Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.515

디지털 포렌식 기법을 이용한 해양사고 조사 방법론

백 명 훈,† 이 상 진‡
고려대학교 정보경영공학전문대학원

A New Investigation Methodology of Marine Casualties and Incidents using Digital Forensic Techniques

Myeong-Hun Baek,† Sangjin Lee‡
Graduate School of Information Management and Security, Korea University

요 약

해양사고 조사의 결과는 원인규명은 물론 가해자 및 피해자의 과실여부와 과실정도를 판단하는 중요한 결정기준이 되고 있다. 그러나 해양사고는 해양이라는 특수한 환경에서 발생하기 때문에 사고현장의 보존, 사고 재연 및 목격자 확보 곤란 등 원인규명의 어려움이 있다. 이러한 해양사고의 특징으로 국제해사기구에서는 최근 발달된 전파통신 및 항해기술을 해상인명안전 협약에 도입하여 일정 규모 이상의 선박에 항해자료기록장치와 선박자동식별장치의 설치를 의무화하였고, 국제적으로 통일된 사고조사와 공조를 위해 발효한 새로운 해양사고 조사코드에서는 각 체약국에게 항해자료기록장치의 분석역량을 갖추도록 권고하고 있다. 이에 따라 본 논문에서는 선박용 블랙박스인 항해자료기록장치의 데이터 유형을 분석하고 디지털 포렌식 절차와 기법을 활용하여 사고원인을 효율적으로 조사할 수 있는 방법을 제시한다.

ABSTRACT

The results of investigations into marine incidents have become an important basis in determining not only possible causes, but also the extent of negligence between the perpetrator and victim. However, marine incidents occur under special circumstances i.e. the marine environment, and this leads to difficulties in identifying causes due to problems in scene preservation, reenactment and acquisition of witnesses. Given the aforementioned characteristic of marine incidents, the International Convention for the Safety of Life at Sea (SOLAS) has adopted mandatory regulations on the carriage of Voyage Data Recorders (VDRs) and Automatic Identification Systems (AIS) for ships of a certain gross tonnage and upwards, so as to reflect recent developments in radio communication and marine technology. Adopted to provide an international standard for investigations and to promote cooperation, the Code of the International Standards and Recommended Practices for a Safety Investigation into a Marine Casualty or Marine Incident (Casualty Investigation Code) recommends member states to build capacity for analysis of VDR data. Against this backdrop, this paper presents methods for efficient investigations into the causes behind marine incidents based on data analysis of VDR, which serves as the black box of ships, as well as digital forensic techniques.

Keywords: Marine Incident, Investigation, Voyage Data Recorder (VDR), IMO, Digital Forensic

접수일(2013년 4월 2일), 수정일(1차: 2013년 4월 22일), 게재확정일(2013년 5월 2일)

† 주저자, mhbaek@gmail.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

I. 서 론

최근 우리나라는 태안반도의 유조선 충돌사고로 인한 해양오염사건, 천안함 침몰사건 등으로 인하여 많은 국민들이 해양사고에 대하여 관심을 가지고 있다. 3면이 바다로 쌓여있고 수역이 좁은 배타적 경계수역(EEZ)의 특수한 사정으로, 인접한 국가와의 영해침범 분쟁 및 어선과 순시선의 충돌 발생으로 인한 뉴스도 자주 접하고 있다. 해양사고는 증거확보가 어려울 뿐만 아니라 항만시설의 입지조건과 안전시설, 선박의 성능과 안전운항 능력, 해양안전관리시스템 등 하드웨어적인 요인이 있고, 항만관리자, 선원 등 선박종사자의 교통안전 의식과 운항관리능력 부족 등의 인적 요인과 근로여건 및 복지환경 요인과 같은 소프트웨어적인 요인이 복합적으로 결합되어 발생되므로 사고 원인 규명이 매우 어려운 특징을 가지고 있다. 그러나 현대 해양사고의 조사는 해양사고 관계자의 자발적인 증언과 증거제출 및 조사관의 경험과 심증에 의존하고 있으며, 사고의 조사와 심판이 분리되지 않은 상태로 이루어지기 때문에 해양사고 관계자로부터 사고의 실체적 진실을 밝히기 위한 정보를 얻기는 구조적으로 어려운 실정이다[1]. 또한 해상 뺑소니 또는 조업으로 인한 영해침범을 다루는 해상사고의 경우, 침몰로 인하여 사고에 대한 증거가 소실되거나 타국적 선박이 자국으로 도주하여 사고대응이 미흡하게 된다면 분쟁은 국제 재판으로까지 이어질 수 밖에 없고 사고 피해자는 엄청난 고통을 받게 된다[2].

최근 건조되는 선박에는 선박자동항법장치, 항해자료기록장치, 선박자동식별장치, CCTV 등 선내 기자재를 하나의 네트워크로 연결하는 선박통합네트워크 기술이 적용되고, 적도 상공 35,786km의 정지궤도에 있는 국제해사위성기구(INMARSAT) 위성을 이용하여 태평양, 인도양, 대서양 지역의 해상・육상 어디에서나 통신서비스를 이용하는 등 IT와 조선기술이 결합되고 있어 해양사고 발생 시 전자장비의 종합적인 분석이 요구되고 있다. 또한 해상교통체계가 점점 복잡해짐에 따라 선박간의 충돌 및 침몰사고 등 해양사고가 많이 발생하고 있으나 증거확보가 곤란해 사고원인규명이 어려워짐에 따라 UN 산하 전문기관인 국제해사기구(IMO)에서는 모든 선박에 대해 항해자료기록장치와 선박자동식별장치의 장착을 의무화하는 규정을 신설했다[3].

따라서 본 논문에서는 해양사고의 사례와 기존 사고조사 방법의 문제점을 살펴보고, 이를 해결하기 위하여 항해자료기록장치를 중심으로 디지털 포렌식 기법을 활용한 조사방법론을 제시하고자 한다.

II. 해양사고 조사 관련 동향

해양안전심판원[4]과 통계청[5]에 따르면 국민들이 해양을 이용하는 기회와 해양과 밀접한 다양한 활동들이 급속도로 증가하는 추세에 있어 선박등록척수와 해양사고 발생건수는 매년 증가하고 있다.[표 1]

[표 1] 연도별 해양사고 발생 현황

척수/건수 \ 연 도	2007	2008	2009	2010	2011	2012
해양사고발생건수	566	480	723	737	946	726
해양사고발생척수	759	636	915	961	1197	941
인명피해	214	240	243	247	280	232

2.1 해양사고의 정의

해양사고의 조사 및 심판에 관한 법률 제2조(정의)에 의하면, 해양사고란 해양 및 내수면에서 발생한 다음 어느 하나에 해당하는 사고를 말하며, 국제기준의 정의도 국내 법률과 동일하다[6][7].

- 선박의 구조·설비 또는 운용과 관련하여 사람이 사망 또는 실종되거나 부상을 입은 사고
- 선박의 운용과 관련하여 선박 또는 육상·해상시설에 손상이 생긴 사고
- 선박이 멸실·유기되거나 행방불명된 사고
- 선박의 충돌·좌초·전복·침몰이 있거나 조종이 불가능하게 된 사고
- 선박의 운용과 관련하여 해양오염 피해가 발생한 사고

2.2 해양사고 조사 관련 제도적 배경

해양사고의 조사 및 심판에 관한 법률 제1조(목적)에 의하면, 해양사고에 대한 조사 및 심판을 통하여 해양사고의 원인을 밝힘으로써 해양안전의 확보에 이바지함을 목적으로 한다. 같은 법 제4조(해양사고의 원인규명 등)에 따르면 심판원이 심판을 할 때는 사람의 고의 또는 과실로 인하여 발생한 것인지 여부, 선박승무원의 인원, 자격, 기능, 근로조건 또는 복무에 관한 사유로 발생한 것인지 여부, 선박의 선체 또는 기관의 구조·재질·공작이나 선박의 의장 또는 성능에

관한 사유로 발생한 것인지 여부, 수로도지·항로표지·선박통신·기상통보 또는 구난시설 등의 항해보조시설에 관한 사유로 발생한 것인지 여부, 항만이나 수로의 상황에 관한 사유로 발생한 것인지 여부와 같은 사항에 관하여 해양사고의 원인을 밝히도록 정하고 있다[6].

또한 선박은 국제적인 무역을 위해 전 세계의 바다를 무대로 활동하고 있으며 해외 국적 선박에도 우리나라 선원들이 많이 승선하고 있어 이들 선박과 선원이 관련된 사고가 발생할 경우 조사와 심판의 대상이 된다. 더욱이 우리나라의 영해는 물론 공해 상이나 타국의 영해 내에서 발생하는 해양사고에 대하여 보다 신속한 조사 착수와 함께 원활하고 정밀한 사고조사 및 심판을 위하여 사고와 관련된 국가와의 정보 및 증거자료 교환 등 조사협력체제 구축이 필요하다.

