◎ **객관식 문제**

1. 아래에 제시된 MS-DOS용 분석 도구 중 수사관들이 수작업으로 사용하는 것은 무엇인가? B

   A. 스마트

   B. Norton DiskEdit

   C. ByteBack

   D. DataLifter

2. 수집 대상 드라이브에서 삭제 된 파일의 조각을 다시 생성하는 기법은? A

   A. 카빙(carving)

   B. 스크래핑(scraping)

   C. 살베이징(salvaging)

   D. 스클럽팅(sculpting)

3. 사이버 포렌식에서 사건의 재구성이 필요한 이유는? A

   A. 범죄시 또는 사건 발생과정에서 어떤 일이 있었는지를 밝혀 용의자가 무엇을 했는지를 재현하기 위해

   B. 두 개로 이루어진 데이트 세트가 동일함을 증명하기 위해

   C. 숨겨진 정보까지 포함하여 용의자의 행동과 관련된 모든 정보를 복사하기 위해

   D. 포렌식 조사관이 수행한 프로세스를 상세하게 보여 줌으로써 보고서나 로그기록을 생성하기 위해

4. 아래에 열거된 것 중 디지털 증거추출을 위한 활동으로 볼 수 없는 것은? A

   A. 논리적 데이터 복사

   B. 암호 해독

   C. 디스크 이미징

   D. 카빙(carving)

5. 아래의 temporary 장소 중 암호가 저장 될 수 있는 곳은? D

A. system32.dll

B. CD-ROM 드라이브

C. 윈도우 레지스트리

D. pagefile.sys

6. 아래에 제시된 옵션 중 플랫폼 특화 암호화 도구의 예로 적당한 것은? C

A. GnuPG

B. TrueCrypt

C. BitLocker

D. Pretty Good Privacy (PGP)

7. 키워드 검색은 사이버포렌식 절차 중 어느 단계에 해당하는가? C

A. 보고서 작성

B. 사건 재구성

C. 증거 추출

D. 증거 획득

8. 디스크 수집을 수행하는 과정에서 원시 데이터 포맷을 복제하기 위한 UNIS/Linux의 명령은 무엇인가? D

A. format

B. Tar

C. dump

D. dd

9. 해시 값을 생성하거나 다른 유사한 방법을 통해 두 세트의 데이터가 동일하다는 것을 증명하는

것을 무엇이라고 하는가? C

A. 검증(verification)

B. 타당성 검사(validation)

C. 무결성 입증(integration)

D. 편집(compilation)

10. 사이버 포렌식에 대한 정의로 적당한 것은? D

A. 범죄를 해결하기 위해 컴퓨터를 사용하는 것이다.

B. 전자 증거를 조사하는 것이다.

C. 인터넷상의 의사소통 패턴을 분석하는 것을 말한다.

D. 사이버 공간에서 발생한 인간의 범죄를 이해하기 위해 현재의 범죄 패턴을 분석하는 것이다.

11. 안티포렌식에 대한 설명으로 부적합한 것은? D

A. 안티포렌식의 주요 4가지 형태는 파괴, 은닉, 접촉회피 및 암호화이다

B. 디가우싱 장비를 이용하는 경우 자기장에 노출되어 단 시간내 삭제가 가능하고 디스크 재활용이 불가하여 데이터복구가 불가능하다

C. 주로 활용되는 증거자료 은닉장소는 Partition Gap, 슬랙공간, 파일내부, Bad block 등이 사용된다

D. Data Hiding은 숨기고자 하는 파일을 다른 파일 내부에 심어 은닉하는 방법을 말한다

12. 컴퓨터 바이러스와 웜의 차이점은 무엇인가? A

A. 웜은 컴퓨터 시스템 전부분에서 스스로 복제되고 확산되는 바이러스 유형을 말한다.

B. 바이러스는 스스로 복제하는 성향을 가지고 있으며, 웜은 내·외부 시스템을 상호 연결시키는 속성을 가진다.

C. 바이러스는 시스템 및 응용 프로그램 소프트웨어를 공격 대상으로 하는데 비해, 웜은 컴퓨터 파일을 대상으로 활동한다.

D. 바이러스 및 웜은 차이점이 없기 때문에 서로 바꿔 써도 무방하다.

13. 컴퓨터에서 실행되는 모든 키 스트로크 및 마우스 클릭을 기록하는 프로그램은 무엇이라고 하는가? D

A. 키보드 레코더

B. 트로이 목마

C. 바이러스

D. 키 로거

14. 신분 도용(identity theft)에 대한 설명으로 옳은 것은? D

A. 웹상 활동이 많아지면서 자신에 대한 지각을 상실한 상태

B. 게임 등을 하면서 스스로가 게임의 주인공으로 행세하는 행위

C. 어떤 사람이 자신의 외형을 변화시켜 다른 사람으로 보이게 하는 것

D. 어떤 사람이나 단체가 사기행위를 할 목적으로 다른 사람의 신분으로 가장하는 것

15. 기업이 자사의 컴퓨터 시스템에 침입시키기 위해 고용하는 컴퓨터 보안 전문가를 무엇이라고 하는가? C

A. 해커

B. 모험지향 해커

C. 화이트 해커

D. 블랙 해커

16. 사이버 반달리즘(사이버공간 질서 파괴행위)에 해당하는 행위를 하는 인물은? D

A. 스크립트 키디 B. 모험주의해커 C. 화이트 해커 D. 블랙 해커

17. 응용 툴을 활용하지 않고 삭제 된 컴퓨터 파일을 복구할 수 있는 방법은? D

A. "안전 모드"에 있지 않으면 가능

B. 불가능

C. 가능, 하지만 삭제된 직후 시점에서만

D. 휴지통에서 복구가 가능

18. 기업이 상품 및 서비스를 광고하는 것으로 사용자가 수신을 원치 않는 메일을 무엇이라고 하는가? B

A. 컴퓨터 바이러스 B. 스팸 C. 쿠키 D. 악성웨어

19. 사이버 포렌식에서 휘발성 증거 수집이 필요한 이유로 적당한 설명은? A

A. RAM에 저장된 정보를 조사하기 위해

B. 인터넷 질서를 문란케 하는 인물을 찾아내기 위해

C. 컴퓨터 자원에 대한 위협 요인을 식별하기 위해

D. 범죄를 자행 중에 있는 범인을 검거하기 위해

20. 현재 작업하고 있는 가정 컴퓨터에서 연구원(직장)의 랩탑으로 자료를 보내고자 할 때 필요한 무선장치는? C

A. RFID

B. Bluetooth

C. WiFi 또는 Bluetooth

D. 마이크로파

21. 컴퓨터를 내장 하드 드라이브와 함께 처분하고자 할 때 타인이 나의 개인정보에 접근하지 못하도록 하기 위해 취해야 할 가장 적당한 조치는? D

A. 애플리케이션 소프트웨어를 복사했는지 확실히 확인한다.

B. 내 문서(my document) 폴더 안에 저장된 문서들을 백업한다.

C. 내 문서, 임시 인터넷 파일 및 시스템 환경 설정에 저장된 파일들만 삭제하면 된다.

D. 개인파일을 모두 삭제하고, 컴퓨터 조각모음 및 디스크 청소 절차를 진행한다.

22. 컴퓨터 파일을 삭제하면 어떻게 되는가? C

A. 해당 디스크 드라이브에서 파일이 지워지고 해당 공간은 새 파일에 할당된다.

B. 디렉토리에서 파일이름과 내용이 모두 삭제된다.

C. 파일이 휴지통으로 이동된다.

D. 파일은 삭제된 것으로 표시되면서 휴지통으로 이동하고, 원래 공간에서 지워진다.

23. 진정성 유지를 위해 신중한 증거 처리가 요구되는 사이버포렌식의 단계는? D

A. 수집 단계

B. 보고 단계

C. 증거 현출단계

D. 위의 모든 단계

24. 다음 중 생체 인식 장치로 볼 수 없는 것은? D

A. 눈

B. 지문

C. 얼굴 특징

D. 사용자 ID/암호

25. 다음 중 사이버 포렌식 수행절차를 바르게 나타낸 것은? B

① 증거 수집 ② 증거분석 및 보고서 작성 ③ 증거제출 ④ 증거 확인 ⑤ 증거 포장 및 이송

A. ④ → ① → ② → ⑤ → ③

B. ④ → ① → ⑤ → ② → ③

C. ① → ② → ④ → ⑤ → ③

D. ① → ④ → ② → ⑤ → ③

26. 귀하의 웹 활동 정보를 저장하려는 사업체의 시도를 어떻게 차단할 수 있겠는가? B

A. 인터넷에서 제품 및 서비스를 구매하지 않는다.

B. 쿠키 생성을 막는다.

C. SpamWare를 사용한다.

D. SpyWare와 SpamWare를 설치 사용한다.

27. 파일 마지막 부분에 사용하지 않은 체 비어있는 공간을 무엇이라고 하는가? B

A. 할당 공간

B. 슬랙 스페이스

C. 여유 공간

D. 쉼 공간

28. RAID(Redundant Array of Independent Disk)에 대해 잘못 설명한 것은? D

A. 여러 개의 하드 디스크에 데이터를 나눠서 저장하는 기술로 복수배열 독립 디스크라고도 한다

B. Stripping 방식은 여러 개의 하드디스크에 동시에 저장하는 방식이다

C. Mirroring 방식은 데이터의 안전성을 우선으로 하여 같은 데이터를 중복 보관한다

D. Parity Across 방식은 최소 3개 이상의 디스크를 필요로 하며 디스크 용량 전부를 사용하게 된다

29. 다음 중 전자 메일 개인 정보 보호 정책 조항의 일부가 아닌 것은 무엇인가? D

A. 합법적인 전자 메일 사용자가 누구인지 정의한다.

B. 메일 백업 절차를 알려준다.

C. 누군가의 전자 메일을 읽는 합법적인 근거를 설명한다.

D. 전자메일이 외부로 전송되면 기관에서 전적인 통제권을 갖는다는 것을 사람들에게 알려준다.

30. 디스크에 숨겨져 있는 정보를 찾을 수 있는 공간을 골라라. D

A. 삭제된 파일

B. 슬랙 공간

C. 게시 공간

D. 위의 것 모두

31. 네트워크를 통한 데이터 전송시 암호화가 필요한 것은 전송과정에서 암호를 절취할 수 프로그램이 있기 때문이다. 이때 사용되는 패스워드 절취 프로그램을 무엇이라고 하는가? C

A. 트로이 목마

B. 몰 웨어

C. 스니퍼

D. 애드웨어

32. 사이버 포렌식 활동은? B

A. 의사가 하는 일

B. 수사관이 하는 일

C. 자동차 판매원의 업무

D. 교수의 연구 활동

33. 임시 인터넷 파일에 대한 분석방법으로 잘못된 것은? A

A. 방문한 사이트에 대한 임지저장 파일로 동일 웹페이지에 재접속시 인터넷에서 손쉽게 주소를 가지고 오도록 작용하는 파일이다

B. 삭제된 임시 파일은 Encase 등 도구를 사용하여 복구할 수 있다

C. 방문한 사이트의 웹페이지, 이미지, 스크립드 등이 저장되어 있어 해당 사이트의 내용을 확인할 수 있다

D. 이메일, 주민번호, 수신 메일 등도 확인이 가능하다

34. 증거 인증 과정에서 타임스탬프 기록을 복제해야 하는 이유는? C

A. 컴퓨터 재판매를 위해

B. 지워질 수 있기 때문

C. 증거로서 받아들여질 수 있도록

D. 필요한 경우 변경하기 위해

35. 497. History 파일 분석에 대한 분석방법으로 틀린 것은? B

A. History 파일은 브라우저를 사용해서 접속했던 웹사이트의 URL목록을 말한다

B. 모든 기록은 주간 단위로 기록된다

C. Hits 수로 자주 방문하는 사이트 조회가 가능하다

D. 검색 사이트의 경우 URL의 Query String에 검색 키워드가 남아있어 어떤 검색을 시도했는지 확인이 가능하다

36. 컴퓨터 전원을 차단하면 작업 중이던 데이터가 사라지는 저장매체는? A

A. RAM

B. Disk

C. DVD

D. CD-ROM

37. 방화벽으로 외부 인터넷과 접속을 차단하고 기관 내부에서만 사용하도록 설정된 네트워크를 무엇이라고 하는가? C

A. Dedicated Internet

B. Extranet

C. Intranet

D. Private Internet.

38. 캐쉬 메모리(Cash Memory)란? A

A. 처리 대기 중에 있는 데이터를 임시적으로 저장하는 장소

B. 데이터 파일을 저장하는 특수 저장소

C. 복호화를 위한 장비

D. 이미 처리된 데이터를 저장하는 장소

39. RAM과 CPU의 차이를 설명한 것으로 올바른 것은? B

A. RAM은 통상 컴퓨터 외부에 위치하고 CPU는 내부에 장착되어 있다.

B. CPU는 자료처리를 할 수 있다.

C. RAM은 컴퓨터의 두뇌에 해당한다.

D. RAM은 CPU의 옛말이다.

40. 기밀성(confidentiality)에 대한 설명으로 적당한 것은? A

A. 메시지와 데이터에 대한 접근 허가를 받은 사람만 볼 수 있도록 보증하는 것

B. 컴퓨터와 인터넷을 기업윤리에 맞게 사용하도록 규정한 정책이나 절차

C. 원할경우 타인의 관찰을 받지않고 자신의 소유물에 대한 통제권을 가지고 혼자 있을 권리

D. 다른 사람을 대하는데 있어 취해야 할 행동규범을 정한 원칙이나 표준

41. 증거추출 행위로 분류할 수 없는 것은? A

A. logical data copy

B. decrypting

C. bookmarking

D. carving

42. NTFS 파일 복구에 대해 잘못된 것은? B

A. Index는 파일이 삭제되면 재정렬이 수반되어 Index에서 파일 명과 path을 얻을 수 없다

B. 파일이 삭제되는 경우 MFT Entry의 모든 항목도 사라진다

C. 파일이 Resident인 경우 $DATA 속성을 이용하여 완전 복구가 가능하다

D. 윈도우는 MFT Entry를 할당할 때 'first-available' 방식으로 동작하기 때문에 삭제보다 추가가 많을 경우 복구에 실패할 가능성이 높아진다

43. E-mail log자료에서 확인할 수 없는 것은? D

A. E-mail messages an account received

B. Sending IP address

C. Receiving and reading date and time

D. Sender's name

44. 악성 봇에 감염된 컴퓨터를 일컫는 말은? A

A. 좀비

B. 안드로이드

C. 웜

D. 트로이목마

45. 휘발성 데이터에 대해 잘못 설명된 것은? C

A. 전원이 끊어지면 손실되는 데이터를 말한다

B. 현재 시스템의 날짜와 시간, 프로세스 정보, 접속자 신원, 열려있는 포트정보 등이 해당한다

C. 레지스트리 정보, 이메일, 암호화된 파일 등은 전원을 끊기 전에 수집해야 한다

D. 메모리에 남아있는 최근 접속기록도 휘발성 정보에 해당한다

46. 네트워크에 연결된 저장매체 압수시 고려해야 할 점은? D

A. 데이터 전송 속도 파악

B. 네트워크에 대한 접근권한 확보

C. 안티 바이러스, 안티 스파이웨어 및 방화벽 작동 여부 확인

D. 위의 것 모두

47. 사회공학적 기법(Social Engineering)이란? A

A. 상대방으로 하여금 기밀정보를 누설하거나 이러한 행동을 하도록 하는 유도하는 행위

B. 도로, 항만, 댐 등과 같은 물리적 건축물에 대한 도안, 건설 및 유지를 위한 공학적

C. 분석, 설계, 생산 등 물리학에 적용되는 공학 원칙

D. 현대 DNA기술을 이용하여 인류의 장기 게놈을 직접 조작하는 행위

48. 피싱 이메일에 대한 설명으로 적당한 것은? C

A. 온라인에서 가장 싸게 피싱 장비를 구입할 수 있는 사이트 소개한 친구의 이메일

B. 지저분한 내용이 들어 있는 이메일

C. 이유 없이 패스워크, 신용카드 번호 등과 같은 개인정보를 요구하는 이메일

D. 친구로부터 낚시하러 가자고 제의 받은 메일

49. 루트킷(rootkit)에 대한 설명으로 바른 것은? C

A. 생물학자가 식물을 보살필 때 쓰는

B. 사전 정의된 UNIX 디렉토리를 일컫는 용어

C. 컴퓨터 보안체계의 침해를 막기 위한 DNS root zone에 설치된 서버

D. 컴퓨터 시스템 하위 레벨에서 작동하는 운영체제(OS)

50. 시스템 트레이에서 윈도우 버전을 보기 위해 사용되는 것은? A

A. 레지스터리 편집기(registory editor)

B. 그룹 정책 편집기(group policy editor)

C. 디스크 유틸리티(disk utilities)

D. 디스크 포멧(disk format)

51. 모바일 데이터 수집 요령에 부합하지 않는 것은? C

A. 수집과정과 관련없는 것은 모바일 데이터를 변경할 수 있으므로 주변에서 제외

B. 모바일 단말기 접근을 위해 포번호, 패스코드. 패턴 락, PIN등 관련정보 사전 수집

C. 단말기 데이터를 즉시 수집하기 어려운 경우 공범 등으로부터 추가연락을 예상, 전원 ON 상태에서 증거수집을 계속

D. 모바일 전원 차단이 어려운 경우에는 비행기 모드 또는 데이터 변형이 일어나지 않도록 차폐장치 사용 등 네트워크 차단대책 강구

52. 다음 중 우리나라 형사소송법에 규정되어 있지 않은 내용은? C

A. 임의수사의 원칙

B. 사인 수집 위법수집증거 활용 원칙

C. 전문증거 원칙

D. 위법수집증거 배제의 법칙

Case 1

법원의 명령장(court order)에 따라 법규를 위반한 A사의 메일 서버에서 2천 6백만명 이상의 전자우편이 조사대상이 되었다. 사이버포렌식 전문가인 귀하는 수사당국으로부터 메일 서버에 대한 포렌식 조사를 요청받았다

