해상 디지털 포렌식의 필요성에 대한 연구

이규안*

A Study on Maritime Digital Forensic with Necessity

Gyu-an Lee*

요 약

3면이 바다로 덮여있는 해양국가인 우리나라에서 해난 사고는 다양한 원인과 결과를 보여준다. 매년 600-700건씩 발생하는 해난 사고는 소형선박인 어선이 대부분을 차지하고 있으며, 연안에서 발생하는 선박과 조업하는 어선과의 충돌, 유조선의 침몰등으로 인한 인명손실과 대규모의 환경오염에 대한 책임, 실종선박에 대한 수색 등은 반복되는 해난 사고의 유형이다. 21세기가 시작되면서 대형화된 선박과 선원들의 감소로 인하여 디지털 선박이 등장하게 되었고, 선박에 설치된 장비들에 대하여 디지털 데이터가 저장되고, 저장된 데이터 속에서 필요한 정보를 추출하고 분석하는 해상 디지털 포렌식이 필요하게 되었다. 해난 사고에 대한 원인 규명과 책임, 손해 배상 등을 다투기 위한 증거를 수집하는 방안으로 해상 디지털 포렌식을 제안하며 이를 이용하여 디지털 증거를 수집하는 방안을 제시한다.

ABSTRACT

Marine accidents show various causes and effects in Korea where 3 sides of the country are surrounded by the ocean. Every year, 600 to 700 marine accidents occur mostly by small fishing boats. There are repeated accidents which involve crashes of coastal ships with fishing boats, which produce casualties and massive environmental hazard and the need for underwater search for shipwrecks. From the beginning of 21st century, the decrease of large ships with large number of crews led to the emergence of digitalvessels and the digital data storage of the installed equipments on the vessels, marine digital forensic - the extraction and analysis of the stored digital data within digital vessels - became necessary. This article is intended to suggest marine digital forensics as a solution of collecting evidence for discovering the causes, liabilities and compensations of marine accidents.

키워드

Marine Accident, Maritime Digital Forensic, Digital Ship, Digital Evidence

Ⅰ. 서 론

우리나라의 해역에서 운송되고 있는 해상 물동량은 계속 증가하고 있으며, 원거리 수역에서 조업을 하는 소형선박은 증가하고 있다. 그 원인으로 항공 운송이나 육상운송에 대한 운송비와 북한을 이용한 육상 운송의 제한 등의 원인으로 인하여 해상운송의 중요성과 물동량도 증가하고 있는 것이다. 또한 연안 해역의 어획량 남획과 중국 어선의 배타적 경제수역 침범 조업등도 소형선박의 원근해 조업과 항로상에서 조업을 하는 원인이 되고 있다. 상선의 경우 선원에 대한 선호도는 낮아짐으로 선원은 부족한 상태가 되었고 선

* 숭실대학교
1차 수정일자 : 2008. 11. 18
접수일자 : 2008. 09. 26
심사완료일자 : 2008. 12. 12

박은 대형화 되고 있다[1]. 이와 같은 악조건을 해결하기 위하여 디지털 선박이 등장하게 되었고, 디지털 선박에 대한 디지털 증거자료는 해난사고에 대한 중요한 증거자료가 된다. 하지만 우리나라는 디지털 선박에 대한 연구도 미비하고 무엇보다 선박에 장착된 디지털 장비의 표준화와 통합화에 대한 연구는 거의 전무하다 할 것이다. 3면이 바다로 둘러 쌓인 해양국가로서 우리나라는 선박의 항로에서 조업을 하거나, 출입항을 하는 항구 부근에서 조업이 이루어져 선박 상호간 충돌도 빈번한 가운데 있다. 이와같은 사고의 원인을 규명하고 잘못에 대한 손해배상을 청구하기 위하여 증거가 수집되어야 한다[1][2][3][4].

