**1. 증거사본 이미지를 생성하고 무결성을 입증하시오.**

사본 이미지 정보

|  |  |
| --- | --- |
| 사본 이미지 파일명 | 22-1-234.E01 |
| Hash Value(SHA1) | e4acdfd72d327eca5d7f67ebde340bfc0fdaeb14 |

무결성 유지를 위한 이미지 생성 절차

1) 영상촬영

- 증거사본 생성의 전 과정을 영상으로 상세히 촬영하여 생성과정 중 이상이 없었음을 객관적으로 증명할 수 있도록 기록해야함.

2) 쓰기방지 설정

- 원본의 훼손을 막고 원본과 사본의 동일성 및 무결성 유지를 위하여 쓰기방지를 설정하여 읽기 전용인 상태로 이미지 생성

가. 쓰기방지장치 사용

나. 쓰기방지설정

레지스트리 수정: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolices\ 의 ‘WriteProtect’의 값을 1로 설정

3) 자동실행 방지 설정

- usb연결시 자동으로 인식되어 내용이 변조되는 것을 막기 위해 자동실행 방지를 설정.

- 제어판 -> 하드웨어 및 소리 -> 자동실행 -> 모든 미디어 및 장치에 자동실행 사용 체크 해제

|  |
| --- |
|  |
| 그림1-1 자동실행방지 |

4) 이미지 생성

- 복제장치가 있는 경우: 쓰기방지장치가 부착된 복제장비의 Source(원본)과 Destination(사본)에 각각 증거원본과 저장될 사본 매체를 연결하여 복제 또는 이미징

- 복제장치가 없는 경우 : 논리적 쓰기방지 설정 후 포렌식 소프트웨어를 이용하여 복제 또는 이미징

5) Hash값 및 로그파일 확인

- 이미지 생성 완료 후 생성된 보고서와 산출된 Hash 값을 입회인이나 참관인, 관계자등에게 확인 후 서명날인 받아야 함

6) 봉인 및 확인

- 이미지 생성이 완료된 후 증거원본은 정전기 방지 봉투에 넣은 후 충격보호케이스에 포장하여 상세정보를 기록

- 봉인 후 입회인이나 참관인, 관계자의 서명 날인을 받아 연계보관성이 유지되도록 해야함.

**2. 대법원 판결에 근거하여 원본과 증거사본의 동일성을 증명하기 위한 조치를 기술하라.**

1) 대법원 판례

대법원은 증거사본의 동일성을 증명하기 위해서는 피압수·수색 당사자가 정보저장매체의 원본과 하드카피 또는 이미징한 매체의 해시(Hash)값이 동일하다는 취지로 서명한 확인 서면을 교부 받아 법원에 제출하는 방법에 의하여 증명하는 것이 원칙이라 판시하였다. 다만 예외적으로 원칙과 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우, 정보저장매체 원본에 대한 압수·봉인·봉인해제·하드카피 또는 이미징 등 일련의 절차에 참여한 수사관이나 전문가 등의 증언에 의해 정보 저장매체 원본과 하드카피 또는 이미징한 매체 사이의 해시값이 동일하거나, 정보저장매체 원본이 최초 압수 시

부터 밀봉되어 증거 제출시까지 전혀 변경되지 않았다는 등의 사정을 증명하는 방법, 또는 법원이 그 원본에 저장된 자료와 증거로 제출된 출력 문건을 대조하는 방법 등으로도 그와 같은 무결성·동일성을 인정할 수 있다고

판시하였다.

2) 무결성 유지를 위한 절차 준수

사본 생성과정 중에 이상이 없었음을 객관적으로 증명할 수 있도록 전 과정을 영상 및 사진으로 촬영을 하고 쓰기방지 장치(또는 소프트웨어적 쓰기방지)를 이용하여 원본을 읽기 상태에서만 사본을 생성함으로써 원본이 훼손되지 않도록 해야하며, 사본 생성 후(하드카피 또는 이미징) 산출된 해시(Hash)값을 입회인 등에게 확인시켜 준 후 서명을 받아야 한다. 증거의 매체에 맞게 물리적 파손이나, 정전기등으로 데이터가 훼손되지 않도록 포장 후 봉인하고 봉인지를 부착하여 해당 증거에 대한 정보를 기입 후 입회인 등에게 봉인 상태를 확인하도록 하여 봉인에 이상이 없었음을 서명날인을 받는다. 증거의 수집·봉인·이송·분석의 모든 과정에 걸쳐 연계보관성이 유지될 수 있도록 각 과정마다 모든 절차를 문서로 만들고 확인자의 서명을 받아야 한다.

