【디지털포렌식개론】

1. 사이버범죄 포렌식 분석 보고서가 법정에서 증거로 채택되기 위한 기본원칙으로 가장 적절하지 **않은** 것은?

① 구현의 원칙: 법정에서 다시 네트워크에 접속하여 범행을 시연하면, 사이버범죄 현장과 같은 범죄 행위가 구현되어야 한다.
② 정당성의 원칙: 수사관이 해킹하여 수집한 범죄 집단의 디지털 증거는 증거능력이 인정되기 어렵다.
③ 무결성의 원칙: 수집 당시의 증거자료 해시값과 법정제출 시점의 증거자료 해시값은 반드시 일치해야 한다.
④ 연계보관성의 원칙: 수집된 증거자료의 이송-보관-분석-법정제출의 각 단계에서 담당자의 확인이 있어야 한다.

2. 전자적 증거(디지털 증거)의 특징에 대한 설명으로 가장 적절하지 **않은** 것은?

① 전자적 증거는 저장매체에 독립된 정보 내용이 증거가 된다.
② 전자적 증거는 삭제, 변경, 훼손 등 변조가 쉽다.
③ 인위적으로 생성되는 전자적 증거로는 문서 파일, 인터넷 사이트 접속 기록 등이 있다.
④ 전자적 증거는 공간을 초월하여 전송되므로 관할권의 문제와 국경을 넘을 경우 국가의 주권문제까지 연관 될 수 있다.

3. 사이버 도박 범죄 현장에서 수사관의 휘발성 데이터 수집 방법에 대한 설명으로 가장 적절하지 **않은** 것은?

① 범죄 현장의 컴퓨터에서 사용자를 분리시키고, 현재 화면과 시스템을 사진으로 촬영한다.
② 데이터 증거수집은 우선 '디스크 정보→시스템 메모리→라우팅 테이블 정보' 순서로 한다.
③ 현재 네트워크에 연결된 시스템의 시간과 로그인, 사용자 정보를 확인한다.
④ 현재 네트워크에 연결된 시스템의 IP 주소를 확인한다.

4. 수사관이 증거로 확보한 시스템에서 웹 브라우저와 관련된 데이터를 조사하고 있다. 이에 대한 설명으로 가장 적절하지 **않은** 것은?

① 웹 히스토리(Web History)에는 사용자가 방문한 웹 사이트의 내역이 저장된다.
② 쿠키(Cookie)에는 사용자가 만든 동영상이 자동으로 저장된다.
③ 웹 캐시(Web Cache)에는 웹 사이트 방문 시에 빠른 재접속을 위하여 이미지 파일 등이 자동으로 저장된다.
④ 임시 인터넷 파일(Temporary Internet File)에는 임시 파일의 URL, 임시 파일의 이름, 임시 파일의 저장위치 등이 저장된다.

5. 스마트폰 포렌식에서 데이터의 추출 방법에 대한 설명으로 가장 적절하지 **않은** 것은?

① 운영체제를 커널(kernel)에 올려주는 Boot Loader를 통해서, 비할당 영역의 데이터를 추출한다.
② 메모리 칩을 스마트폰에서 분리하고, 메모리 리더기를 통해 데이터를 추출한다.
③ 파티션 단위로 데이터를 추출하여, 삭제 파일이나 슬랙(slack) 공간의 데이터를 추출한다.
④ 스마트폰을 부팅한 후, 운영체제 명령어를 통해 bit 단위의 데이터를 추출한다.

6. 메타 데이터(Meta data)는 NTFS가 볼륨을 관리하기 위한 파일이다. ㉠~㉣에 해당하는 용어를 순서대로 나열한 것으로 가장 적절한 것은?

㉠ MFT entry의 복사본을 별도로 저장
㉡ 볼륨에서 사용되는 속성에 대한 정보를 저장
㉢ 파일이나 디렉터리의 변경 사항에 대한 정보를 저장
㉣ 파일 시스템의 루트 디렉터리에 대한 정보를 저장

	㉠	㉡	㉢	㉣
①	$UsnJrnl	$MFTMirr	$.	$AttrDef
②	$AttrDef	$.	$UsnJrnl	$MFTMirr
③	$.	$UsnJrnl	$MFTMirr	$AttrDef
④	$MFTMirr	$AttrDef	$UsnJrnl	$.