먼저 디지털 선박에 대한 디지털 증거를 분석하기 위한 해상 디지털 포렌식의 정의와 조건, 절차에 대하여 알아보고 우리나라 해상 디지털 포렌식의 도입에 대한 문제점과 해결 방안에 대하여 살펴본다. 본 논문을 통하여 해상 디지털 포렌식의 도입이 활성화되고 선박 상호간의 책임을 다룰 뿐만 아니라 국내외적으로 분쟁의 소지가 있는 해난사고의 원인과 사고에 대한 책임 소재를 구분할 수 있다.

II. 본 론

2.1 디지털 포렌식

디지털 포렌식은 디지털과 포렌식의 합성어로서 0과 1로 구성되어 필요한 정보를 소유하는 디지털과 '법정의' '변론의'의 의미를 가진 'forensic'의 합성어로서 디지털로 된 증거물들을 수집하고 분석하여 법정에 제출되는 모든 과정이라고 말할 수 있다[1]. 보통 수사기관에서 유비쿼터스 시대가 도래함에 따라 거의 모든 증거들이 디지털화 되었고 삭제되거나 은닉되어진 디지털 증거를 추출하고 분석하여 법정에 제출하는 것으로, 일반적인 컴퓨터의 하드디스크를 분석하는 디스크 포렌식, 네트워크 포렌식, 데이터베이스 포렌식, 모바일 포렌식으로 구분하기도 하고, 전원의 공급여부에 따라 데이터의 존재여부를 구분하여 휘발성 데이터 수집 포렌식과 비휘발성 데이터 수집 포렌식으로 구분하기도 한다.

2.2 해상 디지털 포렌식

선박에 설치된 기기들이 디지털화 됨에 따라 선박에 장착된 장비들을 분석하고 필요한 증거를 추출하여 형사상의 책임유무를 판단하고 민사상 손해배상을 결정할 수 있는 자료를 제공할 수 있다.

국내에서 선원에 대한 선호도 감소와 대형화되는 선박 기술에 따라 디지털 선박이 등장하게 되었고, 이러한 디지털 선박은 컴퓨터 등을 이용하여 선박통합시스템을 구성하게 되었고, 이러한 선박 통합시스템은 선박내 네트워크, 육상국과 교신을 위한 무선네트워크, 위성네트워크 등으로 구성된다[2].

선박에 장착된 장비를 분석하는 선박 디지털 포렌식과 육상의 기지국에 장착된 장비를 분석하는 육상 디지털 포렌식으로 구분할 수 있다.

선박 디지털 포렌식에서는 2001년 개정된 SOLAS 협약 제5장에 의해 모든 선박이 구비하여야 할 항해장비를 분석할 수 있어야 한다. 이러한 장비로는 위성항법장치(GPS), 선박자동식별장치(AIS), 항해자동기록기(VDR), 전자해도(ECDIS)가 있으며 일부 선박에서는 이러한 장비들을 중앙 컨트롤하거나 저장할 수 있도록 하여 선박용 블랙박스를 장착하기도 한다.

육상 디지털 포렌식 장비로는 선박모니터링 시스템(VMS), 선박자동식별시스템(AIS), 해상교통관제서비스(VTS), 해양안전종합정보시스템(GICOMS)등이 있다[3].

이러한 장비들은 디지털 장비들이라고 할 수 있으므로 디지털 데이터가 보존되고, 보존된 디지털 데이터들을 분석하면 수사의 증거나 민사상의 책임을 구분할 수 있다.

III. 해상 디지털 포렌식의 절차

3.1 해상 디지털 포렌식의 3요소

디지털 포렌식에서는 무결성과 진정성을 입증하기 위해서는 최소한 3가지를 갖추어야 한다.