3) 자격을 갖춘 분석가와 도구의 선정

무결성 유지를 위한 수집·분석 절차와 더불어 증거를 수집하고 분석하는 분석가는 객관적으로 인정할만한 자격을 갖춘 자 이어야 하며, 디지털 포렌식 과정에서 사용하는 분석도구는 정확하고 객관적인 결과를 일관성있게 도출

할 수 있어야 하기 때문에 신뢰할 수 있는 도구를 선택해야한다.

**3. 증거를 탐색하던 중 본 사건 유출과는 관계없는 다른 위법행위에 대한 증거를 우연히 발견했을 경우 취해야할 조치에 대해서 대법원 판례에 근거하여 기술하라.**

- 별건정보가 우연히 발견 됐을시에는 영장(제1영장)에 기재된 기존 증거에 대한 분석은 진행가능하나 별건정보에 대한 탐색은 중지하고 새로운 압수·수색 영장(제2영장)을 발부받은 뒤 탐색을 진행해야한다

- 별건정보가 우연히 발견 됐을시에는 영장(제1영장)에 기재된 기존 증거에 대한 분석은 진행가능하나

별건정보에 대한 탐색은 중지하고 새로운 압수·수색 영장(제2영장)을 발부받은 뒤 탐색을 진행해야한다

**4. 수집한 증거 USB를 복구하고, 복구방법에 대해서 상세히 기술하시오.**

1) 무결성을 유지하며 증거 USB를 이미징한 후, 이미징한 파일인 ’22-1-1234.E01’을 FTK Imager(4.7.3.81)를 이용하여 확인한 결과 총 3개의 파티션을 확인, 두개의 파티션이 ‘Unrecognized file system’ 이라는 메시지와 함께 내부를 확인할 수 없었으며, 다른 1개의 파티션은 ‘Recovered’라는 메세지와 함께 내부 구조를 확인할 수 있었으나 MBR의 Partition table이 훼손된 것으로 추정.

|  |
| --- |
|  |
| [그림 4-1] FTK Imager를 이용하여 22-1-234를 확인한 결과 |

2) 파티션을 복구하기 위해서, 증거 USB를 무결성을 유지하며 DD(RAW)파일로 다시 이미징을 하였으며 파일명은 ’변속기기술유출.001’로 이미징을 완료한 후, Hex Editor인 'HxD'를 이용하여 불러옴.

|  |
| --- |
|  |
| [그림 4-2] HxD를 이용하여 불러온 ‘변속기기술유출.001’ |

3) MBR의 파티션 테이블을 확인한 결과, 첫 번째 파티션과 두 번째 파티션은 시작 섹터값(Starting LBA Address)을 확인할 수 있으나, 세 번째 파티션은 파티션 테이블의 모든 값이 ‘00’으로 되어있는 것을 확인하였으며, 첫 번째·두 번째 파티션의 정보는 아래와 같음.

|  |  |  |  |
| --- | --- | --- | --- |
|  | 파일시스템 | 시작섹터 | 총 섹터수 |
| 첫 번째 파티션 | NTFS | 128 | 4,096,000 |
| 두 번째 파티션 | FAT32 | 4,096,128 | 614,400 |

[표4-1] 확인된 각 파티션의 정보

4) 첫 번째 파티션의 BR을 확인하기 위해서 128번 섹터로 이동하였으며, 확인결과 128번 섹터의 BR영역이 삭제된 것으로 보이며, 첫 번째 파티션의 파일시스템이 'NTFS'인 점과, 파티션의 총 섹터수가 4,096,000임을 생각해 봤을 때, BR의 복사본은 첫 번째 파티션의 마지막 섹터인 4,096,127번 섹터에 있을거라 생각되어 4,096,127번 섹터를 확인한 결과, 복사본이 존재하여 4,096,127번 섹터를 복사한 후 BR의 위치인 128번 섹터에 덮어씀

|  |
| --- |
|  |
| [그림 4-3] 첫 번째 파티션의 BR 복구 |

5) 두 번째 파티션의 BR을 확인하기 위해서 4,096,128번 섹터로 이동하였으며, 확인결과 4,096,128번 섹터의 BR영역이 훼손된 것으로 보이며, 두 번째 파티션의 파일시스템이 'FAT32'임을 생각 해봤을 때, BR의 복사본은 4,096,134번 섹터에 있을거라 생각되어 4,096,134번 섹터를 확인한 결과, 복사본이 존재하여 4,096,134번 섹터를 복사한 후 BR의 위치인 4,096,128번 섹터에 덮어씀

|  |
| --- |
|  |
| [그림 4-4] 두 번째 파티션의 BR 복구 |

6) 두 개 파티션의 BR을 복구한 후 파일명을 ‘변속기기술유출-복구.001’로 저장하여 FTK Imager로 확인해본 결과 MBR의 Partition Table이 훼손된 세 번째 파티션을 제외하고 나머지 파티션은 정상적으로 접근이 되는 것을 확인함.

