

[시나리오1 - 변속기 기어 유출사건]

[사건개요]

국내 굴지의 자동차 회사인 AWG社は 3500억원의 개발비가 투입된 10단 자동 변속기 개발에 성공하였다. 이 기술은 연비를 기존대비 약 40% 향상시킬수 있는 기술로, 개발소식이 공개되면서 AWG社の 주가는 급등하였다.

AWG社は 이 기술을 2019년 하반기에 출시되는 차량부터 적용하기로 결정하고 양산 준비를 하고 있었으나, 개발공식발표가 있는지 1달도 안되어서 중국의 자동차 제조사인 BAUDI社 역시 10단 자동변속기를개발하였으며 새로운 기술의 대부분이 AWG社가 개발한 변속기와 동일하였다.

이에 AWG社は 자사의 기술이 유출된 것으로 판단하여 내부 감사를 진행하였고, 최근에 퇴사한 개발팀 과장 최유출의 컴퓨터에서 USB를 이용해서 자료를 전송한 흔적을 발견, 해당 USB를 특정할수 있었다.

이에 AWG社は 경찰에 신고를 하였고, 출국금지조치가 내려진 최유출은 인천국제공항에서 출국하려는 과정에서 붙잡혔다. 체포당시 최유출은 노트북을 소지하고 있었으며, 노트북 가방에서 USB 1개가 발견되었고, 최유출은 처음보는 USB라며 자신의 소유가 아니라고 진술했으며, 노트북에서는 별다른 유출 흔적이 발견되지 않았다. 이에 경찰청 디지털 포렌식 분석가는 USB를 분석하려 했으나 USB를 정상적으로 확인할 수 없었다.

* 자료를 전송한 매체로 추정되는 USB의 시리얼 넘버 : 4C530012200403114081

1. 증거사본 이미지를 생성하고 무결성을 입증하시오.
2. 대법원 판결에 근거하여 원본과 증거사본의 동일성을 증명하기 위한 조치를 기술하라.
3. 증거를 탐색하던 중 본 사건 유출과는 관계없는 다른 위법행위에 대한 증거를 우연히 발견했을 경우 취해야할 조치에 대해서 대법원 판례에 근거하여 기술하라.
4. 수집한 증거 USB를 복구하고, 복구방법에 대해서 상세히 기술하시오.
AUTOPSY에서 복구된거확인만 캡처하면끝
5. 수집한 증거 USB 매체 볼륨 중 운영체제가 설치된 볼륨의
① 파일시스템의 종류 ② 총 용량 ③ 총 섹터수 ④ 클러스터의 크기를 기술하시오.
6. 유출된 파일을 찾고 그 과정을 상세히 기술하시오.
7. MD5 해시값이 '72c405d49e367e70acf6590d0121a66e'인 파일을 찾고 해당 파일의
① 시그니처 ② 파일의 크기(Logical) ③ 파일이 시작되는 위치의 섹터
④ 시간정보 값을 기술하라.

8. 'l.zip - 바로 가기.lnk' 파일을 분석하여 ① 원본 파일이 다른 저장매체에 존재했던 경로
② 원본 파일의 시간정보 ③ 원본매체의 볼륨시리얼 ④ 원본파일의 크기를
기술하시오
9. 증거 USB의 소유자를 확인할 수 있는 단서를 모두 찾아 기술하시오.
10. 최유출이 기술 유출을 한 방법과 그에 대한 댓가는 무엇인지 알 수 있는 증거를
모두 찾고 기술하시오.

문제1~10까지의 답은 각 폴더 내 존재

11. 결론

최유출은 중국 Baudi社의 헤드헌팅업체인 헤드헌터코리아의 김경욱 과장으로부터 자신이 담당
하여 개발중이었던 AWG社의 10단 자동변속기 기술 유출 내용을 포함한 내용의 이직 스카우트
제의를 받고, 유선으로 김경욱 과장과 해당 내용에 대해 모의한 것으로 추정됨.

유선에서 최유출은 해당 스카우트 조건(연봉 등)에 대해 질문한 것으로 보여지며, 최유출은 1차
적으로 자신의 업무용 pc 내 관련 자료들을 USB를 이용해 복사하고, 해당 자료를 촬영하여 시
그니처변조, 암호화해 저장한 후 유출한 것으로 추정됨.

이에 김경욱은 이메일로 스카우트 조건에 대한 답신과 함께 해당 자료들에 대한 다른 형식과 해
당 파일에 대한 FTP서버로의 송신을 요구하였고, 이에 최유출은 김경욱이 메일의 첨부한 파일인
'전기자동차 해외진출 타당성조사 지원사업 제출서류 양식' 내에 해당 자료를 2차적으로 유출한
것으로 추정되며, 이에 대한 보상으로 5억원의 현금이 최유출의 신한은행 계좌에 입금된 것으로
보여짐.

또한, 체포당시 수집한 증거 USB에 최유출의 공인인증서가 존재하는 점, 최유출의 신한은행
입출금 내역이 시그니처 변조되어 저장되어 있는 점, 1차유출로 의심되는 파일인 사진과 영상에
등장하는 업무용 PC의 관리책임자가 최유출인 점, 김경욱과의 연락(카톡 캡처 사진 및 이메일
송수신 내역)에서의 상대방이 최유출로 특정되는 점, 그 외 영수증 스캔 파일과 최유출이 담당이
었던 10T50 성능테스트 결과보고서 및 각종 변속기 관련 파일들이 존재하는 점 등을 미루어보아
해당 USB는 최유출의 소유일 가능성이 굉장히 높아보임. 추가적으로, 한글 파일 내 삽입되어 유
출된 자료인 사진 3장 이외에도 다른 도면들이 있는 것으로 미루어보아 추가적인 유출 가능성에
대해서도 조사가 필요해 보임.