이에 따라 대검찰청에서는 디지털 포렌식 전문가란 디지털 포렌식에 대하여 교육을 이수하고 실무를 쌓아야 하며 실무에 종사하는 동안 컴퓨터와 네트워크의 발전에 부응하기 위하여 일정기간 교육을 이수하

여야 한다고 규정하고 있으며, 디지털 포렌식 전문가 양성과정으로 이론 교육을 6개월, 실무교육을 4개월 동안 실시하고 있다.

또한 국제적으로 인증된 장비 및 프로그램을 이용하여 분석하여야 하므로 가디언스사의 EnCase외에도 국내 프로그램으로 파이널데이터(주)와 공동으로 연구 개발한 DEAS2 프로그램을 이용하고 있다. 이외에도 원본프로그램의 훼손이나 변경을 막기 위하여 FastBlock 등의 쓰기방지 장치를 사용하고 있다.

마지막으로 표준화된 절차나 규정을 요청하고 있으므로 경찰청에서는 디지털 포렌식 표준절차를 규정하고 있고, 검찰청에서는 디지털 증거 압수수색 및 분석 절차를 규정하고 있다.

이와같이 해상 디지털 포렌식에서도 추출된 데어터의 무결성과 진정성을 입증하기 위하여 별도의 디지털 포렌식 교육을 이수한 전문가를 양성하여야 하며, 인증된 프로그램과 표준화된 절차를 제정하여야 한다.

3.2 해상 디지털 포렌식의 절차

해상 디지털 포렌식은 육상에서 사용하는 디지털 포렌식과는 약간 상이점이 있다. 무엇보다 선박 항해라고 하는 이동성속에 네트워크가 구성되어 있으며,

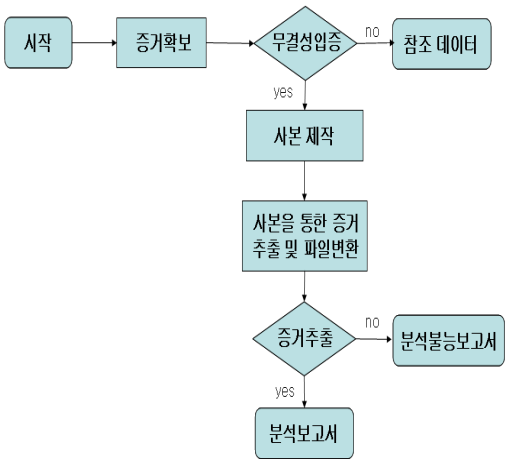

그림 1. 해상 디지털 포렌식의 절차
Fig. 1 Marine Digital Forensic Procedure

디지털 증거를 분석하는 기간동안 선박이 머무를 수 없다는 것이다. 그러므로 해상 디지털 포렌식에서는 원본 저장장치에서 분석하기 보다는 원본과 동일한 사본을 만들어 사본을 이용하여 선박의 데이터를 계속 저장할 수 있도록 하여야 하며, 이를 도식화 하면 그림1과 같다[4].

가) 증거확보

그림 2. 데이터 복구 프로그램
Fig. 2 Data Recovery Program

선박용 블랙박스 또는 개별 저장장치에 저장된 디지털 데이터를 통하여 필요한 자료를 추출하는 방법이다. 원본데이터는 보존하기 위하여 분석을 해서는 안된다. 원본과 동일한 사본을 복사하여 사용하여야 하며 원본과 사본이 동일하면 데이터가 변경되지 않았음을 입증하는 무결성 또한 디지털 포렌식 전문가의 책임이다. 선박의 특수성으로 인하여 운항을 계속하여야 하는 경우가 발생할 수 있으므로 사본을 2개 작성하여 사본 중 1개를 반환하여 운항에 지장이 없도록 조치하여야 하며, 남은 사본 1개를 이용하여 필요한 데이터를 추출하거나 삭제된 데이터를 복원하여야 한다. 현재 일반적으로 삭제된 데이터를 복구하는 프로그램으로 그림 2와 같이 국산제품으로 FinalData 사의 'FinalForensic'가 있으며, 국외제품으로 Guidance 사의 'EnCase'제품이 있다[5].