|  |
| --- |
|  |
| [그림 4-5] 1~2번 파티션의 복구결과 확인 |

7) 두 개의 파티션을 복구한 ‘변속기기술유출-복구.001’ Raw파일을 Autopsy(4.20.0)에 불러와서 확인한 결과, FTK Imager에서 [Recovered] 메시지를 확인했던 세 번째 파티션은 볼륨에 접근이 가능함을 확인하였으며, 이에 분석을 진행함.

|  |
| --- |
|  |
| [그림 4-6] autopsy에서 확인한 3개의 파티션 |

**5. 수집한 증거 USB 매체 볼륨 중 운영체제가 설치된 볼륨의**

**① 파일시스템의 종류 ② 총 용량 ③ 총 섹터수 ④ 클러스터의 크기를 기술하시오.**

운영체제가 설치된 볼륨은 [vol\_vol2]이며, FTK Imager에서 확인한 해당 볼륨의 정보는 아래와 같다.

|  |  |
| --- | --- |
| 파일시스템의 종류 | NTFS |
| 총 용량 | 2,097,147,904 Bytes |
| 총 섹터수 | 4,096,000 |
| 클러스터의 크기 | 4,096 Bytes |

[표 5-1] 운영체제가 설치된 볼륨 정보

|  |
| --- |
|  |
| [그림 5-1] FTK Imager에서 확인한 운영체제가 설치된 볼륨의 정보 |

**6. 유출된 파일을 찾고 그 과정을 상세히 기술하시오.**

1) 신청서.pdf

1. 확장자변조파일로 의심되는 ‘신청서.pdf’를 발견하여, 헤더 시그니처를 확인해보니 압축파일인 ‘.zip’ 파일로 확인이 되었고, 추출하여 압축을 해제하려 하였으나 암호화되었음을 확인하였다.

|  |  |
| --- | --- |
| 파일명 | 신청서.pdf |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol2/Users/yc.choi/Downloads/ |
| 파일용량(Bytes) | 114,441,490 |
| Hash Value(MD5) | af93280abed1c26b547ebd63aa9e11e1 |
| 특이사항 | 확장자변조, 암호화 |

[표 6-2] 신청서.pdf

1. ‘-.eml’ 파일을 확인한결과 ‘o>0, I>1’이라는 내용이 적힌 사진(첨부파일)을 확인할 수 있었고, 압축해제시 사용된 암호과 연관이 있을거라 추정하였다.

|  |  |
| --- | --- |
| 파일명 | -.eml |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol2/Users/yc.choi/Downloads/ |
| 파일용량(Bytes) | 4,102,391 |
| Hash Value(MD5) | f0cc9882e81257968b3afd144c9d0abb |
| 특이사항 | 최유출이 김경욱에게 보낸 이메일 |

[표 6-2] -.eml

|  |
| --- |
|  |
| [그림 6-1] -.eml 파일에 첨부된 사진 |

1. ‘temp.jpg’ 파일은 헤더시그니처가 훼손되어 있었으며, 복구를 하여 확인해보니, 위 ‘-.eml’에서 확인한 최유출이 김경욱에게 보낸 이메일의 첨부파일의 원본으로 보이는 사진을 확인할 수 있었다. 또한 temp.jpg의 exif 정보를 확인한 결과 촬영일시와 촬영기기의 정보를 확인할 수 있었다.

|  |  |
| --- | --- |
| 파일명 | temp.jpg |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol2/Users/yc.choi/Downloads/ |
| Hash Value(MD5) | 4077a66c5347fce95505447c4107b581 |
| 파일용량(Bytes) | 2,997,182 |
| 특이사항 | 헤더시그니처를 훼손한 사진파일 |
| 촬영일시 | 2018-10-09 17:20:43 KST |
| 촬영기기 정보 | Samsung / SM-G950N |