53. 아래 설명 중 메일서버 구성파일을 넘겨 받은 포렌식 전문가가 수행해야 할 업무를 바르게 표현한 것은? A

A. 관리자, 시간적 범위, 키워드, 의심파일을 걸러낼 정보와 같은 검색 범위와 관련성이 있는 정보를 확보한다

B. 인덱싱 도구에 저장소를 불러들여 관리자별, 날자별로 정리한다

C. 전자우편 도구를 사용하여 .eml 파일로 변환한 후 날자별로 정리한다

D. 소스와 원본에 대한 독립적인 수사를 진행하고, 전자우편 사용자를 인터뷰하여 사용자 인터액션의 개요를 만든다

54. 다음 중 저장소를 분석하기 위한 툴을 선정하기 위해 따라야 하는 접근 방식은? C

A. 전자우편의 메타데이터 파괴를 막기 위하여 전자우편 시스템 개발자가 만든 소프트웨어를 사용한다.

B. 저장소를 .eml 형식으로 변환하기 위한 유료 툴을 사용한다

C. 포렌식적으로 알맞은 툴로 저장소의 내용을 처리한다

D. 호환되는 전자우편 툴을 사용하여 주고 받은 내용의 패턴을 파악하고, 관련 메일을 출력한다

55. 모바일 포렌식의 문제점이 볼 수 없는 것은? C

A. 데이터를 획득하고 저장하는데 표준적인 매뉴얼이 부재

B. 다양하고 첨단기술을 응용한 하드웨어와 소프트웨어가 존재

C. 오늘날 다양한 모바일 단말기 등장으로 포렌식 기술도 급속도로 발전

D. 포렌식 도구들이 메모리에 직접 접근하지 못하고 모바일 S/W나 H/W 인터페이스에 의존

56. 침입방지 시스템에 대한 설명으로 틀린 것은? A

A. 보안을 높이는데 가장 일차적인 장치로 내부 네트워크를 지나는 패킷을 사전 약정된 규칭에 따라 차단하거나 보내주는 기능을 수행

B. 시스템 및 네트워크 자원에 대한 다양한 침입 행위를 실시간으로 탐지, 분석하여 비정상 패킹을 차단하는 시스템

C. 네트워크 기반 IDS와 호스트기반 IDS로 구분

D. 인가된 사용자의 악의적인 행동 감시가 필요한 환경에서도 적용

Case 1

동료 여직원으로부터 자신의 상사에게서 받은 전자우편에 대해 조사해 달라는 요청을 받았다. 전자우편은 내용은 상사가 여직원을 협박하는 용어들이 포함되어 있으며 메일의 헤더는 아래와 같다.

```
Delivered-To: SallySmith@xyzzzy.com
Received: by 11.36.81.3 with SMTP1 id e3cz239nzb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)
In-Reply-To:<20050329231145.62086.mail@mail.emailprovider.com>
Return-Path:
Received: from mail.emailprovider.com (mail.emailprovider.com [111.111.11.111]) by mx.gmail.com with SMTP id
h19si82r631rnb.2005.03.29.15.11.46; Tue, 29 Mar 2005 15:11:47 -0800 (PST)
Message-ID: <20050329231145.62086.mail@mail.emailprovider.com>
Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue, 29 Mar 2005 15:11:45 PST
Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST)
From: Loverboy <loverboy2343@wa12hoo.mx>
Subject: Hello
To: Sally
```

57. 다음 중 헤더의 어떤 부분이 조작된 것으로 판명되는가? A

A. 2개의 동일한 Message-ID 가 헤더에 존재한다

B. 송/수신 마커의 타임 존이 동일하다

C. SMTP는 메일의 프로토콜이 아니다

D. 타임 존의 오프셋 -0800 은 PST (Pacific Standard Time)와 맞지 않는다

58. 메일 발신자를 알아내기 위해 가장 먼저 접촉하여야 할 대상은 누구인가? C

A. 11.11.111.111의 메일 관리자

B. mail.emailprovider.com 의 메일 관리자

C. wa12hoo.mx 의 메일 관리자

D. samspade.org 의 메일 관리자

59. 다음 중 송신자의 네트워크 주소를 성공적으로 숨길 수 있는 기술은? A

A. Onion routing

B. Virtual Private Network (VPN)

C. Web Crawling

D. 답장 주소 변경

Case 2

기업 네트워크가 외부로부터 침입을 당했다. 침입자는 방화벽 시스템을 우회하여 침투한 것으로 확인되었으며, System V기반 UNIX 서버를 점령하고 있다. 따라서 서버에 대한 라이브 포렌식 분석이 필요한 상황이다.

60. 다음 중 동작 중인 서버가 중지시킬 경우 소실될 수 있는 잠재적 증거는? B

A. Complementary Metal Oxide Semiconductor (CMOS) Chip data

B. Random Access Memory (RAM) data

C. bash_history file

D. File system superblock

61. 넷북의 HDD는 NTFS 시스템으로 1섹터당 512Byte, 클러스터당 4 Sector로 포맷되어 있다. 전문가가 의심하는 “hacked.exe”라는 파일의 크기는 7,712Byte로 확인되었다. 이 파일이 가진 slack 공간의 크기는 무엇인가? B

A. 240 bytes

B. 480 bytes

C. 512 bytes

D. 8,672 bytes

62. 음성 로깅 파일을 일반 오디오 CD로 제작할 때, CD제작 프로그램 또는 음성 처리 소프트웨어가 기록하기 전에 수행해야 하는 것은? A

A. 44.1kHz로 다시 샘플링한다.

B. 잡음 감쇄 필터를 적용한다.

C. 목소리 정보의 음량을 높인다.

D. 녹음된 정보를 받아쓴다.

63. 사이버포렌식 전문가가 범죄 현장에서 안드로이드 폰을 수집하였다. 정보를 획득하기 위해서 루팅을 고려하고 있다. 다음 중 옳은 것은? A

A. 루팅으로 얻은 증거는 사용자 데이터가 변경되지 않으므로 법정에 제출할 수 있다.

B. 루팅하는 방법은 안드로이드 버전과 무관하게 동일하다.

C. 루팅을 하면 제조사의 A/S를 받을 수 없다는 점이 있고 불법으로 간주된다

D. 루팅은 증거를 획득하기 위한 물리적 기술을 무효화 한다.

64. ISO 27037(디지털증거 확인, 수집, 보존에 대한 가이드라인)에 따른 디지털 증거 취급 원칙으로 옳지 않은 것은? B

A. 사이버포렌식 전문가는 잠재적 디지털 증거의 취급을 최소화 하여야 한다.

B. 사이버포렌식 전문가는 행위를 문서화하고, 일반에 공개하여 다른 전문가가 검증할 수 있도록 해야 한다.

C. 사이버포렌식 전문가는 증거에 대한 국내 규칙과 규정을 준수하여야 한다.

D. 사이버포렌식 전문가는 능력을 벗어나는 행동을 취하지 않아야 한다.

Case 3

수사기관에서 12월 1일 불법인 "badimagexxx.jpg" 이미지가 인터넷에서 다운로드 된 사실을 확인하고 다운로드에 사용된 IP주소를 추적하여 당사자가 Jane Doe임을 확인하였다. 또한 수사기관은 Jane Doe가 소유한 컴퓨터 하드드라이브에서 키워드 검색을 통해 위 이미지 파일 뿐 아니라 다음과 같은 잔존 증거도 복되하였다

1) "INDEX.DAT"에서 불법 이미지의 이름이 발견되었으며, 인터넷 히스토리 파일에서 해당 파일이 12월 1일에 한번 다운로드된 것으로 확인되었다
2) "creepy.htm"에서 <img border="0" src="badimagexxx.jpg"> 내용이 검색되었으며, 이 파일은 인터넷 캐쉬에서도 발견되었다.
3) "creepy.htm"은 12월 1일 한번 다운로드 되었다.

이에 "creepy.htm"을 키워드 검색을 해 본 결과 아래와 같은 추가증거가 발견되었다.

1) "message.htm" 이라는 파일이 인터넷 캐쉬에서 발견되었고 내용중에 <body onload="windows.open("http://creepy.htm/")"> 가 발견되었다.
2) "message.htm" 은 12월 1일에 한번 다운로드 되었다.

64. 이 분석을 통하여 증명될 수 있는 것은 무엇인가? D

A. Jane Doe가 불법 이미지를 알고서 다운로드 하였다

B. Jane Doe가 불법 이미지인지 모르고 다운로드 하였다

C. Jane Doe 소유의 컴퓨터가 불법 이미지 다운로드에 사용되었다

D. Jane Doe는 불법 이미지가 포함된 웹 페이지를 미리 알고서 방문한 것이 아니다

65. 다음 중 컴퓨터로부터 디지털 증거를 획득하기 위해 해야 할 첫 번째 활동은 무엇인가? C

A. 데이터의 해쉬 값을 반드시 구한다

B. 각 디지털 매체의 시리얼 번호를 Chain-of-custody 양식에 기록한다

C. 구동중인 시스템의 휘발성 데이터를 획득한다

D. 데이터 변경을 막기 위하여 네트워크로 부터 분리한다

66. e-Discovery를 수행하는 경우 올바른 순서에 맞추어 끌어다 놓으시오. B

① Identification ② Processing, Review and Analysis ③ Presentation ④ Production ⑤ Preservation and collection

A. ④ → ① → ② → ⑤ → ③

B. ① → ⑤ → ② → ④ → ③

C. ① → ② → ④ → ⑤ → ③

D. ④ → ① → ⑤ → ② → ③

67. 수집한 데이터의 무결성을 보장하기 위해서 가장 중요한 것은? A

A. MD5 등 해쉬함수를 이용해서 해쉬 값을 계산하고, Chain of custody를 유지한다

B. 수집한 데이터 전부에 대한 사본을 만든다

C. 수집한 데이터의 유효성을 법적으로 확인받는다

D. 포렌식 소프트웨어가 최신 버전이며 테스트 된 것임을 보장한다

69. 다음은 파일시스템 유형과 그 내용에 대해서 설명하고 있다. 올바르지 못한 것은? D

A. Disk Filesystem - HDD와 같은 데이터 저장장치에 파일을 저장하기 위해 설계된 Filesystem

B. Flash Filesystem - 플래쉬 메모리 저장장치에 파일을 저장하기 위해 설계된 파일시스템

C. Tape Filesystem - Tape storage에 파일을 저장하기 위해 설계된 파일시스템

D. Transactional Filesystem - log를 저장하기 위해 설계된 파일시스템

70. 다음 중 디스크 파일시스템 형태에 해당되지 않는 것은? B

A. HFSX

B. YAFFS

C. ext4

D. UFS

71. 다음은 하드디스크의 구성 요소를 설명한 것이다. 잘못 설명한 것은? A

A. Platter: 데이터 저장 디스크가 고정되는 축

B. Header : 데이터 저장 디스크에 기록된 데이터를 읽거나 쓰기위한 장치

C. Actuator: 디스크를 가로질러 Head를 움직이고, 원하는 Track으로 Head가 찾아가게 하는 장치

D. Voice Coil: Actuator를 움직이게 하는 장치

72. 다음 하드디스크의 섹터에 대한 설명으로 올바른 것은? B

A. 파일의 최소 저장 단위

B. 물리적으로 데이터를 읽고, 쓰는 최소 단위

C. 논리적으로 데이터를 할당하는 최소 단위

D. 파일의 메타데이터가 저장되는 영역

73. 컴퓨터를 부팅하거나 시동시킬 때 사용자가 컴퓨터를 사용할 수 있도록 외부 기억 장치로 부터 운영 체계를 읽어와 주기억 장치에 설치해 주는 프로그램을 무엇이라 하는가? C

A. Framework

B. Platform

C. Bootloader

D. MBR

74. 다음은 하디디스크에 접근하는 기본 단위에 대해서 설명한 것이다. 올바르지 못한 것은? D

A. CHS(Cylinder, Head, Sector) 모드는 실린더, 헤드, 섹터 순서로 하디드스크에 접근한다

B. CHS 모드는 최대 8GB까지 주소 지정이 가능하다

C. LBA(Logic Block Addressing) 모드는 섹터 단위로 하디디스크에 접근한다

D. LBA 모드는 28bit로 주소를 지정한다

75. 다음 중 파티션과 볼륨의 차이점으로 가장 적절한 것은? B

A. 동일한 의미이다

B. 파티션은 하나의 디스크를 나누는 방식이고 볼륨은 하나 이상의 디스크를 논리적으로 묶어 하나의 블록으로 만들 수 있다

C. 섹터가 연속되는 경우 볼륨으로 볼 수 있고, 연속되지 않을 수 있는 경우 파티션이라 할 수 있다

D. 모든 파티션은 볼륨을 포함한다

76. 하드디스크 저장장치의 첫 번째 섹터에 해당하는 MBR에 대한 설명으로 틀린 것은? C

A. 파티션으로 나뉘어진 기억 장치의 첫 섹터인 512 바이트의 시동 섹터에 해당

B. MBR에는 Boot Strap Code, Partition Table Entry와 당 섹터의 오류 유무를 확인하기 위한 값(0xAA55)을 가진 Signature 정보가 있다

C. MBR의 파티션 정보는 16Byte로 구성된다

D. MBR에 기록되는 파티션 정보는 4개까지 가능하다

77. 다음 중 클러스터의 크기에 따른 장단점으로 올바르지 못한 것은? D

A. 클러스터가 클 때: Slack Space가 많이 발생한다

B. 클러스터가 클 때: 버려지는 용량이 많다

C. 클러스터가 작을 때: 파일 저장을 위한 오버헤드가 많다

D. 클러스터가 작을 때: 파일 저장 속도가 개선된다

78. 다음 중 FAT 파일시스템에서 영역 접근 방법이 섹터 단위가 아닌 것은? D

A. 부트 레코드

B. 예약된 영역

C. FAT 영역

D. 데이터 영역

79. 다음 중 FAT 파일시스템에서 부트 레코드 영역의 끝을 나타내는 Signature 값은? B

A. 0x5500

B. 0xAA55

C. 0x0000

D. 0xBAAD

80. FAT 파일시스템에서 Directory Entry에 파일에 대한 정보를 저장하고 있다. 파일의 Name 항목에 저장되는 파일명의 첫 번째 Byte가 0xE5인 경우 어떤 의미인가? B

A. 해당 파일은 디렉터리를 나타냄

B. 해당 파일은 삭제된 파일임

C. 해당 파일의 파일명은 일본어임

D. 해당 Entry는 비어있음

81. FAT 파일시스템의 Directory Entry에 Create Time이 존재한다. 세부 항목에서 Seconds가 6일 때 실제 몇 초인가? C

A. 6초

B. 7초

C. 12초

D. 13초

82. FAT 파일시스템의 Directory Entry에 Create Date가 존재한다. 세부 항목에서 Year가 30일 때 실제 몇 년인가? C

A. 1930년

B. 2000년

C. 2010년

D. 2011년

83. FAT 파일시스템의 Directory Entry에 존재하지 않는 Date/Time은? D

A. Write Date

B. Write Time

C. Last Access Date

D. Last Access Time

84. FAT의 Directory Entry에는 Name 항목이 있다. Slack Space에서 Name 항목의 값으로 dot을 찾고 연속하여 double dot을 찾았다면 얻을 수 있는 정보로 가장 적절한 것은? A

