에 삽입할 수 없다.
라. 한 부서에 여러 명의 사원이 근무하는 경우, 동일한 부서 정보가 여러 번 반복되는 중복 현상이 발생한다.

54. 다음의 '사원' 테이블에서 아래 SQL 명령문이 실행된 후의 결과는 무엇인가?

```
SELECT  COUNT(*)
FROM    학생
WHERE   (나이 > 30)
```

<사원> 테이블

사번	이름	나이
100	홍길동	32
101	홍길동	32
102	홍길동	null
103	null	32
104	null	null

가. 3
나. 2
다. 5
라. 1

55. 다음은 함수 종속(functional dependency)의 정의이다. 괄호 안을 옳게 채워 나열한 것은?

X와 Y를 각각 릴레이션 R의 속성(들)이라 하자. 함수 종속 X → Y는 R에 속한 임의의 두 개의 튜플 t1과 t2에 대해, 만약 (①)이면 (②)가 성립해야 한다.

가. ① t1[X] = t2[X] ② t1[X] ≠ t2[X]
나. ① t1[X] = t2[X] ② t1[X] = t2[X]
다. ① t1[X] ≠ t2[X] ② t1[X] = t2[X]
라. ① t1[X] ≠ t2[X] ② t1[X] ≠ t2[X]

56. 다음 중 전자금융사고 예방을 위한 전자금융 거래법과 관련 한 설명사항 중 옳은 것은?

가. 금융회사는 전자금융거래법에 의거 전자금융거래 내역을 확인할 수 있도록 인터넷 뱅킹의 경우 금융거래 이용자 ID, 거래일시, 계좌번호, 입출금 계좌 정보 등을 관리한다.
나. 금융 회사는 전자금융소비자의 전자금융 거래시 발생되는 IP정보를 활용한 금융거래 장소 정보의 특성을 활용할 수 있다.
다. 신용카드회사는 금융거래 발생장소인 가맹점의 위치정보 또는 금융거래의 발생 시간차 등의 정보를 활용하는 위험거래인지시스템을 구축, 운영

하나 금융소비자의 보호를 위한 위험 관리가 충분히 가능하지 않다.
라. 국내에서 사용되고 있는 모든 IP정보는 집중관리기관인 한국인터넷진흥원에서 관리하고 있으며, 전자금융 거래시 발생되는 이용자 IP정보는 해당 금융 회사에서 관리하고 있다.

57. SQL 인젝션(injection) 공격의 대응 조치에 대한 설명으로 옳은 것은?

가. 프로그램의 취약점을 빨리 분석하기 위하여 사용자에게 적절한 에러 메시지를 제공해야 한다.
나. UNION 연산자를 사용하면 질의 결과가 다른 질의의 결과와 결합되므로 가능한 UNION 연산자를 사용하지 말아야 한다.
다. 이미 구성된 SQL 문장을 사용하는 것은 위험하므로 조건에 따라 구성되는 동적 SQL 사용이 권장된다.
라. 프로그램에서 SQL을 매개 변수화하여 사용하는 것은 비교적 안전하다.

58. MS-SQL서버에서 SQL Injection의 흔적을 알 수 있는 증거내용으로 옳지 않은 것은?

가. WebKnight 등의 웹 방화벽 오류나 버그 로그
나. 웹사이트 연동 데이터베이스의 테이블 목록
다. xp_cmdshell과 같은 Master DB의 확장 프로시저 이용 로그
라. IIS 홈 디렉토리, wwwroot, system32 등의 디렉토리에 포함된 스크립트(Script)화된 공격 코드

59. 다음 중 주어진 세션(Session)을 추적(Track)하기 위해 SQL 서버에서 사용되는 유일한(Unique) 값은?

가. Transaction ID
나. Server Process ID
다. Page ID
라. Slot ID

60. 데이터베이스 포렌식을 수행할 때 주의해야 할 사항으로 옳지 않은 것은?

가. 포렌식을 수행할 DB의 스키마(Schema)를 파악한다.
나. 데이터 타입 스토리지의 포맷을 확인한다.
다. 대용량 데이터 세트(Dataset)를 줄인다.
라. 데이터베이스 디스크 상의 값(On-disk Value)만을 증거로서 인정한다.

