제 1과목 컴퓨터 구조와 디지털 저장매체

제 1과목

컴퓨터 구조와 디지털 저장매체

문제

1. 　　중 하드디스크 복구와 관련 없는 용어는? (3회 출제)

가. disk partition

나. file system

다. master boot record

라. RISC

정답 : 라
CPU 설계 종류
RISC (Reduced Instruction Set Computer)

2. 다음 프리커(phreaker)에 대한 설명으로 옳지 않은 것은? (1회 출제)

가. 스튜어드 넬슨은 MIT에서 장거리 전화를 무료로 쓸 수 있는 톤을 생성하는 방법을 알아냈다.

나. 존 드레이퍼는 장난감 호루라기를 불면 2600Hz의 신호가 나오는데 그 신호로 AT&T의 장거리 전화를 걸 수 있다는 사실을 확인했다.

다. 2600 Magazine은 2600Hz 전화 프리킹 주파수에서 유래했다.

라. 스티브 잡스는 드레이퍼 밑에서 일하면서 블루박스를 생산·판매했다.

정답 : 라
애플을 창업한 스티브 잡스와 스티브 워즈니악은 1970년대 초에 블루 박스를 만들어 팔았다고 한다. 단, 워즈니악이 스티브 잡스를 만나기 전에 Draper 밑에서 일했다.

3. 멀티 프로그래밍에서 각 프로그램을 메모리의 한정된 구역에 제한시키는 작업은 무엇인가?

가. 가상기억장치(Virtual Storage)

나. 메모리 보호(Memory Protection)

다. 인터럽팅(Interrupting)

라. 시분할(Time-sharing)

정답 : 나
메모리 보호는 컴퓨터 메모리의 사용을 제어하는 방법이며 모든 운영 체제에서 중요한 쟁점사항 중 하나이다. 운영 체제에서 실행하고 있는 프로세스가 자신에게 할당되지 않은 영역의 메모리에 접근하는 것을 막는 것이 메모리 보호의 주된 목적이다. 이를 통해 프로세스 내의 버그가 다른 프로세스의 동작에 영향을 미치는 것을 예방하며 악성 소프트웨어가 시스템에서 허가되지 않은 접근권한을 갖고 시스템에 영향을 끼치는 것을 막아준다.

4. 컴퓨터들은 처리 속도를 높이기 위한 기법의 하나로 메모리 액세스 시간을 단축하고자 캐시(cache) 메모리를 둔다. 다음 중 캐시 메모리에 저장되어 있는 내용을 가져와서 액세스가 이루어지는 것을 의미하는 것은? (1회 출제)

가. 캐시 미스(cache miss)
나. 캐시 히트(cache hit)
다. 가상 메모리(virtual memory)
라. 병렬처리(parallel processing)

정답 : 나
성공할 경우 캐시 히트, 실패할 경우 캐시 미스라 한다.
[디지털 논리와 설계, Moris Mano, 강철희 등 역, p.621]

5. 메모리 중 RAM과 프로세서 사이에 위치하며 프로세서가 데이터를 찾을 경우, 제일 먼저 찾는 메모리는?

가. 하드디스크
나. L1 캐시 메모리
다. L2 캐시 메모리
라. EPROM

정답 : 나
사이버범죄 소탕작전 컴퓨터
포렌식 핸드북 P156

6. 다음 프로그램 상태 중 다중 쓰레드 프로세스의 쓰레드들 사이에 공유되는 것은?

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

정답 : 나
쓰레드와 프로세스의 차이점중 하나는 쓰레드는 프로세스와 달리 공유되는 메모리 공간을 가지고 있다는 것이다.
이것은 장점인 동시에 단점도 될 수 있다. 왜냐하면 메모리 공간을 쓰레드끼리 공유한다는 의미는 쓰레들간 통신을 하기에는 쉬우나, 쓰레드들이 동시에 메모리에 접근했을 때는 문제를 일으킬수도 있다는 의미가 된다.
결국 프로세스기반으로 프로그래밍하는 것보다도 많은 주의를 기울여야 한다.

7. 다음 중 인터럽트의 설명으로 옳지 않은 것은? (3회 출제)

가. 인터럽트를 확인 할 수 있는 플래그(flag)가 있다.
나. 인터럽트 벡터를 사용한다.
다. 인터럽트를 처리하는 전용 서비스루틴을 만들어 놓아야 한다.
라. 인터럽트가 걸리면 무조건 처리해야 한다.

정답 : 라
상황에 따라 인터럽트를 무시할 수도 있다.(디지털 포렌식 검정시험 교재 5쪽)

8. 영문자, 숫자, 특수문자 등은 크기가 얼마인 코드로 표시되는가?

가. 1 bit

나. 1 byte

다. 1 kilo byte

라. 1 mega byte

정답 : 나
최신 컴퓨터 개론 P108
컴퓨터 동작 원리 P22

9. "A"에 대한 ASCII 이진표현이 "01000001"일 때, "01000111"은 어떤 문제에 대한 ASCII 이진표현인가?

가. "D"

나. "G"

다. "b"

라. "f"

정답 : 나
"A"의 6번째 뒤 문자는 "G"이다.

10. 다음 중 ASCII 코드에 대한 설명으로 옳지 않은 것은?

가. American Standard Code for Information Interchange를 의미하며, 2진 코드이다.

나. 영어 대문자와 소문자를 표시할 수 있다.

다. 패리티비트를 포함한다.

라. 제어문자를 포함한다.

정답 : 다
ASCII 코드는 1967년에 표준으로 제정되어 1986년에 마지막으로 개정되었다. ASCII는 7비트 인코딩으로, 33개의 출력 불가능한 제어 문자들과 공백을 비롯한 95개의 출력 가능한 문자들로 이루어진다. 제어 문자들은 역사적인 이유로 남아 있으며 대부분은 더 이상 사용되지 않는다. 출력 가능한 문자들은 52개의 영문 알파벳 대소문자와, 10개의 숫자, 32개의 특수 문자, 그리고 하나의 공백 문자로 이루어지고, 패리티비트는 포함되지 않는다.

11. 다음 중 다수의 사용자가 서로 다른 작업을 처리하기 위해서 디스크 입출력을 요구할 때 좀 더 효율적으로 요청을 처리하기 위한 디스크 스케줄링 기법으로 옳지 않은 것은? (1회 출제)

가. FCFS

나. SSTF

다. SCAN

라. LRU

정답 : 라
Least Recently Used로 가상 메모리의 페이지 교체 알고리즘으로 가장 오랫동안 참조되지 않았던 페이지를 교체하는 알고리즘

12. 다음 중 하드디스크 여러 개를 동시에 연결하여 동일한 데이터를 다른 위치에 중복하여 저장하는 것을 무엇이라 하는가? (2회 출제)

가. 백업(backup)

나. RAID(redundant array of independent disks)

다. 버퍼(buffer)

. 불량섹터(bad sector)

정답 : 나
하드디스크 포맷+복구 (리트머스(김기만)저, 영진닷컴, 2004), 20 ~ 21쪽

13. 디스크에 지정된 데이터를 찾는 데 걸리는 시간을 무엇이라 하는가?
    가. 접근시간
    나. 직접시간
    다. 데이터 전송시간
    라. 실린더 시간

정답 : 가
최신 컴퓨터 개론 P187

14. 다음 중 USB 드라이브로 많이 쓰이는 플래시 메모리에 대한 설명으로 옳지 않은 것은? (2회 출제)
    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.

정답 : 라
플래시 메모리는 램 대용으로 사용할 수없다. 비록 플래시 메모리가 램처럼 읽고 쓰는 일이 가능한 구조를 채택하고 있지만, 데이터를 써넣기 위해서는 시간이 상당히 오래 걸리는 구조를 가지고 있으며, 램처럼 쉽게 설계할 수 없기 때문이다.

15. 비휘발성 메모리를 뜻하는 것은 어느 것인가?
    가. 전원공급이 끊어져도 데이터를 계속 기억하는 기억장치
    나. 전원이 공급되는 동안만 데이터를 기억하는 기억장치
    다. 프로그램이 실행에 필요한 데이터 저장소
    라. 실행중인 프로그램을 저장하는 메모리

정답 : 가
비휘발성 메모리는 전원공급이 끊어져도 데이터를 계속 기억하는 기억장치이다.

제 2과목 파일시스템과 운영체제

제 2과목

파일시스템과 운영체제

문제

1. 작업 스케줄링 등에 응용되는 것으로 가장 적합한 자료구조는?

가. 스택(Stack)

나. 큐(Queue)

다. 그래프(graph)

라. 트리(Tree)

정답 : 나
큐는 FIFO(First-In-First-Out) 특성을 가지며 가장 먼저 자원을 요청한 작업에게 우선적으로 서비스를 제공하는 스케쥴링에 사용되는 자료 구조이다.

2. 디스크에서 원하는 데이터 블록(block)을 찾아서 주기억 장치의 버퍼(buffer)로 가져오는데 소요되는 전체 시간은 다음의 시간들을 합한 시간이다.