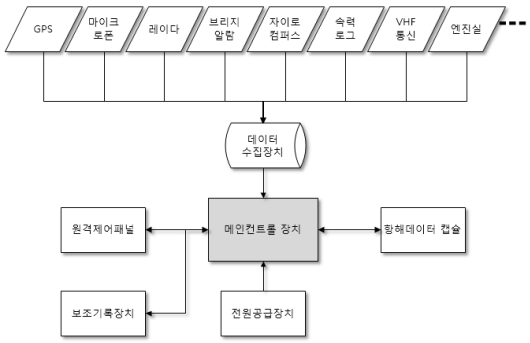
이에 따라 국제해사기구에서는 해양사고의 안전한 조사를 위한 국제기준 및 조사방법에 관한 코드를 2008년에 채택하고 2010년 1월 1일 발효하였다. 이 코드의 구성은 목적 및 적용에 대한 일반사항을 규정한 Part I, 사고조사 권한, 요건, 조사 국가간의 관계 및 협력사항, 사고조사 보고서 등과 같은 사항을 규정한 Part II 및 조사방법을 기술한 Part III로 구성되어 있다. 이를 근거로 해양사고 조사 시 외국 조사기관의 협조를 받아 사고선박을 조사 및 심판할 수도 있다[8].

III. 항해자료기록장치를 통한 해양사고 조사

항해자료기록장치(Voyage Data Recorder)는 선박운항에 관련된 주요 장치에 센서를 설치해 각종 정보를 수집하고 주요 항해 데이터, 선박의 위치, 속도, 날짜, 시간과 레이더 영상, 조타실에서의 각종 대화와 교신내용 등을 저장장치에 기록하는 장치로 항공기의 블랙박스와 유사한 시스템이다. 사고가 발생할 경우 다운로드 버튼을 누르면 사고발생 12시간 전부터의 기록을 보조기록장치에 보관할 수 있도록 되어있다. 사고원인 규명에 주요자료로 사용되기 때문에 임의조작 방지를 위한 보호장치가 설치되어 있고 신속한 회수를 위해 눈에 잘 띄는 색깔과 역반사 물질로 표면이 덮여있으며 위치표시장치도 설치되어 있다. 해상인명안전 협약(SOLAS)[3]과 국내 선박안전법에 따른 선박설비기준[9]에 설치근거를 두고 있어, 국제항행에 종사하는 선박으로 근해구역 이상을 항행구역으로 하는 총톤수 150톤 이상의 여객선과 여객선 이외의 선박으로서 총톤수 3,000톤 이상의 선박에는 설치를 의무화하고 있다.

3.1 항해자료기록장치의 구성

항해자료기록장치는 선박운항의 모든 정보를 저장하고 비상시 데이터를 보호하기 위해 여러 가지 장치들이 상호연결되어 구성되어 있다. 제조사마다 각 장치들의 명칭과 구성된 시스템의 차이가 조금씩 있으나 일반적으로 정보를 기록하고 제어하는 메인 컨트롤 장치(Main Control Unit), 최종기억매체를 포함하고 있는 항해데이터 캡슐(Voyage Data Capsule), 데이터 수집장치(Data Acquisition Unit), 무정전전원공급장치(UPS)가 포함된 전원공급장치(Power Supply Unit), 다운로드 버튼과 경고메세지가 표시되는 원격제어패널(Remote Control Panel), 보조기록장치 등으로 구성되어 있다.[그림 1]



[그림 1] 항해자료기록장치의 구성

3.1.1 메인컨트롤 장치(Main Control Unit)

메인컨트롤 장치는 항해자료기록장치의 각종 정보의 기록 및 제어를 담당하는 핵심장치로서 보통 선내에 위치하여 있다. 제조사에 따라 Main Control Unit(MCU), Data Management Unit(DMU), Data Acquisition Unit(DAU), Main VDR Unit(MVU), Main Electronics Enclosure (MEE)와 같이 다른 명칭을 사용하기도 한다.

장비 내부의 하드디스크 또는 플래시메모리에 모든 정보가 기록되며, 제조사별로 약간의 차이는 있으나, 보통 [그림 2]와 같이 착탈식으로 되어 있어 사고 발생 시 하드디스크만 분리하여 수거가 가능하다.

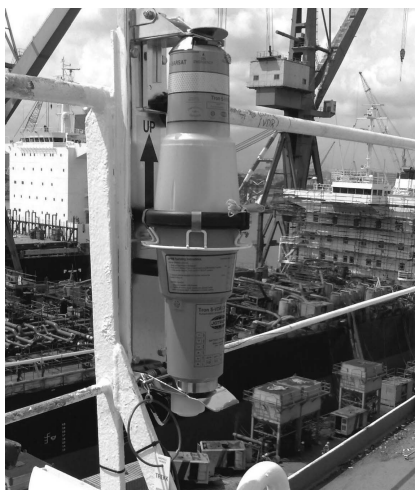
〔그림 2〕 메인컨트롤 장치 샘플사진

3.1.2 항해데이터 캡슐(Voyage Data Capsule)

항해데이터 캡슐은 메인컨트롤 장치에 저장된 자료가 최종기억매체에 동기화 저장하도록 되어 있는데, 선박 침몰시 데이터를 보호하기 위하여 캡슐화되어 있어 데이터보호장치(Protected Data Unit)라고도 한다. 침몰사고 후의 잔존과 회수의 가능성을 최대로 하기 위해 선교 근처의 노출갑판 부근에 설치하며 부양형과 선체고정형이 있다.〔그림 3〕〔그림 4〕

3.2 저장 데이터의 내용

항해자료기록장치는 메인컨트롤 장치와 항해데이터 캡슐에 포함된 저장매체에 항해와 관련된 각종 데이터



〔그림 3〕 부양형 항해데이터 캡슐 샘플사진

〔그림 4〕 선체고정형 항해데이터 캡슐 샘플사진

들을 저장하고 있다. 특히 선박의 위치, 선박의 대수속력 및 대지속력, 선박의 침로, 선교에서 발생하는 대화내용, 선박 운항과 관련된 초단파대를 사용한 통신내용, 레이더에 표시되는 자료 등의 정보는 해양사고 원인규명에 영향을 미칠 수 있는 중요한 정보이므로 데이터의 형식을 미리 숙지할 필요가 있다.

기록되는 자료들은 재생 및 분석을 위하여 다음과 같은 데이터들이 날짜와 시간에 확실하게 상호연관이 될 수 있는 방법으로 기록된다〔9〕. 밑줄 친 7가지 항목은 2002년 7월 1일 이전에 건조된 총톤수 3,000톤 이상의 선박일 경우 설치 가능한 간이항해자료기록장치(S-VDR)에 기록되는 데이터이다.

- 날짜 및 시간
- 선박의 위치
- 선박의 대수속력 및 대지속력
- 선박의 침로
- 선교에서 발생하는 대화내용
- 선박운항과 관련하여 초단파대를 사용한 통신내용
- 레이다에 표시되는 자료
- 음향측심자료
- 선교에 표시되는 경보사항
- 타의 상태
- 주기관의 상태 및 바우스러스터(Bow thruster)가 설치된 경우 그 상태
- 선교에서 표시가 의무화된 모든 상태 정보를 포

함한 선체의 개구 상태
- 선교에서 표시가 의무화된 모든 상태 정보를 포함한 수밀문 및 방화문의 상태
- 선체응력 및 응답 감시장치가 설치된 선박의 경우 사전에 선택된 모든 자료
- 풍속 및 풍향(측정 센서가 있는 선박의 경우)

날짜와 시간, 선박의 위치 및 속력 등의 정보는 NMEA 0183 규격에 따라 기록되며 보통 serial이 포함된 파일명 또는 폴더명으로 저장된다. NMEA 0183 데이터들은 주로 자이로컴퍼스, GPS, 나침반, 관성항법장치에 사용되고 아스키 형태의 데이터로 생성되며 직렬 방식의 통신을 이용한다. 데이터는 물리적 계층, 데이터링크 계층, 어플리케이션 계층의 3가지 계층으로 구성된다. NMEA 0183 규격에서는 어플리케이션 계층에서 데이터를 전송하는 문장에 대한 규약을 기술하고 있다[10][11].

선교의 각종 음향 및 선박의 운항과 관련된 VHF 통신내용은 오디오 파일 형태로 압축하여 저장이 되며 이를 위해 제조사마다 다른 코덱을 사용하고 있다. 선교에 설치된 한 개 또는 두 개 이상의 마이크가 조선위치, 레이더 화면, 해도테이블 등의 장소 또는 그 가까이에서의 대화가 적절히 기록되도록 분산 배치되어 있어 선교에서 내부자간 통화, 선내방송장치 방송내용, 각종 가청경보음이 파일로 저장된다. 오디오 채널에 따라 audio1, audio2와 같은 형태의 단어가 포함된 파일명 또는 폴더명으로 저장된다.

레이더 데이터는 기록할 당시에 사용 중인 선박의 레이더설비 중, 한 레이더의 메인화면에 실제적으로 표현된 모든 정보를 기록하는 전자신호 정보를 포함한다. 재생하는 방법이 항해자료기록장치의 작동에 중요한 어떠한 대역폭 압축기술의 범위 내에 있다고 할지라도 기록할 당시에 볼 수 있는 레이다 전체화면의 신뢰할만한 복제품으로 표현 가능한 기록방법을 사용하도록 하고 있다[12].