나) 증거입증

추출된 증거는 원본과 동일하다는 것을 입증하면서 위변조되지 않았음을 증명하여야 한다. 디지털 데이터의 특징으로 불가시적인 특성이 있으므로 이를 가시적으로 변환하여야 하는데 문서로 변환을 하여 출력

을 하던지, 화면으로 보여주는 것이라고 할지라도 원본 데이터와 동일하며 변환하는 과정에서 변하지 않았다는 것을 입증하여야 전문증거로서 증거능력이 있다고 할 것이다.

다) 증거분석

추출된 디지털 자료에서 필요한 정보를 추출, 처리, 판단하는 단계로서 분석용 도구를 이용하여 디지털 자료를 분석한다. 자료를 분석하는 단계에서는 검사대상의 자료가 분석되지 않도록 쓰기방지장치를 사용한다.

라) 증거제출

마지막 단계로서 추출된 증거가 목적에 맞도록 작성되는 것이다. 분석보고서를 작성하거나 시각적으로 볼 수 있도록 추출된 증거는 사용한 프로그램과 분석자, 분석일시, 분석시간 등 필요한 모든 내용을 기재한다. 증거제출 단계에서는 재판관이나 심사관들이 잘 이해할 수 있도록 6하원칙에 의하여 쉬운 용어를 사용하고, 필요한 모든 내용들이 표현될 수 있도록 상세한 기록을 하여야 한다. 무엇보다 개인적인 의견이 삽입되지 않고, 객관적으로 판단할 수 있는 내을 기재함으로 판단에 도움이 될 수 있도록 하여야 한다.

Ⅳ. 해상 디지털 포렌식의 문제점과 해결방안

4.1 해상 디지털 포렌식의 문제점

소형선박에 대한 디지털장비의 장차에 대한 의무규정이 존재하지 않는다. 소형선박에 장착된 VHF 장비가 있지만 원거리에서 통화는 불가능하고 무엇보다 아날로그식 음성통신을 위한 장비이므로 디지털 증거가 보존되지 않는다. 현재 일부 디지털 통신용으로 교체가 되고 있으나 소형선박을 운영하는 선주의 재정적인 여건과 유가인상, 어가 하락 등 여러 가지 원인으로 디지털 장비의 장착은 어려운 실정이다.

SOLAS 협약을 준수하는 중·대형 선박이라고 할지라도 장비을 운항중에 계속 운용하여야 함에도 불구하고 여러 가지 원인으로 디지털 매체에 저장하지 않고 있다.

2006년 5월 12일 오전 3시 5분경 중국 옌타이 남동쪽 38마일 해상에서 제주선적 3,800톤급 화물선 '골든로즈'호가 중국 국적의 진성호와 충돌하면서 한국 선원 7명을 포함하여 선원 16명이 숨지거나 실종되는 해난 사고가 발생하였다. 이때 진성호 선원들은 구조의무를 이행하지 않고 사고 현장을 이탈하여 한국민들의 공분을 샀다. 중국 선원들은 짙은 안개로 인하여 육안으로 골든 로즈호를 발견할 수 없었고, 충돌 후 초단파 무선 전화로 호출을 하였으나 아무런 응답이 없어 골든로즈호가 충돌 후 도주한 것으로 판단, 항해를 계속하였다고 하였으나 선박이 충돌을 한 경우에는 즉시 자국 또는 자회사에 연락을 취하고 조치를 취하여야 함에도 불구하고 상당한 시간동안 사고현장을 이탈한 후에 중국에 입항한 것은 사고후 침몰사실을 알았음에도 불구하고 사고사실을 은폐하기 위한 것으로 추정되나 국적이 중국이었고, 우리나라에서는 조사관을 파견하여 선박자동식별장치(AIS)를 분석하였다고만 나와 있을 뿐 다른 디지털 데이터는 분석하였다는 기록은 없다. 이러한 사항은 해상 디지털 포렌식을 이용하여 선박에 장착된 모든 디지털 장비에 대한 디지털 증거의 추출과 분석을 시도함으로 진성호의 사고에 대한 책임과 구조에 대한 회피 사항을 파악하여 국제재판에 제출할 수 있어야 할 것이다.