제2회 디지털 포렌식 전문가 2급 필기 시험

디지털 포렌식 개론

61. 다음 중 압수수색 절차에서 각 컴퓨터별 OS에 따른 올바른 shut-down 방법으로 옳지 않은 것은?

가. Windows XP - 플러그를 제거한다.
나. DOS - 플러그를 제거한다.
다. Linux - 플러그를 제거한다.
라. Windows 2000 - 플러그를 제거한다.

62. 다음 중 사후에도 영장을 요하지 않는 것은?

가. 구속영장을 집행한 후 피의자의 의사에 반하여 그 피의자가 소유하고 있는 물건을 압수한 경우
나. 변사체를 검시한 후 영장 없이 그 사체를 해부한 경우
다. 범행직후의 범행 장소에서 피의자의 의사에 반하여 그 피해자가 소지 중인 물건을 영장 없이 압수한 경우
라. 구속영장이 발부된 피의자를 발견하기 위하여 타인의 주거를 수색한 경우

63. 디지털 증거 처리에 관한 기본적인 원칙으로 옳지 않은 것은?

가. 디지털 증거를 처리함에 있어서 원본과의 동일성을 유지하도록 해야 한다.
나. 증거의 원본을 보존시켜야 한다.
다. 문서파일은 반드시 출력하여 보전하여야 한다.
라. 디지털 증거물의 처리 과정과 결과에 대한 문서화가 수반되어야 한다.

64. 다음 중 디지털 증거물의 봉인방법에 대한 설명으로 옳지 않은 것은?

가. 압수물인 각 원본 디지털 저장매체는 압수된 후 그 자리에서 봉인되어야 한다.

나. 수사기관이 압수물에 대한 복제작업, 이미지 작업을 위해 봉인을 해제하는 과정과 작업 후 재봉인하는 과정에 압수·수색 대상자가 참여하여 방해하지 못하도록 하여야 한다.
다. 수사기관은 압수물의 봉인 및 봉인해제, 재봉인 시에 항상 압수·수색 대상자들로부터 확인서를 받는다.
라. 봉인 및 봉인해제, 재봉인의 전 과정을 캠코더로 녹화한다.

65. 영장에 의하지 않고 압수할 수 있는 것을 모두 고른 것은?

㉠ 임의제출 된 물건	㉡ 범죄현장에서의 증거물
㉢ 유류물(遺留物)	㉣ 우체물
㉤ 공무원이 소지한 공무상 비밀문서	

가. ㉠ ㉣ ㉤
나. ㉠ ㉡ ㉢
다. ㉡ ㉢ ㉣
라. ㉢ ㉣ ㉤

66. 디지털 증거 및 디지털 포렌식과 관련하여 우리나라 법원 입장으로서 옳지 않은 것은?

가. 우리나라 대법원은 디지털 저장매체로부터 출력된 문건이 진술증거로 사용되는 경우에는 그 기재내용의 진실성에 관하여 전문법칙이 적용된다는 것이 일관된 입장이다.
나. 이른바 '일심회 사건' 당시 우리나라 법원은 1심 판결에서 전자적 정보의 증거능력 판단에 전문법칙을 적용하지 않고, 전자적 정보자체의 진정성 입증에 의해 증거능력을 인정한 판결을 내린 바 있다.
다. 우리나라 대법원은 이른바 '일심회 사건' 최종 판결에서 검증에 사용된 프로그램의 신뢰성에 대하여 국내에서 신뢰성 있는 기관에 의한 검증의 필요성을 언급하였다.
라. 이른바 '영남위원회 사건'에서 법원은 컴퓨터 디스켓에 들어 있는 문건이 증거로 사용되는 경우 그 기재내용의 진실성에 관하여는 전문법칙이 적용되므로 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다고 판시한 바 있다.

67. 다음 중 컴퓨터의 전원을 껐을 경우 잃게 되는 정보가 아닌 것은?

가. RAM 메모리내의 데이터
나. 프로세스 메모리 정보
다. 클립보드의 내용
라. 삭제된 파일의 MFT Entry 정보

68. 다음 중 영상녹화물에 관한 설명 중 옳지 않은 것은?