3.3 사고 선박의 항해자료기록장치 확보 및 조사

국제해사기구에서 발표한 항해자료기록장치의 소유 및 자료 회수에 관한 가이드라인[13]에 따르면 항해자료기록장치의 정보는 증거의 보전을 위해 사고 발생 후 최대한 빨리 회수되어야 하고, 선주는 선원들을 통해 이 증거가 적절한 시기동안 보존될 수 있도록 조치할 책임을 지도록 하고 있다. 항해자료기록장치 회수 과정에서 선주의 책임범위와 항해자료기록장치 데이터의 소유권 등 항해자료기록장치 운영상의 문제에 대해 소유권은 선박 소유자에게 있되 사고 발생 후 조사권을 갖는 자에게 접근이 허락되고 또 조사를 위하여 내장정보의 판독을 하여야 하므로 보관·판독·접근성은 조사자에게 보장해주고 있다[14].

3.3.1 항해자료기록장치의 데이터 추출

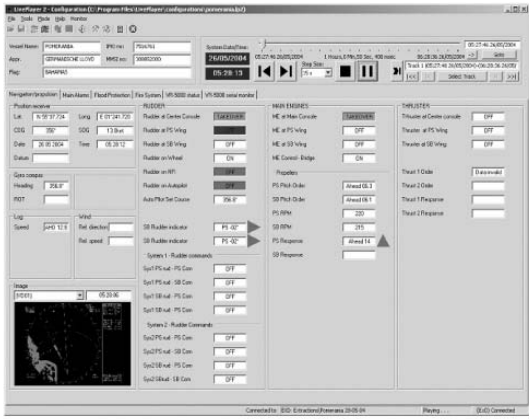
해양사고 발생 시 항해자료기록장치에 저장된 데이터에 대하여 물리적, 전자적으로 임의변경 및 삭제에 대한 보안 유지와 인터페이스를 통한 저장된 데이터를 다운로드하거나, 저장매체를 착탈하여 데이터를 추출하여 사본을 생성하는 과정은 매우 중요한 절차에 해당된다. 이러한 절차를 Saving Process라고 정의하는데, 최종 기록 매체에 저장된 정보의 복사본을 저장하는 절차를 의미하며, 저장된 정보는 권한이 없는 자의 정보 접근 또는 부주의한 관리로 인해 삭제되는 것으로부터 보호되어야 한다[15].

사고 발생 시점에 Saving Process가 제대로 진행되지 않은 채 시간이 흐르게 되면 항해자료기록장치에 아무런 조작을 하지 않아도 전원이 연결되어 있을 경우 운영체제가 저장매체에 있는 데이터를 변경한다. 12시간 이전의 데이터부터 순차적으로 덮어쓰기가 진행되고 항해데이터 캡슐은 메인컨트롤 장치의 데이터와 항상 동기화되므로 함께 데이터 변경이 진행된다. 항해데이터 캡슐의 저장매체 용량은 메인컨트롤 장치의 저장매체에 비해서 상당히 적은 용량이므로 데이터 덮어쓰기가 진행될 경우 복구가능성이 현저히 낮아진다.

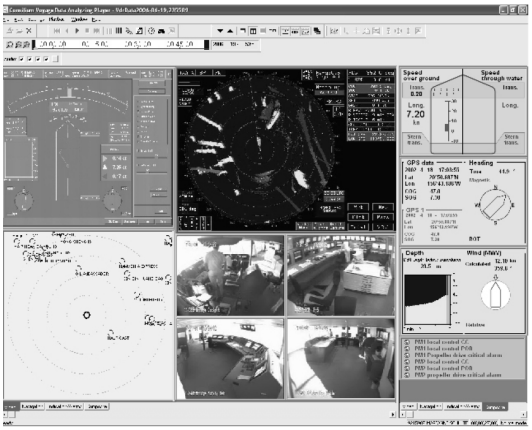
3.3.2 재연프로그램을 통한 재연

항해자료기록장치에 기록된 데이터는 재연프로그램(Playback Program) 또는 재생장비를 통해 사고 당시 상황을 재연하여 사고원인을 분석하는데 사용한다. 재생장비는 기록매체와 자료를 복구하기 위하여 사용되는 장비를 말하며, 원본자료인 장비에 적합하게 재생 또는 표현을 하는 하드웨어 및 소프트웨어를 포함할 수도 있다. [그림 5][그림 6]과 같이 항해자료기록장치에 기록되는 데이터의 형식과 재연프로그램은 제조사마다 다르므로 사고조사 재연을 위해서는 해당 항해자료기록장치의 제조사가 제공하는 재연프로그램의 준비가 필요하다. 데이터 보호 및 무결성 유지를

위하여 재연프로그램 실행 시 암호입력이 필요한 제품도 있다[16][17].



[그림 5] Furuno사 재연프로그램 화면 샘플



[그림 6] Consilium사 재연프로그램 화면 샘플

3.4 항해자료기록장치 관련 해양사고 사례

대부분의 해양사건 심판에 따른 재결서에는 항해자료기록장치의 데이터 보존여부와 분석결과가 기재되어 있을 정도로 항해자료기록장치의 데이터는 해양사고 조사에 영향을 미치는 중요한 정보이지만, 제대로 데이터가 저장되어 있지 않거나 의도적인 조작 또는 무단반출이 될 경우 사건해결에 어려움을 겪게 된다.

3.4.1 화물선 퍼시픽 캐리어호·컨테이너선 현대 컨피던스호 충돌사건

이 사고는 2011. 12. 14. 여수광양항 교통안전특정해역 남단부근에서 입항을 위해 북상 중이던 퍼시픽 캐리어호와 부산항을 향해 동진하던 현대컨피던스호가 서로 횡단하는 상태로 만나 충돌한 사건으로 양 선박의 항적과 상호 교신 내용 등이 국토해양부 선박모니터링 시스템, 여수 해상교통관제시스템 및 양 선박의 항해자료기록장치에 매우 자세히 녹화 및 녹음되어 있어 사고의 사실 확인과 원인 규명에 큰 도움이 되었다. 하지만 퍼시픽 캐리어호의 경우 항해자료기록장치에 보관된 자료 중 일부가 기준시간 12시간에 못 미치는 2시간 분량만 저장되어 현대 컨피던스호의 자료와 같이 사실 확인 등에 도움이 되지 못한 아쉬움이 있어 향후 선박검사기관에서는 선박검사 시에 항해자료기록장치 저장기능의 기계적 결함 등을 확인할 수 있도록 해야 한다는 교훈을 남긴 사건이었다[18].

3.4.2 삼성1호·유조선 허베이 스프리트호의 충돌로 인한 해양오염사건

2007년 12월 7일 인천에서 거제로 예인선 삼성 T-5호, 삼호 T-3호에 예인되어 가던 크레인 피예인부선 삼성1호가 강한 풍파에 밀려 태안 앞바다에서 정박 중이던 대형 유조선 허베이 스프리트호와 충돌함으로써 허베이 스프리트호에 실려있던 원유 약 12,547 kℓ가 바다로 유출되어 서해안 일대를 크게 오염시킨 우리나라 역사상 최악의 해양오염 사건이 발생하였다. 사고 당시 허베이 스피리트호는 항해자료기록장치를 설치하고 있었음에도 의도적으로 저장하지 아니하였고, 사고발생 후 자료저장 가능시간(12시간)이 훨씬 경과한 후에 보험회사 검정원이 이를 선외로 무단 반출함으로써 사고 당시의 증거자료를 확보할 수 없어 원인규명에 어려움이 많았다. 2008년 12월, 2심 재결이 날 때까지 만1년간 심판이 진행되었으며, A4 용지로 1만5천여 페이지에 달하는 방대한 심판기록만 봐도 이 사건이 얼마나 사회적으로 이슈가 되었고, 난해한 사건이었는지 알 수 있다. 이 사건은 2011년 3월에 최종 판결되었는데, 대법원에서는 삼성 측의 주장을 기각하고 중앙해양안전심판원의 재결을 확정함으로써 3년 4개월만에 사건이 종결되었다[19]. 업계에서는 당시 항해자료기록장치만 제때 회수했어도 사고 책임 여부에 대한 명확한 판정이 더욱 쉬워졌을 것이라는 견해가 지배적이다[20].

3.4.3 LPG운반선 오션US호의 어선충돌 사건

2013. 3. 4. 01:27경 2967톤급 부산선적 LPG운

반선 오션US호가 전남 진도 해상에서 조업 중이던 9.77톤급 어선 대광호에 충돌사고를 일으켜 전복시킨 뒤 달아나 선장과 선원 7명의 실종자가 발생하게 한 사건으로, 오션US호의 항해자료기록장치에서는 충돌 사고를 전후한 4시간 가량의 운항기록이 없어져서 사건 분석에 어려움이 있었다[21].

3.5 문제점과 고려사항

해양사고 직후에 항해자료기록장치를 확보하지 않으면 시간이 지나면서 충돌사고 전후 상황의 정보가 저절로 소실되게 된다. 항공기의 경우 이미 1960년대부터 블랙박스의 설치가 의무화되어, 25시간 이상 비행자료 기록이 가능한 비행자료기록장치(FDR)와 2시간 이상 조종실 내의 음성을 기록이 가능한 조종실 음성기록장치(CVR)의 설치를 법으로 정하고 있다[22][23][24].