- 탐구시간(seek time : s)
- 회전지연 시간(rotational delay : r)
- 전송 시간(transfer time : t)

위의 시간들 중 오래 걸리는 것에서 적게 걸리는 순서대로 나열한 것은?

가. s > t > r

나. s > r > t

다. r > s > t

라. r > t > s

정답 : 나
디스크 접근 시간은 우선 원하는 트랙을 먼저 찾아야 하고, 다음에 원하는 블록을 찾은 후 이 블록을 버퍼로 전송하는 시간의 합니다. 여기서 각각을 탐구 시간, 회전 지연 시간, 전송 시간이라 한다. 여기서 원하는 트랙을 찾기 위해서는 디스크 헤드가 이동해야 한다. 따라서 일반적으로 탐구 시간이 가장 오래 걸리며, 이는 회전 지연 시간과 전송 시간을 합한 시간보다 더 크다.

3. 리눅스에서 파일 시스템관리 설명 중 잘못된 것은? (3회 출제)

가. sticky bit는 모든 사용자가 쓰고 삭제할 수 있는 디렉터리에 적용한다.

나. SetGID와 SetUID는 파일을 실행할 때 그 파일의 소유자 또는 그룹의 권한으로 실행하도록 하는 것이다.

다. ls의 실행 허가권은 기본 755이다.

라. /usr/bin 디렉터리는 시스템 바이너리 디렉터리이다.

정답 : 라
/usr/bin은 압축파일, 네트워크 실행파일, 자료 전송 파일등이 저장되어있다.

4. Linux 보안을 위하여 다양한 도구를 제공하고 있다. 이에 대한 설명으로 옳지 않은 것은?

가. Shadow password : /etc/passwd에서 password를 제거하고 /etc/shadow 파일에 암호화된 형태로 password를 저장한다.

나. md5sum : 파일을 암호화하고 이 파일에 대한 hash값을 생성하여 보안성, 일관성을 향상시켜 준다.

다. tripwire : 파일에 대한 변경 여부를 알 수 있도록 한다.

라. lsof : 프로세스에 의해서 열린 파일 핸들의 목록을 보여준다.

정답 : 나
md5sum은 파일에 대한 hash값을 생성하거나 변경되지 않았는지를 검증하는 도구로 사용되며 암호화 기능은 제공하지 않는다.

5. 다음 중 리눅스의 보안 프로그램에 대한 설명으로 옳지 않은 것은? (1회 출제)

가. Snort는 오픈소스 방화벽으로 실시간 트레픽 분석을 시행하며 서로 다른 수많은 공격자로부터 오는 공격을 막을 수 있다.

나. Wireshark는 패킷 스니퍼링과 프로토콜 분석 도구이다.

다. Nmap은 오픈소스로 사용하기 용이하며, 가벼운 포트 스캐너 및 네트워크 분석 도구의 역할을 할 수 있는 프로그램이다.

라. Netcat은 포트 스캔, 파일 전송, 커맨드 라인에서의 원격 네트워크 서비스와 상호작용 등 광범위한 용도를 위해 사용 될 수 있다.

정답 : 가
Snort는 오픈소스 침입 탐지 및 방지 시스템이다.

6. windows 2003 Server에서 파일을 복사하거나 이동할 때 NTFS 권한의 변화에 대한 설명으로 옳지 않은 것은?

가. 동일한 NTFS 파티션에서 파일을 복사할 경우 대상 폴더의 권한을 상속받는다.

나. 동일한 NTFS 파티션에서 파일을 이동할 경우 대상 폴더의 권한을 상속받는다.

다. 서로 다른 NTFS 파티션에서 파일을 복사할 경우 대상 폴더의 권한을 상속받는다.

라. 서로 다른 NTFS 파티션에서 파일을 이동할 경우 대상 폴더의 권한을 상속받는

정답 : 나
동일한 NTFS 파티션에서 파일을 이동할 경우 원본 파일의 권한을 그대로 유지한다.

7. 다음 프로그램 상태 중 다중 쓰레드 프로세스의 쓰레드들 사이에 공유되는 것은?

가. 레지스터 값들

. 힙메모리

다. 전역 변수들

라. 스택 메모리

정답 : 다
쓰레드는 같은 프로세스에 속한 다른 쓰레드와 코드, 데이터 섹션 그리고, 열린 파일이나 신호와 같은 운영체제 자원들을 공유한다.

8. 다음은 Windows Server 2008에서 사용하는 파일 및 폴더의 사용 권한에 대한 설명으로 옳지 않은 것은? (2회 출제)

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.

[정답] 나
사용자 권한은 속한 그룹 구성원의 모든 권한의 합계에 기반 한다.
[Windows Server 2008 실전가이드, p610]

9. Windows에서 프로그램이 실행되어 그 실행코드와 관련 데이터들이 Memory에 저장된다. Process의 정보가 저장되는 Memory의 EPROCESS Block에 대한 설명으로 옳지 않은 것은?

가. 해당 Process에 관련된 Thread Block를 포함하고 있다.

나. EPROCESS Block의 Size는 Windows 버전, SP 버전 별로 다를 수 있다.

다. 하나의 EPROCESS Block은 하나의 Process 관련 정보만을 포함하고 있다.

라. EPROCESS Block들은 서로 Double Linked List로 연결되어 있는데, 이 특성을 이용한 Process Hiding 기법으로 DKOM(Direct Kernel Object Manipulation)을 들 수 있다.

정답 : 가
EProcess Block은 Thread 정보를 저장하고 있는 EThread Bock에 대한 Pointer만을 가지고 있다.

10. Windows의 Exception에 대한 설명으로 옳지 않은 것은?

가. Interrupt와 다르게 Exception은 어떠한 시간에도 발생할 수 있다.

나. Windows에서는 Exception이 발생했을 때 Application이 제어권을 획득할 수 있도록 하기 위하여 Structured Exception Handling이라는 메커니즘을 사용한다.

다. Termination Handling은 어떠한 코드가 실행된 후 반드시 실행되도록 하는 기능을 제공한다.

라. Vectored Exception Handling은 Structured Exception Handling 보다 향상된 메커니즘을 제공하는 Frame-based Exception Handling이다.

정답 : 라
Vectored Exception Handling은 Frame-based exception handling이 아니다.
(http://msdn.microsoft.com/en-us/library/ms681420(v=VS.85).aspx 참조)

11. 　　중 Active Directory에 대한 설명으로 옳지 않은 것은?

가. 네트워크상에 존재하는 모든 Resources를 식별하고 사용자와 응용프로그램에 Resources에 대한 정보를 제공하는 네트워크 서비스이다.

나. Active Directory 관리자는 중앙 관리 인터페이스를 통하여 네트워크 서비스, 분산된 Desktop, 응용프로그램들을 관리할 수 있다.

다. Active Directory는 네트워크에 연결된 Resources에 대하여 Single Sign-on을 제공한다.

라. Windows 2003 Server의 Active Directory에는 객체들을 체계화하고 그룹화하기 위해서 Organization Unit을 사용한다. 즉, 다양한 Domain에서 동일한 목적을 갖는 객체들을 묶어 그룹화하는 기능으로 이용된다.

정답 : 라
Organization Unit은 다른 Domain의 객체를 포함시킬 수 없다.
(http://technet.microsoft.com/en-us/library/cc758565(WS10).aspx 참조)

12. 리눅스 시스템에서 사용하는 로그 파일에 대한 내용으로 옳지 않은 것은? (2회 출제)

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.

[정답] 다
secure 파일은 Telnet, FTP, 원격접속 등 인증과정을 거치는 모든 로그를 저장한다.
[한빛미디어, 정보보안 개론과 실습, pp501]

13. 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

정답 : 다
계층형 구조는 루트 디렉토리 밑에 여러 개의 하부 디렉토리를 갖는 트리 형태를 갖으며, UNIX와 Window 운영체제 등이 이 구조에 속한다.

14. HDD 내부에 플래쉬 메모리를 내장한 Hybrid HDD(Flash Memory + HDD)는 운영체제가 부팅될 때 빠른 처리를 위해 부팅관련 데이터를 Hybrid HDD의 Flash Memory 영역에 별도로 저장하고 HDD를 읽고 쓰는 Cache로 이용되도록 하는 Windows Vista 등에서 제공되는 기술은?

가. ReadyDrive

나. ReadyBoot

다. SuperFetch

. BitLocker

정답 : 가
ReadyBoot는 USB 플래시 드라이브와 같은 메모리 장치의 메모리를 사용할 수 있는 기능을 제공한다. SuperFetch는 지능적 메모리 관리를 통해 데이터에 신속하게 액세스할 수 있도록 한다. BitLocker는 드라이브 암호화 기능을 제공한다. ReadyDrive는 혼성 장치의 핵심인 비휘발성 캐시를 능동적으로 관리하여 혼성 하드 디스크 드라이브의 추가 기능을 제공한다.