A. 삭제된 폴더

B. 삭제되어 휴지통에서 비워진 파일

C. 삭제된 볼륨 정보

D. 삭제된 파일의 정보

85. 다음 중 파일시스템의 Slack Space에 대한 설명으로 올바르지 못한 것은? C

A. 파일을 디스크에 쓰고자 하는 크기가 클러스터보다 작아 발생하는 여분의 영역

B. 파일을 디스크에 쓰고자 하는 크기가 섹터보다 작아 발생하는 여분의 영역

C. 파일이 삭제되었지만 실질적으로 파일에 대한 정보만 삭제되고 데이터는 삭제되지 않은 영역

D. 파일이 삭제되고 다른 파일로 할당되어 overwrite 되었지만 남아있는 영역

86. 다음은 NTFS의 특징에 대한 설명이다. 잘못 설명한 것은? C

A. 신뢰성을 높이기 위해 볼륨에서 수행하는 모든 작업에 대해 트랜잭션 단위로 기록하고 있다.

B. 암호화 기능으로 EFS를 제공한다.

C. 4TB까지의 디스크 용량을 지원한다.

D. ADS라고 하는 다중 데이터 스트림을 지원한다.

87. 다음은 NTFS와 FAT를 비교 설명한 것이다. 잘못 설명한 것은? A

A. NFTS는 FAT 이후 개발된 것으로 FAT보다 호환성이 더 뛰어나다.

B. 구현 난이도 측면에서 NTFS가 더 어렵다.

C. FAT는 단편화 현상이 NTFS보다 높게 나타난다.

D. NTFS는 FAT보다 안정성이 높다.

89. 다음 중 MFT Entry Header에 저장되어 있는 Signature 값은? A

A. “FILE"

B. "NTFS"

C. "BAAD"

D. "MFT0“

90. 다음 중 NTFS에서 모든 볼륨의 파일과 디렉토리 정보를 저장하고 있는 테이블은? C

A. PME

B. FAT

C. MFT

D. MBR

91. NTFS에서 클러스터 주소 지정방식 중 파일의 첫 번째 클러스터부터 순차적으로 지정되는 주소 방식은? A

A. Virtual Cluster Number

B. Logical Cluster Number

C. Physical Cluster Number

D. Relative Cluster Number

92. NTFS에서 Sparse라는 속성이 존재한다. Sparse 속성에 대한 설명으로 올바른 것은? D

A. 파일이 단편화되어 2개 이상의 Extent로 분리되어 있는 경우를 나타낸다.

B. 파일이 향후 확장될 것을 고려하여 미리 할당된 클러스터 영역을 나타낸다.

C. ADS을 위한 데이터 영역을 나타낸다.

D. 파일을 위해 할당될 클러스터의 데이터가 모두 0일 경우 실제 할당하지 않고 클러스터 개수만을 표시한 것을 나타낸다.

93. NFTS의 $STANDARD_INFORMATION 속성에 저장되어 있는 MAC Time에 대한 설명이다. 잘못된 것은? A

A. Local Time으로 저장된다

B. UTC Time으로 저장된다

C. 각 Time은 1961년 1월 1일 기준으로 1/100초 단위로 64bit에 저장된다

D. Time은 모두 GMT Time으로 저장된다

94. NFTS의 $STANDARD_INFORMATION 속성에 MFT Modified Time이 있다. 이에 대한 설명으로 올바른 것은? C

A. 파일이 생성된 시간

B. 파일이 수정된 시간

C. MFT의 내용이 마지막으로 수정된 시간

D. MFT가 생성된 시간

95. 파일 할당 최소 단위는 클러스터 단위이기 때문에 NTFS에서는 실제 파일의 크기보다 크고 클러스터 크기의 배수인 실제 파일 할당 크기 정보를 저장하고 있다. 파일의 할당 크기가 클러스터 크기의 배수가 아닌 경우는 어떠한 경우인가? D

A. 시스템 파일인 경우

B. 삭제되어 휴지통에 존재하는 파일인 경우

C. 파일이 연속되지 않고 단편화 되어 분산되어 있는 경우

D. 파일의 크기가 작아 $MFT의 $DATA 속성에 Resident 형태로 저장되는 경우

99. 다음에서 ext2 파일시스템에 대한 설명으로 거리가 먼 것은? D

A. UFS를 기반으로 하여 제작된 파일시스템이다

B. ext2 파일시스템은 리눅스에서 많이 사용된다

C. ext2 파일시스템에 저널링 기능이 추가된 ext3가 있다

D. UFS가 오래된 파일시스템으로서 ext2는 이러한 것을 극복하기 위하여 UFS를 모두 승계하고 부가적인 기능을 추가한 형태가 ext2이다

100. ext2의 inode에 저장되는 정보로 적절하지 못한 것은? C

A. file mode

B. Owner ID

C. Journal Inode number

D. MAC Time

101. ISO9660 파일시스템의 Directory Record에서 "Recording Date and Time" 내용 중 년도 값으로 50을 얻었다. 실제 몇 년에 해당되는가? A

A. 1950년

B. 1951년

C. 2010년

D. 2011년

99. 다음은 HFS와 HFS+ 파일시스템에 대하여 비교 설명한 것이다. 잘못된 것은? C

A. HFS는 블록을 16bit 주소로 사용하며 HFS+는 32bit를 사용한다

B. 파일명의 길이의 경우 HFS는 31, HFS+는 255이다

C. 최대 파일 크기의 경우 HFS는 2의 16승이고 HFS+의 경우 2의 32승이다

D. 파일명 encoding의 경우 HFS는 MacRoman이고 HFS+의 경우 Unicode이다

100. 물에 빠진 자동차에서 수거한 Hard Drive에 저장된 데이터를 법정에 제출할 필요성이 제기되었다. 아래 설명 중 해당 Hard Drive에서 정보를 수집하기 위해 가장 좋은(BEST) 접근 방법은 무엇인가 ? D

A. 마를 때까지 기다렸다가 완전히 마르면 데스크 탑에 설치하고 정상적인 운영시스템 명령을 통해 정보의 검색을 위한 시도를 한다

B. 포렌식 오븐에 넣어 말리고 나서, 디가우서(Degausser)로 습기를 완전히 제거한 다음 랩탑에 Drive를 장착하고 OS로 정보를 추출한다

C. Drive가 아직 습한 상태로 있는 동안, Drive가 자연 상태(Native state)로 보존되고 있음을 보증할 수 있도록 포렌식 Bit to Bit 복사 프로그램을 사용 한다

D. 전문적인 데이터 복구 조직에 연락하여 상황을 설명하고 그들에게 포렌식 이미지(Forensic image) 획득을 요청 한다

※ 참고: For heavily damaged media, professional data recovery services are the best chance for recovery.

101. 필요시 적절한 포렌식 활동을 수행할 수 있도록 하기 위해 사고현장 대응활동으로 가장 적절한 것은? D

A. 법률 자문회의(Legal Council)는 현장 대응활동이 포렌식의 일부가 아님을 확실하게 하여

이해의 충돌을 피하도록 한다.

B. 정기적으로 모든 데스크 탑과 서버에 대한 포렌식 이미지를 생성한다.

C. 법률 적용을 위해 공개되지 않은 사고(Closed incidents)에 대해서만 포렌식 활동을 적용한다.

D. 사건 자체로 인한 피해가 없다고 하더라도 범죄 연관성이 있을 수 있으므로 모든 것이 명료해 질 때까지 주의해서 취급해야 한다.

※ 참고: An incident may be harmless but it may also be the start of an investigation. Therefore all incidents must be handled with care until proven begin.

102. 디지털증거에 대한 증거 연계보관성(Chain of Custody) 원칙에 가장 부합하는 것은? D

A. 범죄 현장을 절대로 변형(alter) 시켜서는 안된다.

B. 반드시 법정에서 완벽하게 재현할 수 있어야 한다

C. 국가 내부적으로 오직 하나의 결과만 나와야 한다

D. 반드시 공식적인 문서화(documentation) 절차를 따르도록 한다

103. 범죄 현장(crime scene)에서 디지털 증거를 취급하는 요령으로 가장 적합한 것은? D

A. 절대로 현장을 변형(alter) 하지 말아야 한다

B. 반드시 법정에서 완벽하게 재현할 수 있어야 한다

C. 국가 내부적으로 오직 하나의 결과만 나와야 한다

D. 가능한 한 오염의 정도(amount of contamination)가 최소화 할 수 있도록 하여야 한다

※ 참고: Given the importance of the evidence that is available at a crime scene, the ability to deal with a scene in a manner that minimizes the amount of distraction, contamination, or destruction of evidence.

104. Forensic bit stream image의 무결성을 입증하는 방법으로 가장 적합한 것은? A

A. 원본 매체와 사본 매체간 Hash값의 동일 여부

B. 적정한 기록 유지

C. 사진 촬영

D. 암호화된 Key

※ 참고: Like incident response, there are various computer forensics guidelines(e.g. International Organization of Computer Evidence(IOCE), Scientific Working Group on Digital Evidence(SWGDE), Association of Chief Police Officers(ACPO).

105. 법률학자 및 인문 학자들의 저서에서 영향을 받아 법률의 이론적 개념을 가장 잘(BEST) 강조하고 있는 것은 다음의 어느 것인가? B

A. 범죄법(Criminal law)

B. 민법(Civil law)

C. 종교법(Religious law)

D. 행정법(Administrative law)

106. 다음 중 증거처리의 5가지 규칙(rules)을 설명한 것으로 가장 적당한 것은? B

A. 원본성(Authentic)이 있어야 한다. 여분이 있어야 한다(Redundant), 법적 허용성이 있어야 한다(Admissible)

B. 완전해야 한다(Complete), 원본성이 있어야 한다(Authentic), 법적 허용성이 있어야 한다(Admissible)

C. 완전해야 한다, 여분이 있어야 한다, 확실성이 있어야 한다

D. 여분이 있어야 한다, 수용성이 있어야 한다, 완전해야 한다

※ 참고: At a more generic level, evidence should have some probative value, be relevant to the case at hand, and meet the following criteria (often called the five rules of evidence) : be authentic, be accurate, be complete, be convincing, be admissible

106. 범인이 범행을 저지르는 과정에서 수사관이 사건 추적을 할 수 있도록 하는 단서를 남길 수밖에 없다는 원칙을 무엇이라고 하는가? D

A. 법적 면제의 Meyer's principle

B. 범죄적 Principle

C. IOCE/사이버 포렌식 Principle

D. Locard's principle

107. DVD-R 저장장치에 저장되었던 기밀정보가 남아있지 않도록 하는 가장 확실한 방법을 아래에서 고른다면? C

A. 삭제(Deletion)

B. 소자(Degaussing)

C. 파손(Destruction)

D. 덮어쓰기(Overwriting)

108. 다음 중 디지털 포렌식 규칙(digital forensic rule)의 일부가 아닌 것은? A

A. 인정(Assurance)

B. 보존(Preserving)

C. 수집(Collection)

D. 분석(Analyzing)

109. 다음 중 증거 수집의 실시간 대응에 대한 중요성으로 인식할 수 있는 항목으로 바람직하지 않은 것은? D

A. 전자 상거래는 시스템 down시 막대한 금전적 손실을 가져온다.

B. 하드 디스크 이미징에 있어서 많은 시간이 걸린다.

C. 시스템 동작 상태에서 증거 수집이 필요할 때가 있다.

D. 시스템 down시 신속하고 정확한 절차를 지켜야 한다.

110. 다음 중 휘발성 데이터와 관계가 가장 먼 것은? C

A. Cache Memory

B. Network 세션 연결 정보

C. Flash Memory

D. 프로세스 정보

111. 다음 중 비휘발성 데이터에 대한 설명으로 올바르지 않은 것은? D

A. 일반적으로 전원이 끊어져도 손실 없이 보존되는 데이터

B. 일반적으로 비휘발성 데이터는 압수, 디스크 이미징 등의 방법으로 수집한다.

C. 일반 파일, 로그 파일 등의 파일이 이에 해당한다.

D. 일반적으로 전원이 끊어지면 손실되는 데이터를 의미한다.

112. 다음 휘발성/비휘발성 데이터가 “휘발성-비휘발성” 순으로 되어 있지 않은 것은? D

A. Connected Network Session - Network Topology

B. Process Memory - Flash Memory

C. Process Table - Disk

D. Archival media - Archive File

113. 다음 중 실시간 증거 수집 방법론으로 잘못 설명된 것은? B

A. Local Response Methodology: 대상 시스템 콘솔에서 증거 자료를 수집하고 USB 등의 저장 매체에 저장하는 방법

B. Local Response Methodology: 조사자 시스템 콘솔에서 증거 자료를 수집하는 방법

C. Remote Response Methodology: 대상 시스템을 네트워크로 접속하여 정보를 수집하는 방법

D. Remote Response Methodology: 대상 시스템에 설치된 agent로 하여금 증거자료를 수집하도록 Remote에서 명령을 내리는 방법

114. 해킹 피해를 입은 Windows XP가 설치된 PC에서 증거 자료를 수집하고자 한다. 다음 중 조사자가 해야 하는 행동으로 올바르지 못한 것은? C

A. 우선, 핸드폰 등을 이용하여 정확한 현재 시간을 파악하고 time 명령어로 시스템 시간과의 차이를 기록한다

B. FIRE, FRED, IRCR 등의 증거 수집 자동화 도구를 이용하여 기본적인 증거 수집 하며, 수집된 증거는 무결성을 위해 SHA-1과 같은 Hashing 도구를 사용한다.

C. 조사자는 조사 행위로 발생되는 시스템 변경을 미연에 방지하고 시스템의 모든 증거 자료를 보존하기 위해 조사 개시 즉시 전원을 차단하고 디스크 이미징을 수행한다.

D. 조사자는 동작중인 피해 시스템에서 증거 수집을 하는 동안 휘발성 데이터가 유실되지 않도록 주의해야 한다.

115. 실시간 대응 증거 수집에서 시스템 기본 정보를 수집하는 의미로 잘못된 것은? B

A. 해킹 등의 침해가 발생한 시스템을 분석하는데 Hotfix의 경우 취약성 범위를 한정하는데 도움을 준다.

B. OS의 Build Number에 따라 시스템 구성의 차이가 현격하므로 분석 오류를 최소화 할 수 있다.

C. OS 버전에 따라 분석에 필요한 설정 정보, 사용 파일, 사용 폴더 등이 상이할 수 있어 이를 파악하여 분석 시 활용할 수 있다.

D. OS에 따라 상세 메모리 구조(예, 프로세스 구성 요소 및 그 값)가 상이하므로 메모리 분석하는데 OS 및 SP 버전은 중요하다.

116. 다음은 Windows Batch File(.bat)에서 널리 사용되는 명령어에 대한 설명이다. 잘못된 것은? D

A. 화면에 원하는 문자열을 출력하기 위해서는 echo 명령어를 사용한다.

B. 파일을 생성하여 저장하고자 할 때 “>”를 사용한다.

C. echo 명령어를 사용할 때 화면상에 echo되는 명령어 라인을 없애기 위해 “echo off” 명령어를 사용한다.

D. bat 파일 실행 시 어떠한 동작도 하지 않고 단지 comment를 작성하기 위해서는 “//”을 사용한다.

117. 다음 중 실제 시간을 구하는 방법으로 잘못된 것은? D

A. 핸드폰 시간

B. Time Server 동기화

C. 한국표준과학연구원의 UTCK3 이용

D. CMOS Time

118. 다음 중 Windows에서 날짜를 구하는 CMD 명령어는? C

A. date B. time C. date/t D. time/t

119. 다음 중 Windows에서 제공하는 명령어로 현재 로그인 한 사용자 정보를 얻는 CMD 명령어는? A

A. set user B. net user C. login D. loginuser

120. 다음 중 SHA1의 암호화 bit수는? C

A. 56 B. 128 C. 160 D. 256

121. 다음 중 MD5의 암호화 bit수는? B

A. 56 B. 128 C. 160 D. 256

122. 다음 중 윈도우즈 Registry Hive 중에서 현재 로그온한 사용자들에 대한 등록 정보 등을 저장하고 있는 것은 무엇인가? B

A. HKCR B. HKCU

C. HKLM D. HKCC

123. 다음 중 윈도우즈 Registry에서 얻을 수 없는 USB 저장장치 사용 관련 정보는 무엇인가? C

A. USB 제조사, 제품명, 버전

B. USB 저장장치 사용 볼륨(C:, D: ...)

C. USB 저장장치 최초 연결 시점

D. 마지막 부팅 후 최초 USB 연결 시간

124. 다음 중 NOR와 비교했을 때 NAND Flash Memory의 특징으로 잘못된 것은? C

A. 셀이 직렬로 연결되어 있다.

B. 제조단가가 싸고 대용량이다.

C. 데이터 읽기 속도가 빠르다

D. 데이터 저장장치로 많이 이용된다.

125. 다음 중 Disk상에서 데이터를 읽거나 쓰는 최소 단위는 무엇인가? A

A. 섹터 B. 클러스터 C. 블록 D. 페이지

126. 다음 중 파일의 Disk 할당 최소 단위는 무엇인가? B

A. 섹터 B. 클러스터 C. 블록 D. 페이지

127. 다음 파일시스템 중 분류로 봤을 때 Disk 파일시스템이 아닌 것은? B

A. NTFS B. JFFS

C. HFS+ D. EXT4

128. 파일시스템의 특징으로 파일의 크기가 커서 연속되거나 분산된 여러 개의 클러스터에 저장하고 이를 연결한 구조 및 형태를 무엇이라 하는가? A

A. Cluster Chain B. Fragmentation

C. Chain of custody D. De-duplication

129. 파일시스템에서 MBR(Master Boot Record)은 OS 부팅을 위한 부트 코드를 포함하여 파티션 정보를 포함하고 있다. 규약상 MBR에 최대 몇 개의 주 파티션 정보를 포함할 수 있는가? B

A. 2 B. 4 C. 10 D. 63

130. 다음 중 파일시스템이 손상되어 파티션과 파일 메타데이터가 손실된 상황에서 파일의 구조, 시그니처 등의 특징을 이용하여 파일을 복구하는 기법을 무엇이라 하는가? C