선박의 경우는 최근에 들어서야 일정 규모 이상의 선박에 대해 항해자료기록장치 장착을 의무화 하였고 통상 12시간 정도의 보관만 하고 있다. 더욱이 운행하는 선박의 사고가 자주 있는 일이 아니므로 항해자료기록장치의 비상 시 작동법을 모든 항해사가 완벽하게 잘 숙지하고 있으리라 기대하기는 어려운 점이 있다. 또한 사고발생 이후 불리한 상황이거나 선박이 범죄에 사용되었을 경우 항해사가 고의적으로 항해자료기록장치의 데이터를 삭제하여 증거인멸 시도를 할 수가 있으며, 저장버튼을 누르지 않았을 경우 시간이 지나면 12시간 이전부터의 데이터가 저절로 지워지는 점을 악용하여 항해자료기록장치의 저장버튼을 고의적으로 누르지 않았음에도 사고발생 시 버튼을 눌렀으나 마치 오작동을 한 것처럼 변명하는 경우도 있다.

국제해사기구는 항해자료기록장치의 소유 및 자료회수에 관한 가이드라인을 통해 선박의 사고 발생 시 항해자료기록장치의 정보는 증거의 보전을 위해 사고 발생 후 최대한 빨리 회수되어야 하고, 선주는 선원들을 통해 이 증거가 적기에 보존될 수 있도록 조치할 책임을 져야 한다고 규정하고 있다[13]. 하지만 위 가이드라인에는 규정의 실효성을 확보하기 위해 필수적인 강제규정 및 위반자 제재에 관한 규정이 부족하여 시급한 개선이 필요하다. 국내의 경우 해양사고 조사업무 처리지침[25]에 따라 해양사고와 관련된 선박의 선장 또는 선박운항자 등이 항해자료기록장치 정보의 회수를 거부하거나 협조하지 아니한 경우 200만원 이하의 과태료를 부과하도록 하고 있다.

문서자료로는 선박의 선장이나 항해사가 기재하는 항해일지와 어선의 경우 조업일지(logbook) 등을 제출하지만 항해일지의 경우 일정한 시간마다 항해경로를 기재하는 것으로 사고 등의 어떠한 돌발 상황에는 제대로 기재하지 못하고, 조업일지의 경우 조업장소나 조업시간에 대한 기재는 선장이나 항해사의 감각에 의하는 경우가 많고 별도의 장부에 기재하거나 혹은 허위로 기재하는 경우가 많아 열람이 되더라도 분쟁의 해결을 위한 증거로서 의미를 상실하는 경우가 발생한다[2].

따라서 위와 같은 상황이 발생 시 진술과 문서자료 이외의 증거확보와 사실확인 및 조작여부 검사를 위해서는 디지털 포렌식 기법을 적용하여 저장매체에 존재하는 데이터 보존 및 무결성을 검증하고, 삭제된 데이터와 잔류정보의 복구 및 시스템 로그자료 분석 등의 조사가 반드시 필요하다.

IV. 디지털 포렌식을 활용한 해양사고 조사 절차

4.1 사고 발생 시 우선 조치사항

해양사고 발생 시 즉시 그 사실을 조사하고 증거를 수집하여 증거가 채택되도록 하기 위해서는 사고 발생 즉시 항해자료기록장치의 저장버튼을 누르고 데이터를 다운로드 받은 후, 그 데이터가 변경되거나 손상되지 않도록 잘 보전하는게 가장 우선이다. 데이터 다운로드가 완료되면 12시간 이전부터 사고 당시까지의 데이터 존재 여부를 확인한다. 하지만 이와 같은 작업은 디지털 포렌식 전문가가 아닌 항해사가 항해자료기록장치의 비상작동법 매뉴얼에 따라 진행할 수 밖에 없고, 선박의 환경과 여건에 따라 확인이 불가능한 경우가 있으니 상황에 따라 적절하게 판단하여 조치해야 한다.

제조사마다 차이가 있지만, 통상적으로 항해자료기록장치의 원격제어패널에 있는 다운로드 버튼을 5초 이상 누르고 있으면 부저가 울리기 시작하고 이 시점에 버튼을 한번 더 누르면 데이터의 다운로드가 진행되고 있다는 것이 메시지 창에 보이게 된다. 다운로드가 완료되면 경보장치가 부저를 울리며 완료 메시지를 표시하게 된다. [그림 7]은 조타실에서 전기기기실로 향하는 입구에 설치된 Rutter사 항해자료기록장치의 원격제어패널 사진이며, [그림 8]은 JRC사의 원격제어패널 사진이다.

〔그림 7〕 Rutter사 항해자료기록장치 원격제어패널 샘플 사진

〔그림 8〕 JRC사 항해자료기록장치 원격제어패널 샘플 사진

4.2 해양사고 조사 절차

해양사고 조사 시에 분석해야 할 항해자료기록장치의 기록은 디지털 증거의 모든 특성을 그대로 가지고 있어 표준화된 디지털 포렌식 조사 모델을 활용 가능하다. 국내에는 경찰과 검찰의 디지털 증거분석지침이 존재하고, 미국과 영국 등 해외에도 다양한 디지털 증거분석 모델이 존재하며 여러 학자들에 의해 연구되어 왔다. 디지털 포렌식 모델들의 전반적인 내용은 상당히 유사하고, 법적인 면과 기술적인 면을 모두 고려하고 있으나 각 국가와 기관의 환경에 따라 조금씩 차이를 보이고 있다. 주의할 점은 디지털 증거의 특성상 수집, 보존, 분석, 법정 제출에 이르는 일련의 처리과정에서 진정성과 무결성이 보장되었음을 증명하고 검증할 수 있는 절차로서 연계 보관성의 유지가 필요하다는 점이다〔26〕. 따라서 본 논문에서는 기존 모델들을 참조하여, 관련 법과 해양사고 환경을 고려하여 디지털 포렌식 절차를 제시한다.

4.2.1 조사 준비

조사관은 해양사고가 발생한 사실을 알게 되면 즉시 사실을 조사하고 증거를 수집하여야 한다. 이때, 선박에 설치된 항해자료기록장치의 제조사 및 모델명을 확인하여 장치의 규격과 특성을 파악하고, 기록된 데이터를 회수하기 위해 제조사로부터 해체용 특수공구 또는 인터페이스 장치를 확인한다. 항해자료기록장치는 선박의 여러 시스템과 복잡하게 연결이 되어 있고 분해가 까다로우니 가급적 현장 방문 전에 제조사에 요청하여 엔지니어의 협조가 필요하다. 키보드와 마우스는 항해자료기록장치의 설정과 유지보수 시에만 필요하므로 평소 메인컨트롤 장치에 연결되어 있지 않으니 현장 방문 전에 반드시 준비가 필요하다.

항해자료기록장치에는 통상적으로 사고 발생 직전에 원인규명에 필요한 데이터가 기록되어 있을 확률이 높으므로 비록 사고 발생 직후 Saving Process가 제대로 진행되지 않았더라도 이후 12시간 이내에 항해자료기록장치가 확보될 경우 사고조사에 큰 도움이 된다. 하지만 12시간이 지났더라도 사고 직전의 기록을 복구하거나 잔류정보를 검색해 낼 수 있는 확률을 높이기 위해서는 지체없이 항해자료기록장치를 확보하기 위해 서둘러 현장에 도착하여야 한다. 항해자료기록장치를 얼마나 빠른 시간 내에 확보하는가는 해양사고 조사의 성과를 결정짓는 매우 중요한 역할을 한다. 경우에 따라 현장 도착 전에 조사관의 허가를 받은 후 항해자료기록장치의 전원을 차단하거나 착탈식 하드디스크 분리를 위해 사고 선박 승무원의 협조를 고려할 필요도 있다.

4.2.2 현장 대응

부득이한 경우를 제외하고 조사관의 허가를 받지 아니하고는 누구든지 항해일지 등의 기록사항이나 선박 안의 기록의 파기 또는 변경과 선박의 손상된 선체기관 및 각종 계기와 그 밖의 부분에 대한 수리를 할 수 없도록 하고 있으므로, 조사관, 해양사고 관련자 또는 심판변론인의 참여하에 현장조사를 진행해야 한

다. 조사관, 참여인, 시간, 위치, 기기의 모델명, 기기의 훼손여부 등을 상세히 기록하고, 사진을 촬영한다. 제조사의 엔지니어와 항해사로부터 기록된 항해기록 데이터의 재생이 가능한 장비가 있는지 또는 재연프로그램이 설치되어 있는지 여부를 확인한다. 그리고 증거 수집 시의 표준시간과 항해자료기록장치의 시간차를 반드시 확인해야 한다. 또한 증거인멸 및 훼손방지를 위해 증거확보 및 수집이 완료될 때까지 현장을 잘 보존하고 사고조사와 관계없는 자가 접근하지 않도록 통제해야 한다.

4.2.3 디지털 증거 확보 및 수집

침몰된 선박의 경우 항해데이터 캡슐을 우선 수집하고, 그 외의 상황에는 메인컨트롤 장치의 저장매체와 항해데이터 캡슐을 동시 수집한다. 저장매체를 수집하면 원본 보존과 추후 분석을 위해서 증거분석용 이미징 작업을 진행해야 한다. 저장매체의 이미징 작업은 조사 과정에서 발생할 수 있는 원본데이터에 대한 손상을 방지하는 작업 과정으로 디지털 포렌식 수행 절차의 중요한 초기 단계이다.