15. Windows 운영체제에 있어 공유 메모리 기능과 유사한 기능을 수행하려 한다. 이때 사용할 수 있는 Windows 운영체제의 기능은 무엇인지 선택하시오. (3회 출제)

가. Memory-mapped I/O

나. Semaphore

다. Shared Socket

라. Named PIPE

정답 : 가
Windows에서는 파일을 가상 메모리 공간에 mapping하여 두고, 이를 다른 프로세스 간에 공유할 수 있음.
memory-mapped I/O 소개
(http://en.wikipedia.org/wiki/Memory-mapped_I/O)

제 3과목 응용프로그램과 네트워크의 이해

제 3과목

응용프로그램과 네트워크의 이해

문제

1. 증거 수집 방법 중 시간확인 작업 시 중요도가 가장 낮은 항목은? (2회 출제)

가. 점검 시간 (Checked Time)

나. 변경 시간 (Modified Time)

다. 접근 시간 (Accessed Time)

라. 생성 시간 (Created Time)

[정답] 가
인사이드 윈도우포렌식,할렌카비(저),정상민·정명주(번역) p.285 MAC시간 참조

2. 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

정답 : 가
인사이드 윈도우포렌식, 할렌카비(저), 정상민·정명주(번역)
p.29 netstat에 관한 설명 참고

3. 다음과 같은 특징을 갖는 LAN 토폴로지는?

- 고장 발견이 쉽고 유지 보수가 용이하다
- 한 호스트의 고장이 전체 네트워크에 영향을 미치지 않는다.
- 호스트의 숫자가 늘어날수록 설치비용이 크게 증가한다.
- 중앙 제어 장치가 고장이 나면 전체 네트워크가 작동하지 않는다.

가. 버스형

나. 링형

다. 트리형

라. 성형

정답 : 라
성형은 중앙에 다른 호스트들이 1:1로 연결된 형태로 다른 호스트들의 고장이 네트워크에 영향을 주지 않지만 중앙 제어장치의 고장은 모든 네트워크에 영향을 주게 되며, 호스트의 숫자가 늘어날수록 설치비용이 크게 증가한다.
(컴퓨터 네트워트, 정진욱,김현철,안성진,조강홍, 22p)

4. 방화벽(Firewall)에 대한 설명으로 옳지 않은 것은? (2회 출제)

- 비트 스트림을 프레임이라는 데이터 단위로 나눈다.
- 송신자와 수신자의 물리 주소를 지정한다.
- 흐름제어와 오류제어를 한다.

. 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.

[정답] 다
베스천 호스트는 보호하고자 하는 네트워크의 외부에 존재한다.(TCP/IP와 인터넷, 정진욱, 김현철, 446~448p)

5. 마이크로소프트 아웃룩에서 전자우편을 복구할 때 사용되는 파일은? (1회 출제)

가. Outlook.bak

나. Outlook.dat

다. Outlook.nk2

라. Outlook.pst

정답 : 라
아웃룩 매뉴얼 참고
.dat 파일은 명령 모음 및 메뉴 사용자 지정 파일

6. 인터넷에서 사용되는 TCP/IP 프로토콜에서 네트워크 계층의 프로토콜에 해당하지 않는 것은?

가. IP

나. ICMP

다. IGMP

라. SCTP

정답 : 라
SCTP는 전송계층에서 사용하는 프로토콜이다.
(데이터 통신과 네트워크, Forouzan, 41p)

7. 다음과 같은 특징을 가진 기술로 가장 적절한 것은?

- 10m 이내의 PC주변기기, 헤드셋, 홈 네트워크 등에 사용될 수 있다.
- 피코넷(piconet)이라는 네트워크를 만든다.
- 2.4GHz에서 1MHz 사이를 1초에 1600번 바꾸어 가며 주파수 도약한다.
- 신호 변조 방법으로는 GFSK를 사용하고 TDD방식으로 데이터를 송수신한다.

가. Bluetooth

나. HSDPA

다. UWB

라. ZigBee

정답 : 가
블루투스는 10m 이내의 휴대폰, PDA, 노트북과 같은 휴대용 무선 연결을 위한 기술 규격으로 2.4GHz의 비인가 주파수 대역에서 1MHz 대역폭의 채널 79개를 1초에 1600번 바꾸어 가며 송수신하는 주파수 도약 방법을 사용한다. 신호 변조방법으로는 GFSK(Gausisan Frequency Shift Kyeing)를 사용하고, 슬롯화 된 TDD(Time Division Duplex) 방식으로 데이터를 송수신한다.
(데이터 통신과 네트워크, Forouzan, 661p)

8. IPv6 특징에 대한 설명으로 옳지 않은 것은?

가. IPv4의 주소 고갈 문제 해결을 위해 IETF에서 표준화 하였다.

나. 128비트의 주소 공간을 갖는다.

다. 유니캐스트, 멀티캐스트, 브로드 캐스트 주소를 갖는다.

라. 기존의 IPv4와의 호환을 위해 이중스택을 사용할 수 있다.

정답 : 다
IPv6는 유니캐스트, 멀티캐스트, 애니캐스트의 주소를 갖는다.
(컴퓨터 네트워트, 정진욱, 김현철, 안성진, 조강홍, 404p)

9. IDS(Intrusion Detection System)의 특징으로 옳지 않은 것은 ?

가. IDS는 외부의 공격을 탐지하는 데는 효과적이지만 내부의 공격에는 취약하다.

나. IP를 구별하지 않고 모든 패킷에 대한 검사를 수행하므로 더욱 안전한 보안 기능을 제공한다.

다. 탐지 기법으로는 오용기반 (misuse-based) 탐지와 이상기반 (anomaly-based)탐지로 나눌 수 있다.

라. HIDS는 호스트의 보안 감시로그, 시스템 로그, 사용자 계정 정보 등을 이용하여 침입을 탐지하는 시스템이다.

정답 : 가
IDS는 모든 패킷을 검사하기 때문에 내부의 공격도 감지 할 수 있는 특징을 가지고 있다.

10. 호스트의 IPv4 주소는 10.12.14.46이고 서브넷 마스크는 255.255.255.240 일 때 네트워크 주소로 옳은 것은 ? (1회 출제)

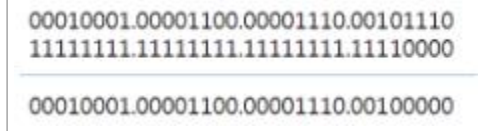
가. 10.12.14.0

나. 10.12.14.32

다. 10.12.14.48

라. 10.12.14.128

정답 : 나
10.12.14.46과 255.255.255.240을 2 진수로 바꾸어 &연산을 하면 아래와 같다



결과를 10진수로 바꾸면 10.12.14.32이다
(데이터 통신과 네트워크, Forouzan, 556p)

11. TCP는 흐름제어를 위해 슬라이딩 윈도우를 사용한다. TCP에서 사용하는 슬라이딩 윈도우에 대한 설명으로 옳지 않은 것은?

가. 윈도우는 윈도우 크기 필드를 이용하여 지정할 수 있다.

나. 슬라이딩 윈도우의 윈도우 크기는 수신윈도우와 혼잡윈도우 중 더 작은 값이다.

다. 수신자는 임시적으로 윈도우를 폐쇄할 수 없다.

라. 윈도우 크기를 0으로 지정하여 닫을 수 있다.

답 : 다
수신자는 임시적으로 혼잡제어를 위해 윈도우를 폐쇄할 수 있다.
(데이터 통신과 네트워크, Forouzan, 729p)

12. (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.

답 : 다
베스천 호스트는 보호하고자 하는 네트워크의 외부에 존재한다.

13. 침해사고가 발생한 PC를 조사하는 과정에서 정보유출 악성코드에 감염된 사실을 확인하였다. 조사관은 중요문서가 외부로 유출된 것으로 판단하여 보안장비 A와 B를 이용하여 정보유출시간을 확인하였다. A와 B는 무엇인가?

가. 방화벽(Firewall)과 가상사설망(VPN)

나. 침입탐지시스템(IDS)와 침입방지시스템(IPS)

다. 방화벽(Firewall)과 침입탐지시스템(IDS)

라. 침입탐지시스템(IDS)과 가상사설망(VPN)

답 : 다
방화벽 로그에서 유출된 자료의 파일크기와 침입탐지시스템에서 악성코드 감염시간과 중간경유지 위치를 확인할 수 있다.

14. 네트워크 명령어 중 현재 사용 중인 TCP, UDP 및 세션 정보를 알 수 있는 명령어는 무엇인가? (1회 출제)

가. netstat

나. net share

다. ipconfig

라. arp

정답 : 가
인사이드 윈도우포렌식,
할렌카비(저),정상민·정명주(번역)
p.29 netstat에 관한 설명 참고

15. VPN에서 사용하는 터널링 프로토콜에 해당하지 않은 것은?

가. L2TP

나. IPSec

다. SSL

라. MPLS

정답 : 라
SSL은 응용계층과 전송계층 사이에서 클라이언트와 서버간의 안전한 채널 형성과 웹브라우저와 웹서버간의 보안통로 설정에 사용되는 암호화 프로토콜이다.