A. Undelete

B. Steganograph

C. Carving

D. Decoding

131. 엔티-포렌식의 범주가 아닌 것은 ? D

A. 데이터 숨김,

B. 아티팩트 제거,

C. 흔적 난독 처리

D. 네트워크에 대한 공격

132. 증거물 지우기(Artifact wiping) 기법과 연관이 없는 것은 ? B

A. 디스크 클리닝 유틸리티

B. 데이터 암호화 소프트웨어

C. 파일 삭제 유틸리티

D. 디스크 자기 제거 / 파괴 기술

133. 안티-포렌식 도구가 추구하는 성과로써 가장 뛰어난 기능은 ? C

A. 데이터 은닉(Hiding)

B. 데이터 조작(Manipulation)

C. 해시 값의 무결성

D. 포렌식 절차 훼손

134. 디가우징(Degaussing)은 효과적인 데이터 삭제 수단임에도 엔티-포렌식에서 사용이 드문 이유는 ? B

A. 목표 성능 불투명

B. 도구 비용

C. 조작의 어려움

D. 복구 가능성 존재

135. 안티-포렌식 대응기법에 포함되지 않는 것 ? A

A. 원격 코드 실행

B. 패스워드 크랙

C. 은닉 데이터 탐지

D. 데이터 복구

136. 안티-포렌식의 목적과 거리가 먼 것은? C

A. 탐지 및 분석시간 지연

B. 디지털 포렌식 도구 기능 훼손

C. 데이터 이중화

D. 범죄 흔적이나 도구사용 흔적 발견 방해

137. 시스템에 흔적을 거의 남기지 않는 방법으로 부적당한 것은 ? C

A. 포터블(Potable) 프로그램 이용

B. 라이브 CD나 부팅 가능한 USB 이용

C. 클라우드 이용

D. 가상 머신(Virtual Machine) 이용

138. 하드드라이브 1개의 클러스터는 8개의 섹터로 포멧이 되어있다. '동국포렌식.doc'라는 파일이 12,000 바이트 크기를 가지고 있다면 몇 개의 클러스터가 사용되어야 하는가? C

A. 1 B. 2 C. 3 D. 4

139. 컴퓨터 저장장치를 나타내는 말로 ROM은? D

A. Random Only Memory

B. Random Open Memory

C. Read Open Memory

D. Read Only Memory

140. 컴퓨터 하드웨어의 하나인 RAM은 아래의 무엇에 해당하는가? C

A. Relatively Access Memory

B. Relative Address Memory

C. Random Access Memory

D. Random Address Memory

141. 컴퓨터 BIOS에 대한 설명으로 옳은 것은? B

A. Ram이 넘치면 메모리 페이지를 삭제하는 역할을 한다.

B. 전원이 들어오면 컴퓨터 시스템을 확인하고 작동체계를 갖춘다

C. 컴퓨터 주 기억장치를 말한다

D. 디지털 증거 원본성을 확보하는 기법이다

142. 컴퓨터 전원이 꺼져 있을 경우 우선적으로 조사자가 취해야 할 조치는? B

A. 전원을 켠다

B. 그 상태에서 증거수집을 시작한다

C. 타이핑 작업을 한다

D. 스위치를 교체한다

143. 압수수색 장소에서 포렌식 조사자가 우선하여 취해야할 올바른 행동은? B

A. 증거를 찾아보기 시작한다

B. 범죄현장이 안전하게 보존되도록 조치한다

C. 증거를 수집한다

D. 컴퓨터 전원이 꺼지지 않도록 주의한다

144. '소프트웨어 절도(sofrware piracy)' 설명으로 가장 적절한 것은? A

A. 컴퓨터 프로그램을 불법적으로 복제하는 행위

B. 하드를 리폼하여 이를 새것으로 속여 판매하는 행위

C. 바이러스로 하드웨어를 감염시키는 행위

D. 중고 컴퓨터 중앙처리장치를 판매하여 이익을 취하는 행위

145. 유용한 컴퓨터 프로그램으로 위장하여 활동하는 바이러스 형태를 말하는 것은? A

A. 트로이목마

B. 해커

C. 웜

D. 무단 복제행위

146. 이메일(메세지)을 보낼 때 실제 신분을 숨기고 다른 사람이 보낸 것처럼 보이도록 하는 기법은? D

A. 스팸(spam)

B. 팝업(popup)

C. 유령(ghost)

D. 위장(spoof)

147. 아래 제시 중 CPU를 바르게 표기한 것은? C

A. Computer Processing Unit

B. Central Peripheral Unit

C. Central Processing Unit

D. Computer Processing User

148. 다음 중 기업포렌식에서 가장 주된 목적이 되는 것은? A

A. 본연의 서비스를 계속하도록 하는 것

B. 기업의 명예

C. 형사상 기소

D. 보안

149. 아래 기술된 내용 중 틀린 것은? B

A. 디지털 포렌식 전문가는 항상 객관적인 태도를 유지하여야 한다

B. 수사관의 임무는 피의자의 유무죄 여부를 결정하는 것이다

C. 수사관은 사건과 관련된 사실을 정확히 보고할 책임이 있다

D. 수사관은 수사기밀을 유지하여야 한다.

150. 다음 중 유닉스 운영체제의 특징으로 볼 수 없는 것은? D

A. 대화식 운영체제(SHELL)

B. 멀티 태스킹

C. 계층적 파일 시스템

D. 오픈소스 운영체제

151. 파일시스템의 구성요소에 해당하지 않는 것은? A

A. 아이노드(i-node) 영역

B. Reserved 영역

C. 파일 할당테이블(FAT) 영역

D. 데이터 영역

132. FAT32 파일시스템에서 파일을 삭제하였을 경우 발생하는 변화에 해당하지 않는 것은? C

A. 삭제 대상 파일의 디렉토리 엔트리 첫 바이트를 0×E5 값으로 변경한다.

B. FAT 영역에서 해당 파일이 할당하고 있는 FAT 엔트리를 모두 0으로 초기화한다

C. 디렉토리 엔트리가 모두 0으로 채워지기 때문에 겉으로는 파일이 지워지지 않은 것으로 보인다

D. 디렉토리 엔트리의 첫 바이트 외 다른 부분은 0으로 채워지지 않는다

133. 다음 중 파일시스템이 아닌 것은? C

A. FAT

B. NTFS

C. Linux

D. ExEAT

134. SSD(Solid-State Drive) 저장매체에 대한 설명으로 틀린 것은? B

A. 낸드 플래시 메모리를 기반으로 한다

B. 파일 시스템의 모든 속성정보를 나타내는 메타데이터를 담고 있다

C. 비휘발성 기억장치이다

D. 전기적으로 데이터를 지우고 다시 기록할 수 있다

135. 디스크 이미징에 대한 설명으로 옳은 것은? A

A. 시스템에서 사용중인 디스크의 모든 물리적 데이터를 파일 형태로 만드는 것을 말한다

B. 저장매체 전체의 내용을 byte 단위로 복사하기 때문에 데이터를 모두 복사하기 어렵다

C. 포렌식 분석에 활용되지 않는 비할당 영역은 복제하지 않는다

D. 일반적으로 소프트웨어적 방법에 비해 하드웨어 장비를 이용한 복제 속도가 훨씬 느린 것으로 알려지고 있다.

136. USB 장치 접속흔적을 추적하기 위한 요소를 열거한 것으로 틀린 것은? D

A. 장치의 형식, 제조사명, 상품명, 버전을 나타내는 장치 클래스 ID(Device Class Identifier)

B. 부팅 후 최초 연결시각과 마지막 연결시각

C. 사용자별 USB 마운트 내역

D. 접속한 USB의 외부 형태

137. 웹 브라우저 포렌식을 통해 확인 가능한 정보가 아닌 것은? A

A. 파일의 생성, 수정, 마지막 접근 일시

B. 임시인터넷 파일

C. 웹 사이트 방문 히스토리

D. 쿠키 정보

138. 윈도우 프리패치(prefetch)에 대한 설명으로 틀린 것은? C

A. 윈도우 xp 이후 운영체제에서 실행파일을 메모리로 로딩할 때 효율을 높이기 위해 개발된 프로그램을 말한다

B. 사용자가 파일을 실행할 경우 미리 저장된 정보를 이용해서 초기 실행 속도를 향상시킨다.

C. 웹 사이트를 재방문할 경우 빠른 웹 페이지 로딩을 목적으로 한다

D. 종종 파일시스템 분석으로 찾을 수 없는 파일의 실행여부를 확인할 수 있다.

139. 썸네일 파일(thumb nail file)에 대한 설명으로 맞는 것은? B

A. 썸네일 분석은 파일을 미리보기 형태로 보여 주는 것으로 찾고자 하는 파일의 존재 여부와는 전혀 상관이 없다.

B. 썸네일 파일은 Thumbchche_##.db형태로 저장되며, 이때 ##은 썸네일의 크기를 나타낸다

C. 운영제체에서 별도의 썸네일 설정을 하여야 기록이 남게 된다

D. 원본이 삭제되면 썸네일 파일도 따라서 삭제 된다

140. 안티 포렌식의 유형으로 볼 수 없는 것은? C

A. 데이터 은닉(Data Hiding)

B. 증거자료 삭제(Artifact Wiping)

C. 데이터 절취(Data Theft)

D. 데이터 조작(Data Manipulating)

141. 안티포렌식기법 중 데이터 은닉(Data Hiding) 유형으로 보기 어려운 것은? A

A. 공개 통신(Public Channels)

B. 스테가노그라피

C. 사용자 신원 은닉(Anonymity)

D. 워터마킹(Watermarking)

142. 이메일 파일 구조에 대한 설명으로 옳은 것은? C

A. 이메일 헤더에는 송·수신자, 출발지 IP주소, 도착지 IP주소를 포함하여 메일의 내용까지 포함하고 있다.

B. 이메일은 헤더(Header)와 내용(Contents) 영역으로 구분되며, 메타데이터는 콘텐츠에 포함되어 있다.

C. 이메일의 제목, 시간, 발신자 정보, 수신자 정보 등은 헤더영역에서 확인할 수 있다.

D. 이메일의 발신자 ID나 IP는 네트워크에서 자동 생성되도록 되어있어 조작을 할 수 없다

143. 사이버 포렌식의 기본원칙으로 보기 힘든 것은? C

A. 무결성의 원칙

B. 재현의 원칙

C. 휘발성의 원칙

D. 연계보관성 원칙

144. 사이버 포렌식 원칙 중 정당성의 원칙에 대한 설명으로 틀린 것은? C

A. 형소법 제308조의 2에 따르면 증거수집 절차에 위반하여 수집된 증거는 위법수집증거 배제원칙(Exclusionary Rule)에 따라 재판과정에서 이를 증거로 활용할 수 없다

B. '독수의 과실(fruit of poisoned tree)'론에 따르면 위법하게 수집된 증거에서 발견된 2차적 증거 역시 증거능력을 갖지 못한다

C. 영장에 기재된 범죄사실과 무관한 범죄와 관련 증거를 발견하였을 때는 '우연히 발견한 증거'에 해당하므로 계속 압수수색을 진행하여야 한다

D. 위법수집증거 배제원칙은 피의자(피고인)의 권리와 사생활을 보호하기 위한 형사소송법상의 취지를 반영한 것이다

135. 증거에 대한 설명으로 맞는 것은? A

A. 증거는 간접증거와 직접증거로 나눈다

B. 직접 증거는 직접 요증사실의 증명에 이용되는 증거를 말하며, 지문, 혈흔, 증인의 증언 등이 이에 속한다

C. 간접증거는 간접사실을 증명함으로서 요증사실의 증명에 이용되는 것으로 자백, 위조통화 등이 있으며, 컴퓨터가 생성한 자료(generated data)가 이에 해당한다

D. 디지털 증거에는 간접증거가 있을 수 없다

136. 디지털증거를 존재 형식에 따라 분류한 것이다. 틀린 것은? C

A. 휘발성 증거

B. 매체에 저장된 증거

C. 간접증거

D. 전송중인 증거

137. 디지털 증거의 특징으로 볼 수 없는 것은? A

A. 현출성

B. 취약성(변조용이성)

C. 복제용이성

D. 잠재성

138. 디지털 증거로서 인정받기 위한 선결요건에 해당하지 않는 것은? B

A. 진정성(authenticity)

B. 사본성(copy)

C. 무결성(integrity)

D. 원본성(originality)

139. 다음 중 해쉬함수에 대한 설명으로 옳은 것은? C

A. 수학적 알고리즘을 이용하의 임의의 긴 입력 값에 대응하는 고정된 길이의 값으로 나타낸 것으로 계산하는 방식에 따라 다소 차이가 발생한다

B. 경우에 따라서는 출력한 해쉬값을 이용하여 역으로 원래 입력한 값을 유추할 수도 있다

C. 법정에서는 증거 원본의 해쉬 값과 분석에 사용된 사본의 해쉬값을 비교하여 일치하면 무결성이 입증된 것으로 본다

D. 동일한 해쉬값 을 갖는 임의의 입력 값 2개를 찾아내는 것이 가능하다

140. 디지털 증거 허용 요건의 하나인 신뢰성을 확보하기 위한 요건으로 틀린 것은? A

A. 저장매체의 첨단성

B. 컴퓨터의 기계적 정확성

C. 프로그램의 신뢰성

D. 조작자의 전문적인 기술능력과 정확성

141. 디지털 증거의 무결성을 확보하기 위한 압수 절차에 어긋나는 것은? D

A. 저장매체를 압수한 뒤 피의자의 서명을 받아 봉인한다

B. 압수, 서명, 봉인의 전 과정을 녹화한다.

C. 이미지 파일을 생성시에는 쓰기방지장치(Write Block)을 반드시 연결한 후 실행한다

D. 공판과정에서 피의자가 무결성을 부정하고 나올 경우에는 대항 방법이 없다

142. 다음 중 전문증거에 해당하지 않는 것은? C

A. 경험사실을 기재한 진술서

B. 경험사실을 들은 타인이 법정에서 행하는 진술

C. 경험자 자신이 법정에서 경험한 사실을 직접 진술하는 것

D. 경험사실을 득문한 타인이 서면으로 기재한 진술 녹취서

143. 증거능력과 증명력의 차이점에 대한 설명으로 틀린 것은? C

A. 증명력은 증거가 가지는 실질적 가치를 말한다

B. 증거능력은 엄격한 증명의 자료로 사용될 수 있는 법률상의 자격을 말한다

C. 증거능력이 결여된 증거에 대해서도 법관은 자유심증에 따라 증명력을 판단할 수 있다

D. 증거능력은 법률에 따라 형식적, 객관적으로 법정화되어 있다.

144. 아래 설명에서 틀린 것은? C

A. 동일성과 무결성이 보장되기 위해서는 원본과 사본의 해쉬 값이 같아야 한다

B. 증거로 채택되기 위해서는 연계보관성유지(Chain of Custody)를 하여야 한다

C. 위법수집증거 배제의 법칙(Exclusionary Rule)은 사인의 행위에는 적용되지 않는다

D. 디지털 증거는 수집, 보관, 분석되는 과정에서 수정, 변경, 손상이 없어야 한다.

145. 전문증거에 대한 우리나라의 판례를 설명하고 있다. 틀린 것은? B

A. 전문증거의 증거능력을 배제하는 것은 증거법상 원칙의 하나이다

B. 피고인 소유 컴퓨터에서 출력된 서면이라 할지라도 피고인이 “작성자를 전혀 모른다”라고 주장할 경우 증거능력을 부여할 수 있는 방법이 없다

C. 비록 작성자가 성립의 진정을 부인하더라도 과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되면 이를 증거로 할 수 있다.

D. 특히 신용할 만한 정황에 의하여 작성된 문서는 전문법칙의 적용을 받지 않는다

146. 데이터베이스에서 증거자료를 추출 순서를 설명한 것으로 옳은 것은? C

① 운영체제, DB종류, 설정정보 확인 ② DB운영자 등 대상 설계개념, 사용목적 및 추가 백업 데이터 여부 조사 ③ 추출된 DB 복사본 또는 저장 증거파일의 해쉬값 계산 후 보관 ④ DB 접속후 Memory 등 휘발성 정보 조사 ⑤ DB 서버을 압수할 경우 DB 셧다운후 O/S 종료