이미징 작업은 크게 조사 대상 저장매체를 분리하여 조사용 시스템에 부착해서 이미지를 생성하는 경우와 조사 대상 시스템의 인터페이스에 직접 외부 저장매체를 연결하여 이미지를 생성하는 경우로 나누어 볼 수 있다. 하드디스크 드라이브 형태의 경우 메인컨트롤 장치에서 분리한 후 쓰기방지장치를 통해 조사용 시스템에서 이미징을 하면 된다. 저장매체가 메인컨트롤 장치의 기판에 임베디드 형태의 플래시메모리로 존재하는 경우에는 포렌식용 부팅 씨디롬을 이용하여 부팅 후 USB 등의 인터페이스를 통해 플래시메모리의 이미지를 추출하거나, 기판에서 메모리를 분리한 후 플래시 리더기를 통하여 메모리에 직접 접근해서 이미징하는 방식을 사용해야 한다.

저장매체 이미징 작업에 사용되는 장비 또는 소프트웨어는 원본 증거로부터 사본 또는 이미지 생성과 동시에 해쉬 값을 출력해 주므로, 무결성과 신뢰성 확보를 위해 증거수집 과정에 함께 기록해야 한다.

수집이 완료된 증거물은 정전기방지 봉투 등에 포장 후 심판에 사용될 때까지 위변조되지 않도록 봉인을 해서 잘 보존해야 한다.

4.2.4 증거 운반 및 확인

디지털 증거물은 쉽게 훼손되거나 변조될 수 있어 원본을 운반하는 것은 매우 중요한 일이다. 사고발생 이후 신속히 증거를 확보하는 과정에 사고현장에서 디지털 포렌식용 하드웨어나 소프트웨어의 준비가 어려워 원본을 그대로 운반하는 경우도 있고, 사본을 생성하였다 하더라도 원본은 물론 사본 증거물도 안전하게 심판원에 운반될 수 있도록 각별히 주의하여야 한다. 선박에서는 해양환경의 특성으로 높은 습도와 염분에 의해 저장매체의 전자회로가 쉽게 부식되거나 손상이 될 수 있고, 선박이 진동하거나 이동 중에 흔들릴 수 있으니 수집된 증거물에 충격방지 및 방수 등의 조치를 취하여 운반과정에서 증거물의 훼손이 없도록 주의해야 한다.

4.2.5 조사 및 분석

항해자료기록장치의 데이터에는 사건의 실마리나 결정적인 증거가 저장되어 있을 가능성이 있기 때문에 주의 깊게 살펴보아야 한다. 증거 조사를 할 때에는 비밀을 준수하고 관계인의 명예를 훼손하지 않도록 주의하여야 하므로 증거물 내에 존재하는 대화기록 등은 사고조사를 위한 목적으로만 사용되어야 한다.

조사 및 분석을 진행하기 위해 증거분석용 이미지를 분석용 소프트웨어로 마운트하여 파일시스템을 잘 인식하였는지 확인한다. 제조사에 따라 항해자료기록장치에서 사용되는 운영체제가 다양해서 사용되는 파일시스템도 여러 종류가 있다. 효과적으로 디지털 증거를 분석하기 위해서는 저장매체의 파일시스템 구조를 제대로 알아야 한다.

파일시스템이 인식되어 저장매체의 내용을 열람할 수 있게 되면 먼저 환경설정 파일을 찾아서 항해자료기록장치의 제조사, 모델명, 환경설정 파일의 최종 수정일자, 소프트웨어 버전, 네트워크 IP주소, 선박명 및 선주 회사명, 설치 업체정보, 국제해사기구 선박 아이디, 해상 이동업무 식별부호, 호출부호, GPS 안테나의 위치, 항해데이터 캡슐의 정보, 항해자료기록 파일의 저장경로 등의 일치여부를 확인한다.

사고발생 시 저장된 파일 및 폴더의 존재가 확인되면 재연프로그램을 이용하여 재생이 가능하다. 포렌식 소프트웨어에서는 모든 파일들을 시간순으로 순차정렬하여 내용을 열람할 수 있어 사고발생 시점에 생성된 파일들을 우선적으로 확인하는 것도 가능하다.

4.2.6 보고 및 증언

국내에서는 해양사고 사건을 심판하기 위하여 해양

수산부 소속으로 해양안전심판원을 두고 있으며, 조사관의 심판청구에 따라 공개된 심판정에서 심판을 시작한다. 사실의 인정은 심판기일에 조사한 증거에 의하여야 하고, 증거의 증명력은 심판관의 자유로운 판단에 따르도록 하고 있다. 조사관은 증인·감정인·통역인 또는 번역인을 출석하게 하거나 증언·감정·통역·번역을 하게 하는 일을 할 수 있다. 디지털 포렌식 전문가가 증인이나 감정인으로 심판에 참여하게 되면 대통령령으로 정하는 방법에 따라 선서를 하고 심판원의 신문에 따라 답변해야 한다. 이때 디지털 포렌식과 재연프로그램을 통한 재연과 증거물 분석에 따른 진술이 가능하다.

4.3 연관 데이터 비교 분석

해양사고가 발생한 경우 최대한 빠른 시간 내에 회수된 항해자료기록장치를 통하여 사고의 원인규명을 명확히 할 수 있지만, 해양사고는 여러 가지 복합적인 원인요소에 의해 발생하므로 한 가지 자료만을 무조건적으로 받아들여서는 안 된다. 경우에 따라 항해자료기록장치의 데이터가 제대로 확보되지 않을 수도 있어 연관된 데이터의 수집 및 분석과 비교가 반드시 필요하다. 어선에 설치된 어로용 기기 및 항해장비는 항해자료를 기록하는 기능보다는 어군탐지 및 기상관측 기능에 중점을 두고 있어 제공되는 자료로서는 부족함이 많다.

4.3.1 선박모니터링시스템(VMS)

선박모니터링시스템(Vessel Monitoring System)은 선박의 무선설비, 선박자동식별장치 등 단말기에서 발사된 위치정보가 기지국을 통해 수신되는 시스템으로 종전의 무선교신에 의한 위치보고가 자동으로 처리되고 어선 출입항신고 면제도 가능하다. 세계 어느 해역에서든 선박에 조난이 발생하면 구조요청신호를 자동으로 접수해 조난선박의 위치를 추적할 수 있다. 육지에서 100km 이내에 운행 중인 선박은 선박자동식별장치와 이동통신망을 사용하며, 100~300km 이내에서 운행 중인 선박은 단측파대(SSB)와 위성통신 사용, 300km를 넘는 원양해역을 운항중인 선박은 INMARSAT 위성 시스템을 이용하여 선박의 위치, 속도, 방향 등을 육상에서 감시 가능하며, INMARSAT-C 단말기의 폴링(Polling)과 데이터 보고 기능을 이용해서 선박으로부터 정보를 받아 육상에 있는 선박모니터링시스템의 지도상에 표시하게 된다. 폴링은 육상에서 선박으로 보내는 제어 명령이며, 이 명령을 받은 선박은 위치, 속도, 방향 등을 보고하게 된다.

우리나라 해양수산부에서는 해양안전종합정보시스템(GICOMS)을 구축하여 해양재난안전 관련 정보시스템(33개)을 연계·통합하고 국정원, 행안부, 해경, 해군 등 유관기관 간 시스템을 연계하고 있으며, 인터넷 해양안전종합정보시스템 포털사이트를 구축하여 웹VMS를 제공하고 있다. 2010년 4월 삼호드림호 해적피랍사고를 계기로 한국 국적 선박 이외에 제3국의 국적이지만 한국인이 실소유주이고 한국인이 선원으로 승선하는 선박에도 선박모니터링시스템 서비스를 확대하여 실시하고 있다[27].

4.3.2 해상교통관제시스템(VTS)

해상교통관제시스템(Vessel Traffic Service)은 해상 교통량의 폭주, 위험화물의 증가와 잠재적인 환경오염의 위험 등에서 항만의 안전 또는 항만운영 효율성을 제고하기 위해 실시하는 통항서비스 업무를 말한다. 항만 및 연안에서 운영되는 해상교통관제시스템에서는 선박에 설치된 선박자동식별장치(Automatic Identification System)의 정보를 수신하여 기록하고 있다. 선박자동식별장치의 정보는 선박의 충돌을 방지하기 위하여 자선의 침로, 속력, 위치 등의 정보를 타선에 제공하고 타선의 기본 항해정보를 실시간 검색할 수 있으며 이러한 정보를 바탕으로 해상교통관제시스템에서 효과적인 관제가 가능하다. 때문에 시계가 좋지 않아 주위의 선박을 인식할 수 없는 경우에도 타선의 정보수신이 가능하여 선박충돌방지, 광역 관제, 조난선박의 수색 및 구조 활동 등 선박의 안전관리를 더욱 효과적으로 수행할 수 있다[28].

