【디지털포렌식개론】

1. 범죄와 관련된 사용자 PC의 윈도우 레지스트리 헤더 정보 중 가장 적절하지 **않은** 것은?

① 시그니처(signature)
② 마지막 수정시간
③ 카탈로그 파일(catalog file)
④ 하이브 포맷 버전 번호

2. 문서의 인쇄 SPL(spool file) 포렌식 분석에 관한 설명으로 가장 적절하지 **않은** 것은?

· SPL 문서의 인쇄 작업이 끝나면 스풀(spool) 데이터인 ①shd 파일과 ②spp 파일은 자동으로 삭제된다.
· 삭제된 스풀 파일은 하드디스크의 ③미할당 영역과 ④페이징 파일에서 복구할 수 있어, 인쇄된 기밀 유출 문서를 알아낼 수 있다.

3. 기밀 데이터 유출사건과 관련된 USB 장치 분석에 대한 설명으로 ㉠, ㉡에 알맞은 용어는?

USB를 윈도우 시스템에 연결시키면, 다양한 (㉠)가 (㉡)와 함께 레지스트리에 남게 된다.

	㉠	㉡
①	아티팩트	setupapi.dev.log
②	아티팩트	setup.apidev.db
③	개인정보	usb.read.log
④	개인정보	usb.dev.db

4. 윈도우 시스템의 WinPrefetchView를 이용하여 얻을 수 있는 정보 중 가장 적절하지 **않은** 것은?

① 응용프로그램 이름, 경로 정보
② 응용프로그램 마지막 수행 시간 정보
③ 응용프로그램 수행 시 참조된 DLL, INI 경로 정보
④ 응용프로그램 7초 모니터링 후, 프리패치 526개의 파일 생성 정보

5. 윈도우 시스템의 아이콘캐시(IconCache) 분석으로 가장 적절하지 **않은** 것은?

① IconCache는 Iconographic model을 사용하면 보임
② IconCache_##.db 형태로 저장
③ Fortools 라이브러리를 사용하면 확인이 가능
④ IconCache.db 분석에서 삭제된 응용프로그램의 존재 여부

6. 윈도우 운영체제 이벤트 로그 분석에서 가장 적절하지 **않은** 것은?

· 범죄 관련 증거자료를 포렌식 분석관이 수집 분석할 때, 외부장치 연결, ①공유 폴더 사용/해제, 원격 연결/해제, 네트워크 연결/해제, ②파일/레지스트리 조작, 프로세스 생성, ③이벤트 로그 삭제의 행동 분석이 가능하다.
· 윈도우 시스템의 이벤트를 로그 형태로 관리하며, 이벤트 로그는 윈도우 기본 프로그램인 ④이벤트 리서처(Event Researcher)를 통해서 볼 수 있다.

7. 스마트폰 단말기에 관한 포렌식 분석에서 빈칸에 가장 적절한 것은?

스마트폰 단말기는 휴대폰 장치 및 가입자 식별 모듈로 구성되어 있다. (　　)(은)는 모바일 장치나 단말기를 유일하게 식별하는 데 쓰이는 번호로 처음 6~8자리 숫자는 유형할당코드(type allocation code)이다. 유형할당코드는 무선 장치의 유형을 식별한다.

① 스마트폰 Model-Version
② 스마트폰 S/N(Serial Number)
③ IMEI(International Mobile Equipment Identity)
④ 스마트폰 국제 전화 번호

8. 스마트폰에 들어있는 SIM 카드 포렌식 분석에서 가장 적절하지 **않은** 내용은?

· SIM 카드의 IMSI는 고유번호이다. ①MCC(Mobile Country Code)는 IMSI의 처음 3자리 숫자를 의미하며, 뒤에 오는 2~3자리 숫자는 ②MNC(Mobile Network Code)이다.
· IMSI의 마지막 부분은 최대 10자리 ③MSIN(Mobile Subscriber Identity Number)으로, 휴대폰 통신사에 의해 생성되며 통신망 가입자를 식별하는 역할을 하고 있다.
· ④MSISDN(Mobile Subscriber Integrated Services Digital Network)은 19~20자리 또는 더 작은 수로 SIM 카드에 새겨져 있다.

9. 웹 아티팩트에 관한 설명으로 ㉠, ㉡에 가장 적절한 것은?