가. 피의자에 대한 조사과정을 영상 녹화하는 경우에는 피의자에게 고지하면 충분하고, 피의자가 반대의사표시를 분명히 하더라도 촬영할 수 있다.
나. 성폭력 피해자가 16세미만의 자인 경우에는 진술과정을 영상 녹화하여야 하고, 다만 피해자가 반대하는 경우에는 촬영을 하여서는 안 된다.
다. 사법경찰관 작성 피의자신문조서의 경우 피의자이었던 피고인이 성립의 진정을 부인하면 영상녹화물에 의해 성립의 진정을 인정하여 당해 피고인에 대해 증거로서 사용할 수 있다.
라. 수사과정 이전에 컴퓨터를 이용하여 작성한 진술서의 경우 작성자가 성립의 진정을 다투면 수집과정을 영상녹화하거나 조사자의 증언 등으로 성립의 진정을 인정할 수 없다.

69. 판례에 관한 다음 설명 중 옳지 않은 것은?

가. 몰수대상이 되는지 여부나 추징액의 인정 등 몰수·추징의 사유는 범죄구성요건 사실에 관한 것이 아니어서 엄격한 증명을 요하지 않는다.
나. 검사가 압수·수색영장을 청구하지 않은 부작위 처분은 준항고 대상이 되지 않는다.
다. 압수물은 압수절차가 위법하더라도 압수물의 존재, 형상에는 변함이 없으므로 증거가치에는 변함이 없다.
라. 조서에 대해 성립의 진정을 인정하였다가 증거조사 완료 후에 가서 이를 번복하였다면 조서의 증거능력이 언제나 부정되는 것은 아니다.

70. 디지털 데이터를 확보하기 위하여 물리 메모리 덤프를 사용하고자 할 때의 도구로 옳지 않은 것은?

가. dd
나. Nigilant32

다. KnTDD
라. Snort

71. EnCase에서 증거 파일 추가를 선택하여 증거 파일을 개별적으로 소스 트리에 추가 할 수 있다. 추가 파일로 옳지 않은 것은?

가. 물리적 증거 파일
나. SafeBack 파일
다. VMware 파일
라. Virtual PC 파일

72. 일반 복사과정과 디스크 이미징의 차이점에 대하여 설명한 것으로 옳지 않은 것은?

		디스크 복사	디스크 이미징
가.	저장 방식	디스크 내부의 파일들을 읽어서 순차적으로 복사를 실시	디스크의 첫번째 위치에서부터 끝까지 복사를 실시
나.	저장 대상	디스크의 모든 물리적 섹터	파일과 디렉터리 단위의 정보
다.	정보 손실	시스템파일, 사용중인 파일은 내용을 읽을 수 없으므로 복사가 실패	하드웨어의 물리적 오류를 제외하고 디스크의 모든 정보를 복사
라.	파일 복구	삭제파일의 정보를 수집하지 않음	디스크 섹터의 삭제파일 정보가 남아 있는 경우 복구가능

73. 다음 중 압수·수색의 집행에 관한 설명으로 옳지 않은 것은? (다툼이 있으면 판례에 의함)

가. 압수물 목록은 원칙적으로 압수직후 현장에서 바로 작성하여 교부해야 한다.
나. 압수·수색영장을 한번 제시하고 집행을 마친 것이라면 유효기간 중이라도 동일한 장소, 목적물에 대해서는 재차 집행할 수 없다.
다. 적법한 보관자가 아닌 자로부터 임의제출 받은 물건을 영장 없이 압수한 경우 그 압수물은 위법이라도 그 압수물을 촬영한 사진은 상당한 방법으로 촬영한 것이라면 유죄 인정의 증거로 사용할 수 있다.
라. 영장의 제시는 수색의 착수 전에 이루어져야 하며, 피처분자 개인에게도 제시되어야 한다.