선박자동식별장치 정보는 선박 내에 선박자동식별장치와 연결된 항해자료기록장치, 전자해도, 레이더, 선박 통합시스템에서 수집할 수도 있지만, 동시에 항만 및 연안의 해상교통관제시스템에서도 수집 가능하다. 이는 해양사고 발생 시 해상교통관제시스템 무선통신 업무일지, 관제사 녹취록, 해상교통관제시스템 레이더 자료, 사고선박의 선박자동식별장치 항적자료 등을 통해 가장 먼저 증거자료를 확보할 수 있고 사고 당시의 상황을 시뮬레이션하여 조사에 활용할 수 있는 장점이 있다.

선박자동식별장치에서 전송되는 정보 업데이트 간

격은 선박의 속력과 침로 변경시점에 따라 차이가 있다. 선박 통항이 많은 해역에서는 무선 채널 과부하가 발생하여 정보의 업데이트가 누락되거나 간헐적인 오류가 발생하여 잘못된 정보가 항해자에게 제공될 수 있다. 레이더 영상과 선박자동식별장치 정보가 중첩되어 표시될 때 레이더 영상은 전파의 반사파를 통하여 물표를 표시하지만 선박자동식별장치는 GPS 또는 DGPS의 선위정보를 나타낸 것이므로 이들 사이에는 오차가 발생할 수 있기 때문에 특히 교통량이 많은 해역에서는 주의가 요구된다. 그리고 선박자동식별장치가 레이더보다 정확한 선수방위 및 선속의 변화 등을 나타낼 수 있지만, 선박자동식별장치의 연산로직 및 메모리 오류 등의 내적 원인, 전파방해, 안테나의 파손 및 연결 불량 등의 외적 원인으로 인해 부정확한 정보를 표시하는 경우도 있다.

4.3.3 전자해도표시시스템(ECDIS)

전자해도표시시스템의 주된 기능은 안전항해를 기여하는데 있어 국제해사기구의 협약과 국내 선박설비기준에 따라 성능기준에 대한 요건을 충족해야 한다. 정부가 인증한 수로국에 의해 만들어지고 배포된 안전하고 효율적인 항해에 필요한 모든 해도정보를 표시할 수 있어야 한다. 전체 항해의 항적을 4시간이하의 간격으로 표시하여 기록할 수 있어야 하고, 12시간동안의 항적을 저장할 수 있는 용량을 가져야 하며, 기록된 자료는 조작하거나 변경할 수 없도록 하고 있다. 그리고 시간, 위치, 방향 및 속도 등의 선박의 항적 기록, 전자해도 제공처, 버전, 최신화 이력 등 공식자료의 기록 자료를 1분 간격으로 기록할 수 있도록 하고 있어 항해자료기록장치의 데이터와 상호비교가 가능하다[29].

4.3.4 영상정보처리기기(CCTV)

아직까지 모든 선박에 영상정보처리기기의 비치를 의무화하고 있지는 않지만, 로로여객선의 특수분류 구역이나 로로 화물구역에 대하여는 황천 시 차량의 이동 및 항해 중 승객의 무단출입을 관찰할 수 있도록 텔레비전 감시장치와 같은 효과적 수단에 의한 지속적 순찰이나 감시가 가능한 제한적 요건으로서의 영상정보처리기기의 비치를 의무화하고 있다.

천안함이 침몰된 이후 해저 45m 이하에 한달여간 침수되어 있던 천안함 함내 영상정보가 저장된 영상정보처리기기 컴퓨터 본체를 수거하여 분리한 하드디스크에서 사건 발생일인 2010년 3월 26일 21시부터 21시 30분까지 기록된 데이터를 복구하여 침몰 직전의 함내 상황을 확인한 사례는 대표적인 영상정보처리기기 데이터 활용 사례로 들 수 있다[30].

4.3.5 소형선박의 GPS플로터

어선과 같은 소형선박에서 운항을 목적으로 사용하는 GPS플로터는 제품에 따라 전자해도, 레이더, CCTV, 어탐기능, 메모리백업 등의 옵션기능을 갖추고 있다. 소형선박에는 항해자료기록장치가 설치되지 않아 항해자료가 별도로 기록되지 않지만, GPS플로터의 화면에는 소형선박의 운항경로와 항적자료 및 레이더에 의한 물표 등이 표시되고 일정시간 동안 메모리에 남아있어 사고조사 시 활용할 수 있다. 하지만 선박이 영해침범 등 부정한 목적으로 이용될 경우 선장이 고의적으로 GPS플로터의 전원을 꺼둔 채 선박을 운항하여 증거사용에 어려움을 겪는 경우도 있다.

4.3.6 채증장비 데이터

해경 및 어업관리단에서 불법조업 등의 위반사실에 대한 증거를 확보하는 용도로 많이 활용하는 채증장비로는 카메라, 개인휴대용 캠코더, 비디오선글라스, 헬멧카메라, 해경경비정의 ENG카메라 등이 있다. 채증장비로 수집된 증거는 영해침범 관련 해양사고 발생 시 선원들의 극렬한 저항 상황을 가장 확실하게 입증할 수 있으며, 당시의 선박의 운행위치와 충돌위치에 대한 정확한 증거로 제출될 수 있다. 또한 채증장비로 촬영된 동영상 등은 법규 위반 선원처벌을 위해 선박 소속 국가로 신병을 넘길 때 해당 국가 측에서 강력하게 요청하는 자료로, 2001년 9월 26일 일본 어업지도선의 과잉단속으로 인한 한국어선 삼진호 침몰사건과 같은 주변국과의 해상분쟁 시 중요한 증거자료로 사용되고 있다[31].

하지만 채증장비 사용 시 선원들과의 격렬한 몸싸움으로 채증장비가 바다에 빠지거나 시야가 어두운 야간시간에는 촬영이 제대로 되지 않는 경우가 있어 주의가 필요하다.

4.3.7 승무원이 사용한 모바일 기기

이동통신 사업자의 로밍서비스와 선박용 해상중계

기의 설치로 오늘날에는 육지에서 멀리 떨어진 해상에서도 휴대폰 사용이 가능하다. 최근 스마트폰, 테블릿 등 모바일 환경의 발달로 모바일 기기는 해양사고 등 유사시 통신용도로 사용가능할 뿐만 아니라 선박 운항과 관련된 업무용도에도 사용되고 있다. 사고 발생 직전 선장과 항해사가 사용한 모바일기기 사용 이력은 중요한 증거자료로 사용될 수 있다. 특히 침몰된 선박에서 발견된 모바일 기기에는 통화내역, 문자메세지 등의 전화 관련 기록과 사진, 동영상 등의 멀티미디어 파일, 위치정보, 소셜네트워크 서비스 사용정보 등이 모바일 기기에 내장된 메모리에 기록되어 있어 침몰 직전에 승무원들의 당시 상황이 어떠했는지 알려줄 수 있는 좋은 단서가 될 수 있다.

4.3.8 사고 인근 해역에 있는 선박의 데이터

선박은 충돌방지와 안전을 위해 타선의 선박자동식별장치 정보수신과 VHF 통신 등을 하고 있다. 이는 해양사고가 발생한 선박으로부터 해상교통관제시스템의 관제범위에 있지 않아 선박자동식별장치의 데이터 확보에 어려움이 있을 경우, 해양사고 발생장소 주변에 있는 선박에 설치된 항해자료기록장치, 전자해도표시시스템, GPS플로터 등의 데이터를 신속히 확보하면 사고 당시의 증거수집에 큰 도움이 될 수 있다. 해양경찰청에서는 주변 선박에서 카메라, 휴대폰 등으로 촬영한 선박명, 불법조업 선박이 그물을 올리는 장면, GPS플로터 상의 물표표시 등을 해양긴급신고전화번호 122를 통해 제보를 받아 불법조업 어선 등의 단속 및 검거 시 증거자료로 활용하고 있다[32].

4.4 디지털 증거 조사 기법

수집된 디지털 데이터를 통하여 사건의 증거를 찾을 수 있는 다양한 조사 기법 중에서 해양사고 조사에 반드시 필요한 기법을 기술하였다. 이에 따라 디지털 포렌식 기법을 종합적으로 적용한 해양사고 조사 절차를 [그림 10]과 같이 정리하였다.

4.4.1 데이터의 복구

항해자료기록장치는 어느 정도의 충격과 습도에 견딜 수 있도록 제작되어 있으나, 선박의 해양사고 특성상 충돌 시의 충격과 침몰 시의 침수로 인해 저장매체가 하드디스크인 경우 물리적인 손상이 발생할 수도 있다. 하드디스크 속도가 급격히 감소하거나 비정상적인 소음이 발생하는 등의 이상 증상이 나타날 경우 즉시 전원을 차단하고 충분한 설비를 갖춘 복구수리 전문업체에 의뢰하여 손상된 하드디스크로부터 데이터 추출작업을 진행해야 한다. 만일 하드디스크의 하드웨어적인 손상이 발생했을 때 무리하게 이미징 작업을 진행하는 경우 손상을 더욱 심화시켜 증거데이터가 소실될 위험이 매우 크기 때문이다.