[표 6-3] temp.jpg

|  |
| --- |
|  |
| [그림 6-3] temp.jpg |
|  |
| [그림 6-3] temp.jpg의 EXIF |

1. ‘출력할가족사진2.jpg’는 헤더 시그니처 훼손이 되어있어서 확인이 되지 않아 복구를 하여 확인해보니 김경욱과 최유출이 주고받은 것으로 보이는 카카오톡 대화 내용을 확인할수 있었다. 대화 내용중 최유출이 신청서를 접수 했다며 비밀번호에 대해서 언급을 했고, ‘자동변속기(Automatic)’을 확인하라는 내용을 확인할수 있었다. 위의 ‘Automatic’이라는 단서와 ‘-.eml’과 ‘temp2.jpg’에서 확인한 ‘o>0, I>1’이라는 단서를 종합해 봤을 때 ‘신청서.pdf’의 압축해제 암호는 ‘Automatic’이라는 단어에서 알파벳 ‘o’를 숫자 ‘0’으로, 알파벳 ‘i’를 숫자 ‘1’로 치환하라는 의미로 추정되어 ‘Aut0mat1c’으로 입력한 결과, 압축을 해제 할 수 있었다. 압축파일에서는 ‘1.mp4’ 파일과 ‘2.jpg’파일을 확인할 수 있었는데, 내용을 확인해보니 모니터에 붙어있는 재산관리태그의 관리책임자 정이 최유출인 것을 볼 때, 최유출의 사무실 자리로 보이는 장소에서 설계도면 으로 보이는 화면을 영상과 사진으로 촬영한 것으로 보인다.

|  |  |
| --- | --- |
| 파일명 | 출력할가족사진2.jpg |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol4/DCIM/ |
| Hash Value(MD5) | 2,897,290 |
| 파일용량(Bytes) | 5594449eb4f3a3fbaaf780b07cf7e099 |
| 특이사항 | 헤더 시그니처 훼손, 스테가노그래피 |

[표 6-4] 출력할가족사진2.jpg

|  |
| --- |
|  |
| [그림 6-4] 1.mp4 |

|  |
| --- |
|  |
| [그림 6-5] 2.jpg |

|  |
| --- |
|  |
| [그림 6-6] 출력할가족사진2.jpg |

1. 또한 ‘출력할가족사진2.jpg’파일은 스테가노그래피 파일로써, 1개의 사진을 추가로 은닉한 점도 확인하였다. 은닉한 사진은 접속주소와 로그인 정보로 추정되는 내용이 담긴 포스트잇 사진으로, 내용은 아래와 같았다. 이는 ftp서버로 접속하기 위한 정보를 담은 것으로 추정된다.

|  |  |
| --- | --- |
| 포스트잇 내용 | kwkim.ftp.com  kwkim / kwkim575 |

[표 6-5] 출력할가족사진2.jpg에 은닉한 포스트잇 정보

|  |
| --- |
|  |
| [그림 6-7] 출력할가족사진2.jpg에 은닉한 Jpg 파일 |

2) 전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp

|  |  |
| --- | --- |
| 파일명 | 전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol3/정부사업/ |
| 파일용량(Bytes) | 804,864 |
| Hash Value(MD5) | 41081b581df45997a08ae37771c507e7 |
| 특이사항 | 일반문서 내 설계도면 삽입 |

[표 6-6] 전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp

1. ‘전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp’ 라는 한글 문서파일은 김경욱이 최유출에게 신청서를 다시 보내달라는 이메일의 첨부파일 중 하나로 일반적인 신청서식이었으나, 최유출이 해당 문서를 다운로드 한 후 2~4페이지에 ‘신청서.pdf’에서 확인한 영상과 사진파일에서 볼 수 있었던 설계도면등을 삽입한 것을 확인할 수 있었다. 이는 최초 ‘신청서.pdf’라는 파일로 설계도면을 유출했으나, 다시 보내달라는 김경욱의 요청에 따라 2차로 설계도면을 유출한 흔적으로 추정된다.

|  |
| --- |
|  |
| [그림 6-7] 전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp Page 1~6 |

**7. MD5 해시값이 ‘72c405d49e367e70acf6590d0121a66e’인 파일을 찾고 해당 파일의**

**① 시그니처 ② 파일의 크기(Logical) ③ 파일이 시작되는 위치의 섹터 ④ 시간정보 값을 기술하라.**

|  |  |
| --- | --- |
| 파일명 | 20101205\_설명자료\_자동차온실가스기준2.hwp |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol3/정부사업/ |
| 시그니처 | D0 CF 11 E0 A1 B1 1A E1 |
| 파일의 크기 | 41,472 Bytes |
| 파일이 시작되는 위치의 섹터 | 4,104,368 |
| 시간정보 (UTC+9) | Modified: 2018-10-09 16:27:40 KST  Accessed: 2022-10-12 00:00:00 KST  Created: 2022-10-12 17:23:00 KST |
| Hash Value(MD5) | 72c405d49e367e70acf6590d0121a66e |
| 특이사항 | 일반문서 내 설계도면 삽입 |