2007년 12월 7일 충남 태안군 만리포 북서방 약 5마일 해상에서 원유 운반선 Hebei Spint 호와 크레인 부선 삼성 1호가 충돌하여 원유 12,547 kl이 유출되는 사상 초유의 해양 오염사태가 발생했다[6].

선박 상호간에 교신을 시도하여 사고를 미연에 방지하고자 하는 노력을 시도 하였다고 하지만 당시 통신을 시도하였던 흔적과 내역 등의 디지털 증거가 존재하지 않아 재판 도중 잘못에 대한 책임공방이 진행되고 있다.

위와 같은 사고 당일에도 Hebei Spint 호에서는 육상 기지국과 수차례 통화를 시도하였고, 실제 통화가 있었음에도 불구하도 어떤 내용이 언제 통화되었으며, 사고 후의 대처에 대한 진행 과정도 근거가 남아 있지 않았다는 것은 선박과 육상국간 통신 내역조회 뿐만 아니라 내용을 보존하여야 함에도 디지털 증거의 보존과 분석에 대한 문제점이 존재한다.

4.2 해상 디지털 포렌식의 문제점 해결방안

소형선박을 위한 문자,영상이 전송가능한 어선용 단말기 개발과 저렴한 가격으로 보급을 하여야 한다. 또 우리나라의 통신 인프라라고 할 수 있는 휴대폰은 거의 모든 국민들이 보유하고 있으므로 해상용 위치 추적 프로그램을 개발하여 소형선박 입출항시 신고토록 하여 소형선박의 이동경로와 해난 사고에 대비하여야 한다.

중·대형 선박을 위해서는 선박용 블랙박스가 장착된 선박의 경우 운행 중인 경우뿐만 아니라 항구에 입항 후에도 일정기간동안 선박용 블랙박스에 데이터를 저장할 수 있도록 저장기간을 지정하고 임의로 데이터 전송을 중단하거나 삭제할 수 없도록 법적 조치를 취하여야 한다. SOLAS 협약의 운영부분을 강화하여 국내외의 모든 항구를 입·출항하는 선박은 일정기간동안 데이터 보존을 의무화 하여야 하며 임의로 데이터를 변경할 수 없도록 하여야 한다. 저장된 데이터는 변조가 불가능하도록 일방향성으로 저장하여야 하며 선박에 장착된 모든 데이터는 별도로 저장 또는 통합 저장할 수 있도록 하여야 한다.

육상에 장착된 장비들은 통합 저장 공간으로 스토리지를 사용하여 일정기간동안 선박의 운항경로나 통화내역을 저장하여야 한다. 특히 우리나라의 경우 협소한 항구와 조업중인 선박과 운항중인 선박의 충돌사고가 빈번함에 따라 선박 모니터링 시스템과 해양안전 종합정보시스템의 디지털 데이터는 최소한 6개월이상 보존함으로 선박의 안전과 해난사고에 대한 책임을 구분할 수 있는 근거를 마련해야 한다. 무엇보다 선박과 육상 기지국간에 정보의 송·수신 시간과 내역등 디지털 정보를 저장할 수 있는 법적근거를 마련하여야 하고, 백업데이터는 분석이 용이하도록 국제적인 규격을 이용하거나 국내에서 개발하여 추가 장착을 하여야 한다.

백업받거나 삭제된 데이터를 복원한 디지털증거라고 할지라도 국제항해에 종사하는 선박의 경우 자국의 디지털 장비에 맞추어진 프로그램과 저장 포멧을 사용하기 때문에 증거로 제출되는 것은 한계가 있다.