제 4과목 데이터베이스

제 4과목

데이터베이스

문제

1. 프로그래밍 언어에서의 데이터와 비교하여 데이터베이스가 갖는 특성이 아닌 것은? (2회 출제)

가. 일반적으로 대용량이다.

나. 휘발성(volatile)이다.

다. 보조 기억 장치(secondary storage)에 저장된다.

라. 데이터에 대한 접근 속도가 상대적으로 느리다.

정답 : 나
데이터베이스는 일반적으로 비휘발성 저장장치인 디스크에 저장된다.

2. ER 모델은 어느 데이터 모델에 속하는가?

가. 개념적(conceptual) 모델

나. 물리적(physical) 모델

다. 관계형(relational) 모델

라. 논리적(logical) 모델

정답 : 가
데이터베이스 설계는 개념 설계, 논리 설계, 물리 설계의 3 단계의 절차로 이루어지며, 여기서 ER 모델은 개념 설계에서 사용되는 모델이다.

3. 약 엔티티 타입(weak entity type)이란 무엇인가?

가. 다른 엔티티 타입과 관계(relationship)를 갖지 못하는 엔티티 타입

나. 키(key)가 존재하지 않는 엔티티 타입

다. 키(key)가 여러 개 존재하는 엔티티 타입

라. 다른 엔티티 타입과 항상 관계(relationship)를 갖는 엔티티 타입

정답 : 나
데이터베이스 설계는 개념 설계, 논리 설계, 물리 설계의 3 단계의 절차로 이루어지며, 여기서 ER 모델은 개념 설계에서 사용되는 모델이다.

4. 한 릴레이션에서 고유하게 튜플들을 식별할 수 있는 속성은 키(key)이다. 다음 중 키의 종류에 대한 설명으로 옳지 않은 것은?

가. 기본키(primary key)는 대표로 선정된 하나의 속성이다.

나. 수퍼키(super key)는 튜플들을 유일하게 식별할 수 있다.

다. 외래키(foreign key)는 참조되는 다른 릴레이션의 기본키로 선정된 키이다.

. 보조키(secondary key)도 튜플체를 유일하게 식별할 수 있다.

정답 : 가
기본키는 여러 개의 키들 중에서 데이터베이스 운영 중에 사용하려고 선택된 키이다. 기본키는 여러 개의 속성들로 구성
될 수 있으며, 여기서 하나의 속성으로만 구성된 경우 이를 단일키(single key)라고 한다. 하나 이상의 속성으로 구성될 수도 있다.

5. '학생' 이란 릴레이션에서 학점에 대한 값이 {A, B, C, D, F}로 정의되었다고 하자. 만약 학점의 값을 잘 못 입력했을때 (예를 들면, 'K' 라고 입력했를때), 이는 다음 중 어느 것을 위반한 것인가?

가. 데이터 종속성(dependence)
나. 데이터 독립성(independence)
다. 데이터 무결성(integrity)
라. 데이터 중복성(redundancy)

정답 : 다
데이터 무결성은 데이터베이스 설계시 정의된 제약조건을 반드시 준수해야 성질을 의미한다.

6. 두 개의 릴레이션(relation)들 사이에 참조 무결성(referential integrity)이 위반되었는지를 검증하기 위해 SQL 트리거(trigger) 연산이 사용된다. 다음 중 검증을 할 필요가 없는 연산은? (3회 출제)

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

정답 : 다
참조 무결성은 참조되는 테이블에서 insert를 하는 경우에는 참조하는 테이블의 외래 키에는 아무런 영향을 미치지 않는다.
(포렌식 교재: SQL 참조)

7. 두 릴레이션(relation)들 간의 관계(relationship)를 표현하기 위해, 어느 키(key)들이 사용되는지 올바르게 나열한 것은?

가. 보조 키(secondary key)와 외래 키(foreign key)
나. 외래 키(foreign key)와 기본 키(primary key)
다. 외래 키(foreign key)와 수퍼 키(super key)
라. 기본 키(primary key)와 보조 키(secondary key)

정답 : 나
두 릴레이션(relation) R1과 R2들 간의 관계(relationship)는 R1의 외래 키가 R2의 기본 키를 참조함으로서 실현되며 이를 참조 무결성이라 한다. 여기서 R1을 "참조하는", R2를 "참조되는" 릴레이션이라 한다.

8. 릴레이션(relation)이 갖는 특성이 아닌 것은?

가. 행(column)과 열(row)로 구성된 2 차원 테이블이다.
나. 튜플(tuple)들의 순서에는 아무 의미가 없다.
다. 각 속성(attribute)은 단지 한 개의 값만 가질 수 있다.
라. 같은 값을 가진 튜플들이 존재할 수

.

정답 : 라
릴레이션 안에는 같은 값을 같는 동일한 튜플들이 두 개 이상 있을 수 없다. 이는 릴레이션의 정의가 중복된 원소들을 허용하지 않는 집합의 개념에서 근거를 뒤기 때문이다. 참고로 SQL의 테이블에서는 값을 같는 동일한 튜플들을 허용한다는 것을 유의하자.

9. 트랜잭션(transaction)이 준수해야 하는 특성에 해당하지 않는 것은?
   가. 원자성(Atomicity)
   나. 일관성(Consistency)
   다. 지속성(Durability)
   라. 무결성(Integrity)

정답 : 라
무결성은 트렉젝션 처리와 관련이 없는 일반적인 데이터가 준수해야 하는 제약조건이다.

10. 데이터 표준화에 관한 설명으로 가장 적합하지 않은 것은? (3회 출제)
   가. 데이터 명칭에 대한 표준화는 동음이의어 및 이음동의어의 조정이 필요하다.
   나. 데이터 형식은 데이터 표현 형태의 정의를 통해 데이터 입력 오류와 통제위험을 최소화하는 역할을 한다. 데이터 형식은 업무 규칙 및 사용 목적과 일관되도록 정의한다.
   다. 표준 도메인은 칼럼에 대한 성질을 그룹핑한 개념이다. 도메인은 크게는 문자형, 숫자형, 일자형, 시간형으로 분류할 수 있고, 더 세부적으로는 명, 주소, ID(이상 문자형), 금액, 율, 수량(이상 숫자형) 등으로 분류될 수 있다.
   라. 일반적으로 데이터 관리자(DA, Data Administrator)와 데이터베이스 관리자(DBA, DataBase Administrator)는 같은 역할을 갖는다.

정답 : 라
데이터 관리자(DA, Data Administrator)와 데이터베이스 관리자(DBA, DataBase Administrator)는 역할이 구분되어야 한다.
(한국데이터베이스 진흥원, DBGuide.net, 데이터 표준화)

11. 릴레이션 스키마를 설계하는 지침으로 올바르지 않은 것은?
   가. 널(null) 값을 자주 가질 수 있는 애트리뷰트를 가능한 한 기본 릴레이션의 애트리뷰트로 포함하지 않는다.
   나. 가능한 한 기본 키(primary key)나 외래 키(foreign key)를 가지고 동등 조건으로 조인할 수 있는 릴레이션을 설계한다.
   다. 중복이나 갱신 이상이 발생하지 않도록 릴레이션을 분해한다.
   라. 가능한 한 여러 개의 다른 엔티티 타입(entity type)들을 섞어서 하나의 릴레이션으로 구성한다.

정답 : 라
여러 개의 다른 엔티티 타입들을 섞어서 하나의 릴레이션으로 구성하면, 데이터 중목 혹은 갱신 현상이 발생하는 문제가 발생한다. 또한 중복이나 삽입, 삭제, 갱신 이상 등의 문제점들이 발생한다. 직관적으로 하나의 릴레이션이 하나의 엔티티 타입과 대응되게 설계하는 것이 보편적이다.

12. ER 릴레이션 스키마로 변환할 때, 따로 릴레이션을 생성하여야 하는 애트리뷰트(attribute)는 어느 것인가?

가. 키(key) 애트리뷰트

나. 유도(derived) 애트리뷰트

다. 다중치(multi-valued) 애트리뷰트

라. 수퍼키(super key) 애트리뷰트

정답 : 다
다중치 애트리뷰트는 여러 개의 값을 가질 수 있다. 릴레이션은 제 1 정규형을 만족해야 하고, 따라서 각 애트리뷰트는 반드시 한 개의 원자 값만 가질 수 있다. 따라서 릴레이션에서 다중치 애트리뷰트를 직접 나타내는 것은 이에 위배되고, 이를 해결하는 방법은 따로 릴레이션을 만들어 여기에 원래의 테이블의 기본 키를 가져와 나타낸다.