· 웹 침해사고 분석을 하는 경우 웹 아티팩트에는 (㉠)가 포함된다.
· 악성코드 유포 사이트로 사용자를 이동하게 만드는 소셜 엔지니어링 공격의 경우, (㉠)의 데이터는 특정 (㉡)로 이동하였음을 알려준다.
· (㉡)을(를) 추출한 후 내·외부의 자료를 근거로 이미 알려진 악성 웹 사이트 목록과 비교해 볼 수 있다.

	㉠	㉡
①	Web history	Mac Marshal
②	Da_destination.db	URL
③	Web history	URL
④	Da_destination.db	Mac Marshal

10. 윈도우 운영체제에서 바로 가기 Link File 분석으로 알 수 있는 것 중 가장 적절하지 **않은** 것은?

① 원본 파일시스템 경로
② LNK 파일 타임스탬프
③ 원본 파일 속성(읽기전용)
④ LNK 파일이 아카이브된 메모리의 주소

11. 타임라인 분석에서 가장 적절하지 **않은** 것은?

· 해킹사고를 조사할 때 응용 프로그램이나 ①파일의 실행 시점은 매우 중요하다.
· 타임스탬프는 응용 프로그램이나 ②메모리 이미지를 검사할 때와 마찬가지로, 또 다른 조사를 수행할 때도 찾을 수 있다.
· 또한, 메모리 이미지에서 특정 ③이미지 파일을 식별하면, 응용 프로그램이나 파일의 ④접근 날짜와 시간을 비교할 수 있고, 시스템에서 관찰됐던 다른 활동과 상호 연관시킬 수 있다.

12. 산업기밀 유출 사고로 압수·수색한 하드디스크 이미징 작업을 수행할 때, 가장 적절하지 **않은** 것은?

① dd 명령어로 파일과 볼륨을 복사하여 이미지를 만들 수 있다.
② 라이브 이미징을 수행하면, 파티션과 마스터 부트 레코드까지 복사된다.
③ 이미지 파일 생성 후에 저장되는 경로에 대한 설정과 파일 압축 크기 설정이 가능하다.
④ 가상화 소프트웨어의 스냅샷 기능을 활용하여 이미지를 만들 수 있다.

13. 섬네일(Thumbnail)은 원본파일이 삭제되더라도 지워지지 않아 증거자료로 사용할 수 있다. 섬네일을 분석한 형식과 설명으로 가장 적절하지 **않은** 것은?

① Thumbcache_32.db - 32×32 픽셀보다 작은 섬네일이 저장되며 모두 GIF 형식이다.
② Thumbcache_96.db - 32×32~96×96 픽셀 사이의 섬네일이 저장되며 모두 BMP 형식이다.
③ Thumbcache_256.db - 96×96~256×256 픽셀 사이의 섬네일이 저장되며 모두 JPEG 또는 PNG 형식이다.
④ Thumbcache_1024.db - 256×256~1024×1024 픽셀 사이의 섬네일이 저장되며 모두 JPEG 형식이다.

14. 피의자에게 압수한 하드디스크를 물리적 볼륨으로 이미징 할 때, FTK Imager 프로그램에 관한 설명 중 가장 적절하지 **않은** 것은?

① FTK Imager의 실행을 위해서는 관리자 권한이 필요하다.
② Create Disk Image를 클릭해 소스 선택창에서 Logical Drive를 선택한다.
③ 압수된 드라이브 보다 이미징 파일이 저장될 드라이브의 용량은 커야한다.
④ 2개는 이미징에 포함된 드라이브이며, Image Destination(s)은 이미지를 저장할 드라이브다.

15. Chrome 웹브라우저의 Cache 폴더의 저장내용으로 가장 적절하지 **않은** 것은?

① data_0 파일에는 인덱스 정보가 저장
② data_0 파일에는 오프셋 0x001부터 0x512바이트 단위로 저장
③ 캐시 데이터가 적은 경우 data_1, data_2, data_3에 저장
④ 캐시 데이터가 큰 경우 f_0001부터 연속된 파일에 캐시 데이터가 저장

16. 「디지털 증거의 처리 등에 관한 규칙(경찰청훈령 제1030호)」 제13조에서 압수·수색·검증 시 참여 보장에 관한 내용으로 가장 적절하지 **않은** 것은?