74. 임의수사에 관한 다음 설명 중 옳지 않은 것은? (다툼이 있으면 판례에 의함)

가. 피의자가 몽고사람이라면 원활한 의사소통을 위해 필요하다고 판단되는 경우에 직권 또는 피의자의 신청에 따라 피의자와 신뢰 관계있는 자를 동석하게 할 수 있다.
나. 동석한 사람이 피의자를 대신하여 진술한 부분이 조서에 기재되어 있다면 그 부분은 피의자의 진술을 기재한 것이 아니므로 그 자체로는 증거능력이 없다.
다. 범죄의 성질·태양으로 보아 긴급하게 증거보전을 할 필요가 있는 상태에서 일반적으로 허용되는 한도를 넘지 않는 상당한 방법에 의한 증거수집은 허용된다.
라. 제한속도 위반이 많은 장소에서 무인카메라를 설치하고 속도 위반차량의 차량번호 등에 대한 사진채집 활동을 하는 것은 임의수사로서 허용된다.

75. 형사소송법상 증거보전에 관한 다음 설명 중 옳지 않은 것은? (다툼이 있으면 판례에 의함)

가. 증거보전절차에서 검사의 청구에 의하여 증인을 신문한 판사는 제척의 대상이 된다.
나. 증거보전의 청구권 자는 검사, 피의자, 피고인(공소제기 후 제1회 공판기일 전), 또는 변호인이므로 사법경찰관은 청구권이 인정되지 않는다.
다. 피고인과 필요적 공범관계에 있는 다른 공범에 대해서는 증인으로 신문할 수 있다.
라. 증인신문과정에서 피의자가 참여하여 반대신문한 피의자의 진술부분은 증거로서 사용할 수 없다.

76. 증거수집의 대상이 되는 시스템의 내용을 확인 하고자 할 때 얻을 수 있는 비휘발성 정보가 아닌 것은?

가. 클립보드의 내용
나. 레지스트리 정보
다. 이벤트 로그
라. 사용자 접속 등의 시스템로그

77. 압수·수색 현장에서 우연히 발견된 별건살인 범죄의 증거임이 명백한 물건에 대한 다음 조치 중 옳지 않은 것은?

가. 살인죄의 현행범으로 체포한 후 영장 없이 압수할 수 있다.
나. 살인죄의 범행 즉후임이 인정되는 경우에는 영장 없이 압수할 수 있다.
다. 피의자를 긴급체포 후 영장 없이 압수할 수 있다.
라. 보관자로부터 임의제출을 요구하고, 이를 거절한 경우 일단 사진을 촬영하여 이를 보존할 수 있다.

78. 압수조서에 대한 설명으로 옳지 않은 것은?

가. 증거물 또는 몰수할 물건을 압수하였을 때에는 조서를 작성하여야 한다.
나. 압수조서에는 품종, 외형상의 특징과 수량을 기재하여야 한다.
다. 조사 또는 처분의 연월일시와 장소를 기재하고 그 조사 또는 처분을 행한 자와 참여한 법원사무관 등이 기명날인 또는 서명하여야 한다.
라. 압수한 경우에는 압수조서를 작성하여 소유자·소지자·보관자 그리고 이에 준하는 자에게 교부하여야 한다.

79. 다음 중 증거물의 보관 방법에 대한 설명으로 옳지 않은 것은?

가. 휘발성 증거는 수집 후 해쉬값 등을 생성하고 문서로 출력하여 입회인의 확인을 받고 보관한다.
나. 하드디스크는 정전기 방지 등이 가능한 곳에 보관해야 한다.
다. 원본 하드디스크는 안전한 장소에 보관하고, 분석은 사본을 대상으로 해서 수행한다.
라. 수집 및 분석 작업 시 생성된 파일과 이미지 파일 등은 변경되거나 훼손되지 않도록 분석용 컴퓨터에 그대로 저장해 놓는다.

80. 증거에 관한 다음 설명 중 옳지 않은 것은? (다툼이 있으면 판례에 의함)

가. 적법한 절차에 따르지 않은 압수물은 원칙적으로 유죄의 증거로 삼을 수 없고, 예외적으로 유죄의 증거로 사용하기 위해서는 특별한 사정에 대해서 검사가 입증하여야 한다.
나. 상고심에서는 직권조사 또는 법령에 특정한 경우가 아닌 새로운 증거조사를 할 수 없다.
다. 당사자가 제출한 증거는 법정에서 증거조사절차를 거쳐야만 증거로 사용할 수 있다.
라. 피고인이나 변호인 측이 무죄에 관한 증거로 제출한 서증이라면 피고인 측의 동의로 간주되어 유죄의 증거로 삼을 수 있다.