A. ① → ② → ④ → ⑤ → ③

B. ① → ② → ⑤ → ④ → ③

C. ① → ④ → ⑤ → ② → ③

D. ① → ⑤ → ② → ④ → ③

147. 데이터베이스 증거자료 우선 수집항목이 아닌 것은? D

A. 휘발성 자료 수집

B. DB 서버 Connection, Session 자료

C. System Event Log

D. USB 작성 자료

148. 데이터베이스에서 추출 가능한 로그기록 분류로 부적당한 것은? C

A. General Log

B. Binary Log

C. Event Log

D. Error Log

149. IP클래스에 대한 설명으로 맞지 않는 것은? A

A. IPv4 주소체계는 클래스 단위로 나뉘며, 32비트로 이루어진 6개 구간으로 구성된다

B. 네트워크 주소는 호스트관리의 효율성을 위해 네트워크 ID와 호스트 ID로 구성된다

C. 네트워크 할당을 위해 사용되는 구간은 A, B, C 세 구간이다

D. C 클래스의 경우 32비트 중 24비트가 네트워크 ID에 해당한다.

150. IPv6 공인주소 포맷에 대한 설명으로 틀린 것은? C

A. IPv4와 비교하면 확장된 주소 체계를 가지고 있다.

B. 브로드캐스트 대신 멀티캐스트를 사용한다

C. 보안과 관련된 인증절차, 데이터 무결성 보호, 메시지의 발신지 확인 등 기능을 제공하지 못한다

D. IPv4에 비하면 보안관련 기능이 크게 향상되었다

151. 스위치에 대한 설명으로 틀린 것은? B

A. 패킷 충돌을 막기 위해 패킷의 목적지로 전송하는 역할을 수행한다.

B. 일반적으로 OSI 계층의 모든 계층에서 동작을 한다

C. L2 스위치는 일반적으로 허브의 개념으로 볼 수 있으며 데이터를 뿌려주는 역할만 한다

D. L3 스위치는 허브와 라우터의 역할을 수행한다.

152. 가상 네트워크(VLAN)에 대한 설명으로 틀린 것은? D

A. Virtual Local Area Network의 준말로 네트워크를 이용하는 대상들을 논리적으로 그룹화한 것이다

B. 네트워크 확장이 용이하다

C. 관리자가 각각의 포트와 사용자를 제어할 수 있어 보안상 이점이 있다

D. 불필요한 브로드캐스팅을 방지할 수 없는 단점이 있다

153. 네트워크 침입탐지 기반에 대한 설명으로 옳은 것은? A

A. 오용탐지 기반(Misuse Detecton)과 이상탐지 기반(Anomaly Detection)로 나눌 수 있다.

B. 이상탐지 기반(Anomaly Detection)는 인식된 공격행위로부터 시그니처를 추출하여 기존 시그니처와 비교 분석하는 방법이다

C. 이상탐지 기반(Anomaly Detection)는 알려진 공격에 대한 시그니처 목록을 유지해야 한다.

D. 오용탐지 기반(Misuse Detecton)은 기존의 정상 작동중인 네트워크를 정상으로 정의하고 이외의 행위를 비정상행위로 규정하여 탐지하는 방식이다

154. 네트워크 증거분석 절차를 바른 순서로 나열한 것은? B

① 사건관련 정보수집(Obtain Information) ② 증거수집 전략수립(Strategize) ③ 증거수집(Collect Evidence) ④ 분석 (Analyze) ⑤ 보고서 작성(Report)

A. ① → ② → ④ → ⑤ → ③

B. ① → ② → ③ → ④ → ⑤

C. ① → ② → ④ → ③ → ⑤

D. ① → ② → ⑤ → ③ → ④

155. 네트워크 포렌식 수행시 살펴보아야 할 네트워크 장비에 해당하지 않는 것은? C

A. 스위치

B. 라우터

C. 운영체제

D. IDS/IPS

156. 미국 국립표준기술연구소(NIST)의 네트워크 보안테스트 절차를 순서대로 바르게 나열한 것은? B

① IDS 구성 보완 및 증거 수집 ② 네트워크에 연결된 인가되지 않은 호스트 점검 ③ 취약한 서비스 식별 ④ 침투테스트 준비 ⑤ 조직의 정보보호정책에서 정의하고 있는 서비스 분석

A. ① → ② → ④ → ⑤ → ③

B. ② → ③ → ⑤ → ④ → ①

C. ② → ① → ④ → ⑤ → ③

D. ② → ④ →① → ⑤ → ③

157. 네트워크 공유기 정보를 확인할 견과 IP타임 공유기로 확인되었다. 해당 공유기에서 수집할 수 있는 증거로 볼 수 없는 것은? C

A. DHCP 할당 정보

B. 시스템 로그 및 포트 포워딩 정보

C. 사용자 정의 데이터 파일

D. 인터넷 연결 및 링크 설정 정보

158. 네트워크 포렌식에서 웹 프록시 로그를 활용할 수 있는 상황으로 부적당한 것은? D

A. 내부 사용자가 웹 브라우저 정책을 위반한 사실을 감지했을 때

B. 내부 시스템 감염으로 웹을 통한 비정상 통신이 감지되었을 때

C. 웹 서버가 해킹당하거나 기밀정보가 유출되었을 염려가 있을 때

D. 시스템이 정상적으로 가동하지 않을 때

159. 가상사설망(VPN)에 대한 설명으로 틀린 것은? C

A. 가상사설망은 게이트웨이와 게이트웨이 또는 게이트웨이와 원격사용자간 안전한 데이터 교환을 위해 유용하다

B. 데이트를 교환할 경우 패킷을 캡슐화하여 보내기 때문에 보안성인 높다

C. 공유 정보의 안전한 통신을 목적으로 자동화된 침해사고대응 시스템에서는 거의 사용하지 않는다

D. 신뢰된 사용자의 IP주소 영역과 호스명 리스트를 관리하는 것이 중요하다

160. 스마트폰 단말기의 IMEI(International Mobile Equipment Identity) 정보에 포함되지 않는 것은? D

A. WCDMA 휴대폰 기기에 내장된 인식번호

B. 단말기의 국적, 제조사, 모델, 단말번호 등 정보 포함

C. 다이얼화면 *#06#로 확인 가능

D. 사용자 인적정보

161. 물리적 모바일 데이터 추출방식의 하나인 JTAG에 대한 설명으로 틀린 것은? D

A. JTAG(Joint Test Action Group)은 IC 레벨에서 인쇄회로 기판(PCB)상에 연결을 검증하는 방법이다.

B. 전자전기기술자협회인 IEEE 1149.1 표준으로 명시된 기법이다.

C. 산업표준으로 모든 임베디드 기기에 적용할 수 있다

D. 우리나라에는 아직까지 이를 적용하지 않고 있다

162. 스마트폰 데이터를 추출, 분석하기 위한 논리적 방법에 해당하지 않는 것은? B

A. 파일스시템 분석(파티션정보)

B. 플래쉬 메모리칩 분리

C. 탈옥(Jailbreak)

D. 루팅(Rooting)

163. 모바일 디바이스에 대한 논리적 추출방법에 대한 설명으로 맞는 것은? A

A. PC 포렌식과 같이 파티션 단위로 데이터를 추출하게 되면 삭제 파일이나 슬랙공간의 데이터를 추출할 수 없는 경우가 있다.

B. 스마트폰을 부팅한 뒤 운영체제 명령어로 bit 단위로 데이터를 추출하는 방법이다

C. 안드로이드에서는 루팅, 아이폰에서는 탈옥이 된 상태에서만 가능하다

D. dd명령어를 사용하여 물리적 이미지를 추출한다

164. 모바일 기기 데이터 추출 및 분석기법으로 chip-off 기법에 대한 설명으로 틀린 것은? D

A. 직접 메모리에 접근하여 내장된 플래쉬 메모리를 물리적으로 덤프한다

B. 추출된 데이터에 대해서는 메모리 리더기를 통해 데이터를 획득한다

C. 가장 확실한 방법이지만 영구 데이터 손실 가능성이 있다.

D. usb 인터페이스를 이용하여 파일시스템내 모든 파일과 디렉토리를 추출한다

165. 안드로이드 모바일 기기의 데이터 복구원리에 대한 설명으로 부적당한 것은? D

A. 안드로이트 데이터의 대부분은 SQLite 데이터베이스에 저장된다

B. 사용자가 데이터를 삭제할 경우 SQLite DB는 해당 레코드가 위치했던 부분을 비할당 영역으로 변경한다

C. SQLite DB가 비할당 영역을 정리하기 전까지 또는 다른 레코드가 덮어쓰기 전까지는 파일내에 데이터가 남아있다.

D. 독자적인 메모리 카드 파일시스템을 사용하고 있어 데이터 카빙 등 방식으로 복구할 수 없다

167. 포렌식 준비도에 대해 기술한 내용으로 맞지 않는 것은? D

A. 포렌식 준비도란 보안사고 조사, 징계절차, 고용 재판, 법정 등에서 디지털 증거를 사용하기 위한 목적으로 증거를 보존, 수집, 분석할 수 있는 적절한 수준의 능력을 말한다

B. 선제적이고 사전적 대응이라는 점에서 사이버 포렌식 조사와 구별된다

C. 소송과정에서 활용을 위해 증거능력이 보장되도록 증거확보하는 것이 필요하다

D. 사이버포렌식 절차와 달리 무결성, 완전성, 신뢰성 등의 보장은 필요 없다

168. 포렌식 준비도의 이점에 대한 설명으로 가장 적합한 것은? A

A. 사건이 발생할 경우에 대비함으로써 비용 및 대응시간을 최소화 할 수 있다

B. 조직이 늘 준비된 상태에 있을 수는 없으므로 사전에 사이버사건을 감지하는 것은 불가능하다

C. 사건 발생 후 효율적인 조사나 신속한 대응에는 별로 도움이 되지 않는다

D. 사건 발생 전부터 대응 준비를 하게 되어 조직의 역량 유출이 우려되는 점이 있다

169. 침해사고 대응 7단계 순서를 바르게 나열한 것은? C

① 사고전 준비 ② 초기 대응 ③ 사고 탐지 ④ 사고 조사 ⑤ 복구 및 해결 ⑥ 대응전략 체계화 ⑦ 보고서 작성

A. ① → ② → ④ → ⑤ → ③ → ⑥ → ⑦

B. ① → ③ → ② → ⑤ → ④ → ⑦ → ⑥

C. ① → ③ → ② → ⑥ → ④ → ⑦ → ⑤

D. ① → ③ → ② → ④ → ⑦ → ⑥ → ⑤

170. 아래 중 웹 로그로 볼 수 없는 것은? C

A. 액세스 로그(Access Log)

B. 시스템 로그(System Log)

C. 에러 로그(Error Log)

D. 에이전트 로그(Agent Log)

171. 윈도우 시스템의 이벤트로그가 아닌 것은? A

A. 관리자 로그(Admin Log)

B. 시스템 로그

C. 디렉터리 서비스 로그

D. DNS 서버 로그

172. 다음 중 시스템 파티션 정보를 확인하기 위한 유틸리티 명령어는? C

A. ps-elf

B. netstat -ano

C. fdisk -l 또는 df -k

D. find

173. 리버스 엔지니어링에 대한 설명으로 부적당한 것은? C

A. 소프트웨어 역공학이라고도 하며, 장치 또는 시스템의 기술적인 원리를 이해하고 구조 분석을 총해 취약점을 발견하고 개선해 가는 과정이다

B. 프로그래머는 개발된 프로그램이 오류를 확인하고 DLL 인젝션을 통해 기능을 추가할 수도 있다

C. 사용자의 프로그램 사용 패턴을 기록하고 추적하는 기술이다

D. 악성코드 분석에서 API를 통해 악성프로그램의 행위를 파악하는 과정이다

174. 악성코드 공격기법의 유형으로 보기 어려운 것은? C

A. DLL 인젝션

B. SSDT 후킹

C. DDoS

D. IAT 후킹

175. 모바일 디바이스의 'SIM card'에서 SIM을 바르게 표기한 것은? A

A. Subscriber Identity Module/Subscriber Identification Module

B. Store International Mobile

C. Standard Identification Mobile

D. Strong Implement Module

176. MBR(Master Boot Record)에 대한 설명으로 틀린 것은? C

A. 시스템 BIOS가 메모리로 로드되도록 하는 실행 코드를 가지고 잇다

B. 실행코드는 MBR이 파티션 테이블을 스캔하여 활성 상태 또는 부팅 가능한 파티션을 찾도록 해 준다

C. 섹터 1에 부팅 정보를 저장한다

D. MBR에는 master boot code, 파티션 데이블 등 파티션 정보가 저장된다

177. 통상 이메일 헤더에 포함되지 않는 것은? A

A. 송신자의 물리적 주소

B. 출발지 IP 주소

C. 이메일의 송신자의 ID

D. 송신자의 도메인 주소

172. 사본 증거의 무결성을 입증하기 위해 사용하는 것은? A

A. 해쉬 값

B. 워터마크(watermarks)

C. 스테가노그라피(steganography)

D. 디지털인증(digital certificates)

173. 다음 중 클라우드 서비스의 기능으로 볼 수 없는 것은? C

A. PaaS(Platform as a service)

B. IaaS(Infrastructure as a service)

C. VaaS(Virtualization as a service)

D. SaaS(Software as a service)

174. 과학적 증거의 허용성(Admissibility of scientific evidence)을 평가하는데 안정적 기준을 최

초로 제시한 사건(판례)은 어느 것인가? C

A. Daubert v. Merrell Dow Pharmaceuticals, Inc

B. Smith v. United States

C. Frye v. United States

D. Dillon v. United States

175. 다음 중 '증거의 일반적 승인의 원칙(general acceptance principle)'이 인정되지 않더라도 법관이 증거의 허용성과 신뢰성을 판단하여 증거능력을 인정할 수 있도록 한 사건(판례)은? A

A. Daubert v. Merrell Dow Pharmaceuticals, Inc

B. Smith v. United States

C. Frye v. United States

D. Dillon v. United States

176. 다음 중 과학적 증거의 허용성과 관련하여 미국의 Frye 판례 이론에 대한 비판으로 옳지 않은 것은? C

A. 어느 정도 입증되어야 동일 과학계의 일반적 승인(general acceptance)을 얻었다고 볼 것인지 모호하다는 비판이 존재한다.

B. 과학적 증거의 신뢰성에 대한 최종적 판단은 과학계의 전문가집단 보다 법관에게 부담지우는 것이 타당하다.

C. 사이비 과학에 의한 오판 가능성을 높이고, 증거의 허용성이 지나치게 완화된다는 비판이 존재한다.

D. Frye 판결을 적용할 경우 문제된 디지털 증거의 보편적 승인을 받기란 거의 불가능에 가깝다.

177. 다음 설명 중 바르지 못한 것은? C

A. Frye 원칙은 과학적 증거는 해단 분야에서 보편적 승인(general acceptance)을 얻어야 한다는 것을 말한다

B. Daubert 기준은 전문가 집단의 보편적 승인기준이 아닌, 판사로 하여금 과학적 증거의 신뢰성을 판단하도록 하였다.

C. '심혈압거짓말측정은 아직까지 생리학적·심리학적 분야에서 지지나 과학적 승인을 얻지 못했다고 판단하는 것은 Daubert 기준을 따른 것이다

D. Daubrert 판결에서 연방대법원은 Frye의 일반적 승인기준은 미연방증거규칙의 제정에 의해 폐기되었음을 선언하였다.

178. 아래에서 국내 IP주소 할당 및 관리를 책임지고 있는 기구는? B

A. iNet

B. KRNIC

C. Google

D. KITRI

179. 소송 당사자가 공정한 재판을 하기 위해 상대방이 보유하고 있는 정보를 요구하고 특별한 사유가 없는 한 제공하는 제도를 무엇이라고 하는가? C

A, 협조 공문

B. 압수수색 영장

C. 증거개시(Discovery)

D. 자료제출 요구

180. 파일 확장자에 대한 정보를 가지고 있는 레지스트리 키에 해당하는 것은? A

A. HKEY_CLASSES_ROOT

B. HKEY_USERS

C. HKEY_LOCAL_MACHINE

D. HKEY_CURRENT_CONFIG

181. 유닉스나 윈도우에서 사용자의 네트워크 활동 상태를 알아보기 위한 명령어는? A

A. netstat

B. ls

C. ifconfig

D. tcpdump

182. 전문가 증언에 대한 설명으로 부적당한 것은? D

A. 법원의 명령에 의한 경우(형소법 제169조)와 수사기관이 촉탁(형소법 제221조의 3)에 의한 경우로 분류된다

B. 특별한 지식과 경험을 가지고 사실의 법칙 또는 그 법칙을 구체적 사실에 적용하여 얻은은 판단을 법정에서 보고하도록 하는 제도이다

C. 포렌식 전문수사관의 증언은 수사기록으로부터 영향을 받아 예단을 갖기가 쉽다

D. 전문가는 해당분야에 대한 학사학위 이상의 학력을 보유한 자를 의미한다.

183. 컴퓨터의 메모리와 같은 1차원의 공간에 여러 개의 연속된 대상을 배열하는 방법을 엔디언(Endian)이라고 하는데, 틀린 설명은? D

A. 빅 엔디언은 큰 단위의 바이트가 앞에 오는 방법이다

B. 반대로 리틀 엔디언은 작은 단위의 바이트가 앞에 오는 방법이다

C. 빅 엔디언은 사람이 숫자를 읽고 쓰는 방법과 같이 0x59654148을 59 65 41 48로 표현한다

D. 이를 리틀 엔디언으로 표기하면 순서가 완전히 뒤바뀌어 84 14 56 95로 표기된다

184. 클러스터에 대한 정의로 볼 수 없는 것은? D

A. 파일을 저장하기 위해 할당되는 디스크 영역의 물리적인 최소 단위는 1 섹터(512 바이트)이다

B. 클러스터는 데이터를 관리를 위해 여러 개의 섹터를 묶은 것을 말한다

C. 따라서 512 바이트 크기의 클러스터는 1개 섹터 크기와 동일하게 된다

D. 4 킬로바이트 클러스터는 7개의 섹터를 가진다

185. 이메일 헤더에 나타나는 SMTP에 대한 설명으로 잘못된 것은? B

A. Simple Mail Transfer Protocol (SMTP)의 약자이다

B. 이메일 송신 뿐만 아니라 수신하는 경우에도 적용되는 프로토콜이다

C. Internet Protocol (IP) 네트워크를 통해 전자메일을 전송하는 인터넷 표준이다

D. HTTP와 함께 인터넷 활성화에 크게 기여한 것으로 평가된다

186. 디지털증거를 획득하기 위해 윈도우를 작동시킬 때 증거의 변형을 막기 위해 사용하는 도구는? D

A. 증거 선서

B. 비트 스트림 복제

C. 수사관 컴퓨터

D. 쓰기방지 장치

187. 증거 발견시 부터 증거를 법정에 제출하기 까지 증거 원본과 사본을 처리하는 과정에서 증거 변형이 일어나지 않았다는 일련의 과정을 보여주어야 한다는 원칙은? B