13. 데이터 참조 모델에 관한 설명 중 가장 적절하지 않은 것은? (1회 출제)

가. 데이터 참조 모델(DRM, Data Reference Model)이란 업무 영역별, 주제 영역별 표준 데이터 집합, 관리 항목들이 표기되어 재사용이 가능한 데이터 모델을 말한다.

나. 데이터 참조 모델은 재사용이 가능한 형태의 데이터 모델로 속성 단위, 엔터티, 개체-관계 다이어그램 등이 가능하며 전체 업무 영역 단위는 개별 기업의 정보 유출 및 보안 문제로 데이터 참조 모델의 단위가 되기에 어려울 수 있다.

다. 새로운 데이터 모델링시 참조 모델을 활용함으로써 정보의 누락을 예방할 수 있으며, 기존에 검증된 데이터 참조 모델을 이용하여 자사 데이터 모델의 오류를 확인하거나 보완할 수 있다.

라. 데이터 참조 모델의 관리 기준은 범용성, 단순성, 표준성, 정확성, 정보이용성, 그리고 분류성이 있다.

정답 : 나
데이터 참조 모델은 재사용이 가능한 형태의 데이터 모델로 속성단위, 엔터티, 개체-관계 다이어그램, 전체 업무 영역 단위 등도 데이터 참조 모델이 될 수 있다.
(한국데이터베이스 진흥원, DBGuide.net, 데이터 참조 모델)

14. 오라클 포렌식에서 증거 획득을 위해 검토해야할 항목으로 적절하지 않은 것은? (1회 출제)

가. TNS(Transparent Network Substrate) 로그

나. 트레이스(Trace) 파일

다. Undo 로그

라. Sysdba Audit 로그

정답 : 다
David Litchfield, Oracle Forensics - Dissection of an Oracle Attack in the Absense of Auditing

15. 오라클 포렌식 분석 시, 시간관련 증거(Time based evidence)에 대한 정확성을 확보하기 위해 함께 검토해야할 자료로 가장 적절하지 않은 것은? (1회 출제)

가. Listener Log

나. Sqlnet Log

. Statspack Script

라. Sysdba Trace

정답 : 다
Pete Finnigan, Oracle Forensics, UKOUG Conference, 2007

제 5과목 포렌식 개론

제 5과목

포렌식 개론

문제

1. 대상이 되는 시스템의 내용을 확인하고자 할 때 얻을 수 있는 비휘발성 정보가 아닌 것은?

가. 클립보드의 내용

나. 레지스트리 정보

다. 이벤트 로그

라. 시스템에 장착된 장치

정답 : 가
클립보드의 내용은 휘발성 정보임.(인사이드 윈도우즈 포렌식, Syngress, 2009, pp.40)

2. 디지털 포렌식 분석 도구 중 EnCase의 특징이 아닌 것은?

가. FAT, NTFS 분석이 가능하다.

나. UFS, Ext2/3, DVD의 분석이 가능하다.

다. 파일 디렉토리 리스트, 지워진 파일 복구, 키워드 검색 등이 가능하다.

라. Andy Rosen 사에서 개발하였으며, 텍스트 기반 UI를 제공한다.

정답 : 라
EnCase는 Guidance에서 개발하였으며 그래픽 UI를 제공한다.(파일 시스템 포렌식 분석, 케이앤피 IT, 2010, pp.36)

3. UNIX 계열의 로그에 대한 설명으로 옳지 않은 것은? (1회 출제)

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

정답 : 다
syslog는 중요한 정보를 많이 담고 있으므로 일반적으로 보안 사고가 발생한 경우 가장 먼저 백업하여 가장 먼저 분석을 수행한다.(시스템 로그 분석, 이비컴, 2005, pp.59)

4. 데이터 중에서 휘발성이 가장 큰 것부터 순서대로 나열한 것은?

가. 레지스터/캐시 – 라우팅 테이블 – 시스템 메모리 – 디스크 데이터

나. 라우팅 테이블 – 레지스터/캐시 – 시스템 메모리 – 디스크 데이터

다. 라우팅 테이블 – 시스템 메모리 – 레지스터/캐시 – 디스크 데이터

라. 레지스터/캐시 – 시스템 메모리 – 라우팅 테이블 – 디스크 데이터

정답 : 가
IEEE 의 인터넷 드래프트에서 제시한 휘발성 순서는 아래와 같다. 레지스터/캐시 – 라우팅 테이블 – 시스템 메모리 – 디스크 데이터(인사이드 윈도우즈 포렌식, Syngress, 2009, pp.7)

5. 다음 보기에 해당하는 디지털 데이터의 특성은 무엇인가? (3회 출제)

"오류에 의한 손상이나 의도적인 변조가 쉬우며, 변조 사실을 찾아내는 것이 어렵기 때문에 법정에서 증거의 조작 여부, 증거 획득 절차의 적정성 등이 문제 될 수 있다"

가. 비가시성

나. 변조가능성

다. 복제용이성

라. 휘발성

정답 : 나
디지털 포렌식 개론 p.66~67

6. 유닉스 환경에서 활성화 혹은 비활성화 된 상태에서 사용자와 관련된 정보를 보기 위한 바이너리 로그들과 유닉스 해당 명령을 나열한 것이다. 이와 관련된 사용 명령을 다르게 표현한 것은?

가. lastcomm => 각 계정 사용자의 명령어를 기록 (Solaris)

나. utmp => w utility (현재 시스템 사용자)

다. lastlog => lastlog utility (각 유저의 최종 로그인 시간)

라. wtmp => finger, who, user utility(현재 사용자 확인)

정답 : 라
(페이지 324)"해킹과보안–김승현, 영진닷컴"

7. 자동 혹은 인위적으로 생성되는 디지털 증거, 휘발성과 비휘발성 증거 등으로 그 특징을 구분 지을 수 있다. 보기 중 디지털 증거의 특징으로 구분 할 때 성격이 다른 하나는?

가. 프로세스

나. 예약작업

다. 메타데이터

라. 메모리

정답 : 다
제 2편 제 1장 디지털 증거의 종류에서 증거의 특징과 그 예를 보면 휘발성 증거는 프로세스, 예약작업, 인터넷 연결 정보, 네트워크 공유정보, 메모리 등이다.

8. 각 클러스터에 4개의 섹터를 가지고 있는 NTFS볼륨에서 "My Note.TXT" 파일의 논리사이즈는 2040byte 이고 클러스터 1500번지에 저장되어 있다. 이 "My Note.TXT" 파일이 삭제되고, 1538byte의 논리적사이즈를 가지고 있는 "사진.jpg"를 클러스터

1500 저장 할 경우 클러스터 1500 번지에서 복구 할 수 있는 "My Note.TXT"의 크기는 얼마인가?

가. 0bytes

나. 502bytes

다. 512bytes

라. 540bytes

정답 : 가
NTFS볼륨에서
1 Cluster=4 sector*512 = 2048bytes
텍스트 파일이 클러스터내에서
2040 = 3*512 + 504 이므로 4개의 섹터를 쓰고 있고 새로 저장되는 jpg 파일은 1538 = 3*512 + 2 이므로 4개의 섹터를 사용한다. 따라서 복구되어지는 텍스트 파일의 크기는 0 bytes 가 된다(RAM 슬랙은 모두 "00"값으로 쓰여진다)

9. 윈도우 XP NTFS볼륨에서 "My Note.TXT" 파일은 "My Note.TXT"라는 긴 파일이름으로 존재하며 "MYNOTE~1.TXT"라는 파일이름의 짧은 파일명이다. 이 파일이 C 볼륨에서 삭제되어 기존에 비워진 휴지통으로 보내졌다. 포렌식분석 프로그램(Encase, FTK)으로 휴지통을 볼 경우, 각각 긴 파일명과 짧은 파일명은 어떻게 보여질까?(3회 출제)

가. My Note.DEL, DC0.DEL

나. My Note.TXT, CD0.TXT

다. My Note.DEL, DC1.DEL

라. My Note.TXT, DC1.TXT

정답 : 라
NTFS 볼륨에서 파일이 휴지통으로 삭제가 되었을 때 긴파일명은 변하지 않고 그대로 유지되며, 짧은 파일명은 D(Delete)C(C 볼륨)1(인덱스번호).원파일의 확장자 형태로 표현된다.

10. 사이버 범죄 수사에서의 증거 문서화 절차와 관련이 적은 것은?

가. 증거를 맨 처음 보관하기 시작한 사람은 증거에 꼬리표를 달거나 표식을 남긴다.

나. 증거 전송 과정을 기록으로 남겨 놓음으로써 증거 담당자 목록이 제대로 유지되고 있도록 한다.

다. 데이터의 무결성 보장을 위해 정전기 방지 가방에 넣어 보관한다.

라. 디스크에 있는 데이터에서 증거를 찾을 때는, 찾을 수 있는 모든 잠재적인 증거를 문서화 해야 한다.

정답 : 다
문서화 절차 중 3번은 해당 사항이 없음.(사이버 범죄 소탕작전 컴퓨터 포렌식 핸드북, 에이콘출한사, 2008, pp.581)

11. 다음은 증거복원에 대한 설명이다. 거리가 먼 것은?

