【디지털포렌식개론】

1. 피의자는 회사의 중요한 설계도면 파일을 업무용 PC에서 개인 USB로 복사하고, 이후 USB를 자신의 개인 PC에 연결하여 해당 파일 복사 후 이메일을 통해 경쟁 회사로 유출하였으나 설계도면 파일을 유출하지 않았다며 부인하고 있다. 위 행위를 입증하기 위한 것으로 가장 적절하지 **않은** 것은?
① USB 연결 시간 ② 파일의 해시(Hash)값
③ 업무용 PC의 파티션 정보 ④ USB 시리얼 번호

2. 디지털 증거 수집을 위한 디스크 복제와 디스크 이미징(Imaging)의 설명으로 가장 적절하지 **않은** 것은?
① 디스크 이미징은 원본 저장매체의 사본을 파일 형태로 만든다.
② 디스크 복제는 디스크 영역 중 비할당영역을 포함하지 않고 사본을 만들며, 디스크 이미징은 디스크 영역 중 비할당영역을 포함하여 사본을 만든다.
③ 디스크 복제와 디스크 이미징은 원본과 사본의 동일함을 증명하기 위한 방법으로 해시값을 이용한다.
④ 디스크 이미징으로 생성한 사본파일은 분석을 위한 분석 전용 소프트웨어가 필요하다.

3. 피의자가 아동 음란물 사이트에 접속해서 아동 음란물을 다운받아 소지한 혐의를 부인하고 있다. 피의자의 혐의를 입증할 수 있는 방법으로 가장 적절하지 **않은** 것은?
① 피의자가 사용한 PC의 인터넷 히스토리(History) 정보에서 해당 아동 음란물 사이트 URL이 발견되었다.
② 피의자가 사용한 PC의 다운로드 폴더에서 해당 아동 음란물과 해시값이 동일한 파일이 저장된 것을 확인하였다.
③ 피의자가 해당 PC를 사용한 시간과 그 PC에서 아동 음란물 사이트 접속한 시간이 일치하여 피의자가 해당 아동 음란물에 접속한 사실을 확인하였다.
④ 피의자가 사용한 PC의 숨김 폴더에 SafeBack 프로그램이 설치된 것을 확인하였다.

4. 피의자는 지하철에서 자신의 휴대폰을 사용하여 타인의 신체를 몰래 촬영한 혐의를 받고 있다. 피의자의 휴대폰에서 범죄 혐의와 관련된 디지털 증거를 획득하는 방법으로 가장 적절하지 **않은** 것은?
① Falcon을 이용한 획득 ② JTAG을 이용한 획득
③ Chip-off를 이용한 획득 ④ 데이터 케이블을 이용한 획득

5. 디지털 증거 수집에 대한 설명으로 가장 적절하지 **않은** 것은?
① 영장에 의한 압수·수색의 경우 범죄사실의 관련성과 피의자에게 혐의가 있다고 인정되는 경우에 한정한다.
② 영장에 의하지 않은 압수·수색 중 증거의 계속 사용을 위해 사후영장을 반드시 요하는 경우는 임의제출물의 압수인 경우다.
③ 도박·음란·기타 불법사이트 운영 사건 등 디지털 저장매체에 저장된 원본 디지털 데이터가 다시 범죄에 이용될 우려가 있는 경우 디지털 저장매체 자체를 압수할 수 있다.
④ 디지털 데이터를 압수하는 경우에는 범죄사실과 관계가 있다고 인정할 수 있는 범위를 정하여 출력하거나 복제하는 방법으로 압수하여야 한다.

6. 다음 웹 로그의 내용 중 ㉠, ㉡, ㉢, ㉣에 해당하는 용어를 순서대로 나열한 것으로 가장 적절한 것은?

> ㉠ 웹 서버 사용자가 사이트에 접근 시 사용자 IP 정보, 시간 정보, 요청 정보가 기록된다.
> ㉡ 웹 서버 내부에서 발생하는 에러와 사용자의 접속실패에 관한 정보가 기록된다.
> ㉢ 현재 웹 서버를 이용하기 전에 어떤 경유지를 거쳐서 도착하게 되었는지에 대한 정보를 알려준다.
> ㉣ 웹 서버 사용자에 대한 정보를 확인할 수 있는 로그로 사용자의 브라우저 종류와 버전, 운영체제의 종류 등에 대해서 알 수 있다.