A. 증거 보관의 원칙

B. 연계 보관성 원칙

C. 증거처리 일관성의 원칙

D. 수사관 행동 기준

188. '통신자료'라 함은? C

A. 가입자의 송·수신 통화내역

B. 가입자가 상대방과 통화한 내용

C. 전기통신 가입원장에 기재된 성명, 주소, 연락처, 설치장소 등 내역

D. 위의 모두

189. 수사관이 정당하게 업무를 집행하던 중 우연히 발견한 다른 범죄 증거를 영장없이 압수할 수 있다는 법 원칙은? B

A. 특수성의 원칙(Principle of Particularity)

B. 육안발견의 원칙(Plain View Doctrine)

C. 상당한 이유(Probable cause)

D. 사인 검색(Private Searches)

190. 파일 공유를 의미하는 뜻으로 주로 사용되는 용어는? A

A. Peer-to-Peer

B. Browser

C. Web Cache

D. Cookies

191. 증거수집 드라이브 내용을 완전히 지우는 이유로 적당한 것은? B

A. 획득하고자 하는 디지털 증거의 양을 확보하기 위해

B. 불필요한 데이터가 남아있지 않도록 하기 위해

C. 증거획득의 신속성을 기하기 위해

D. 위의 것 모두

192. 해쉬 함수에 대한 설명으로 올바른 것은? D

A. 원본파일이 한 비트만 바꾸면 해쉬 값도 한자리만 바뀐다.

B. 해쉬 값을 알고 있으면 원본 데이터를 복구할 수 있다

C. 하나의 파일에 대한 해쉬 값은 사용하는 포렌식 툴에 따라 달리 나타난다

D. 해쉬 값이 동일하면 증거가 변형되지 않았다는 것을 나타낸다

193. 이메일 관련 수사에 대한 설명이다. 맞는 것은? C

A. 이메일 압수를 함에 있어 형사사건에서는 영장을 가지고 하기 때문에 민사사건에 비해 증거확보가 더 쉽다

B. 수사기관이 보다 많은 장비와 기술을 가지고 있기 때문에 이메일 수사가 보다 용이하다

C. 보통 민사사건의 경우 기업 내부에서 압수가 이루어지므로 조사관들이 내부 메일에 접근하기가 쉬워 형사사건보다 이메일 수사가 더 쉽다

D. 민사사건의 경우 ISP들이 자발적으로 메일을 넘겨주므로 형사사건보다 수사가 용이하다

194. 디스크 메니저를 이용하여 확장 파티션을 들여다 보니 확장 파티션의 크기가 논리적 파티션보

다 큰 것으로 나타났다. 무엇을 의미하는가? B

A. 디스크 오염

B. 숨긴 파티션의 존재

C. 통상적인 현상

D. 부적정한 포맷

195. 스테가노그라피를 사용하는 이유는? B

A. 데이터 유효성 검사

B. 데이터 숨김

C. 원격 컴퓨터 접속

D. 비인가자 접속 제한

196. 다음 중 스테가노그라피를 하는데 주로 사용하는 파일 형태는? C

A. 애플리케이션 파일

B. 엑셀 파일

C. JPEG나 MP3

D. 그래픽 파일

197. 패스워드 길이에 크기 좌우되는 패스워드 복구 기법은? D

A. 사전공격

B. 대입공격

C. 무지개공격

D. 무차별 대입공격

198. 다음 중 비어있거나 슬랙공간에 데이터를 숨길 수 있는 파일 시스템은? B

A. NTFS

B. FAT

C. HFSX

D. Ext3fs

199. 키보드에 있는 문자, 숫자 및 특수문자를 사용하여 패스워드를 복구하는 기법은? D

A. Rainbow Table

B. Dictionary Attack

C. Hybrid Attack

D. Brute-force Attack

120. 압수수색 도중 영장범죄 사실과 관련이 없는 새로운 범죄에 대한 증거가 발견되었다. 올바른 조치는? C

A. 범죄증거로 사용하기 위해 계속 수색한다

B. 위법 소지가 있으므로 피의자 또는 변호사를 입회시킨 후 압수수색을 계속한다

C. 즉시 압수수색을 중단하고 새로운 범죄사실에 대한 영장을 발부받아 압수한다

D. 고문 변호사 또는 수사 책임자와 상의해서 결정한다

121. 다음 중 현행 OS 포렌식 기법으로 분석할 수 없는 것은? D

A. FAT12

B. Ext2fs

C. HFS+

D. XFS

122. 윈도우 체제에서 익스플로러 안에 파티션을 숨기거나 노출시키는데 사용하는 명령어는? A

A. diskpart

B. format

C. fdisk

D. grub

123. 다음 중 패스워드 복구를 위한 사전공격(dictionary attack)이나 무차별대입공격(brute force attack) 장비가 아닌 것은? C

A. Last Bit

B. AccessData PRTK

C. OSForensics

D. Passware

124. 일반적으로 안티 바이러스 장비는 몰 웨어 가능성이 있는 파일에 대한 해쉬 값을 생성한다. 하지만 최신 몰 웨어 중에는 이를 피하기 위해 ( ) 기법을 사용하기도 한다. ( ) 속에 적당한 용어는? B

A. Hashing

B. bit-shifting

C. registry edits

D. slack space

125. 파일 내부 정보를 보호할 목적으로 무작위로 bit 배열을 하는 어셈블로 프로그램을 무엇이라고 하는가? C

A. compiler

B. shifter

C. macro

D. script

126. 암호화 및 전사서명 등에 사용되는 키들을 백업 또는 보관하는 시스템을 무엇이라고 하는가? B

A. key vault

B. key escrow

C. bump key

D. master key

127. 정적획득(static acquisition) 기법에 대한 설명으로 옳은 것은? C

A. 증거목록과 이에대한 문서화 내용을 드라이브에 저장하고 난 다음 드라이브를 다시 포맷한다

B. 수집대상 컴퓨터를 가동시킨 후 증거수집을 시작한다

C. 하드드라이브를 탈착한 후 시스템의 CMOS에서 시스템의 날짜와 시간 값을 기록하여야 한다

D. 수집대상 컴퓨터를 네트워크에 연결한 후 포렌식 도구 활용이 가능하도록 업데이트 한다

128. 포렌식 조사를 원활하게 하기 위하여 원격으로 키보드 입력내용을 캡춰하는 프로그램은? B

A. 키그래버(keygrabber)

B. 키로거(keylogger)

C. 패킷캡춰(packet capture)

D. 프로토콜 분석기(protocol analyzer)

129. FTK에서만 작동하면서 육안으로 알려진 프로그램 파일을 필터링하거나, 알려진 불법파일에 대한 해시값을 가진 AccessData의 해싱 DB 프로그램을 무엇이라고 하는가? C

A. DeepScan Filter

B. Unknown File Filter(UFF)

C. Known File Filter(KFF)

D. FTK Hash Manager

130. 스테가노그라피 파일을 탐색하고 분석하는 것은? C

A. carving

B. steganology

C. steganalysis

D. steganomics

132. 대상 저장매체의 파일을 플로피 디스크나 여타 저장매체로 bit-to-bit 방식으로 복사하는 명령어는? C

A. fdisk

B. format

C. dd

D. DiskEdit

133. 아래 파일 확장자 중에서 VMware Virtual Machine과 관련되는 것은? A

A. .vmx, .log, .nvrm

B. .vdi, .ova, .r0

C. .vmx, .r0, .xml

D. .vodx, .vdi, .log

144. VirtualBox에서 가상 하드드라이브(virtual hard drives)의 세팅 값을 가진 파일은? C

A. .vox-prev

B. .ovf

C. .vbox

D. .log

145. 다음 중 파일확장자와 관련된 데이터를 가진 레지스트리 키는? B

A. HFILE_CLASSES_ROOT

B. HKEY_CLASSES_ROOT

C. HFILE-EXTENSIONS

D. HKEY_CLASSES_FILE

146. 호스트 시스템에 가상머신(Virtual Machine)이 설치되었다는 것은 나타내는 것은? B

A. 네트워크 로그(Network Logs)

B. 가상 네트워크 어댑터(Virtual network adapter)

C. 가상화 소프트웨어(Virtualization Software)

D. USB Drive

147. 패킷 분석을 실행하는 OSI 계층은? C

A. 계층 2와 4

B. 계층 4에서 7

C. 계층 2와 3

D. 모든 계층에서

148. 제로데이 공격에 대한 바른 설명은? A

A. 패치작업이 이루어지기 전에

B. 애플리케이션이나 운영체제가 배포된 당일

C. 사용자들이 취약점을 발견한 직후

D. 패치작업이 실행된 직후

150. 다음 줄 잘못된 설명은? A

A. 포렌식 장비는 가상머신(VMs)을 직접 마운트 하지 못한다

B. Type 1 hypervisors는 가용한 RAM, 저장공간, 용량의 크기에 제한을 받는다

C. 허니넷이란 인터넷이나 네트워크 절취행위로부터 정보를 보호하기 위해 개발되었다

D. VM에 대한 포렌식 이미지는 모든 스냅사진을 포함한다

151. 다음 중 VirtualBox 하이퍼바이저와 결합되는 이미지 파일 포맷은? D

A. .vmdk

B. ,had

C. .vhd

D. .vdi

152. 다음 중 이메일 헤더에 포함되지 않는 것은? B

A. 메일 수신 날짜와 시간

B. 발송자의 IP주소

C. 이메일 발송 식별자(ID)

D. 이메일을 발송하는 서버의 주소

153. 스팸메일 발송 근원지 추적을 위해 이메일 헤더의 'Received' 부분을 조사하고자 한다. 틀린 설명은? C

A. from은 메일을 발송하는 서버의 주소 또는 호스트의 이름을 나타낸다

B. with는 사용된 메일 프로토콜을 나타낸다

C. for는 발신자의 이메일 주소를 나타낸다

D. 이메일 헤더에는 수신받는 사용자의 이메일 주소가 명시된다.

154. 해쉬함수의 성격으로 틀린 것은? C

A. 임의 길이의 메세지를 일정 고정 길이의 해쉬 값으로 변환시켜주는 단방향성 알고리즘

B. 단방향성(one-way)이란 결과 값으로는 입력 값을 알 수가 없는 해쉬함수의 특성을 말한다

C. 해쉬 함수는 메세지 내용을 요약한 결과를 말한다

D. 해쉬 값을 달리 'Fingerprint', 또는 MD(Message Digest)라고도 한다

155. 해쉬함수에 대한 설명으로 틀린 것은? B

A. 해쉬 함수를 이용하여 임의 길이의 메세지를 고정(축약) 길이의 값으로 나타낸 것을 해쉬 값이라고 한다.

B. 해쉬 함수의 기본 성질의 하나로 해쉬 값으로부터 입력 값을 쉽게 찾아낼 수 있어야 한다.

C. 해쉬 값이 일치하거나 또 다른 입력 값을 찾아낼 수 없어야 한다

D. 해쉬 값으로부터 임의의 두 입력 값을 찾아 낼 수 없어야 한다.

156. 해쉬함수의 기본 성질(역상저향성)에 대한 설명으로 틀린 것은? A

A. 해쉬 충돌성 : 서로 다른 값을 넣어도 같은 해쉬 값이 나오기도 한다

B. 역상저항성 : 해쉬 값으로부터 입력 값을 찾아 낼 수 없다

C. 두번째 역상저항성 : 해쉬 값이 일치할 것 같은 또 다른 입력 값을 찾아 낼 수 없다

D. 충돌저항성 : 해쉬 값이 같은 임의의 두 입력 값을 찾을 수 없다

157. 클라우드 포렌식에 대한 설명으로 옳은 것은? B

A. 클라우드 포렌식은 증거수집 대상의 물리적 위치나 논리적 위치가 매우 단순하다

B. 클라우드 포렌식은 서비스 제공자의 협조를 받아 스냅 샷 기능으로 수집할 수 있다.

C. 침해당한 클라우드 서버의 관할권이 해외에 있을 경우 원격 압수수색으로 자료를 확보한다

D. 클라우드 서비스를 이용하는 클라이언트 시스템은 증거가 거의 남지 않는다

158. 통상적인 클라우드 서비스 모델에 대한 구분으로 부적당한 하나는? D

A. IaaS

B. PaaS

C. SaaS

D. CaaS

156. 다음 중 기업 포렌식에서 가장 주된 목적이 되는 것은? A

A. 서비스의 지속성

B. 사업의 연속성

C. 사법처리

D. 정보보안

157. 다음 중 법정에서 증거로서 가장 가치가 있는 것은 무엇인가? D

A. 수사서류

B. 증거예시

C. 증언

D. 실물증거

158. 다음 설명 중 잘못된 것은? B

A. 사이버포렌식 수사관은 엄중한 객관성을 유지하여야 한다

B. 수사관은 피의자의 유·무죄를 결정하는 지위를 가진다

C. 수사관은 사건과 관련된 사실에 대해 정확하게 보고할 책임이 있다

D. 수사관은 수사에 참여하는 관계자들과 사건 내용을 토의하는 이외 수사기밀을 유지하여야 한다

159. 다음 중 증거의 무결성을 보장하는데 우선적으로 사용되는 것은? A

A. 해쉬 알고리즘

B. 워터마크

C. 스테가노그라피

D. 디지털 인증

160. 구글 드라이브에서 생성되는 스냅샷 데이터베이스는 윈도우 시스템의 어디에서 찾을 수 있는가? B

A. C:/Program Files/Google/Drive

B. C:/Users/username/AppData/Local//Google/Drive

C. C:/Users/username/Google/Google drive

D. C:/Google/drive

161. 사이버포렌식 전문가는 객관적 사실에 대한 증인(factual witness)과 동시에 또 다른 증인으로서 자격을 갖는다. 적당한 것은? D

A. 직업적 증인

B. 직접 증인

C. 발견 증인

D. 전문가 증인

162. 윈도우에서 앱 작동시간을 줄이기 위해 DLL 경로이름(pathname)과 메타데이터를 포함하고 있는 파일을 무엇이라고 하는가? D

A. 임시파일

B. 캐쉬파일

C. 콘피그(config) 파일

D. 프리패치(prefetch) 파일

163. 사용자의 구체적인 클라우드 접속기록을 저장하는 구글 드라이브 파일은? C

A. loggedtransactions.log

B. sync_log.log

C. transact_user.db

D. history.db

164. 하드 드라이브의 크기에 대한 질문에 대한 대답으로 가장 적당한 것은? C

A. 매우 크다

B. 디스크 데이터 설명 자료에는 용량에 대해 언급이 없다.

C. 3테라바이트 하드인데 자료 저장 공간은 2.78 테라바이트로 확인된다

D. 드라이브가 영어로 설명되어 있어 그 크기를 알 수 없다

165. 악성파일을 추적하는데 사용 도구를 안티바이러스 툴이라고 한다. 안티바이러스 툴로 감지할 수 없도록 하기 위해 최근에 자주 사용되는 기법 중 하나를 고른다면? B

A. 해싱(hashing)

B. 비트 시프팅(bit-shifting)

C. 레지스터리 편집(registry edits)

D. 슬랙공간(slack space)

166. 공격자가 네트워크로 연결된 서버에 과도한 트래픽을 생성시키기 위해 좀비 컴퓨터로 하여금 인터넷 접속을 지속시키는 공격 기법은? B

A. 스머프(smurf)

B. SYN flood

C. spoof

D. ghost

167. 인터넷 서비스 제공(ISP)에 사용되는 상용 암호화 프로그램에서 기억하지 못하거나 시스템 망실로 패스워드를 사용할 수 없을 때 암호화된 데이터를 복구하기 위해 고안된 키 값을 무엇이라고 하는가? A