항공기용 블랙박스와 같이 공통된 규격을 사용하여 음성이나 기타 선박의 데이터를 저장하고, 복구할 수 있는 국제적인 공조체계가 이루어져야 한다.

Ⅴ. 결 론

해상 디지털 포렌식이 필요한 시점에 와 있다. 이는 선박의 대형화와 디지털 선박의 등장으로 디지털 자료가 존재하고 이를 분석하기 위한 해상 디지털 포렌식이 각종 해난 사고의 원인 분석과 책임 공방을 구분할 수 있는 디지털 증거가 존재한다는 말이 된다. 하지만 수사기관에서도 관련 산학기관에서도 어떠한 시도나 연구가 진행되지 않고 있다. 해상국가로서 우리나라 해역을 통과하는 선박의 수는 더욱 많아지고 대형화 되고 있으며, 연안 수사자원의 고갈로 원거리까지 조업을 나가는 소형 선박이 증가하는 시점에서 해난 사고는 증가하고 있다. 이에 대한 대비도 중요하지만, 원인과 책임을 묻는 증거도 매우 중요하다. 과거에서와 같이 심증만 가지고 수사를 하거나 책임을 물을 수는 없다. 유비쿼터스 시대에 맞는 수사관행과 민사적인 보상을 위하여 해상 디지털 포렌식이 필요하고, 국제적으로 규격화된 디지털 데이터에 대한 포맷과 규정이 필요하다. 이를 위하여 수사기관은 물론 관계기관의 지속적인 요청과 산학의 연구가 필요하다. 차후 추출된 정보를 시각화 하기 위한 국제적인 표준이 필요하고, 선박이 침몰하거나 파손되었을 경우에도 디지털 자료가 보존될 수 있도록 항공용 블랙박스처럼 안전하게 보존하고 분석될 수 있도록 저장할 수 있는 장비가 개발되어야 할 것이다. 이를 통하여 선박에서 일어날 수 있는 해난사고를 좀 더 정확하고 객관적으로 분석할 수 있는 해상 디지털 증거 분석기관의 설립과 학계의 지속적인 연구가 진행 되어야 한다.

참고 문헌

[1] 김현선, “미국의 디지털증거 활용실태”, 해외연수검사연구논문집,Vol. 1, pp.138, 2006.
[2] 김재양, “디지털 선박을 위한선박 통합화 시스템 플랫폼 설계 및 구현”, 숭실대학교 박사 논문, 2005.
[3] 이규안, 박대우, 신용태, “분쟛소지가 있는 공해상에서 디지털 포렌식을 이용한 해결방안”, 한국컴퓨터정보학회, Vol. 12, No. 3, pp.138-143, 2007.

[4] 조의주, 김천석, “해양교통 사고 예방 및 어업 정보화를 위한 디지털 통신 시스템 발전에 관한 연구”,한국전자통신학회, Vol. 3, No. 3, pp.193-197, 2008.
[5] www.guidence.com
[6] 신현식, “우리나라의 해상통신의 발전방향에 관한 연구”, 한국전자통신학회, Vol. 3, No. 3, pp.151-160, 2008.

저자 소개

이규안(Gyu-an Lee)

2006년 숭실대학교 정보과학대학원 정보통신학과 졸업 (공학석사)
2008년 숭실대학교 컴퓨터학과 수료 (박사과정)
2000년 벽성대학 정보통신과 겸임교수
2002년 대검찰청 중앙수사부 컴퓨터수사과근무
2005년 대검찰청 과학수사2담당관실 근무
2007년 대검찰청 디지털수사담당관실 근무
2008년 춘천지검 영월지청 컴퓨터범죄수사반 근무
※ 관심분야 : 유비쿼터스 보안, 디지털 포렌식, 해상 디지털 포렌식, 이동통신 보안