7. 디지털 데이터를 포렌식 증거자료로 사용하기 위해 가장 쉽게 복구할 수 있는 경우로 가장 적절한 것은?

① 임의의 숫자로 증거 데이터를 덮어쓰고, 첫 번째 숫자의 보수로 다시 덮어쓴 후, 임의의 숫자로 덮어쓰는 방식을 7회 이상 반복한 자료
② 웹 검색에 사용되는 index.dat 파일을 삭제하고, 최근 사용문서, 열람문서 보관하는 기능도 삭제하며, 히스토리나 캐시에 들어있는 정보를 삭제하고, 자동삭제 기능으로 삭제한 자료
③ 윈도우에서 마우스 오른쪽 버튼을 클릭 '삭제'하여 휴지통으로 이동한 자료
④ 증거 데이터가 있는 하드디스크에 디가우징(degaussing) 방법을 적용한 자료

8. 슬랙 공간(Slack Space)은 파일에 할당된 물리적 공간이 논리적으로는 사용할 수 없는 공간을 말한다. 이전에 사용한 데이터가 남아 있을 가능성이 없는 슬랙 공간으로서 가장 적절한 것은?

① 램 슬랙(RAM Slack)
② 파일 시스템 슬랙(File System Slack)
③ 드라이브 슬랙(Drive Slack)
④ 볼륨 슬랙(Volume Slack)

9. 스마트폰 압수 현장에서 수사관의 주의 사항에 대한 설명으로 가장 적절하지 **않은** 것은?

① 압수수색 현장에서 스마트폰의 잠금해제에 대한 정보를 확인해야 한다.
② 압수수색 후 현장에서 스마트폰의 전원을 다시 켜서, 스마트폰의 정상작동 여부를 확인해야 한다.
③ 사용자가 스마트폰 보안설정을 한 경우, 암호정보를 확보해야 한다.
④ 스마트폰을 비행기 모드로 설정하고, WiFi를 비활성 모드로 한다.

10. 파일 카빙(File Carving)은 삭제된 파일을 복구하는 방법 중 하나이다. 파일 카빙에 대한 설명으로 가장 적절하지 **않은** 것은?

① 파일 카빙은 파일의 메타 데이터를 활용하지 않고 파일의 고유한 정보를 이용하여 복구한다.
② 램 슬랙 카빙은 미들 시그니처(Middle Signature)를 활용하는 방법이다.
③ 파일 구조체 카빙은 파일 포맷 내부에 여러 개의 시그니처가 존재할 수 있으므로 파일 구조를 분석하여 카빙하는 방법이다.
④ 파일 카빙은 디스크의 비할당영역에 있는 파일 조각을 조합하여 삭제된 내용을 복구하는 방법이다.

11. 스마트폰 데이터의 논리적인 추출 방법으로 가장 적절하지 **않은** 것은?

① 탈옥(jailBreak)
② 루팅(Rooting)
③ Backup 메커니즘을 이용한 데이터추출
④ Rawshark의 필드 집합 출력

12. 윈도우 레지스트리에서 <보기 1>과 <보기 2>를 가장 적절하게 연결한 것은?

<보기 1>

(가) HKEY_CURRENT_CONFIG
(나) HKEY_LOCAL_MACHINE
(다) HKEY_CLASSES_ROOT

<보기 2>

㉠ 시스템 전체에 적용되는 하드웨어와 소프트웨어의 설정 데이터를 저장
㉡ 시스템이 시작할 때 사용되는 하드웨어 프로파일 정보를 저장
㉢ 파일 확장자에 대한 정보, 각 파일과 프로그램 간의 연결정보, 마우스 오른쪽 단추의 등록 정보를 저장

	(가)	(나)	(다)
①	㉡	㉠	㉢
②	㉢	㉡	㉠
③	㉢	㉠	㉡
④	㉠	㉢	㉡

13. 스마트폰 포렌식 분석 보고서에 필수적으로 포함되어야 할 사항으로 가장 적절하지 **않은** 것은?