A. key escrow

B. key vault

C. bump key

D. master key

168. 획득 대상 데이터를 하드 디스크 또는 외장 하드 등으로 비트스트림(bit-stream) 방식으로 복사하는 방식을 무엇이라고 하는가? C

A. fdisk

B. format

C. dd

D. DiskEdit

169. 모든 이메일 관련 로그정보를 저장하는 시스템 로그는 어디에서 찾을 수 있는가? D

A. /usr/log/mail.log

B. /var/log/message

C. /proc/mail

D. /var/log/maillog

170. 프리패치(prefetch) 파일에서 어플리케이션의 최종 접속 날짜와 시간은 나타내는 오프셋은? D

A. 0×80

B. 0×88

C. 0×D4

D. 0×90

171. 피고의 책임을 경감시키거나 면제케 하는 증거를 나타내는 용어는? D

A. 반박증거

B. 피고증거

C. 유죄증거

D. 면책증거

172. 다음 중 수사기관이 전자정보를 획득하는 방법에 해당하지 않는 것은? A

A. 수색영장(search warrant)

B. 자료요구 공문(subpoenas)

C. 법원 명령장(court order)

D. 압수영장(seizure warrant)

173. 모바일 장치에서 플래시 메모리 칩을 분리하여 2진수의 데이터를 수집하는 기법을 무엇이라고 하는가? A

A. chip-off

B. 논리적 추출

C. 마이크로 해독

D. 수작업 추출

174. 다음 중 구글 드라이버의 snapshot.db file에서 찾을 수 없는 것은? D

A. 수정 및 생성 시간(modified and created times)

B. URL 경로(URL pathnames)

C. 파일 접근기록(file access records)

D. 파일의 해시값과 크기

175. 다음 중 일반적인 Type 1 하이퍼바이저가 아닌 옵션은? D

A. VMwar vSphere

B. Microsoft Hyper-V

C. Citirx XenServer

D. Oracle VirtualBox

176. 네트워크가 활성화된 상황에서 네트워크 트래픽을 검사하고자 하는 명령어는? D

A. netstat

B. ls

C. ipconfig

D. tcpdump

177. 대형 Libpcap 파일에서 검사하고자 하는 시간을 확정하는데 사용하는 툴은? B

A. Tcpstat

B. Tcpslice

C. Ngrep

D. tcpdump

178. 가상머신에서 RAM으로 사용되는 VM paging files 저장하는 파일은? B

A. .nvram

B. .vmen

C. .vmpage

D. .vmx

179. 이메일 헤더, 채팅로그 도는 웜이나 바이러스의 네트워크 통신을 분석하는데 가장 유용한 유틸리티는? C

A. tcpdump

B. Argus

C. Ngrep

D. Tcpslice

180. 공격자가 서버에 과부하를 야기할 의도를 가지고 네트워크 연결을 지속적으로 요구하는 공격기법은? B

A. smruf

B. Syn flood

C. spoof

D. ghost

181. 다음 중 이메일 헤더에 포함되어 있는 것은? D

A. 송신자와 수신자의 이메일 주소

B. ESMPT 넘버 또는 reference 넘버

C. 목적지 도달시 까지 경유한 이메일 서버

D. 위의 것 모두

182. 이메일 조사시 가장 주의깊에 보아야 할 정보는? B

A. 송·수신자 이메일 주소

B. 출발 도메인 또는 IP 주소

C. 제목 내용

D. 메세지 번호

183. Microsoft Outlook의 이메일 저장 파일은? A

A. .pst와 ,ost

B. res1.log와 res2.log

C. PU020102.db

D. evolution

184. 범죄피해자 컴퓨터에서 이메일을 조사할 때 송신자 신원확인을 위해 필요한 정보는? D

A. 이메일 헤더

B. 사용자 이름과 패스워드

C. 인터넷 로그

D. 위의 것 모두

185. Phishing 공격이란? B

A. DNS poisoning을 사용하는 것

B. 허위정보로 사용자에게 해킹사이트 접속을 유도하는 것

C. 가짜 웹 사이트를 만드는 것

D. IP주소를 속이는 것

186. 다음 중 현재 사용중인 이메일 포맷 기준은? B

A. SMTP

B. MIME

C. Outlook

D. HTML

187. 이메일 계정에 접속하고자 할 때 사용하는 컴퓨터 구조 형태는? C

A. 메일 프레임과 미니컴퓨터

B. 도메인

C. 클라이언트/서버

D. IP Tracer

188. 이메일 헤더의 IP 주소를 추적하기 위해 사용하는 서비스는? C

A. 인텔사의 AnyOne Who 온라인 디렉토리

B. Verizon사의 수퍼 페이지

C. arin.net/internic.com/whois.net 등과 같은 도메인 찾기 서비스

D. AT&T의 Yellow 페이지

189. 이메일 Router에 대한 설명으로 옳은 것은? C

A. 메세지 내용

B. 붙임 처리된 파일 내용

C. 이메일 서버 포트에서의 데이터 흐름 추적

D. 메일 삭제본 저장

190. 이메일 서버에 대한 로그인 옵션에 대한 설명으로 옳은 것은? D

A. 서버 관리자가 로그인 제지 가능

B. 순환적 로그인 체계를 설정

C. 덮어쓰기 전에 특정 크기를 인식

D. 위의 것 모두

191. 유닉스계열 시스템에서 서로 다른 형태의 이메일 로그파일을 저장할 곳을 결정하는 것은? C

A. 메일로그

B. /var/spool/log

C. syslog.conf

D. log

192. 이매일 헤더 정보로 알맞지 않은 것은? D

A. 블라인드 처리되지 않은 참고 수신자 주소

B. 인터넷 주소

C. 도메인 이름

D. 이메일 내용

193. 이메일 서버 조사시 유용한 정보를 얻을 수 있는 파일은? C

A. .dbf 파일

B. .emx 파일

C. .log 파일

D. .slf 파일

194. 이메일 수사시 이메일 서버에 로그기록이 남아있지 않고, 피해자 텀퓨터에도 이메일이 삭제되었을 경우 대처방법으로 옳은 것은? B

A. 포워딩된 메세지에 대한 로그파일을 조사

B. 백업 시스템에서 이메일 서버를 복구하여 조사

C. 서버에 남아있는 현재의 이메일에 대해 정밀 조사

D. 삭제된 메일은 복구할 수 없으므로 모든 활동을 중단

195. 다음 설명 중 바르지 못한 것은?

A. 대부분의 이메일 헤더는 Notepad를 이용해서 볼 수 있다

B. 이메일 조사를 위해서는 반드시 이메일 서버의 내부 작동원리에 대해 알아야 한다

C. 웹 브라우저를 사용하여 인터넷 이메일에 접속할 경우 Temporary folder에 기록이 남는다

D. 헤더 정보에는 이메일을 보낼 때 사용된 서버이름이 기록되어 있다

196. 메일을 보낼 때 메시지 처리를 담당하는 파일은? A

A. sendmail.cf

B. syslog.conf

C. mese.ese

D. mapi.log

197. 설명이 잘못된 것은? D

A. 이메일 도메인 키는 메시지가 전달되는 도메일 이름을 확인하고 스팸을 차단하는 기능을 한다

B. pagefile.sys 파일은 instant 메세지 애플리케이션에서 생성되는 메시지조각을 포함하고 있다.

C. 이메일 주소에서 @ 이전의 모든 기호는 도메인 이름을 나타낸다

D. 범죄자들은 수사기관의 추적을 피할 목적으로 이메일은 거의 사용하지 않는다

198. Unix 시스템에서 로그 디렉토리를 찾아주는 명령어는? D

A. show log

B. detail

C. search

D. find

199. Microsoft Outlook에서 .ost와 .pst파일을 보수하는데 사용되는 유틸리티는? B

A. fixmail.exe

B. scanpst.exe

C. repairpst.exe

D. rebuildpst.exe

200. 이메일 관리자가 메일 로그기록이 일정 용량수준에 도달했을 때 덮어쓰기 하는 것을 무엇이라고 하는가? A

A. circular logging

B. log recycling

C. log purging

D. log cycling

201. 일반적으로 syslog는 이메일 관련 로그 정보를 아래 파일에 저장하는 역할을 한다. 옳은 것은? D

A. /usr/log/mail.log

B. /var/log/message

C. proc/mail

D. var/log.maillog

202. 이메일 해독을 위해 이진데이터를 텍스트로 변환할 때 생성되는 파일은? B

A. .txt

B. .tmp

C. .exe

D. .log

203. UNIX 시스템에서 사용자 메일이 저장되는 장소는? D

A. /var/mail

B. /var/log/mail

C. /username/mail

D. /home/username/mail

204. 다음 페이스북 프로파일 중 영장이 있어야 수사기관에 제공되는 것은 파일은? D

A. private file

B. advanced file

C. basic file

D. Neoprint profile

205. sendmail 경로를 정확하게 나타낸 것은? A

A. /etc/mail/sendmail.cf

B. /var/etc/sendmail.cf

C. /var/mail/sendmail.cf

D. /usr/local/sendmail.cf

206. 아래 기관 중 IP 주소를 도메인으로 변환시키는 기능을 가진 기관은? B

A. iNet

B. ARIN

C. Google

D. Facebook

207. 아래 예시 중 VMware와 VirtualPC에서 파일을 복구하는데 사용되는 프로그램은? B

A. FookesAid4mail

B. DataNumen Outlook Repair

C. EnCase Forensics

D. AccessData FTK

208. SIM카드에 저장되는 정보가 아닌 것은? A

A. 휘발성 메모리

B. 발신 데이터

C. 서비스와 관련된 데이터

D. 저장 전화번호 목록

209. 다음 중 잘못 기술된 것은? B

A. SIM 카드 리더기로 읽지 않은 메시지를 읽은 것으로 표기하는 등 증거를 변경할 수 있다

B. 모바일 디바이스 수사시 PC에 연결된 디바이스는 기기 상호간 작용상태를 이해하기 위해 연결 상태를 지속하여야 한다.

C. 인터넷 사업자로부터 증거를 확보하려면 통상 영장이 필요하다

D. 해시 값을 기록해 두는 근본적인 목적은 데이터 변형이 이루어지지 않았다는 것을 증명하는데 있다

210. 모바일 장비를 원격으로 삭제할 경우 해당 사항이 아닌 것은? B

A. 계정정보 삭제

B. 절도범을 추적할 수 있는 GPS 비컨 활성화

C. 공장초기화 세팅

D. 연락처 삭제

211. 모바일 단말기의 내용을 검증하는데 수색영장이 필요하다는 미국 대법원 판례를 이끌어 낸 사건은? C

A. Miles v. North Dakota

B. Smith v. Oregon

C. Riley v. California

D. Dearborn v. Ohio

212. 무선통신 서비스를 위해 네트워크와 단말기를 연결하는 무선통신설비는? A

A. Base transceiver station(BTS)

B. Base station controller(BSC)

C. Mobile switching center(MSC)

D. Base tansceiver controller(BTC)

213. GSM을 지원하기위해 개발되어 현재 휴대전화 고속 무선 데이터 패킷 통신규격으로 사용되고 있는 기술을 나타내는 말은? B

A. WiMAX

B. LTE

C. MIMO

D. UMB

214. RAM 분석을 위한 접속시 수정된 부트로더를 사용하는 것을 의미하는 용어는? C

A. Chip-off

B. Manual extraction

C. Hex dumping

D. Micro read

215. 모바일 단발기 내용을 페이지마다 일일이 살펴보고 그림이나 문서를 찾아내는 포렌식 기술은? A

A. 수작업 추출(manual extraction)

B. 칩-오프(chip-off)

C. 마이크로 리드(Micro read

D. 논리적 추출(Logical extraction)

215. 모바일 단말기가 무선신호를 수신할 수 없도록 격리하는 조치로서 적당하지 않은 것은? A

A. 단말기를 비닐봉지에 넣어 둔다

B. 단말기를 무선전파를 차단하는 페인트를 사용한 보관함에 넣어 둔다

C. 단말기를 비행모드로 해 둔다

D. 단말기 전원을 차단한다

216. 모바일 포렌식에서 플래시 메모리 칩을 단말기에서 분리하여 2진 정보를 수집하는 것을 나타내는 말은? B

A. 논리적 추출(Logical Extraction)

B. Chip-off

C. Micro read

D. Manual Extraction

217. 스마트폰에서 운영체제(OS)가 저장된 곳은? C

A. RAM

B. Microprocessor

C. ROM

D. flash memory

218 다음 중 PDA에서 사용되는 주변 메모리 장치가 아닌 것은? D

A. Secure Digital(SD)

B. Compact Flash(CF)

C. Multimedia Card(MMC)

D. RamBus(RB)

219. 정보 보안의 3요소에 해당하지 않는 것은? D

A. Confidentiality

B. Integrity

C. Availability

D. Monitering

220. 다음 중 잘못 기술되고 있는 것은? C

A. 최근 스마트폰이 불법적 활동에 이용되는 사례가 증가하고 있다

B. 모바일 폰에 대한 압수수색시 적법절차 준수는 컴퓨터 압수 절차 못지않게 중요하다

C. 클라우드 시스템에서 취득한 데이터는 서로 섞여 있어도 크게 문제되지 않는다

D. 모바일 디바이스는 무선환경에서 접속하기 때문에 데이터의 변형이 더욱 쉽게 발생한다

221. 전자증거를 획득하기 위한 수단으로 부적당한 것은? B

A. 법원허가서를 발부받아 통신내용 확보

B. 수사기관 발행 공문으로 인터넷 로그기록 입수

C. 수사기관 발행 공문으로 전자 통신자료 입수

D. 대상자의 동의를 받은 전자기록 입수

222. 형사소송법이 규정한 전자증거 확보방법으로 볼 수 없는 것은? A

A. 통신서비스 제공업체에 대한 전자증거 보존명령

B. 허가서에 근거한 전자증거 압수

C. 허가서에 근거한 통신내역 확인

D. 압수수색 영장에 근거한 저장된 전자증거 확보

223. 클라우드에서 스마트폰에 접속하여 증거가 발견하였을 경우 이때 클라우드 서비스의 형태는? C

A. IaaS

B. Haas

C. SaaS

D. PaaS

224. 다음 클라우스 서비스 형태중 보안문제에 대해서는 거의 신경을 쓰지 않는 것은?

A. Hybrid Cloud

B. Public Cloud

C. Community Cloud

D. Private Cloud

225. 아래 설명에서 잘못된 것은? C

A. 인터넷은 미국 고등연구계획국 네트워크(Advanced Research Projects Agency Network, ARPANET)이 진화한 것이다.

B. 전문 시스템 및 네트워크 관리자는 종종 근무하고 있는 업체에서 가장 먼저 사건을 인지하는 경우가 많다

C. 수색영장은 민/형사를 구분하지 않고 사건처리를 위해 활용되고 있다

D. 통신제한조치 허가서 발부요건을 규정하고 있는 법은 통신비밀보호법이다

226. 다음 중 클라우드 서비스의 형태로 볼 수 없는 것은? C

A. PaaS(Platform as a Service)

B. IaaS(Infrastructure as a Service)

C. VaaS(Virtualization as a Service)

D. Saas(Software as a Service)

227. 우리나라 법원에서 인터넷 접속기록 등과 같은 데이터를 확보할 수 있도록 허가하는 문서는? B

A. 영장

B. 허가서

C. 공문서

D. 명령장

228. 마이크로소프트 사에서 애플리케이션의 구동 시간을 줄이기 위해 DLL경로, 메타데이터 등을

포함해서 만든 파일은 무엇인가? D

A. temp

B. cache

C. config

D. prefetch

229. 아래 사항 중 구글 드라이브의 snapshot.db파일에 기록되지 않는 것은? D

A. 수정 및 생성 시간

B. URL 경로자료

C. 파일 접근기록

D. 해시값과 크기

230. 가상환경에서 클라우드 시스템이 구동 중일 때 사건 발생 전후 및 현재 발생중인 주요 기록들을 저장하는 파일은? D

A. 카빙(carving)

B. 실시간 수집(live acquisition)

C. 램(RAM)

D. 스냅샷(snapshot)

231. 우리나라 수사기관이 전자정보를 획득하기 위해 사용하고 있는 법률적 제도에 해당하지 않는 것은? D

A. 수색영장

B. 조회 공문

C. 법원 허가서

D. 압수 명령장

232. 배치방식에 따른 클라우드 시스템에 해당하지 않는 것은?