81. 검찰은 컴퓨터 디스켓을 압수하여 그 출력물을 증거로 제출하였다. 다음 설명 중 옳지 않은 것은? (다툼이 있으면 판례에 의함)

가. 컴퓨터 디스켓에 들어 있는 문건이 증거로 사용되는 경우 위 컴퓨터 디스켓은 그 기재의 매체가 다를 뿐 실질에 있어서는 피고인 또는 피고인 아닌 자의 진술을 기재한 서류와 같다.
나. 압수 후의 보관 및 출력과정에 조작의 가능성이 있으며, 기본적으로 반대신문의 기회가 보장되지 않는 점 등에 비추어 그 기재내용의 진실성에 관하여는 전문법칙이 적용된다.
다. 사인이 수사를 받기 이전의 사적인 상황에서 작성한 것이라면 형소법 제313조 제1항에 의하여 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다.
라. 이적표현물을 컴퓨터 디스켓에 저장, 보관하는 방법으로 이적표현물을 소지한 행위 그 자체는 전문법칙의 적용을 받는 전문증거가 아니다.

82. 민사소송법상 문서에 관한 다음 설명 중 옳지 않은 것은?

가. 서증의 진정성립에 관하여 상대방이 부인하는 경우, 이에 대한 입증책임은 그 서증을 제출한 자에게 있다.
나. 당사자 또는 그 대리인이 고의나 중대한 과실로 진실에 어긋나게 문서의 진정을 다툰 때에는 법원은 과태료를 부과한다.
다. 문서가 외국어로 표기된 경우 이를 서증으로 제출할 때에는 그 번역문을 첨부하여야 한다.
라. 문서의 진정성립이 다투어지는 경우 당해 문서에 현출된 작성 명의인의 필적 또는 인영이 다른 문서의 필적 또는 인영과 동일한지 여부를 판단하기 위해서는 반드시 감정을 하여야 한다.

83. 통신비밀보호법상 범죄수사를 위한 통신제한조치에 대한 설명으로 옳지 않은 것은?

가. 통신제한조치는 형법상 모든 범죄들에 대해서 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있다.
나. 검사는 통신제한조치의 허가요건이 구비된 경우 군사법원을 포함한 법원에 대하여 각 피의자별 또는 각 피내사자별로 통신제한조치를 허가하여 줄 것을 청구할 수 있다.
다. 검사, 사법경찰관 또는 정보수사기관의 장은 특별히 긴급한 사유가 있는 때에는 법원의 허가 없이 통신제한조치를 할 수 있다.
라. 통신제한조치는 이를 청구 또는 신청한 검사·사법경찰관 또는 정보수사기관의 장이 집행한다. 이 경우 체신관서나 기타 통신기관등에 그 집행을 위탁하거나 집행에 관한 협조를 요청할 수 있다.

84. 다음 중 Encase에 대한 설명으로 옳지 않은 것은?

가. SafeBack이 그래픽 인터페이스를 제공해 주는 것에 반해 Encase는 DOS 기반의 프로그램을 제공해 준다.
나. 디스크에 있는 내용중 문서, zip으로 압축된 파일, 이메일 첨부파일은 자동으로 검색되고 분석된다. 조사를 하는 중에는 타임스탬프와 기타 데이터가 변경되지 않는다.
다. 조사를 하는 중에는 타임스탬프와 기타 데이터가 변경되지 않는다.
라. '미리보기' 모드에서 수사자는 널 모뎀 케이블 또는 이더넷 연결을 통해 다른 머신에서 원본 데이터를 볼 수 있다.

85. 다음 중 「통신비밀보호법」상의 전기통신사실에 관한 자료로서 '통신사실확인자료'에 해당하지 않는 것은?