① 스마트폰 제조사, 모델
② 스마트폰 판매자 정보
③ 스마트폰 증거분석관 정보
④ 스마트폰 접수일시

14. 안티 포렌식(Anti Forensic) 기법에 대한 설명으로 가장 적절한 것은?

① 삭제된 증거 데이터를 복구한다.
② 암호화된 데이터 파일의 패스워드를 전수 조사한다.
③ 증거 자료에 대한 이미지를 생성할 때 반드시 BitLocker를 꺼야 한다.
④ 운영체제에서 자동으로 생성되는 정보 중에서 증거가 될 만한 모든 정보를 생성 즉시 자동으로 삭제한다.

15. 포렌식 분석에서 ADB(Android Debug Bridge) 작동 명령어에 대한 설명으로 가장 적절하지 **않은** 것은?

① adb devices: 현재 연결된 디바이스의 TCP/IP 포트 번호 확인이 가능하다.
② adb install: -i 옵션은 다른 디바이스로 복사되어 넘어가는 것을 방지하는 것이 가능하다.
③ adb shell: -s 옵션은 특정 디바이스를 지정하여 접속이 가능하다.
④ adb push: 현재 연결된 디바이스에서 PC로 파일 및 디렉터리 복사가 가능하다.

16. 포렌식은 원래 범인이 남긴 흔적을 대상으로 과학의 힘을 빌려 법적인 문제를 해결하는 작업을 의미한다. 괄호 안에 들어갈 용어로 가장 적절한 것은?

( )은(는) 접촉하는 두 물체 사이에는 반드시 흔적이 남는다는 이론이다. 범죄자가 범죄 현장을 드나들 때 무엇인가를 가지고 가며 범죄자는 흔적을 남긴다는 것이다. 디지털 세계에서도 범인은 파일 개방, 방문 기록, 프로세스 실행기록, 파일 삭제 흔적 등 다양한 흔적을 남기게 된다.

① 로카르드의 교환 법칙(Locard's Exchange Principle)
② 증거 규칙(Rules of Evidence)
③ 정당성(Legitimacy)의 원칙
④ 전문 증거(Hearsay Evidence)

17. 안드로이드 스마트폰의 포렌식 분석에 대한 설명으로 가장 적절하지 **않은** 것은?

① Manifest.mbdb에는 파일의 도메인, access 시간이 기록되어 있다.
② 캐시(cache) 파티션에 App 설치 파일 등 임시파일이 있다.
③ 데이터는 SQLite, Local file 형식으로 저장되어 있다.
④ Preference에는 주로 환경설정 값이 저장되어 있다.

18. 디스크 이미징(Disk Imaging)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 디스크의 모든 물리적 섹터를 복제한다.
② 비트스트림 사본은 CRC(Cyclic Redundancy Check) 계산법을 사용하여 원본 데이터와 차이가 없는 지를 확인한다.
③ 디스크 섹터에 삭제 파일 정보가 남아 있는 경우 복구가 가능하다.
④ Source Read & Destination Write 저장 방식이다.

19. Access Point를 통하여 해킹을 당하고 있다. IEEE 802.11 패킷 수집을 위해 포렌식 수사관이 사용해야 할 도구로 가장 적절한 것은?

① FTK(Forensic Tool Kit)
② Autopsy
③ Airpcap
④ ProDiscover

20. 해시(Hash)와 관련된 설명으로 가장 적절하지 **않은** 것은?

① 잘 알려진 파일들의 해시 값을 모아놓은 것을 참조 데이터 셋(Reference Data Set)이라 한다.
② 원본 데이터에 대한 이미지 파일의 무결성 입증에 사용된다.
③ 해시 함수에 입력한 데이터의 크기에 따라 출력 해시 값의 길이는 가변적이다.
④ 특정 파일의 존재 여부를 확인하는 검사에 사용되는 데이터 세트로서 NSRL(National Software Reference Library)을 공개하고 있다.