A. 커뮤니티 클라우드(Community Cloud)

B. 공공 클라우드(Public Cloud)

C. 사업지향형 클라우드 (Targeted Cloud)

D. 사적 클라우드(Private Cloud)

233. 사용자간 공유 디렉토리에 대한 정보 및 드랍박스(클라우드)와 사용자 시스템간 파일 전송기록을 저장하는 파일은? C

A. read_filejournal

B. filetx.log

C. filecache.dbx

D. filecache.dll

234. prefetch 파일에서 애플리케이션의 최종 접속 날짜와 시간을 나타내는 오프셋은? A

A. 0×90

B. 0×D4

C. 0×88

D. 0×80

235. prefetch 파일에서 최초 생성 날짜와 시간을 나타내는 오프셋은? D

A. 0×90

B. 0×D4

C. 0×88

D. 0×80

236. 구글 드라이브에서 생성된 snapshot.db가 저장되는 윈도우 경로는? B

A. C:/Program Files/Google/Drive

B. C:/Users/username/AppData/Local/Google/Drive

C. C:/Users/username/Google/Google drive

D. C:/Google/Drive

237. 사용자의 클라우드 접속내역을 구체적으로 기록하는 구글 드라이브 파일은? B

A. loggedtransactions.log

B. sync_log.log

C. transact_user.db

D. history.db

238. 전문가 증언(expert witness)에 관한 내용으로 맞는 것은? D

A. 의견이나 추론, 결론은 일반인의 통상적인 경험의 범주가 아닌 지식, 기술과 훈련에 기반하는 것을 말한다

B. 증언자는 해당 전문분야에서 자질을 인정받은 사람이다 결론에 관해 합리적인 수준의 확신성을 및

C. 증언자는 자신의 의견인 추론, 결론에 대해 합리적인 수준에서 확신성을 가지고 증언하여야 한다

D. 위의 것 모두

239. 포렌식 분석보고서를 작성할 때 가장 중시해야 하는 것은? A

A. 일관성(Consisitency)

B. 깨긋한 외양

C. 글자의 크기

D. 문장 부호와 표식의 명확한 활용

240. 자동화된 보고서 형식을 따르더라도 전문가 입장에서 고려해야 할 것은? B

A. 보고서 형식에 대한 설명

B. 증거의 중요성에 대한 설명

C. 수집도구의 우수성에 대한 설명

D. 위의 것 모두

241. 다음 설명 중 내용이 틀린 것은? B

A. 보고서는 증거에 대한 추가 수집을 정당화하고, 신문을 하는 상당한 근거가 된다.

B. 전문가 증언을 하기위해 법정에 출석할 때는 보고서를 제출할 필요가 없다

C. 보고서 작성시 어려운 기술적인 용어들은 판사나 변호사 등이 알아듣기 쉽게 일반적인 용어를 사용한다

D. 전문가 보고서는 과학적이고 객관적인 입장에서 기술하여야 한다

242. 포렌식 보고서 작성 소프트웨어는 보통 모든 형식의 워드문서를 열어볼 수 있도록 되어 있다. 이렇게 설정된 파일 형식은? B

A. HyperText Markup Language(HTML)

B. Rich Text Format(RTF)

C. Extensible Markup Language(XML)

D. Microsoft Word Document format

243. 분석보고서 작성시 '요약'은 몇 글자가 가장 적당한가? C

A. 50-100 단어

B. 100-150 단어

C. 150-299 단어

D. 200-250 단어

244. 보고서 작성의 목적, 핵심 내용에 대한 언급, 결론의 도출 및 미흡한 사항 등을 기술하는 것은 보고서의 어느 부분에 해당하는가? B

A, 본문

B. 결론

C. 붙임물

D. 참고사항

245. "전문가 증언이 해당 과학분야에서 일반적으로 수용되는 원칙이나 발견된 사실과 합치되어야 한다"는 과학수사 원칙을 무엇이라고 하는가? B

A. 스미스 원칙 (Smith Principle)

B. 프라이 원칙(Frye Principle)

C. 딜론 법칙(Dillon Principle)

D. 머렐 원칙(Merrell Principle)

246. 소송 당사자가 법원의 요청 없이 상대방이나 제3자로부터 소송과 관련딘 증거자료 공개를 요구할 수 있도록 하는 제도를 무엇이라고 하는가? C

A. 소환제도

B. 공무조회 제도

C. 증거개시제도

D. 증거확인제도

247. 사실증언(fact testimony)에 대해 가장 적당한 설명은? A

A. 증거분석과정에서 복구한 정보를 설명하는 과학적 또는 기술적 증언을 말함

B. 사법수사기관 수사요원이 하는 증언

C. 사건 관련내용에 대해 제3자로부터 득문한 사람의 증언

D. 엄격한 법리적 다툼이 있는 소송단계에서는 가치가 없는 증언

248. 전문가증언(Expert Testimony)이란? A

A. 배심원들에게 일반인의 지식 수준을 넘는 문제에 대한 결심을 하도록 지원해 주는 증언

B. 배심원단이 결정한 사건에 대한 문제를 정의하는 증언

C. 과학적, 기술적 및 기타 전문적 지식이나 경험을 필요로 하지 않는 증언

D. 사실관계나 목격자의 신뢰성에 의구심을 주기 위한 증언

249. 증언에서 그래픽을 사용할 때 고려해야 할 사항을 잘못된 것은? D

A. 배심원들이 그래픽 내요을 충분히 인지할 수 있도록 할 것

B. 법원에 출석하여 당황하지 않도록 사전에 충분히 연습할 것

C. 설명은 분명하면서도 알아듣기 쉽게 할 것

D. 시간이 주어지면 보다 전문적인 지식으로 설명할 수 있음을 설득하여 증언시간을 확보할 것

250. 사실 증언자(fact witness)가 증언과정에서 취해야 할 태도는? C

A. 중요한 증거에 대한 전문적인 의견 제공

B. 재판과정에서 결정되어야 할 이슈에 대한 정의

C. 객관적 사실만 제공

D. 증언한 내용에 대한 관측결과 제공

251. 증언 도중 답변을 할 수 없는 질문을 받았을 경우 취할 태도로 바람직한 것은? B

A. 아무 말도 하지 않는다

B. 자신의 전문(지식) 영역이 아니라고 말한다

C. 해당 질문에는 대답하고 싶지 않다고 말한다

D. 그런 내용에 대해서는 다른 전문가에게 물어보라며 대답을 회피한다.

252. 의견을 진술하는 과정에서 실수 또는 잘못 진술한 사실을 알았을 때 취해야 할 행동으로 올바르지 않은 것은? A

A. 진술세션이 계속 중이라면 잘못한 부분을 얘기하고 수정하도록 한다

B. 아주 사소한 실수라면 얘기하지 않고 뭉개버린다

C. 해당 세션이 끝났을 경우 수정 절차가 복잡하므로 모른체 넘어간다.

D. 상대방 변호인에게 잘못 진술한 내용을 알려 준다

253. 사실 증언 또는 전문가 증언에서 명심해야 할 것은? B

A. 증언자로서 사건 재판경과에 대해 책임을 가지고 있다

B. 증언자로서 가진 기술적·과학적 발견 사실을 보고하고 정직한 의견을 제공한다

C. 증언에 대한 댓가를 얼마나 받았는지에 대한 대답은 회피한다

D. 아무것도 없다

254. 증인으로 출석하기 전에 꼭 해야 할 일에 해당하는 것은? A

A. 변호사와 증언 계획을 수립

B. 증언 내용과 관련한 보수와 출석 경비를 받았다는 사실을 다시 한번 상기

C. 머리를 말쑥하게 정리

D. 조사과정에서 미처 정리하지 못한 원고 입력

255. 하드드라이브의 크기에 관한 설명을 요청 받았을 때 가장 적절치 못한 대답은? A

A. 매우 큰 드라이브라고 표현한다

B. 드라이브에 부착된 기술설명서에는 3테라바이트라고 적혀 있다는 것을 말한다

C. 3테라바이트 크기이지만 사용가능한 영역은 2.78 데라바이트라고 설명한다

D. 디스크가 너무 심하게 손상이 돼서 육안상 크기를 알아볼 수 없다고 대답한다

257. 사용한 툴이나 증거에 대한 무결성이 유지되고 있다는 것을 확신케 하는 알고리즘은? A

A. 해쉬 알고리즘

B. 워터마크

C. 스테가노그라피

D. 디지털 인증

258. 물리적 장치에 저장된 디지털증거 취급시 유의사항으로 틀린 것은? C

A. 운반시 충돌이나 부딪힘이 발생하지 않도록 주의한다

B. 저장매체에 지나친 진동이 있을 경우 자기장치의 변화로 증거훼손 또는 변경이 발생할 수 있다.

C. 디지털 증거는 정전기에 영향을 받지 않으므로 정전기 노출을 문제가 되지 않는다

D. 강한 자력에 노출되는 경우 증거가 인멸 또는 소실될 수가 있다

259. 쓰기방지장치(write-block)에 대한 설명으로 적당하지 않은 것은? D

A. 하드웨어 형태와 소프트웨어 형태가 있으며, 하드웨어 형태가 보다 강력한 쓰기방지 기능을 가지는 것으로 알려진다.

B. 증거획득 과정에서 저장매체 변경이 일어나지 않는 상태로 증거획득이 가능하게 해 준다

C, 쓰기방지 장치는 반드시 증거획득 대상 장비를 장착하기에 앞서 작동시켜야 한다

D. 쓰기방지 장치가 작동하는 동안에는 대상 파일을 읽을 수 없다

260. 아래에서 광학 저장장치(Optical Disc)로만 묶여져 있는 것은? A

A. CD, DVD, BDA

B. RAM, ROM, Flash Memory

C. 자기 테이프, 플로피 디스크, 하드 드라이브, ZIP 드라이브, Jaz 드라이브

D. Magnetic Disk, Blu-ray Disk Association, Flash Memory

261. Flash Memory에 대한 설명으로 틀린 것은? D

A. 1984년 도시바가 '플래시 EEPROM' 논문을 발표한 것에서 유래

B. 비휘발성 메모리로서 디스크형 보조기억장치를 대체 경향

C. 셀이 직열로 연결되는 NAND 방식과 셀이 병렬로 연결되는 NOR 방식으로 구분

D. 인텔사가 개발한 NOR방식은 주로 USB Drive, Memory Card 등에 사용

262. SSD 저장매체에 대한 설명으로 틀린 것은? B

A. 플래시 메모리의 장점을 활용하여 하드 디스크 드라이브(HDD)와 동일한 형태로 개발된 대용량 플래시 메모리를 말한다

B. 그러나 HDD와는 전혀 다른 연결 인터페이스를 사용한다

C. 저전력을 사용하여 고속으로 데이터 입출력이 가능하다

D. HDD에 비해 외부의 충격으로 데이터 손상을 받을 가능성이 적다

263. HDD에 대한 설명으로 부적당한 것은? A

A. 섹터는 HDD상의 물리적인 최대 저장 단위를 말한다.

B. 섹터와 클러스터를 구분하는 가장 큰 이유는 평균적 저장단위가 커진 입장에서 섹터단위로 관리하는 것이 비효율적이기 때문

C. 윈도우에서는 포맷시 클러스터 크기를 지정하는 것이 가능

D. 클러스터는 파일의 디스크 할당 최소 단위를 말한다

264. HDD의 논리적 주소지정 방식은 CHS Address 방식을 말한다. 이에 대한 설명으로 맞는 것은? C

A. HDD의 모든 섹터를 논리적으로 1차원적인 Sector들로 나열하는 방식

B. 초기에는 LBA 방식이 주로 사용되었으나, 최근에는 CHS 방식을 주로 이용

C. 실린더(C), 헤더(H), 섹터(S)로 형성되며, 지정된 주소의 크기가 작아 대용량 HDD에서는 사용하지 않음

D. 실린더와 헤더, 섹터 주소는 모두 0부터 시작한다

265. 플래시 메모리에 대한 설명으로 틀린 것은? B

A. 비휘발성 메모리로 전자거으로 일고 쓰기가 가능

B. NAND와 NOR방식이 있으며, NOR 방식은 오류가 적으나 삭제와 쓰기 속도가 빠르다

C. NAND는 고집적도를 가지며 비용이 저렴하나 NOR에 비해 안정성과 읽기 속도가 떨어진다

D. 따라서 일반적으로 NOR은 프로그램 저장과 실행, NAND는 데이터 저장용으로 활용된다

266. 파일시스템에 대한 설명으로 틀린 것은? C

A. 컴퓨터에서 파일이나 자료를 쉽게 발견 및 접근할 수 있도록 보관 또는 조직하는 체계

B. 구조가 간단하다는 장점을 가지고 있어 일반 시스템 이외 메모리 카드, 디카, 플래시 메모리 등에 많이 사용

C. 저장매체에만 사용되며 네트워크 파일시스템에서는 사용되지 않음

D. 파일시스템은 암호화/ 압축 등 다양한 기능을 제공

267. 파일시스템은 일반적으로 부트섹터, 인덱스(메타데이터), 데이터 영역으로 구분된다. 파일의 이름, 형태, 크기, 상태, 시간정보, 삭제유무 등 정보는 어디에 저장되는가? B

A. 부트섹터

B. 인덱스섹터

C. 데이터 영역

D. 부트섹트와 인덱스 섹터

268. 하드 파티션을 하는 이유로 부적당한 것은? D

A. 중요 데이터를 안전하게 저장하기 위해

B. 하나의 컴퓨터에서 다양한 운영체제 설치가 가능

C. 연속된 저장공간을 하나 이상의 연속되고 독립된 영역으로 나누어 사용

D. 연속된 섹터를 분할로 파일탐색시 헤드의 움직임을 증가시켜 HDD의 부담이 커진다

269. MBR(Master Boot Record)에 대한 설명으로 틀린 것은? D

A. 일반적으로 윈도우 *86환경에서 사용되며 파티션에 대한 위치 정보를 포함

B. 최근 저장매체가 커지면서 GUID 파티션(GPT)으로 대체도는 추세

C. OS 부팅을 위한 부트코드는 ROM에 있는 부트로더에 의해 실행

D. MBR은 4개의 파티션 정보를 포함하는 파티션 테이블을 가지고 있으며, 4개의 파티션은 동등한 기능을 수행

270. FAT 파일시스템을 바르게 설명한 것은? C

A. MS-DOS, windows98 등에서는 사용되지 않았다

B. USB형 플래시 메모리, 메모리카드 등 저장매체는 FAT보다 NTFS 방식을 선호

C. FAT12에서 숫자 12는 비트수로 최대 표현 가능한 클러스터 수를 표시

D. FAT32는 가장 진보된 FAT 방식으로 파일의 최대 크기는 무제한이다

271. FAT 파일시스템에 대한 설명이다. 옳은 것은? D

A. 시스템 구조는 예약된 영역, Root Directory 영역 및 데이터 영역으로 나누어진다

B. Boot record는 1st 섹터에 위치하며, 해당 볼륨의 여러 가지 설정 값, 부팅을 위한 실행코드 등을 포함

C. FAT영역은 FAT#1과 FAT#2으로 구성되는데, FAT#1영역이 소진되면 FAT#2에 기록이 된다

D. Root directory는 Boot record에 그 위치가 표시되며, FAT32부터는 데이터 영역의 어느 곳에나 위치할 수 있다

272. 현재 로그인 중인 사용자에 대한 정보를 확인할 수 있는 레지스터리는? B

A. KEY_LOCAL_MACHINE

B. HKEY_CURRENT_USER

C. HKEY_CLASSES-ROOT

D. HKEY_USERS

273. Window Registry 분석을 하는 이유로 틀린 것은? D

A. 익스플로러에서 실행한 이메일 수신자 주소 확인

B. 최근에 열었거나, 실행 또는 수정한 문서에 대한 사용흔적 추적

C. 윈도우 서버에서 불법계정 생성 여부 확인

D. 인터넷 익스플로러, 명령창에 입력한 URL 리스트, 명령어 등 기록 확인

274. 다음 중 잘못된 설명은? A

A. Created Time - 최초 파일 작업을 완료한 시간

B. Modified Time - 파일이 수정된 시간

C. Accessed Time - 파일이 마지막으로 읽혀진 시간

D. Created Time - 최초 파일이 생성된 시간

275. 파일을 다운로드 받았을 경우 MAC시간 변경 내용을 바르게 설명한 것은? C

A. 최초 파일을 생성하면 만든날짜만 생성되고 수정날짜와 접근날짜는 생성되지 않는다

B. 파일이름을 변경할 경우 만든날짜가 새로운 것으로 바뀐다

C. 파일을 다운로드 받을 경우 만든날짜, 수정날짜 접근날짜 모두 새롭게 생성된다

D. 파일 내용을 수정하면 수정날짜만 바뀐다

276. Windows 파일의 이벤트 로그분석을 통해 얻을 수 있는 정보로 잘못된 것은? ㅊ

A. 사용자가 측정 파일에 접근했는지 여부

B. 누가 시스템 로그인에 성공 또는 실패했는지

C. 윈도우 운영체제 변경이 있었는지 여부

D. 특정 어플리케이션이 사용되었는지 여부

277. 현재 열려있는 파일을 확인하기 위한 명령어는 ? C

A. ps

B. who

C. lsof

D. lsmod

278. Super Block관련 내용으로 틀린 것은?

A. 리눅스의 각 파일시스템의 메타 데이터 정보를 저장

B. 파일 시스템의 첫 시작에서 2섹터를 건너 뛴 영역에 위치

C. 블록의 크기는 1024byte만 사용하기 때문에 슬랙공간 생성될 가능 농후

D. Block Group 0에 있는 Super Block이 primary이며 나머지는 모두 backup에 해당

279. 윈도우와 MAC 타임의 차이에 대한 설명으로 바른 것은? A

A. NTFS에서는 메타데이터가 변화하면 접근시간(A)과 생성시간(C)이 변경

B. UNix/Linux도 메타데이터가 변화될 경우에는 접근시간(A)과 생성시간(C)에서 변화

C. 수정시간(M)은 두 경우 모두 동일하게 변화

D. 전혀 차이가 없음

280. OSI 7계층 네트워크 프로토콜에 대한 설명으로 틀린 것은? D

A. 국제표준기구에서 개방형 통신을 할 수 있게 만든 참조 모델

B. Physical Layer는 데이터의 전기적 흐름에 따라 전송하는 계층

C. Data Link Layer는 MAC주소로 통신하며 네트워크를 통해 데이터가 전송될 때 전송로 역할

D. Network Layer는 시스템 종단 간에 투명한 데이ㅓ 전송을 양방향으로 행하는 계층

281. 침입탐지시스템(IDS)의 기능으로 볼 수 없는 것은? A

A. 보안관리 담당관의 시스템 관리실태 분석 및 관찰

B. 설정된 시스템에 대한 보안 상태 테스트

C. 잘 알려진 공격방법에 대한 패턴 기반 대응

D. 패턴 기반 정상적인 행위에 대한 통계(비정상행위 도출)