【디지털포렌식개론】

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)

2. 디지털 증거의 특성으로 가장 적절하지 **않은** 것은?

① 대량성 ② 가시성
③ 초국경성 ④ 변조의 용이성

3. 흔글 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

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

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)

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

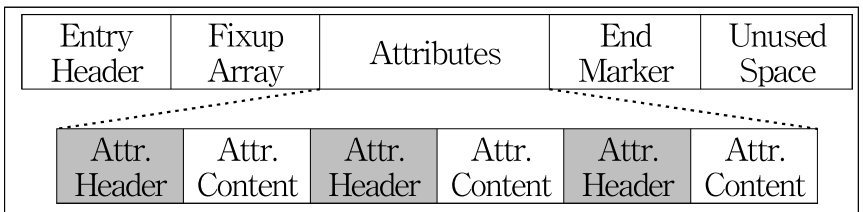
① ㉠㉡㉢ ② ㉡㉢㉣
③ ㉢㉣㉤ ④ ㉣㉤㉥

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

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

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)

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)

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

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)

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

	정보	데이터베이스
①	웹 서버에 접근한 사용자에 대한 정보	history data
②	방문한 URL의 접근 횟수에 따른 순위	top sites
③	자동 완성 폼 채우기 기능에 사용된 정보	login data
④	브라우저 상단에 방문 사이트 아이콘 정보	web data

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)

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)

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

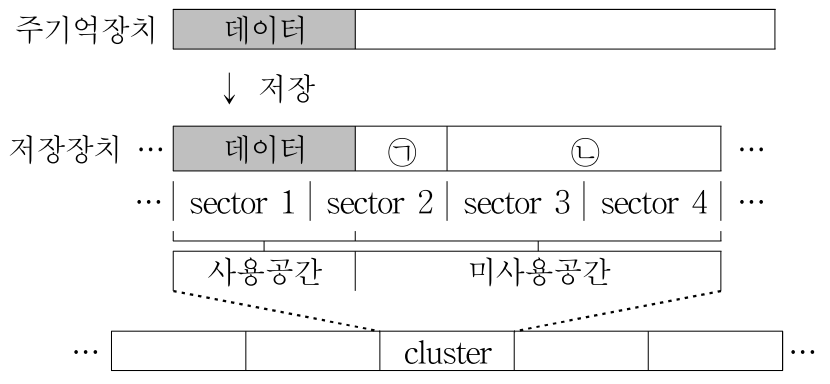
① MountedDevices 키(key)의 일부에 드라이브 문자(drive letter)가 저장된다.
② USB 사용자별 고유한 값이 고유 인스턴스(unique instance) ID에 저장된다.
③ 제조사, 제품명 그리고 버전정보는 장치 클래스(device class) ID에 저장된다.
④ 드라이브로 인식된 USB 장치에 대한 정보는 USBStor의 하위 키로 저장된다.

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

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

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

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)