[표 7-1] 20101205\_설명자료\_자동차온실가스기준2.hwp

|  |
| --- |
|  |
| [그림 7-1] autopsy와 ftk imager에서 확인한 20101205\_설명자료\_자동차온실가스기준2.hwp |

**8. ‘I.zip – 바로 가기.lnk’ 파일을 분석하여**

**① 원본 파일이 다른 저장매체에 존재했던 경로 ② 원본 파일의 시간정보 ③ 원본매체의 볼륨시리얼 ④ 원본파일의 크기를 기술하시오**

|  |  |
| --- | --- |
| 다른 저장매체에 존재했던 경로 | F:\I.zip |
| 시간정보 | Target Creation Time : 2020-10-08 4:17:00 AM  TargetAccessTime : 2022-10-11 5:00:43 PM  TargetWriteTime : 2020-10-08 4:17:01 AM |
| 원본매체의 볼륨시리얼 | b236b174 |
| 원본 파일의 크기 | 137,765 Bytes |

[표 8-1] 바로가기 파일의 시간정보

|  |
| --- |
|  |
| [그림 8-1] LNK Parser에서 확인한 ‘I.zip – 바로 가기.lnk’ 파일의 분석 결과 |

**9. 증거 USB의 소유자를 확인할 수 있는 단서를 모두 찾아 기술하시오.**

1) 최유출의 개인 공인인증서

|  |  |  |
| --- | --- | --- |
| 파일명 | 저장위치 | Hash(MD5) |
| signPri.key | /img\_변속기기술유출-복구.001/vol\_vol4/NPKI/yessi  gn/User/cn=최유출()012345698413574875400002  3,ou=SAH,ou=personal5JC,o=yessign,c=kr/ | 35bd7907e7afcf43b39e01308d0dbc43 |
| signCert.der | ab4d36bec83a241b7a481cc733f2eb91 |

[표 9-1] 최유출의 공인인증서

|  |
| --- |
|  |
| [그림 9-1] 최유출의 공인인증서 |

2) 유출한 자료를 촬영한 컴퓨터를 추정할 수 있는 사진과 영상

|  |  |
| --- | --- |
| 파일명 | 신청서.pdf |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol2/Users/yc.choi/Downloads/ |
| 파일용량(Bytes) | 114,441,490 |
| Hash Value(MD5) | af93280abed1c26b547ebd63aa9e11e1 |
| 특이사항 | 확장자변조, 암호화 |

[표 9-2] 신청서.pdf

1. 압축파일(.zip)을 pdf파일로 확장자를 변조한 ‘신청서.pdf‘는 암호화된 압축파일로 복호화하면 ‘1.mp4’와 ‘2.jpg’ 파일을 확인할 수 있으며 두 개의 파일의 정보는 아래와 같다.

|  |  |
| --- | --- |
| 파일명 | 1.mp4 |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol2/Users/yc.choi/Downloads/신청서.pdf |
| 파일용량(Bytes) | 108,773,943 |
| Hash Value(MD5) | c3078dc66f8de145d6c61dc2bb8b3367 |
| 특이사항 | 최유출의 사무실로 추정되는 곳에서 촬영한 영상 |

[표 9-3] 1.mp4

|  |  |
| --- | --- |
| 파일명 | 2.jpg |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol2/Users/yc.choi/Downloads/신청서.pdf |
| 파일용량(Bytes) | 5,656,629 |
| Hash Value(MD5) | 10afec2533851eb591535bc867941269 |
| 특이사항 | 최유출의 사무실로 추정되는 곳에서 촬영한 사진 |

[표 9-4] 2.jpg

1. 두 개의 파일에서 확인된 설계도면이 나와있는 모니터의 관리책임 태그를 확인하면, 모니터는 AWG Motors의 자산으로 보이며, 이 모니터의 관리책임자는 ‘정:최유출, 부:서진호’인점을 고려할 때, 해당 영상과 사진은 최유출의 사무실에서 최유출이 사용하는 모니터를 촬영한 것으로 추정된다.

|  |
| --- |
|  |
| [그림 9-2] 2.jpg |

1. 또한 2.jpg 파일의 EXIF 정보를 확인한 결과는 아래와 같다.

|  |  |
| --- | --- |
| 파일명 | 2.jpg |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol2/Users/yc.choi/Downloads/신청서.pdf |
| 촬영일시 | 2018-10-07 오후 6:32 |
| 촬영기기 | Samsung / SM-G950N |

