【디지털포렌식개론】

1. 디지털 포렌식 수행절차에 대한 순서가 가장 적절한 것은?
① 디지털포렌식보고서→증거수집→증거포장 및 이송→증거분석
② 증거수집→디지털포렌식보고서→증거포장 및 이송→증거분석
③ 증거수집→증거포장 및 이송→증거분석→디지털포렌식보고서
④ 증거수집→디지털포렌식보고서→증거분석→증거포장 및 이송

2. 디지털 포렌식에서 저장 매체에 대한 복제를 수행할 때 가장 적절하지 **않은** 것은?
① 원본 디스크에 포렌식 도구인 쓰기방지 장치를 연결하고, 복제본을 생성한다.
② 원본 디스크의 저장 용량을 확인한 후, 원본 용량보다 더 많은 용량의 디스크를 사용하여 복제본을 생성한다.
③ 현장에서 원본 디스크에 대한 복제본을 생성 시, 원본과 복제본의 무결성을 입증하기 위하여, 해시 값을 생성하고, 원본과 복제본의 해시 값이 일치하는 것을 확인한다.
④ 원본 디스크를 인터넷 네트워크에 연결하여 복제본 디스크로 쉽게 복사하도록 하고, 네트워크 로그(log) 기록을 남기고 나서, 네트워크 접속을 차단한다.

3. 디지털 포렌식에서 하드디스크 '쓰기방지 장치'로 가장 적절한 것은?
① HxD ② Tableau
③ StegoHunt ④ Intella

4. 컴퓨터 하드디스크의 이미징 기능을 수행하는 포렌식 도구로 가장 적절하지 **않은** 것은?
① dd ② WireShark
③ Adepto ④ LinEn

5. 디지털 포렌식 사본 이미지 생성에 사용되는 것으로 가장 적절한 것은?
① Live Search ② KFF(Known File Filter)
③ OS Artifacts ④ FTK Imager

6. 윈도우즈 PC의 압수·수색과정에서 발견된 'Thumbs.db'에 대한 설명으로 가장 적절하지 **않은** 것은?
① 사진이나 이미지에 관한 작은 그림이 포함된 파일 형태로 저장된다.
② Thumbs.db는 사용자가 직접 생성하며, 기본적으로 숨김 속성은 해제되어 있다.
③ 특정시간에 해당 파일을 열었다는 사실의 입증이 가능하다.
④ 사진이나 이미지를 삭제해도 Thumbs.db 파일이 남아 있을 수 있다.

7. 압수된 10개의 컴퓨터 하드 디스크를 10명의 포렌식 수사관이 증거분석하고 있다. 법정에서 증거 채택을 위하여 디지털 포렌식에서 지켜야 할 가장 적절한 사항은?
① Normal NAT
② 연계 보관성(Chain of custody)
③ 데이터 부하분산(Data load balancing)
④ 패킷 필터링(Packet filtering)

8. 리눅스 운영체제에서 데이터를 수집하는 방법으로 가장 적절하지 **않은** 것은?
① 실행 중인 프로세스 정보를 획득하기 위하여 'ps -aux' 명령을 사용하였다.
② 현재 로그온 상태인 사용자를 확인하기 위하여 'who' 명령을 사용하였다.
③ IP 설정 정보를 확인하기 위하여 'ipconfig /all' 명령을 사용하였다.
④ ARP 정보를 확인하기 위하여 'arp -a' 명령을 사용하였다.

9. 디지털 포렌식 증거 수집에 대한 설명으로 가장 적절한 것은?
① 정보저장매체 또는 전자정보를 수집할 때부터 법정에 증거로 제출할 때까지, 변경 또는 훼손되지 않도록 무결성을 유지하여야 하고 그 과정을 기록하여 수사기록에 첨부하여야 한다.
② 증거 획득과정에서 증거로 판단되는 디지털 파일은 데이터 이미지 절차나 원본 데이터의 무결성 유지에 앞서, 현장에서 사용자가 직접 클릭하여 확인한다.
③ 디지털 증거의 획득 시에 오류가 생겨도, 제3의 전문가를 통해 정당한 증거로 입증 받을 수 있다.
④ 디지털 증거에 대한 증거분석은 증거 획득과정에서 원본 이미지와 사본 이미지를 모두 실행하여 인터넷 네트워크에 접속하고, 즉시 원본과 사본의 이미지의 실행 결과가 일치하는지를 확인해야 한다.