① 전자정보를 압수·수색·검증할 경우에는 피의자 또는 변호인, 소유자, 소지자, 보관자의 참여를 보장하여야 한다. 이 경우, 압수·수색·검증 장소가 「형사소송법」 제123조제1항, 제2항에 정한 장소에 해당하는 경우에는 「형사소송법」 제123조에 정한 참여인의 참여를 함께 보장하여야 한다.
② 경찰관은 제13조 제1항에 따른 피의자 또는 변호인의 참여를 압수·수색·검증의 전 과정에서 보장하고, 미리 집행의 일시와 장소를 통지하여야 한다. 다만, 위 통지는 참여하지 아니한다는 의사를 명시한 때 또는 참여가 불가능하거나 급속을 요하는 때에는 예외로 한다.
③ 경찰관은 피압수자 등이 전자정보의 압수·수색·검증 절차 참여 과정에서 알게 된 사건관계인의 개인정보를 공지하여, 피압수자 등에게 협조를 요청할 수 있다.
④ 전자정보 압수·수색·검증에 따른 참여의 경우 경찰관은 참여인과 압수정보와의 관련성, 전자정보의 내용, 개인정보보호 필요성의 정도에 따라 압수·수색·검증 시 참여인 및 참여 범위를 고려하여야 한다.

17. 파일의 미리보기, 삭제 및 제거에 관한 설명 중 ㉠, ㉡에 가장 적절한 것은?

> · 윈도우 운영체제에서는 로딩속도가 빠른 작은 이미지들을 따로 만들어 놓고 실제 이미지 대신 미리보기를 해준다. 미리보기 이미지가 생성되어 저장된 것을 (㉠)(이)라 한다.
> · (㉡)를 사용하는 운영체제는 파일 저장을 더욱 효율적으로 하고자 삭제된 파일 복구가 어렵게 제거하는 경우가 있다.

	㉠	㉡
①	링크파일	SAS 드라이브(Serial Attached SCSI Drive)
②	임시인터넷파일	솔리드 스테이트 드라이브(Solid State Drive)
③	index.dat	SAS 드라이브(Serial Attached SCSI Drive)
④	thumbs.db	솔리드 스테이트 드라이브(Solid State Drive)

18. 다음 중 포렌식 도구에 관한 설명으로 가장 적절하지 **않은** 것은?

① FTK는 포렌식 응용 프로그램으로 네트워크를 통한 이미징이 가능하다.
② BitLocker는 디스크 데이터를 복제하고 암호화 키를 제공하는 하드웨어 장비로, 데이터의 이미징과 완전 삭제, 복구를 지원한다.
③ EnCase는 주로 하드 드라이브와 기타 저장매체를 사용하는 디지털 증거조사에 관한 작업을 수행하며, 분석관이 요약 형식으로 사건 데이터를 출력할 수 있도록 보고기능을 갖고 있다.
④ X-Ways Forensics는 네트워크 접속이나 원격 캡처의 기능 없이 포렌식을 수행한다.

19. 윈도우10 시스템의 기본 전자우편(e-mail) 프로그램 대상 포렌식 분석으로 확인할 수 있는 것 중 가장 적절하지 **않은** 것은?

① 전자우편(e-mail) 관련 메타데이터는 store.vol 파일에서 일부 찾을 수 있다.
② 윈도우 기본 아티팩트 폴더 안에는 일정규칙을 가진 .dat파일이 있다.
③ 발송한 전자우편(e-mail)이 경유한 라우터 IP주소를 알 수 있다.
④ 레지스트리 경로에서 기본 전자우편 연동 프로토콜을 확인한다.

20. 다음은 디지털 증거의 증거능력에 관한 소위 '왕재산 사건'의 판례이다. ㉠~㉢에 가장 적절한 것은?

> · (중략) 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 (㉠)이 담보되어야 한다.
> · (중략) 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 검증된 프로그램의 (㉡), (중략) 피압수·수색 당사자가 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체의 (㉢)이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법으로 증명하는 것이 원칙(중략)

	㉠	㉡	㉢
①	무결성	신뢰성	Hash값
②	동일성	신뢰성	Hash값
③	신뢰성	Hash값	무결성
④	Hash값	무결성	신뢰성