[표 9-5] 2.jpg의 EXIF

|  |
| --- |
|  |
| [그림 9-3] 2.jpg |

3) 영수증 스캔파일

|  |  |  |
| --- | --- | --- |
| 파일명 | 저장위치 | Hash(MD5) |
| 20180204-1.jpg | /img\_변속기기술유출-복구.001/vol\_vol4/scan/ | c0d2207b570467ec6b9c5a75e0de98bb |
| 20180206-1.jpg | 995829cf0944f2f2d6b997752eacf7ec |
| 20180505-1.jpg | 3fea271cf3e0893b969c55860e5911be |
| 20180812-1.jpg | c84600a666e52ff2f13e7db642336686 |

[표 9-6] 영수증 스캔 파일

* KTX 영수증과 주유 영수증으로, 영수증상에 결제 신용카드의 번호를 일부 확인(신한카드 9999-3597-\*\*\*\*-8888)할 수 있었으며, 최유출 소유의 신용카드를 비교해서 스캔한 영수증의 결제자가 최유출인지 확인이 가능할 것으로 추정.

|  |  |
| --- | --- |
|  |  |
| 20180204-1.jpg | 20180206-1.jpg |
|  |  |
| 20180505-1.jpg | 20180812-1.jpg |
| [그림 9-4] 영수증 스캔 파일 | |

4) 업무관련 보고서

|  |  |  |
| --- | --- | --- |
| 파일명 | 저장위치 | Hash(SHA1) |
| FinalTest\_report.pdf | /img\_변속기기술유출-복구.001/vol\_vol3/연구개발/ | cc7397dbc62f4c487caee310fb8fb924 |

[표 9-7] 최유출이 작성한 보고서

* 10단자동변속기(개발명:10T50)의 성능테스트 결과보고서 파일로 작성자가 최유출로 기재되어있는 보고서

|  |
| --- |
|  |
| [그림 9-5] FinalTest\_report.pdf |

5) 증거 USB가 최유출 소유로 추정되는 근거

1. 금융업무 등을 이용하기 위한 개인 공인인증서가 최유출의 이름으로 저장이 되어있고, 이러한 공인인증서의 특성상 공용 USB에 저장하지 않는 점
2. 유출된 것으로 의심되는 10단자동변속기의 여러 도면들이 촬영된 영상과 사진이 관리책임자가 최유출로 되어있는 AWG 社의 자산관리태그가 붙어있는 모니터 앞에서 이루어진 점
3. 최유출이 작성한 10단자동변속기 성능 테스트 보고서가 발견된 점
4. 변속기 관련 사진, 모터쇼 사진, 변속기에 관련된 여러 문서들 등 최유출이 재직시 맡았던 업무와 많은 관련이 있어 보이는 사진 및 문서들이 다수 발견된 점

등을 종합하여 볼 때, 본 증거 USB는 최유출의 개인 USB로 추정이 되며 추가로 발견된 영수증 스캔 파일들에서 확인한 결제 신용카드 번호 일부를 최유출 소유의 신용카드와 비교해보면 더 정확하게 특정할 수 있을 것으로 보인다.

**10. 최유출이 기술 유출을 한 방법과 그에 대한 댓가는 무엇인지 알 수 있는 증거를 모두 찾고 기술하시오.**

|  |  |  |
| --- | --- | --- |
| 파일명 | 저장위치 | Hash(MD5) |
| HeadHunter Korea 안녕하세요 최유출님. 헤드헌터코리아의 김경욱 과장이라고 합니다..msg | /img\_변속기기술유출-복구.001/vol\_vol3/정부사업/ | 8b05ed8f4d2fdfcbaa37c6e6e1fe6390 |
| HeadHunter korea  안녕하세요.  김경욱입니다..msg | /img\_변속기기술유출-복구.001/vol\_vol3/정부사업/ | cb83eaaedecc649329a66340e8b38215 |
| 신청서 보내드립니다..eml | /img\_변속기기술유출-복구.001/vol\_vol2/Users/yc.choi/Downloads/ | 1960f0a98efaa256faebdb1486841eed |
| 요청하신 신청서 서식 다시 보내드립니다..msg | /img\_변속기기술유출-복구.001/vol\_vol3/정부사업/ | 1dfebe9c7e1ad1f7ba0af1645fbd38e5 |
| filezilla.log | /img\_변속기기술유출-복구.001/vol\_vol2/Users/yc.choi/Documents/ | f2e20dafe2b3a360677b92006cf43a30 |
| 출력할가족사진2.jpg | /img\_변속기기술유출-복구.001/vol\_vol4/DCIM/ | 5594449eb4f3a3fbaaf780b07cf7e099 |