가. 이용자의 성명, 이용자의 주민등록번호
나. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료
다. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료
라. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료

86. 다음 중 과학적 증거와 관련된 미국 판결에 대한 설명으로 옳지 않은 것은?

가. 미국의 Frye 판례 이론에 대하여 사이비 과학에 의한 오판 가능성을 높이고, 증거의 허용성이 지나치게 완화된다는 비판이 존재한다.
나. 미국의 Daubert 판결에서 과학적 증거의 허용성에 대하여 전문가 집단의 보편적 승인기준이 아닌, 판사로 하여금 과학적 증거의 신뢰성을 판단하도록 하였다.
다. 미국의 Frye 판례 이론에 대하여 빠르게 진화하는 정보기술 영역에 있어서 Frye 판결을 적용할 경우 디지털 증거의 보편적 승인을 받기란 거의 불가능에 가깝다는 비판이 존재한다.
라. 미국의 Daubert 판례 이론은 과학영역 뿐만 아니라 전문기술 영역의 증거에도 적용되며 범위가 확대되어 Kumho Tire Co. v. Charmichael 사건에도 적용되었다.

87. 디지털 포렌식 조사의 일반원칙으로 옳지 않은 것은?

가. 정당성의 원칙
나. 신속성의 원칙
다. 이동성의 원칙
라. 연계보관성의 원칙

88. 다음 중 통신비밀보호법에서 금지하고 있는 행위로 옳은 것은? (다툼이 있으면 판례에 의함)

가. 시사 월간지 기자가 과거 국가안전기획부 직원들이 불법적으로 도청, 제작한 녹취록과 녹취보고서의 내용 전문을 월간지에 게재한 행위
나. 3인 간의 대화에 있어서 그 중 한 사람이 그 대화를 녹음하는 행위
다. 골프장 운영업체가 예약전용 전화선에 녹취시스템을 설치하여 예약담당직원과 고객 간의 골프장 예약에 관한 통화내용을 녹취한 행위
라. 음식점에 도청마이크를 설치하여 타인간의 대화를 녹음하려 시도하거나 청취한 행위

89. 다음 중 디지털증거의 특성으로 옳지 않은 것은?

가. 매체독립성 : 디지털증거는 매체와 독립된 혹은 중립된 정보 내용이 증거로 되는 경우이며 이 정보는 값이 같다면 어느 매체에 저장되어 있든지 동일한 가치를 지닌다.

나. 비가시성·비가독성 : 디지털증거의 경우 하드디스크를 제시하는 것만으로 증거가 되는 내용을 인지할 수 없고, 모니터상에 나타내거나 인쇄기를 통해 인쇄되어 제시되었을 때 비로소 가시성·가독성이 주어진다.

다. 조작곤란성 : 디지털증거는 위·변조 및 삭제가 어렵다.

라. 대량성 : 최근 저장기술의 발달로 아주 작은 저장매체에도 방대한 분량의 정보를 저장할 수 있다.

90. UNIX 계열의 로그에 대한 설명으로 옳지 않은 것은?

가. wtmp - 사용자들의 로그인-아웃 정보를 갖고 있음

나. sulog - 날짜/시간, 성공/실패, 사용한 터미널 등의 정보를 갖고 있음

다. syslog - 보안 사고가 발생한 경우 최후 분석을 하는 경우가 많음

라. acct - 시스템에 들어온 사용자가 어떤 명령을 수행하였는지 확인할 수 있음

91. 대검찰청 디지털 증거 수집 및 분석 규정(대검예규)에 따를 경우, 다음 중 컴퓨터 등 정보처리시스템의 압수·수색에 관한 진술로 옳지 않은 것은?

가. 컴퓨터 등 정보처리시스템을 압수할 경우에는 가능하면 정보처리시스템으로부터 저장매체만을 분리하여 압수하는 것을 원칙으로 한다.

나. 저장매체를 분리할 경우 수사목적을 달성할 수 없거나 기기 또는 디지털 자료가 손상, 훼손될 우려가 있더라도 정보처리시스템 전부를 압수할 수 없다.

다. 압수·수색·검증의 현장에서는 전산관리자 또는 책임자를 통하여 대상 정보처리시스템의 구성 및 주변장치의 연결 상태 등을 파악하고 특별한 사정이 없는 한 이를 촬영한 후 특이사항을 기록하여야 한다.