① 엑세스 로그(Access Log) – 에러 로그(Error Log) – 에이전트 로그(Agent Log) – 레퍼러 로그(Referrer Log)
② 에이전트 로그(Agent Log) – 엑세스 로그(Access Log) – 에러 로그(Error Log) – 레퍼러 로그(Referrer Log)
③ 레퍼러 로그(Referrer Log) – 에러 로그(Error Log) – 엑세스 로그(Access Log) – 에이전트 로그(Agent Log)
④ 엑세스 로그(Access Log) – 에러 로그(Error Log) – 레퍼러 로그(Referrer Log) – 에이전트 로그(Agent Log)

7. 디지털 포렌식 분석에서 키워드, 시그니처 등으로 대상 파일들을 검색한다. 이에 대한 내용으로 가장 적절하지 **않은** 것은?
① 동일한 키워드라도 인코딩 방식에 따라 전혀 다른 값이 되기 때문에 검색하고자 하는 키워드의 형태를 결정해서 검색을 수행해야 한다.
② 단순한 일회성 검색은 로우 서치(Raw Search)를 이용하고, 키워드를 바꾸어 가며 여러 번 수행하는 검색은 인덱스 서치(Index Search)를 이용하는 것이 바람직하다.
③ 윈도우 기반 파일에서 시그니처에 따른 파일 확장자는 MBR Entry에 있으며, 확장자에 따라 연결되는 어플리케이션 정보는 레지스트리(Registry)에 저장하고 있다.
④ 데이터 은닉을 위해 파일의 확장자를 변경하는 경우가 있으므로 파일 확장자와 시그니처가 일치하는지 여부를 확인해야 한다.

8. 사용자의 인터넷 사용 흔적을 찾는 방법은 디지털 포렌식에서 유용하게 사용된다. 다음 내용 중 ㉠, ㉡, ㉢에 순서대로 들어갈 단어로 가장 적절한 것은?

> · (㉠)는 웹 사이트를 재접속할 때, 웹 페이지 데이터를 다시 다운받지 않고 다운받은 데이터를 사용하게 함으로써 빠른 웹 페이지 로딩을 가능하게 한다.
> · 브라우저 입장에선 사용자가 뒤로가기 버튼을 눌렀을 때 어디로 돌아가야 할지 기억할 필요가 있는데, 이러한 목적으로 만들어진 기능이 (㉡)이다.
> · (㉢)는 인터넷 사용자가 웹 사이트를 방문할 때, 웹 서버로부터 전송받아 저장되는 파일로서 웹 서비스 도메인, 만료시간, 보안 속성 등의 정보로 구성될 수 있다.

① 히스토리(History) – 웹 캐시(Cache) – 쿠키(Cookie)
② 웹 캐시(Cache) – 쿠키(Cookie) – 히스토리(History)
③ 웹 캐시(Cache) – 히스토리(History) – 쿠키(Cookie)
④ 쿠키(Cookie) – 히스토리(History) – 웹 캐시(Cache)

9. 윈도우 10 PC 바탕화면에 원본 파일을 생성하고, 다음 날 복사-붙여넣기로 복사본 파일을 생성하였다. 이 복사본 파일의 속성 정보에 대한 설명 중 가장 적절한 것은?
① 복사본 파일의 '수정한 날짜'는 원본 파일의 '수정한 날짜'와 동일하다.
② 복사본 파일의 '만든 날짜'는 원본 파일의 '만든 날짜'와 동일하다.
③ 복사본 파일의 '액세스한 날짜'는 원본 파일의 '만든 날짜'와 동일하다.
④ 복사본 파일의 '액세스한 날짜'는 원본 파일의 '액세스한 날짜'와 동일하다.

10. 증거 분석관이 인가되지 않은 USB 접속 흔적을 파악하기 위해 윈도우의 레지스트리를 분석 중이다. 관련된 내용 설명으로 가장 적절하지 **않은** 것은?
① USBSTOR는 SubKey를 통해 시스템에서 사용했던 USB 장치를 확인할 수 있다.
② Unique Instance ID는 동일 Device Class ID를 갖는 경우, 장치별로 구별되지 않는다.

③ Device Class ID에서는 연결된 USB의 제조사, 제품명, 버전을 확인할 수 있다.
④ Enum\USB에는 시스템에 접속되었던 모든 USB 장치에 대한 정보를 포함하고 있다.

11. 슬랙 공간(Slack Space)과 발생 원인의 연결이 가장 적절하지 **않은** 것은?
① 램(RAM) 슬랙 – 섹터 크기
② 파일 시스템(File System) 슬랙 – 클러스터 크기
③ 드라이브(Drive) 슬랙 – 볼륨 크기
④ 볼륨(Volume) 슬랙 – 파티션 크기

12. 범죄혐의와 관련된 윈도우 10 PC를 디지털 증거 분석하고 있다. 윈도우 이벤트 로그(Event Log)에 대한 설명으로 가장 적절하지 **않은** 것은?
① 이벤트 로그가 기록되는 로그 파일의 확장자는 .evtx이다.
② 이벤트 로그 '최대 이벤트 로그 크기에 도달할 때'의 기본 설정(Default)은 '필요한 경우 이벤트 덮어쓰기(가장 오래된 이벤트 먼저)'이다.
③ 시스템 로그는 윈도우 시스템 구성요소에서 기록한 이벤트로서, 응용 프로그램 개발자가 이벤트를 정의한다.
④ 보안 로그는 로그온 횟수, 로그인 오류 정보 등을 기록한 이벤트로서 관리자가 이벤트 유형을 지정하고 보안 로그에 기록한다.