가. 논리적 볼륨은 마스터 부트 레코드(MBR) 또는 미사용 디스크 공간을 포함하지 않는 볼륨이다.

나. 물리적 볼륨은 마스터 부트 레코드(MBR) 및 미사용 디스크 공간을 포함한다.

. 대상 미디어보다 훨씬 더 큰 용량의 드라이브에 미디어를 복원하면 복원된 복제 드라이브가 부팅되지 않을 수 있으므로, 복원의 목적을 달성할 수 없다.

라. 대상 시스템을 부팅할 목적으로 드라이브를 복원할 경우, 논리적 복원이 올바른 선택이다.

정답 : 라
대상 시스템을 부팅할 목적으로 드라이브를 복원할 경우, 물리적 복원이 올바른 선택이다.(Encase Forensic User Manual, pp.222)

12. EnCase에서 증거 파일 추가를 선택하여 증거 파일을 개별적으로 소스 트리에 추가 할 수 있다. 추가 파일로 적절하지 않은 것은?(1회 출제)

가. 물리적 증거 파일

나. SafeBack 파일

다. VMware 파일

라. Virtual PC 파일

정답 : 가
추가 유형은 논리적 증거 파일, SafeBack 파일, VMware 파일, Virtual PC 파일, 고스트 파일 등.(Encase Forensic User Manual, pp.170)

13. 디지털 시스템을 분석할 수 있는 도구와 특징이 잘못 연결된 것은?

가. EnCase : 윈도우즈 기반하여 로컬, 네트워크 버전 도구를 이용해 데이터 분석

나. ProDiscover : UNIX에서 동작하며, 로컬과 네트워크 기반의 버전이 있음

다. forensic Toolkit : 윈도우에서 동작하며, 디스크나 파일 시스템 응용프로그램 데이터를 분석하고 수집

라. SMART : 리눅스에서 동작하는 데이터 수집 및 분석

정답 : 나
ProDiscover는 윈도우에서 동작하며 로컬과 네트워크 기반의 버전이 있음.(파일 시스템 포렌식 분석, 케이앤피 IT, 2010, pp.36)

14. 디지털 증거의 특징이 아닌 것은?

가. 근본적으로 파괴되기 쉽다.

나. 컴퓨터 디스크 상에 항상 안전하게 보전 가능하다.

다. 어떤 데이터는 사라지기 쉽다.

라. 의도적으로 변경되기 쉽다.

정답 : 나
디지털 증거는 임시적이며, 손상되기 쉽고, 파괴되기 쉽다. 디스크 상에 저장된 정보는 항상 안전하다고 할 수 없다.(사이버 범죄 소탕작전 컴퓨터 포렌식 핸드북, 에이콘출한사, 2008, pp.558)

15. EnCase 애플리케이션이 지원하는 파일을 포함하는 증거 클래스에 대한 설명으로 옳지 않은 것은? (2회 출제)

가. EnCase 증거 파일 : 수집된 장치의 내용이 포함되며 이는 추후 분석 작업을 위한 기본이 됨

나. 논리적 증거 파일 : 미리 보기 한 파일 또는 기존 증거 파일에서 생성

다. 원시 이미지 : 파일 모음이 포함되어 있으며 EnCase증거 파일이 제공하는 메타데이터 및 압축 해시 값이 포함되어 있음

라. 단일 파일 : 단일 파일 활성화가 선

개별 파일을 사례에 추가
할 수 있음

정답 : 다
원시 이미지 파일에는 파일 모음이 포함되어 있으나 EnCase 증거파일이 제공하는 메타데이터 및 압축해시 값이 포함되어 있지 않습니다.(Encase Forensic User Manual, pp.164)

16. 디지털 포렌식의 기본원칙으로 보기 어려운 것은?
가. 적법절차의 준수
나. 증거 보관의 불연속성
다. 분석자의 전문성과 분석도구의 신뢰성
라. 원본증거의 보존

정답 : 나
'나'는 잘못된 내용이며, 오히려 증거 보관의 연속성 또는 연계보관성(chain of custody)을 디지털 포렌식의 기본원칙으로 볼 수 있다. 보관의 연속성이란, 증거가 수집되어 누구에게 분석, 보존되었는가를 증명할 수 있도록 문서로 기록하는 것을 말한다.

<전상덕 외, "디지털 포렌식의 기술 동향과 전망", 정보화정책 제13권 제4호(한국정보사회진흥원), 2006, 12면>

17. EnCase 폴더 복구 내용 중 설명이 거리가 가장 먼 것은?
가. 폴더 구조를 재구성하는 작업은 보통 짧은 시간 내에 작업이 가능하다.
나. UFS 및 EXT2/3 파티션, UFS 및 EXT2/3 볼륨 복구가 가능하다
다. 미할당 클러스터에서 NTFS 파일 및 폴더를 복구하여, 현재의 마스터 파일 테이블(MFT) fp코드를 통해 상위 폴더 없이 파일에 대한 구문 분석을 계속할 수 있다.
라. 증거 파일에 논리적 볼륨은 표시되지만 디렉터리 구조가 없는 경우, 하드 드라이브가 포맷되었을 가능성이 있다.

정답 : 가
폴더 구조를 재구성하는 작업은 일반적으로 많은 시간이 걸리는 작업이다.(Encase Forensic User Manual, pp.217)

18. 다음 중 디지털 포렌식의 기본 원칙으로 잘못된 것은?
가. 디지털 포렌식의 전과정에서 엄격한 적법절차를 준수하여야 한다.
나. 디지털 포렌식에 있어서 디지털 증거는 반드시 원본만을 획득하여야 한다.
다. 디지털 증거의 무결성 유지를 위해서 원본증거는 안전하게 보존하고, 사본을 통해서 증거의 분석을 행해야 한다.
라. 디지털 증거의 압수·수색 과정에서는 관계자 또는 입회인을 모든 과정에 입회하도록 한다.

정답 : 나
24시간 운영되는 은행서버, 게임서버 등은 원본의 압수가 불가능하다.[이규안 외3, "과학수사를 위한 디지털 포렌식", 7면 이하.]

19. 디지털 증거 수집시의 일반적인 원칙을 제시하고 있는 RFC3227(Internet Society, 2002)의 주요 내용으로 옳지 않은 것은? (2회 출제)
가. 증거 수집시 파일 또는 디렉토리 Access Times을 업데이트 한다.

. 현장에 대한 안전조치를 확보하고 적합한 사고취급 및 법집행 인력을 투입한다.

다. 휘발성(volatile) 증거에서 비휘발성 증거로 수집한다.

라. 증거수집과 증거분석 중 증거수집이 우선한다.

정답 : 가
증거수집시 데이터의 변화를 최소화하기 위해서 파일 또는 디렉토리 Access Times의 업데이트를 피해야 한다.(RFC 3227, 2. Guiding Principles during Evidence Collection)

20. 다음 중 활성시스템 조사 시 사용되는 명령어와 기능이 바르게 짝지어지지 않은 것은?

가. Di - Windows 파티션 구성 정보 확인

나. # cat /proc/diskstats - 유닉스시스템의 파티션 정보 확인

다. # finger -lmsp - 유닉스시스템의 사용자 정보

라. psloggedon - 현재 로그인한 사용자 정

정답 : 나
cat /proc/diskstats - 유닉스시스템의 디스크 상태를 확인하는 명령어
cat /proc/partitions - 유닉스시스템의 파티션정보를 확인하는 명령어

21. 원칙적으로 압수가 금지되는 대상이 아닌 것은?

가. 피고인에게 발송된 것으로 체신관서가 보관하는 우체물

나. 공무상 비밀에 속하는 서류

다. 의사가 보관하고 있는 피고인에 관한 진료기록

라. 변호사가 보관하는 소송의뢰인의 비밀에 관한 서류

정답 : 가
피고인에게 발송된 우체물은 형사소송법 제107조에 의해 압수할 수 있다.

22. 증거에 관한 다음 설명 중 가장 옳지 않은 것은? (다툼이 있으면 판례에 의함) (3회 출제)

가. 피고인이 증거로 할 수 있음을 동의한 서류는 증거능력이 없는 전문증거라도 유죄의 증거로 할 수 있다.

나. 피고인 등이 법정에서 진술을 번복하였다는 이유로 그 탄핵증거로 영상녹화물을 제출하는 것은 허용되지 않는다.

다. 필요적 변론사건이라도 피고인이 재판장의 허가 없이 퇴정하고 변호인마저 퇴정한 경우에는 피고인의 진의와 관계없이 증거동의가 있는 것으로 간주된다.

라. 간이 공판절차의 결정이 있는 사건의 증거에 관하여는 증거의 동의가 있는 것으로 의제됨이 원칙이다.