라. 정보처리시스템을 압수·수색·검증할 경우에는 대상 정보처리시스템의 설정시간을 한국 표준시간과 비교하여 기록하여야 한다.

92. 다음 설명 중 옳지 않은 것은?

가. ProDiscover는 Technology Pathways 포렌식 팀에서 만든 프로그램으로 비트스트림 사본의 생성이 가능하다.

나. Guidance Software社의 EnCase V6는 데이터 획득, 데이터 분석, 분석 결과 기록이 가능한 디지털포렌식 프로그램이다.

다. FTK 2는 ACCESS DATA社의 디지털포렌식 프로그램으로 FAT, NTFS의 분석이 가능하다.

라. EnCase V6는 Dongle이라는 USB 인증키가 없으면 하드디스크의 파일시스템 에 의한 내부 디렉토리 구조까지만 볼 수 있다.

93. 다음 중 증거의 종류에 대한 설명으로 옳지 않은 것은?

가. 피고인의 자백, 피고인의 옷에 묻은 피해자의 혈흔은 직접 증거이다.

나. 범행에 사용된 흉기, 절도죄의 장물은 물적 증거이다.

다. 상해죄의 동시범의 특례에서 피고인이 제출하는 것이 본증이 된다.

라. 보조증거에는 보강증거와 탄핵증거가 있다.

94. 활성데이터(Live Data)수집과 분석기술에 대한 내용으로 옳지 않은 것은?

가. 활성상태에서만 획득할 수 있는 휘발성 정보를 활성데이터라 한다.

나. 활성데이터는 주로 시스템의 상태를 나타냄으로써 동작현황을 파악할 수 있는 명령어를 사용하여 수집한다.

다. 디지털 증거수집 담당자의 조작실수나 누락으로 중요 정보를 취득하지 못하거나 원본증거를 변조시킬 위험성이 있다.

라. Forensic Script의 형식은 순차적 자동실행을 위해 정해진 형식에 따라 수행하여야 한다.

95. 다음 중 당연히 증거능력이 있는 서류에 해당하지 않는 것은? (다툼이 있으면 판례에 의함)

가. 공소장
나. 다른 사건의 공판조서
다. 외국공무원이 직무상 작성한 문서
라. 세관공무원의 시가감정서

96. 다음 중 대검찰청 디지털 증거 수집 및 분석 규정(대검예규)에 따를 경우, 디지털 기기의 압수 · 수색 시 유의해야 할 사항으로 옳지 않은 것은?

가. 대상 정보처리시스템으로부터 사용자를 격리하여 시스템 강제종료 등 임의적인 조작행위를 방지하여야 한다.
나. 압수 · 수색 · 검증 대상 정보처리시스템이 네트워크에 연결되어 있고 압수 · 수색대상자가 네트워크로 접속하여 저장된 자료를 임의로 삭제할 우려가 있을 경우에는 네트워크 연결 케이블을 차단하여야 한다.
다. 대상 정보처리시스템내의 링크파일의 등록정보를 확인하는 등으로 휴대용 디지털 저장매체의 사용여부를 확인하고 그 사용 흔적이 발견된 경우에는 해당기기의 식별 값(Volume Serial Number)을 특정하고 이를 압수할 수 있도록 현장에서 적절한 조치를 취하여야 한다.
라. 디지털기기를 압수 · 수색 · 검증하거나 디지털 자료를 수집하는 현장에서 분석을 실시하는 경우에는 쓰기방지장치의 사용 없이 신속하게 자료를 수집하여야 한다.