13. 디지털 증거의 무결성에 대한 내용으로 가장 적절하지 **않은** 것은?
① 디지털 증거의 해시값을 확인 후, 소유자(관련자)의 서명을 받아야 한다.
② 저장매체를 압수한 경우 디지털 증거의 무결성 증명을 위해 피의자의 서명을 받아 봉인하고, 서명 봉인 과정을 영상 녹화한다.
③ 피고인이 재판과정에서 무결성을 부정하는 경우, 압수한 저장장치의 해시값과 사본파일의 해시값을 비교할 수 있도록 법원에 검증을 요구한다.
④ 디지털 증거의 무결성을 위해서는 디지털 포렌식 전 과정이 지체없이 신속하게 진행되어야 한다.

14. 피의자의 범죄혐의와 관련된 윈도우 PC를 디지털 증거 분석 중이다. 그 중 레지스트리의 하이브(Hive) 파일에 대한 설명으로 가장 적절하지 **않은** 것은?
① SAM은 로컬 계정 정보와 그룹 정보로 시스템 계정만 접근 가능하다.
② HARDWARE는 시스템의 하드웨어 장치 드라이버 매핑정보를 가지고 있다.
③ SYSTEM은 시스템 부팅에 필요한 전역 구성정보를 가지고 있다.
④ SECURITY는 패스워드들의 해시 정보를 가지고 있다.

15. 디지털 포렌식과 관련된 설명으로 가장 적절하지 **않은** 것은?
① 비트락커(BitLocker)가 설치된 PC가 로그온 상태라면 비트락커 해제를 위한 공격을 하지 않고도 데이터를 복원할 수 있다.
② 트루크립트(TrueCrypt)는 실시간 암호화 기능을 제공한다.
③ 윈도우 PC에서 빠른 포맷(Format)을 사용한 후에는 증거 데이터를 복원할 수 없다.
④ 스테가노그래피(Steganography)를 이용하여 사진이나 동영상 같은 파일에 메시지나 데이터를 숨길 수 있다.

16. 디지털 증거 수집을 위해 사용되는 다음의 디스크 이미징 툴 중, 이미징 소프트웨어로 가장 적절하지 **않은** 것은?
① SuperImager ② Forensic ToolKit
③ EnCase ④ ProDiscover

17. 윈도우의 NTFS 파일 시스템에는 다수의 메타 데이터 파일(Meta Data File)이 사용된다. 볼륨 내의 클러스터 할당 상태 정보를 관리하는 파일로서 가장 알맞은 것은?
① $MFT ② $Bitmap ③ $AttrDef ④ $LogFile

18. 이메일이나 첨부파일로 기업의 핵심기술이 외부로 유출될 수 있으므로 이메일 분석은 중요한 요소이다. 다음 내용 중 ㉠, ㉡, ㉢, ㉣에 들어가는 용어의 순서대로 가장 적절한 것은?

> 이메일 파일은 자체적인 포맷을 기반으로 한 Lotus Notes의 (㉠), Outlook의 PST와 (㉡), Outlook Express의 (㉢) 등이 있으며 MIME 형식을 기반으로 한 Mozilla Thunderbird의 MBOX, 다수의 웹 메일, Live Mail의 (㉣) 등이 존재한다.

① NSF – OST – DBX – EML
② OST – DBX – EML – NSF
③ EML – OST – DBX – NSF
④ NSF – DBX – OST – EML

19. 윈도우 PC의 디지털 증거 분석을 위해 프리패치(Prefetch)를 확인하려고 한다. 프리패치와 관련된 내용으로 가장 적절하지 **않은** 것은?
① 부트 프리패칭과 응용프로그램 프리패칭으로 구분할 수 있다.
② 특정 응용프로그램 이름과 실행 횟수를 파악할 수 있다.
③ 프리패치 파일에서 파일시스템 시간 정보(생성, 마지막 접근 시간 등) 획득을 통해 통합 타임라인 분석이 가능하다.
④ 프리패치는 시스템 복원을 목적으로 실행파일의 정보를 시스템에 저장하는 것이다.

20. 데이터베이스 포렌식으로 가장 적절하지 **않은** 것은?
① 데이터베이스 서버가 RAID로 구성되어 있는 경우에는 서버 운영을 정지시키고 RAID가 구성되어 있는 상태에서 EnCase나 DD로 이미지 파일을 추출하는 방법으로 데이터베이스의 데이터를 획득할 수 있다.
② 관계형 데이터베이스의 개체 무결성은 두 개의 릴레이션들 간에 명시되는 제약조건이며 올바른 연결을 보장하기 위한 제약조건으로 외래키와 기본키와의 관련으로 표현된다.
③ 데이터베이스 분석도구에는 SQLite Expert, Exchange EDB Viewer, EseDbViewer, Oxygen SQLite Viewer 등이 있다.
④ 데이터베이스 백업은 사실을 확인하는 데 중요한 자료가 될 수 있으며 특히 데이터베이스에서 특정의 레코드를 삭제한 것으로 의심되는 경우에 그 효용가치가 높아진다.