정답 : 나
가. 형사소송법 제3318조 제1항,
나. 형사소송법 제318조의2 제2항 참조,
다. 대법원 1991. 6. 28. 선고 91도865 판결
라. 형사소송법 제318조의3

23. 　　중 사전 또는 사후 압수·수색 영장의 청구가 불필요한 경우는 어느 경우인가? (3회 출제)

가. 유류물 또는 임의제출물을 영치하는 경우

나. 체포현장에서의 압수된 물건을 계속 압수할 필요가 있는 경우

다. 범죄장소에서의 긴급을 요하는 압수

라. 긴급체포된 자의 소유물건을 계속 압수할 필요가 있는 경우

정답 : 가
나, 다, 라는 사후 영장을 청구해야 하나, 가는 사전·사후영장이 필요치 않다(형사소송법 제216조, 제217조, 제218조 참조).

24. 다음 중 전문증거에 해당하는 것으로 옳은 것은?(1회 출제)

가. 갑이 을을 살해하는 것을 직접 목격한 병이 이를 서면으로 작성하여 법원에 제출하는 경우

나. "갑이 을을 살해하였다"고 말하는 것을 병으로부터 들은 정이 병의 진술내용을 병의 갑에 대한 명예훼손사건을 심리하는 법원에서 증언하는 경우

다. 갑이 을을 껴안은 것이 폭행이 아니라 애정의 표현임을 설명하기 위하여 당시 갑이 "사랑해"라고 말하는 것을 들은 병이 이를 법원에서 증언하는 경우

라. 병의 정신상태를 증명하기 위하여 "갑이 을을 살해하였다"고 병이 말하는 것을 들은 정이 이를 법원에서 증언하는 경우

정답 : 가
가. 형사소송법 제310조의2 전단, 신동운, 신형사소송법, 법문사, 2008, p.890 ; 이재상, 신형사소송법(제2판), 박영사, 2008, p.551,
나. 다. 라. 각 신동운, 앞의 책, p.891-892 ; 이재상, 앞의 책, p.557-558

25. 다음이 보기 가운데 재판에서 증거로 사용할 수 있는 것은?

가. 법에 규정한 감청절차에 의하지 아니하고 지득 또는 채록된 전기통신의 내용

나. 증거를 인멸할 우려가 있는 구속중인 피의자의 서신을 검열하여 지득한 내용

다. 통신제한조치 허가대상자가 송수신하는 전기통신에 대하여 1년간 행한 감청내용

라. 법원의 허가 없이 긴급통신제한조치를 행한 이후 48시간 만에 지득한 통신내용

정답 : 나
구속 또는 복역중인 사람의 통신은 형사소송법 제91조에 근거하여 "도망하거나 또는 죄증을 인멸할 염려가 있다고 인정할 만한 상당한 이유가 있는 때"에는 검열의 대상이 될 수 있다.

26. 디지털 증거의 압수수색 절차에서 가장 부적절한 것은?

가. 압수한 하드드라이브는 정전기 방지 봉투에 넣은 후 이를 봉인한다.

나. 압수수색할 PC의 설정 시간을 촬영 등의 방법으로 Time Stamping 한다.

다. 디지털 저장매체를 압수하면서 봉인

경우 담당수사관만의 확인으로 충분하다.

라. 피압수수색 대상자 및 관리자의 현장 참여·확인을 보장하여야 한다.

정답 : 다
디지털 저장매체를 압수하면서 봉인할 경우, 참관인으로부터 확인, 서명을 받아 증거물에 부착하여야 한다.
【대검찰청, 디지털포렌식 매뉴얼 P 27】

27. 디지털 증거의 무결성을 확보하기 위한 방안으로 옳지 않은 것은?

가. 일반적으로 증거물에 대한 쓰기방지 기술을 적용하여야 한다.

나. 디지털 증거를 분석시 원본으로 분석하여야 한다.

다. 증거물을 운반하거나 보관할 때에는 충격방지와 자기장/전자파 파폐 등의 조치를 취하여야 한다.

라. 증거담당자 목록을 문서화함으로써 보관의 연속성(Chain of Custody)을 유지하여야 한다.

정답 : 나
디지털 증거의 무결성을 확보하기 위하여는 원본 대신 사본을 작성하여 분석 수행하여야 한다.
【대검찰청, 디지털포렌식 매뉴얼 P 5】

28. 증거에 관한 설명 중 옳지 않은 것은? (1회 출제)

가. 형소법 제313조 제2항에 의하여 감정서는 진술증거로 전문증거에 해당한다.

나. 범행에 사용한 칼은 물건의 존재 내지 상태가 증거로 되는 물적증거에 해당한다.

다. 문서파일은 그 자체로서는 그 내용을 인식할 수 없으므로 이를 출력하여 증거로 사용하여야 하며, 출력한 문건의 내용을 증거로 하고자 하는 경우 이는 진술증거로서 전문법칙의 적용을 받는다.

라. 증인의 증언은 인적증거이며, 그 사람의 진술내용이 증거가 되기 때문에 진술증거에 해당한다.

정답 : 다
문서파일은 그 자체로서는 그 내용을 인식할 수 없으므로 이를 출력하여 증거로 사용하여야 하며, 출력한 문건의 내용을 증거로 하고자 하는 경우 이는 진술증거로서 전문법칙의 적용을 받는다.

29. 강제수사에 대한 설명 중 틀린 것은?

가. 강제수사의 방법으로는 대인적 강제처분인 체포, 구속과 대물적 강제처분인 압수·수색·검증이 있다.

나. 판례에 의하면, 진술거부권을 고지하지 아니하거나 위법한 체포 하에서 얻은 피의자의 자백은 임의성이 인정되더라도 증거능력은 부정된다.

다. 수사기관의 구속기간은 피의자의 경우 10일이고, 피고인은 2개월이나 연장·갱신할 수는 없다.

라. 피고인에 대한 구속의 취소, 집행정지에 대하여는 즉시항고가 가능함에 대하여 피의자의 영장기각에 대하여는 이의신청 제도가 없다.

정답 : 다
피고인의 구속기간은 2개월이며, 연장·갱신할 수 있도록 되어 있다.

30. 관한 다음 설문 중 판례의 입장과 다른 것은?

가. 이미 증언을 마친 증인을 검사가 재차 소환하여 일방적으로 번복시키는 방식으로 조서를 작성한 경우, 피고인이 증거로 할 수 있음을 동의하지 않는 한 동 진술조서는 물론 당해 증인의 법정 증언도 증거능력이 없다.

나. 경찰수사과정에서 사법경찰관의 면전에서 피의자가 작성한 진술서는 형소법 제312조 제3항에 의해 당해 피의자이었던 피고인이 내용부인하면 증거능력이 없다.

다. 피고인이 범행을 자인하는 것을 들었다는 피고인 아닌 자의 진술내용은 형소법 제310조의 피고인의 자백에는 포함되지 아니하지만, 피고인 자백의 보강증거로도 될 수 없다.

라. 녹음테이프 검증조서의 기재 중 피고인의 진술내용을 증거로 사용하기 위해서는 전문법칙의 적용을 받는다.

정답 : 가
대판 2004. 3. 26. 선고 2003도7482 재 번복하는 취지의 진술조서는 증거능력이 부정되더라도 당해 참고인의 법정진술은 증거로 사용될 수 있다.

31. 압수·수색 현장에서 우연히 발견된 다른 범죄의 증거임이 명백한 물건에 대한 다음 초지 중 옳지 않는 것은(다툼이 있으면 판례에 의함)

가. 다른 범죄의 현행범으로 체포한 후 영장 없이 압수할 수 있다.

나. 다른 범죄가 범행 즉후임이 인정되는 경우에는 영장 없이 압수할 수 있다.

다. 다른 범죄가 긴급체포에 해당하는 범죄라면 피의자를 긴급체포 후 영장 없이 압수할 수 있다.

라. 피의자로부터 임의제출을 요구하고, 이를 거절한 경우 사진 촬영하여 이를 보존할 수 있다.

정답 : 가
증거임이 명백한 물건의 소지 자체를 범죄로 하는 경우 현행범으로 체포할 수 있으나 단순히 범죄의 증거라고 하여 항상 현행범이라고 할 수 없으므로 옳지 않다.

32. 증거보전에 대한 설명 중 옳지 않은 것은?

가. 증거보전의 결정에 대하여는 즉시항고로써 다툴 수 있다.

나. 증거보전의 신청은 상대방을 지정할 수 없는 경우에도 할 수 있고, 이 경우 법원은 상대방이 될 사람을 위하여 특별대리인을 선임할 수 있다.

다. 증거보전의 신청은 소를 제기한 뒤에는 그 증거를 사용할 심급의 법원에 하여야 한다.

라. 법원은 필요하다고 인정한 때에는 소송이 계속된 중에 직권으로 증거보전을 결정할 수 있다.

정답 : 가
증거보전신청을 받아들이는 결정에 대하여는 불복신청을 하지 못하나 이를 각하하는 결정에 대하여는 신청인이 항고할 수 있다.