10. 텍스트 문서 name.txt를 name.hwp로 확장자만 수정하였다. 파일의 확장자에 상관없이 name.txt 파일의 본래 유형을 찾으려 할 때, 사용하는 방법으로 가장 적절한 것은?
① 인덱스(Index) 검색 ② 시그니처(Signature) 분석
③ 슬랙(Slack) 검색 ④ 타임 라인(Time line) 분석

11. 사이버범죄에 이용되고 있는 PC의 임시기억장소에 기억된 휘발성 증거를 압수·수색하는 방법으로 가장 적절한 것은?
① PC 종료와 함께 삭제되는 휘발성 정보를 우선적으로 획득하기 위하여, 인터넷 네트워크 접속 정보, 프로세스 정보 등 임시기억장소에 기록되는 정보 자료를 확보하고 범죄관련 화면과 실행 프로그램에 대한 현장 사진의 확보 및 사용자의 진술을 확보하고, 저장매체를 압수·수색한다.
② PC를 인터넷 네트워크를 통한 외부 접속을 실시하여, 저장매체에 대한 출력, 복제를 수행한다.
③ PC 전원을 우선 끄고 저장매체 자체를 압수하는 방식을 고려하여 가까운 장소에서 편리한 도구로 증거를 분석한다.
④ PC의 디스크에 대한 복제를 수행하여 휘발성 정보를 수집한다.

12. 디지털 포렌식에서 삭제된 파일의 복구와 관련된 설명으로 가장 적절하지 **않은** 것은?
① 파일을 삭제할 경우 메타정보와 실제 파일 내용을 초기화하지 않고, 단순히 메타정보의 특정 플래그만 변경시킨다.
② 파일 카빙(Carving)은 파일의 메타정보를 이용하여 삭제된 파일을 복구한다.
③ FAT 파일시스템에서 파일이 삭제될 경우 해당파일 Directory Entry의 오프셋 0x00 값이 삭제를 나타내는 0xE5로 변경된다.
④ 삭제 표시된 Directory Entry에 파일 크기와 시작 클러스터 정보를 이용하여 파일을 복구할 수 있다.

13. 아래 (㉠)에 들어갈 용어로 가장 적절한 것은?

> 윈도우즈 운영체제에서 (㉠)는(은), 파일의 앞부분(header)과 마지막부분(footer)에 있는 파일 고유의 정보이다. 응용 프로그램에서 생성한 파일임을 인식할 수 있도록 파일 내부의 특정위치에 있는 몇 바이트가 항상 동일한데, 이러한 고정 값을 (㉠)(이)라고 한다. 이러한 (㉠)도 의도적으로 변경할 수 있지만 확장자의 변경에 비해서 용이하지 않다.

① 레지스트리(Registry)　② 파일 확장자(File extension)
③ 파일 이름(File name)　④ 파일 시그니처(File signature)

14. 인터넷 네트워크에 접속한 윈도우즈 운영체제에서, 디지털 포렌식 수사관이 인터넷 접속 정보를 수집할 경우에, 필요한 항목으로 가장 적절하지 **않은** 것은?

① Temporary internet files　② Cookie
③ ProcessExplorer　④ Web history

15. 아래 (㉠)에 들어갈 용어로 가장 적절한 것은?

> 윈도우즈 운영체제에서 (㉠)는 부팅과정에서부터 로그인, 서비스 실행, 응용프로그램 실행, 사용자 행위 등 윈도우즈 운영체제의 거의 모든 활동에 관여한다. 특히 원격 접속 흔적, 드라이브 연결 흔적, 저장매체 사용 흔적 등의 정보를 이용하여 추가적인 포렌식 분석 대상을 선별하는데 활용할 수 있다.