97. 다음 중 정보통신망법 이용촉진 및 정보보호 등에 관한 법률에서 금지하고 있는 행위가 아닌 것은? (다툼이 있으면 판례에 의함)

가. 투자금 반환과 관련하여 채권자로부터 지속적인 변제독촉을 받아오던 채무자가 채권자의 핸드폰으로 하루 간격으로 2번 문자메시지를 발송한 행위
나. 자신의 뇌물수수 혐의에 대한 결백을 주장하기 위하여 제3자로부터 사건 관련자들이 주고받은 이메일 출력물을 교부받아 징계위원회에 제출한 행위
다. 은행의 정보통신망에 의하여 보관되고 있는 특성사고 사망자의 주민등록번호를 누설한 행위
라. 법인의 정보통신망에 보관중인 타인의 급여명세서를 열람 및 출력하여 소송계속중인 사건에 증거자료로 제출하는 행위

98. EnCase에서 파티션 복구에 대한 설명으로 옳지 않은 것은?

가. 하드 드라이브를 포맷하고 FDISK를 실행하더라도 데이터는 실제로 삭제되지 않는다.
나. 포맷은 디스크에서 폴더 및 파일의 위치를 나타내는 구조, 데이터를 완전히 초기화 한다.
다. FDISK가 실행된 드라이브는 논리적 볼륨 정보를 표시하지 않으며, 드라이브 전체가 테이블에 미사용 디스크 영역으로 표시된다.
라. EnCase 애플리케이션은 파티션 정보 및 디렉토리와 폴더 구조를 모두 재구성할 수 있다.

99. 다음 중 디지털 포렌식이 필요한 경우로 옳지 않은 것은?

가. 甲은 야간에 버스 안에서 휴대폰 카메라로 옆 좌석에 앉은 여성(18세)의 치마 밑으로 드러난 허벅다리 부분을 촬영하였다.
나. 乙은 특정 회사가 제공하는 게임사이트에서 사설 프로그램('한도우미 프로그램')을 이용하여 약관상 양도가 금지되는 포커머니를 약속된 상대방에게 이전해 주었다.
다. 丙은 야간에 까페에 침입하여 그 곳 내실에 놓여 있던 꺼진 노트북 한 대를 들고 나왔다.
라. 전산시스템에서 관리하고 있던 데이터가 압수될 상황에 이르게 되자 직원 丁은 특정 기간의 데이터를 삭제하였다.

100. 다음 중 압수 · 수색 현장의 조치에 대한 설명으로 옳지 않은 것은?

가. 영장제시 - 현장수사를 지휘하는 책임자는 관계 임원이나 관리자에게 영장을 제시하고 압수 · 수색의 이유와 함께 협조를 구한다.
나. 현장통제 - 현장의 수사관은 전체 조직도, 직원 명부 등을 활용하여 압수 · 수색의 범위를 정한 후 불필요한 사람을 격리시킨다.
다. 현장분석 - 사무실 구조와 전산 시스템의 상태를 검사하여 현장에서 필요한 정보의 추출 및 분석이 필요한지 확인한다.
라. 네트워크 통제 - 네트워크를 통하여 데이터의 삭제 가능성이 있을 경우 네트워크를 부분 차단한다.

2011년 제 2회 디지털포렌식 전문가 2급 필기 답안

컴퓨터구조와 디지털저장매체	
NO.	답
1	라
2	가
3	라
4	다
5	나
6	다
7	다
8	라
9	다
10	라
11	다
12	라
13	가
14	라
15	다

파일시스템과 운영체제	
NO.	답
16	다
17	나
18	라
19	라
20	가
21	라
22	나
23	다
24	다
25	나
26	가
27	라
28	라
29	다
30	라

응용 프로그램과 네트워크의 이해	
NO	답
31	가
32	나
33	라
34	나
35	다
36	가
37	가
38	라
39	다
40	다
41	가
42	나
43	다
44	다
45	나

데이터베이스	
NO.	답
46	나
47	다
48	라
49	나
50	라
51	다
52	다
53	다
54	가
55	나
56	라
57	라
58	가
59	나
60	라

디지털포렌식 개론	
NO.	답
61	다
62	라
63	다
64	나
65	나
66	다
67	라
68	다
69	다
70	라
71	가
72	나
73	다
74	나
75	가

디지털포렌식 개론	
NO.	답
76	가
77	가
78	라
79	라
80	라
81	라
82	라
83	가
84	가
85	가
86	가
87	다
88	라
89	다
90	다

디지털포렌식 개론	
NO.	답
91	나
92	라
93	가
94	라
95	가
96	라
97	가
98	나
99	다
100	라