항해자료기록장치에 기록되었던 파일이 어떤 요인에 의해 소프트웨어적으로 삭제되거나 훼손되었다면 디지털 포렌식 관점에서 삭제된 파일을 복구할 수 있다. 항해자료기록장치에 기록되는 파일명은 데이터의 종류 및 날짜와 시간과 관계가 있어 파일시스템 상에서 관련 플래그만 변경되었을 경우 파일을 복구한 후 삭제된 파일의 메타정보를 이용해서 복구한 파일의 시간 속성을 통해 정상파일과 함께 시간순으로 정렬도 가능하다.

4.4.2 저장매체의 비할당 클러스터에서 잔류정보 분석

비할당 클러스터(Unallocated Clusters) 영역에는 저장매체에서 포맷하기 이전의 데이터 또는 할당되었다가 삭제된 후 메타정보가 사라진 데이터가 남아 있을 수 있다. 비할당 클러스터들은 운영체제의 할당 알고리즘에 영향을 받기는 하지만 매우 오래전의 데이터가 남아 있는 경우가 종종 있으므로 포렌식 관점에서 상당히 의미있는 부분이다[33].

파일의 내용이 저장매체의 여러 부분에 단편화되어 있는 경우 파일 카빙기법을 적용해 하나의 파일로 구성할 수 있으며 파일의 시작부분에 위치하는 헤더(Header) 시그너처와 파일의 마지막에 존재하는 푸터(Footer) 시그너처에 파일의 고유한 특성이 있는 경우만 가능하다.

하드디스크의 비할당 클러스터에 존재하는 데이터를 분석하는 것은 삭제된 데이터를 조사할 수 있다는 점에서 의미가 있지만 비할당 클러스터에 존재하는 데이터는 응용프로그램으로 읽을 수 있는 완전한 파일의 형태가 아닌 단편화된 파편(Fragment)으로 존재하고 있어 오탐 가능성이 있다는 점은 유의할 필요가 있다.

4.4.3 키워드 검색

항해자료기록장치에 기록되는 자료의 형식을 고려

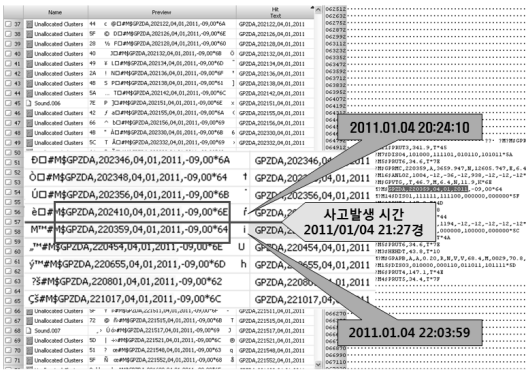
하여 사건과 관련된 키워드를 선정 후, 파일 또는 저장매체 전체를 대상으로 검색 가능하다. 예를 들면, 선박의 위치 및 속력 등의 정보를 나타내는 NMEA 0183 규격의 어플리케이션 계층에서 데이터를 전송하는 문장의 규약은 다음과 같다[10][11].

- '$'로 시작한다.
- 첫 두 자리는 제품의 종류를 나타낸다. GPS 제품일 경우 GP, 수심 측정 장비인 Depth Sounder 제품일 경우 SD 를 사용한다.
- 다음 세 자리는 해당 프로토콜이 가지고 있는 데이터의 종류를 나타낸다.
- 데이터의 구분은 ','로 한다.
- '*'로 끝난다.
- '$'와 '*'사이의 모든 데이터를 Exclusive OR 연산을 하여 체크섬을 만들어 추가한다.
- <CR><LF>를 붙인다.

사용되는 NMEA 0183 데이터에 대한 예시로 $GPZDA,201531,04,01,2011,-09,00*6F를 살펴보면, 여기에서 알 수 있는 것은 날짜와 시간 정보 및 현재지역 시간 기준 시차이다. 세계표준시 기준 2011년 1월 4일 20시 15분 31초를 나타내며, 현재지역시간으로는 2011년 1월 5일 05시 15분 31초이다. 6F는 데이터의 시작($)과 끝(*)을 나타내는 문자를 제외한 모든 문자를 8비트 문자로 XOR 연산 조합을 한 후, 각 4비트 자릿수에 대한 결과값을 아스키 값으로 나타낸 것이다.

$GPGLL의 경우 위도, 경도, 시간, 위성상태를 나타내며, $GPVTG의 경우 진행방향과 속도 정보를, $GPGGA는 시간, 경도, 위도, 시스템의 품질, 사용된 위성 수, 고도의 정보를 나타내는 등 이외에도 여러 가지 문장들이 존재한다.

저장매체에서 데이터가 삭제되었거나, 파일시스템이 훼손되었고 해양사고 발생시간에 기록된 파일이 존재하지 않거나, 삭제가 의심되는 경우 GPZDA 2#####,04,01,2011와 같은 키워드를 사용하여 검색을 하면 [그림 9]와 같이 세계표준시 기준 2011년 1월 4일 20:00~23:59사이에 생성된 $GPZDA 문장을 검색가능하며, 해당 키워드가 검색된 영역 주변 데이터에는 $GPGLL, $GPRMC 등 다른 NMEA 0183 정보가 존재하고 있어 해당 시간에 따른 선박의 위치 및 경로, 선수방향, 속도 등의 정보를 참조 가능하다. 키워드 검색 기능은 디지털 포렌식 소프트웨어



[그림 9] 키워드 검색에 따른 NMEA 0183 정보 샘플

에 따라 지원하는 기능과 문법의 차이가 조금씩 있으나 기본적인 원리만 이해하면 쉽게 활용이 가능하다.

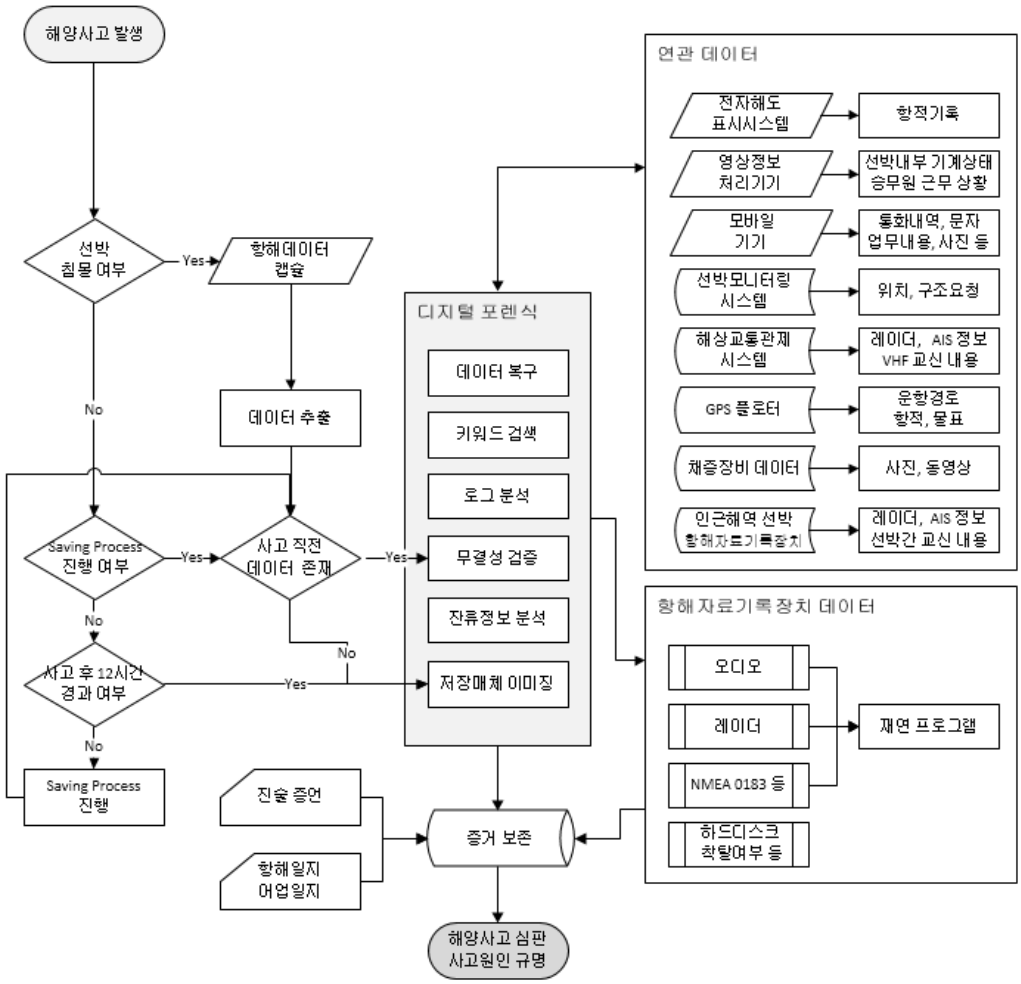
4.4.4 항해자료기록장치 로그 분석

Power On 로그 및 시스템 재부팅 로그, 다운로드 로그, 다운로드 드라이브 교체 로그, 항해자료기록장치 시스템 메시지 로그, 에러 로그, UPS 로그, 통신선로 에러로그 등의 확인이 가능하며, 이와 같은 로그 분석을 통해 사건이 발생한 시점에 시스템의 상황과 사고 발생 이후 항해자료기록장치에 어떤 조치를 취했는지와 에러내용 등의 정보를 확인할 수 있다. 이를 위해서는 운영체제에 따라 생성되는 시스템 로그와 항해자료기록장치 프로그램에 의해 생성되는 로그의 경로와 형식을 숙지할 필요가 있다.