① 레지스트리(Registry)
② 웹 히스토리(Web history)
③ 프로퍼티 리스트(Property list)
④ 메타 데이터(Meta data)

16. 디지털 포렌식 증거 분석에 활용하는, 디스크 브라우징(Disk Browsing) 기술의 설명으로 가장 적절한 것은?

① 디스크 파일 또는 저장매체 전체를 대상으로 특정 키워드인 파일이름, 속성, 내부 문자열, 코드 값, 시그니처를 쉽게 찾는 기술이다.
② 프로그램 정보와 네트워크 시스템 정보에 대한 레지스트리의 기록을 분석한다.
③ 디스크 파일 또는 저장매체에 저장된 파일의 시간정보, 내부 메타 데이터의 시간정보를 분석하는 기술이다.
④ 저장매체 또는 디스크 이미지의 내부 구조와 파일 시스템을 확인하고, 파일시스템 내부에 존재하는 파일에 대응되는 응용프로그램의 구동 없이 쉽고 빠르게 분석할 수 있도록 하는 기법이다.

17. 디지털 포렌식에서 해시 함수(Hash Function)에 대한 설명으로 가장 적절하지 **않은** 것은?

① MD5, SHA-1 등의 해시 함수가 사용되고 있다.
② 디지털 데이터의 위조·변조 문제를 검증하는 수단이다.
③ 파일의 무결성을 검증할 때, 파일의 이름이 바뀌면 해시 값도 바뀐다.
④ 디지털 데이터의 크기에 상관없이, 일정한 길이의 비트열(Bit stream)로 변환되어 해시 값을 산정한다.

18. 디지털 포렌식에서 증거 관련 보고서를 작성하는 방법에 대한 설명으로 가장 적절하지 **않은** 것은?

① 포렌식 수사관은 분석 과정에서 이용한 분석도구, 분석을 수행한 절차, 그리고 분석 결과를 포렌식 보고서에 명확하게 기록해야 한다.
② 포렌식 보고서의 분석 결과를 증거 자료로 인정받기 위해서는, 보고서의 분석 결과를 재현하였을 경우에도 완벽히 일치하여야 한다.
③ 포렌식 분석에 활용되는 증거수집 기술과 방법이 이미 증거 추출 과정에서 사용되었으므로, 보고서에는 증거수집 도구만 기록해도 된다.
④ 포렌식 보고서는 증거 분석에 대한 사실관계를 상세하고 객관적으로 기록해야 한다.

19. 압수된 디지털 저장매체로부터 출력한 문건을 증거로 사용하기 위한 요건으로 가장 적절하지 **않은** 것은?(다툼이 있는 경우 판례에 의함).

① 디지털 저장매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 한다.
② 디지털 저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았음이 담보되어야 한다.
③ 디지털 저장매체 원본과 '하드카피' 또는 '이미징'한 매체를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다.
④ 원본 가용성은 증거능력의 요건에 해당하므로 포렌식 수사관이 그 존재에 대하여 가용성을 구체적으로 주장·증명해야 한다.

20. 수사기관이 압수·수색 영장을 집행할 때의 설명으로 가장 적절하지 **않은** 것은?(다툼이 있는 경우 판례에 의함).

① 정보저장매체인 경우에는 영장 발부의 사유로 된 범죄 혐의사실과 관련 있는 정보의 범위를 정하여 출력하거나 복제하여 이를 제출받아야 하고, 피의자나 변호인에게 참여의 기회를 보장하여야 한다.
② 압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준할 자에게 교부하여야 한다.
③ 압수된 정보의 상세목록에는 정보의 파일 명세가 특정되어 있어야 하고, 수사기관은 이를 출력한 서면을 교부하거나 전자파일 형태로 복사해 주어야 한다. 단, 이메일을 전송하는 방식으로는 할 수 없다.
④ 법원은 압수·수색영장의 집행에 관하여 범죄 혐의사실과 관련 있는 정보의 탐색·복제·출력이 완료된 때에는 지체 없이 압수된 정보의 상세목록을 피의자 등에게 교부할 것을 정할 수 있다.