33. 관한 다음 설명 중 옳지 않은 것은? (다툼이 있으면 판례에 의함) (2회 출제)

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.

정답 : 나
대판 2009.6.23. 선고 2009도1322[공2009하,1242]
동석을 허락할 것인지는 원칙적으로 검사 또는 사법경찰관이 피의자의 건강 상태 등 여러 사정을 고려하여 재량에 따라 판단하여야 할 것이나, 이를 허락하는 경우에도 동석한 사람으로 하여금 피의자를 대신하여 진술하도록 하여서는 안 된다. 만약 동석한 사람이 피의자를 대신하여 진술한 부분이 조서에 기재되어 있다면 그 부분은 피의자의 진술을 기재한 것이 아니라 동석한 사람의 진술을 기재한 조서에 해당하므로, 그 사람에 대한 진술조서로서의 증거능력을 취득하기 위한 요건을 충족하지 못하는 한 이를 유죄 인정의 증거로 사용할 수 없다.

34. 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.

정답 : 라
문서의 진정성립은 필적 또는 인영·무인의 대조에 의하여서도 증명할 수 있고 그 필적 또는 인영·무인의 대조는 사실심의 자유심증에 속하는 사항으로서, 문서 작성자의 필적 또는 인영·무인과 증명의 대상인 문서의 필적 또는 인영·무인이 동일하다고 인정될 때에는 특별한 사정이 없는 한 문서의 진정성립을 인정할 수 있으며, 이 경우 법원은 반드시 감정적으로써 필적, 인영 등의 동일여부를 판단할 필요가 없이 육안에 의한 대조로도 이를 판단할 수 있다

35. 은 乙의 휴대폰으로 공포심이나 불안감을 유발하는 글을 반복적으로 보냈다. 다음 설명 중 틀린 것은? (3회 출제)

가. 甲의 행위는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반으로 처벌 대상이다.

나. 문자정보가 저장되어 있는 휴대전화기를 법정에 제출하는 경우, 휴대전화기에 저장된 문자정보 그 자체가 범행의 직접적인 수단으로서 증거로 사용될 수 있다.

다. 문자메세지로 전송된 문자정보를 휴대전화기 화면에 띄워 촬영한 사진을 증거로 사용하려면 문자정보가 저장된 휴대전화기를 법정에 제출할 수 없거나, 그 제출이 곤란한 사정이 있고, 그 사진의 영상이 휴대전화기의 화면에 표시된 문자정보와 같다는 사실이 증명되어야 한다.

라. 문자정보는 경험자의 진술에 갈음하는 대체물로써 피고인이 성립 및 내용의 진정을 부인하면 증거능력이 인정되지 않는다.

정답 : 라
문자정보는 범행의 직접적인 수단이고, 경험자의 진술에 갈음하는 대체물에 해당하지 않는다(대법원 2008.11.13, 2006도2556 참조).

36. 다음 중 통신비밀보호법에서 금지하고 있는 행위로 옳은 것은? (다툼이 있으면 판례에 의함) (2회 출제)

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 예약담당 직원과 고객 간의 골프장 예약에 관한 통화내용을 녹취한 행위

라. 음식점에 도청마이크를 설치하여 타인간의 대화를 녹음하려 시도하거나 청취한 행위

정답 : 라
음식점 내부에 감시용 카메라와 도청마이크 등을 설치하여 타인간의 대화를 녹음하려 시도하거나 청취한 사안에서, 위 음식점 내에서 이루어진 타인간의 대화는 통신비밀보호법 제3조 제1항의 '공개되지 아니한 타인간의 대화'에 해당한다고 한 사례 [대판 2007.12.27, 2007도9053]

37. 비디오테이프의 증거능력의 판단기준에 관한 설명으로서 옳지 않은 것은?

가. 비디오테이프가 원본이거나 원본으로

복사한 사본일 경우에는 복사과정에서 편집되는 등 인위적 개작 없이 원본의 내용 그대로 복사된 사본이어야 한다.

나. 형사소송법 제313조 제1항에 따라 공판준비나 공판기일에서 원진술자의 진술에 의하여 그 비디오테이프에 녹음된 각자의 진술내용이 자신이 진술한 대로 녹음된 것이라는 점이 인정되어야 한다.

다. 원진술자가 비디오테이프의 피촬영자의 모습과 음성을 확인하고 자신과 동일인이라고 진술해야 한다.

라. 피고인이 그 비디오테이프를 증거로 함에 동의해야 한다.

정답 : 라
대법원 2004. 9. 13. 선고 2004도3161 피해자들의 진술내용을 증거로 삼기 위해서는 위에서 본 법리에 따른 요건을 충족하여야 할 것인바, 제1심법원에 제출된 이 사건 비디오테이프는 원본을 복사한 사본이지만, 비디오테이프를 촬영한 인준경이 검증기일에 출석하여 '피해자 한 사람당 1시간 정도씩 촬영한 분량 중 출연자들이 상담하는 놀이방을 드나드는 과정과 그 사이 일부를 편집한 것일 뿐 피해자들과 최문주 사이의 대화내용에는 상이점이 없다.'고 진술하였고, 이에 피고인의 변호인도 비디오테이프의 제작과정에 대하여 이의가 없다고 진술하고 있으므로, 복사과정에서 편집되는 등의 인위적인 개작 없이 원본의 내용 그대로 복사된 사본이라는 점은 인정된다고 할 것이고, 나아가 같은 검증기일에 피해자들과 상담한 최문주는 비디오테이프를 재생한 내용이 피해자들과 상담한 내용과 동일하고 상이점이 없다고 진술하고, 피해자들도 이 사건 비디오테이프를 모두 시청한 뒤 제1심 재판장으로부터 '화면에 나오는 어린이가 맞느냐.', '그 곳에서 상담 선생님과 이야기를 한 것이 맞느냐.'는 질문에 각자 '예'라고 답하였으므로, 공판준비기일에서 원진술자의 진술에 의하여 그 비디오테이프에 녹음된 각자의 진술내용이 자신들이 진술한 대로 녹음된 것이라는 점이 인정되었다고 할 것이어서, 이 사건 비디오테이프는 그 증거능력이 인정된다고 할 것이다.

38. 다음의 보기 가운데 영장 없이 압수할 수 없는 것은?

가. 미성년 피의자가 사용한 컴퓨터를 부모가 임의로 제출한 경우

나. 체포현장에서 당해사건 이외의 별건의 증거를 발견한 경우

다. 피의자가 유류한 물건

라. 범행현장에서의 증거물

정답 : 나
현장체포시 압수수색영장없이 압수수색할 것은 당해사건의 증거물에 제한되며, 당해 범죄사실과 무관한 별건의 증거를 발견한 때에는 임의제출을 구하거나 영장에 의하여 압수해야 한다.

39. 다음 중 형사소송법 제315조에 의하여 당연히 증거능력이 있는 서류라고 볼 수 없는 것은? (다툼이 있으면 판례에 의함)

가. 사립대학병원의 의사가 작성한 진단서

나. 판결문 사본

다. 상업장부

라. 구속적부심문조서

정답 : 가
사인인 의사가 작성한 진단서는 업무상 필요에 의하여 순서적·계속적으로 작성되는 것이 아니고 개개적으로 작성되는 것이고 그 작성이 특히 신용할 만한 정황에 의하여 작성된 문서라고 볼 수 없으므로, 제313조에 의하여 증거능력이 판단된다.

40. 요청(명령)제도의 도입에 관한 설명으로 타당하지 않은 것은?

가. 물리적 증거와 달리 디지털 증거는 쉽게 삭제, 변경, 훼손될 수 있으므로 증거수집 전단계에서도 자료의 보존이 필요하다.

나. 미국의 경우 전기통신프라이버시법(ECPA)에 기록보존 요청제도를 두고 있다.

다. EU의 사이버범죄방지조약은 데이터의 신속한 보존과 관련하여 컴퓨터 데이터가 손괴 또는 변경될 수 있다고 믿을 만한 근거가 있는 경우에는 전송자료를 포함하여 컴퓨터 시스템 내에 저장된 컴퓨터 데이터의 신속한 보존을 법집행기관이 명령 또는 요청할 수 있도록 하는 절차적 규정을 국내법으로 입법하도록 하고 있다.

라. EU의 사이버범죄방지조약에는 신속한 보존이 필요한 자료가 개인의 소유에 속하는 경우에 대하여는 규정하고 있지 않다.

정답 : 라
EU의 사이버범죄방지조약 제16조제2항에서는 신속한 보존이 필요한 자료가 개인의 소유에 속하는 경우에 법집행기관이 해당 자료를 압수하는 동안에 손괴 또는 변경되지 않도록 개인에게 컴퓨터 데이터의 무결성을 유지하고 보존할 것을 최대 90일까지 명령하는데 필요한 입법을 하도록 규정하고 있다. <권양섭, 디지털 증거수집에 관한 연구, 군산대 법학박사학위논문(2009), pp.70-3>