V. 결론

해양사고 조사는 바다 한가운데에서 선박이 가라앉거나 뒤집혔을 때 사고 원인규명을 위한 증거를 찾아내기가 어렵다는 특징이 있다. 또한 사고 발생 시 불리한 상황이거나 선박이 범죄에 사용되었을 경우 고의적으로 항해자료기록장치의 데이터를 삭제하거나 Saving Process를 수행하지 않는 경우도 발생한다.

최근 안전대책의 일환으로 일정 규모 이상의 선박에는 항해자료기록장치나 선박자동식별장치 등의 항해장비 탑재를 의무화하고 있으며 해양사고의 원인규명 등에 영향을 미치는 중요자료로 사용되고 있다. 2010년 1월에 발효된 국제해사기구의 해양사고조사코드에서는 효율적인 해양사고 조사를 위하여 각 체약국에게 항해자료기록장치 분석능력을 구비할 것을 권고하고 있으나 아직까지 해양사고 조사와 관련 비행기



〔그림 10〕 디지털 포렌식 기법을 이용한 해양사고 조사 절차

의 블랙박스에 해당되는 항해자료기록장치의 데이터를 복구하거나 분석하여 증거를 확보하는 과학적인 방법론과 지침이 없는 실정이다.

이러한 현실에서 본 논문은 항해자료기록장치를 이용하여 객관적이고 과학적으로 해양사고 조사를 수행하기 위한 디지털 포렌식 절차와 기법을 제안하였다. 먼저 법적 증거로 활용이 가능하도록 연계보관성 등을 포함한 적법절차에 의한 증거수집에 대한 절차를 정의하였다. 그리고 해양사고 조사와 심판 시 증거로 활용이 가능한 항해자료기록장치의 주요 데이터 유형을 식별하고, 이러한 데이터의 수집, 복구 및 분석 방법들을 상세하게 기술하였다.

제안한 디지털 포렌식 절차와 기법을 해양사고 조사에 적용하면 해양사고의 원인규명 뿐만 아니라 사고 당시의 상황을 재현하여 현장감 있는 관계자 교육을 할 수 있다. 이 점은 유사사고의 재발방지 및 해양사고 예방에 큰 도움이 될 것이다. 또한 국내 관련 법규와 국제해사기구 해양사고조사 코드와 같은 국제기준을 준수하며 과학적이고 객관적인 해양사고 조사와 심판능력에 대해 국제적으로 신뢰받을 수 있다. 나아가 선도국가로서 국제적인 역량을 강화하고 위상을 증대시키며, 국내 어선들의 조업활동을 보호하여 국가주권을 수호하는데에도 이바지 할 것임을 기대한다.

참고문헌

〔1〕 김홍태, "해양사고조사코드와 인적과실의 원인규명, 하," 해양안전 2010년 봄호, pp. 25-45, 2010년 4월.

〔2〕 이규안, "공해상에서 Digital Forensic 연구," 한국컴퓨터정보학회 2007 하계학술발표논문집& 학회지, 15(1), pp. 209-217, 2007년 6월.

〔3〕 IMO, "International Convention for the Safety of Life at Sea(SOLAS)," Chapter V, Nov. 1974.

〔4〕 해양안전심판원 통계바다, http://www.kmst.go.kr/statistics/yearsStatisticsList.jsp

〔5〕 통계청 e-나라지표, http://www.index.go.kr/egams/stts/jsp/potal/stts/PO_STTS_IdxMain.jsp?idx_cd=1770

〔6〕 법제처, 해양사고의 조사 및 심판에 관한 법률(법률 제11690호), 2013년 3월 23일.

〔7〕 IMO, "Adoption of the Code of the International Standards and Recommended Practices for a Safety Investigation into a Marine Casualty or Marine Incident (Casualty Investigation Code)," Resolution MSC.255(84), pp. 7-8, May 2008.

〔8〕 IMO, "Adoption of the Code of the International Standards and Recommended Practices for a Safety Investigation into a Marine Casualty or Marine Incident (Casualty Investigation Code)," Resolution MSC.255(84), p. 3, May 2008.

〔9〕 국토해양부고시 제2012-075호, 선박설비기준 제108조의7(항해자료기록장치), 2012년 2월 21일.

〔10〕 The National Marine Electronics Association, http://www.nmea.org/content/nmea_standards/nmea_0183_v_410.asp

〔11〕 위키백과, NMEA 검색, http://ko.wikipedia.org/wiki/NMEA

〔12〕 IMO, "Performance Standards for Shipborne Voyage Data Recorders (VDRs)," Resolution A.861(20), Nov. 1997.

〔13〕 IMO, "Guidelines on Voyage Data Recorder (VDR) Ownership and Recovery," MSC/Circ.1024, May 2002.

〔14〕 한국선급, "국제해사기구 제47차 항해안전 소위원회 회의참가 보고서", pp. 17, 2001년 7월.

〔15〕 국토해양부, "국제해사기구 제55차 항해안전전문위원회 최종보고서", pp. 29-32, 2009년 8월.

〔16〕 FURUNO Electric co., ltd., Live Player Pro, http://www.furuno.com/en/business_product/merchant/product/vdr/live.html

〔17〕 Consilium AB, Voyage Data Recorders brochure, 2007, http://consilium.se/marine-safety/navigation/vdrs-vdr

〔18〕 부산지방해양안전심판원, "재결, 화물선 퍼시픽 캐리어호·컨테이너선 현대 컨피던스호 충돌사건," 부해심 제20128-015호, 2012년 3월 27일.

〔19〕 중앙해양안전심판원, "재결, 예인선 삼성T-5호·예인선삼호 T-3호의 피예인부선 삼성1호·유조선 허베이스피리트 충돌로 인한 해양오염사건," 중해심 제2008-26호, 2008년 12월 4일.

〔20〕 이비뉴스, "선박용 블랙박스, 성능 개선된다", 보도기사, 2008년 11월 10일, http://www.ebn.co.kr/news/n_view.html?id=355060

〔21〕 중앙일보, "어선 충돌 후 도주 항해사 구속…사고은폐 정황", 보도기사, 2013년 3월 7일, http://article.joinsmsn.com/news/article/article.asp?total_id=10875927

〔22〕 두산백과사전 두피디아, "비행기록장치", http://www.doopedia.co.kr/doopedia/master/master.do?_method=view&MAS_IDX=101013000751016

〔23〕 법제처, 항공법 시행규칙 제135조의2(사고예방장치 등), 2013년 3월 23일.

〔24〕 국토해양부고시 제2012-868호, 운항기술기준 7.1.17 비행기록장치, 2012년 12월 4일.

〔25〕 법제처, 해양사고 조사업무 처리지침 제2조(조사의 착수), 국토해양부지침, 2012년 3월 12일.

〔26〕 탁희성, 이상진, 디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안, 한국형사정책연구원, pp. 87-127, 2006년 12월.

〔27〕 해양수산부 해양안전종합정보시스템 포털사이트, http://www.gicoms.go.kr/about/about.do?page=01

〔28〕 해양수산부 해상교통관제센터, http://www.vtskorea.info/Service.do?id=intro01

〔29〕 국토해양부고시 제2012-075호, 선박설비기준 제93조(항해용해도 등), 2012년 2월 21일.
〔30〕 이명재, 데이터 복구 사례, 청원: (주)명정보기술, pp. 182-184, 2010년 7월.
〔31〕 헤럴드경제, "한·중 내년 EEZ내 조업 어선수 1600척 합의", 보도기사, 2012년 7월 31일, http://money.joinsmsn.com/news/article/article.asp?total_id=8914428&ctg=1103
〔32〕 해양경찰청 긴급출동 122, http://www.122.go.kr/Web_BlueGuard/BG_intro/intro_122.aspx
〔33〕 이상진, 디지털 포렌식 개론, 서울: 이룬, pp. 225-237, 2010년 8월.

〈저자소개〉

백 명 훈 (Myeong-Hun Baek) 정회원
해기사, 요트, 동력수상레저기구 1급조종
1998년 6월~2002년 12월: 수상안전지도자
2001년 2월: 경성대학교 경영정보학과 졸업
2002년 5월~2003년 12월: 경찰청 사이버테러대응센터 기법개발실 연구원
2004년 6월~2009년 8월: 경찰청 사이버테러대응센터, 부산지방경찰청 사이범죄수사관
2009년 9월~현재: 김·장 법률사무소 전문위원
2010년 2월: 고려대학교 정보보호대학원 수료
〈관심분야〉 정보보호, 경영정보, 해양사고 조사, 디지털 포렌식, 사이버범죄수사

이 상 진 (Sangjin Lee) 종신회원
1987년 2월: 고려대학교 수학과 학사 졸업
1989년 2월: 고려대학교 수학과 석사 졸업
1994년 8월: 고려대학교 수학과 박사 졸업
1989년 10월~1999년 2월 : ETRI 선임연구원 역임
1999년 3월~현재: 고려대학교 정보보호대학원 정교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수