[표 10-1] 최유출과 김경욱과의 이메일 송·수신 흔적 및 파일질라 로그, 카카오톡 대화내용 캡처 파일

1. 이메일 송·수신 흔적
   1. ‘HeadHunter Korea 안녕하세요 최유출님. 헤드헌터코리아의 김경욱 과장이라고 합니다..msg’ 파일은 ‘헤드헌터 코리아’ 소속의 ‘김경욱’과장이 중국의 ‘Baudi社’를 대리해서 최유출에게 자동변속기 개발 파트 총 책임자로 스카웃 제의를 하는 내용의 이메일로 최초 접근을 한 이메일로 보인다.

|  |
| --- |
|  |
| [그림 10-1] HeadHunter Korea 안녕하세요 최유출님. 헤드헌터코리아의 김경욱 과장이라고 합니다..msg |

* 1. ‘HeadHunter korea 안녕하세요. 김경욱입니다..msg’파일을 확인한 결과, 김경욱이 처음 보낸 스카웃 제의에 대해서 최유출은 수락을 한 것으로 보이며, 이에 김경욱이 급여 및 지원내용에 대해서 설명을 한 이메일이며, ‘유선상으로 말씀드린 부분에 대해서는 완료 되는대로 즉시 별도의 보수를 지급할 예정입니다’라는 내용은 이직과 관련된 얘기 외에 기술유출에 대한 별도의 댓가를 제시하고 있는 것으로 추정된다.

|  |
| --- |
|  |
| [그림 10-2] HeadHunter korea 안녕하세요. 김경욱입니다..msg |

* 1. ‘신청서 보내드립니다..eml’ 파일은 최유출이 김경욱에게 발송한 이메일 파일로, ‘신청서 보내드립니다’라는 내용과 함께 ‘신청서.zip’이라는 파일을 첨부한 것으로 보이며, 이 ‘신청서.zip’ 파일은 앞서 발견한 ‘신청서.pdf’의 원 파일로 추정되며 최유출의 책상에서 촬영한 영상과 사진으로 추정된다. 또한 ‘https://drive.google.com/file/d/1\_Pb1VvU3xz9T9K9\_9TnISbEj6uhosu8a/view?usp=drive\_web신청서.zip’ 라는 첨부파일의 링크를 확인할 수 있었고, 첨부파일을 확인한다면 ‘신청서.pdf’과 동일한 파일을 첨부하였는지 확인이 가능할 것으로 보인다.

|  |
| --- |
|  |
| [그림 10-3] 신청서 보내드립니다..eml |

|  |
| --- |
|  |
| [그림 10-4] 신청서 보내드립니다..eml |

* 1. ‘요청하신 신청서 서식 다시 보내드립니다..msg’ 파일은 김경욱이 최유출에게 발송한 이메일로, ‘지난번에 보내주신 신청서는 심사기준에 맞지 않아서 접수가 어렵습니다’라며 새로운 신청서를 보낼 것을 요구하며 전기자동차 관련 지원사업 운영지침과 공고문, 그리고 제출서류양식의 한글파일을 첨부하였고, 신청서를 접수할 이메일주소(elec\_car@korea.kr)가 정부메일을 사칭한 점 등 전체적인 메일의 내용이 기존의 스카웃 제의와 전혀 무관해 보이도록 발송한 것으로 보인다. 또한 메일의 내용 하단부에 FTP 접속 주소와 로그인 정보가 있음을 확인할 수 있었다. 이는 새로운 신청서를 해당 FTP에 접속해서 전송하라는 의도로 추정된다.

|  |
| --- |
|  |
| [그림 10-5] 요청하신 신청서 서식 다시 보내드립니다..msg |

1. FTP 접속기록
   1. ‘filezilla.log’ 파일을 발견할 수 있었고, 로그파일의 내용을 확인한 결과, 앞선 이메일에서 김경욱이 알려준 FTP주소와 로그인정보로 접속을 하였고, ‘전기자동차 해외진출 타당성조사 지원사업 제출서류양식.hwp’파일 (804,864bytes)을 서버에 업로드 한 기록을 확인할 수 있었다. ‘전기자동차 해외진출 타당성조사 지원사업 제출서류양식.hwp’파일(804,864bytes)은 앞서 유출된 증거에서 확인한 파일과 파일명 및 파일의 용량이 같은 점을 봤을 때, 김경욱이 알려준 FTP서버를 이용해서 최유출이 다시 한번 유출을 시도한 것으로 추정된다.

|  |
| --- |
|  |
| [그림 10-7] filezlla.log |

1. 카카오톡 대화 내역과 FTP서버정보가 담긴 포스트잇
   1. ‘출력할가족사진2.jpg’ 파일은 헤더시그니처를 훼손시킨파일로, 시그니처 복구 후 김경욱과 최유출간의 대화내용을 확인할 수 있다. 최유출이 처음으로 유출을 시켰고 암호에 관한 정보를 전달했음을 알 수 있고, 그 후 김경욱이 다시 한번 보내줄 것과 전달방법에 대해서 설명한 내용을 확인할 수 있었다. 또한 ‘출력할가족사진2.jpg’파일은 스테가노그래피 파일로 카카오톡 대화 캡처이미지외에 FTP서버주소와 로그인 정보를 수기로 적은 포스트잇을 촬영한 사진을 확인할 수 있었다. 추출하여 확인한 포스트잇 사진은 EXIF 정보가 포함되어있었고, 이 정보를 통해 촬영시간과 촬영기기, 촬영한 장소에 대한 정보를 확인할 수 있었다.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| [그림 10-8] 출력할가족사진2.jpg와 은닉되어있던 포스트잇 사진 및 EXIF 정보 | | |

|  |  |
| --- | --- |
| 촬영일시 | 2022-10-12 오전 9:46 (UTC+9) |
| 촬영기기정보 | Samsung / SM-N971N |
| GPS정보 | 위도 37; 32; 11.7812399614486196  경도 126; 58; 37.7029197080408096 |

[표 10-2] 출력할가족사진2.jpg에 은닉되어있던 포스트잇 사진의 EXIF

1. 기술유출의 댓가(은행거래기록)

|  |  |
| --- | --- |
| 파일명 | 신한은행\_거래내역\_E1235436844.xlsx |
| 저장위치 | /img\_변속기기술유출-복구.001/vol\_vol4/etc/ |
| 파일용량(Bytes) | 13,543 |
| Hash Value(MD5) | 035649fee333a2e7d18ffef98fad531b |
| 특이사항 | 삭제된 파일, 헤더 시그니처 훼손 |

[표 10-3] 신한은행\_거래내역\_E1235436844.xlsx

* 1. ‘신한은행\_거래내역\_E1235436844.xlsx’ 파일은 최유출의 신한은행 거래내역이 담긴 엑셀 파일로, 삭제 되어 있는 것을 발견하였으며, 헤더 시그니처를 훼손한 상태였다. 추출하여 헤더 시그니처를 복구하여 확인한 결과, 2022.10.18. 3억원과 2억원이 입금되었고 송금자는 ‘B’ 라는 기록과 이체를 받은 당일 최유출이 자신의 다른 계좌로 총 5억원을 다시 이체한 기록을 확인할 수 있었으며, 이는 Baudi로부터 변속기 기술을 유출시킨 댓가를 지급받은 것으로 추정 된다.

|  |
| --- |
|  |
| [그림 10-9] 신한은행\_거래내역\_E1235436844.xlsx |

1. USB 연결흔적(AWG 社에서 확인한 자료를 전송한 USB의 시리얼 넘버)
   1. AWG社 자체 감사 결과 자료가 유출에 사용된 USB의 시리얼 넘버를 특정할 수 있었고, 그 USB의 시리얼넘버는 ‘4C530012200403114081’ 이었다.
   2. 최유출로부터 압수한 USB는 파티션이 3개로 이중 1개의 파티션은 Windows 운영체제가 설치되어있는 파티션이였으며 이 운영체제에 연결됐던 USB 흔적을 확인한 결과, 시리얼넘버가 ‘4C530012200403114081’인USB가 연결됐었던 기록이 있고, 이 시리얼 넘버는 AWG社에서 확인한 유출에 사용된 USB이다. 이렇듯 최유출로부터 압수한 USB에 설치된 운영체제에서, AWG社가 확인한 유출에 사용된 USB의 시리얼넘버와 동일한 USB가 발견됐다는 점은 본 사건이 최유출과 연관이 있다는 점을 더욱 명확히 해주는 것으로 보인다. 자세한 내용은 아래 표와 같다.

|  |  |
| --- | --- |
| Vendor | SanDisk |
| Model | Product: 557C |
| Serial Number | 4C530012200403114081 |
| Last connected Date | 2022-10-11 16:31:34 KST |

[표 10-3] 증거 USB에 설치된 운영체제에 연결됐던 USB 흔적

|  |
| --- |
|  |
| [그림 10-10] 증거 USB에 설치된 운영체제에 연결됐던 USB 흔적 |