

분쟁소지가 있는 공해상에서 Digital Forensic을 이용한 해결 방안

이규안*, 박대우**, 신용태***

Resolution of Complication in Territorial Sea by Using Digital Forensic

Gyu-an Lee *, Dea-Woo Park **, Youg-tae Shin ***

요 약

대한민국은 중국·일본과 같이 바다로 인접하여, 항해를 하거나 조업을 위한 배타적 경제수역(EEZ: Exclusive Economic Zone) 때문에 분쟁의 소지를 담고 있다. 특히 해상 사고에서 어선의 경우 조업일지와 항해장비의 부실 등으로 국가 간 분쟁 시 증거자료 채택할 수 있는 경우는 드물다. 해상에서 컴퓨터 등의 디지털 증거는 무결성이 훼손된다면 결정적인 증거가 재판정에서 기각당하거나 국제적으로 분쟁 시 증거로 채택되지 않는다. 본 논문에서는 이 문제점을 해결하는 방안으로 해상 디지털 포렌식을 제안하면서, 공해상 선박에서 디지털 포렌식 자료를 위한 주요내용, 요구사항, 적용사항 및 선박 디스크, 선박 네트워크, 선박 무선 포렌식 자료를 추출하고 이를 입증하는 방법을 제시한다. 그리고 실제 공해상에서 해상 디지털 포렌식의 사례에 관한 실증연구를 하여, 분쟁소지가 많은 선박에서 과학수사의 일환으로 활용될 것이며, 디지털 포렌식의 증거가 채택되는 국제 간의 공해상 분쟁해결의 중요한 열쇠가 될 것이다.

Abstract

Korea's seas have the potentials of dispute against China or Japan due to the overlap of the territorial waters and EEZ. In case of marine accidents, the nature of the sea tends to eliminate much of the track, making it another hardship in evidence adoption in case of an international dispute along with the false entries of fishing vessels' journals. Marine Digital Forensics protects the functions of computers and IT appliance on vessels and extracts evidence of voyage and accidents to resolve international dispute. The digital evidence, if tampered with its integrity, may lead to the rejection to a critical claim or may even fail to make a case. As a solution, this thesis suggests Marine Digital Forensics as a way to extract evidence and prove a claim. This may be utilized as means of scientific investigation on sea as overseas exchange increases and the vessels digitalize, leading to a solution in international disputes that may occur in the future.

▶ Keyword : Digital Computer Forensics, Digital Evidence, Marine Digital Forensic

• 제1저자 : 이규안

• 접수일 : 2007.5.31, 심사일 : 2007.6.25, 심사완료일 : 2007. 7.20.

*숭실대학교 대학원 컴퓨터학과

**호서대학교 벤처전문대학원

*숭실대학교 컴퓨터학부

1. 서론

대한민국은 3면이 바다로 둘러싸여 있는 한반도라는 지리적 여건으로 구성되어 있다. 이는 주변 국가들의 해양학적 관점에서 보면 일본열도와 중국대륙에 둘러싸여진 반폐쇄된 해역에서 타국으로 항해를 하거나 혹은 조업을 하는 경우에 모두 주변 연안국들 간 해역이 중복되는 관계라고 할 수 있다. 이때 조업하는 선박이 배타적 경제 수역을 넘어 조업을 하다가 적발되어 국가 간 문제가 발생하거나, 항해 하는 선박이 유류를 전달하기 위한 항해라고 할지라도 어획물을 선적하고 있다면 불법 어획물에 대한 압수라는 명목으로 나포할 수 있으며, 어선이 조업수역에서 조업을 마치고 귀항도중 배타적 경제수역(EEZ)을 통과하는 경우 불법조업으로 나포하는 경우가 있다[1].

표 1. 한국 어선의 일본 영해 침범 및 벌금 실태
Table. 1 Violation & Penalty of Korean Fishing Ships against Japanese territorial Waters & EEZ

연도	경해침범조업	배타적 경제 수역 침범 조업	비고
2004년	·	19척	1억9천만원 담보
2005년	1척	14척	2억8천만원 담보
2006년	·	10척	1억1백만원 담보
2007년	4척	·	계류중
계	5척	43척	·

이러한 경우 일반적으로 항해하는 선박에서는 항해일지를 제출하거나 관련 장부들을 제출하게 되고, 어선인 경우에는 조업일지 등을 제출하여 해당 선박이 배타적 경제수역을 항해하거나 혹은 조업을 완료하고 귀항 또는 귀국중임을 증명하지만 항해일지의 경우 일정한 시간마다 항해경로를 기재하는 것으로 나포 혹은 어떠한 돌발 상황에 대한 데이터는 존재하지 않으므로 정보의 증거력은 약하다고 할 것이며, 조업일지의 경우 조업장소와 조업시간에 대한 기재는 선장이나 항해사의 감각에 의하는 경우가 많고 별도의 장부에 기재하거나 혹은 허위로 기재를 하고 열람이 되더라도 분쟁의 해결을 위한 증거로서 의미를 상실하는 경우가 발생한다[2].

특히 어선의 경우 기본적인 항해 장비를 제외한 어로 장비는 데이터를 보존하는 장치보다는 어획상황을 판독하거나 기상에 관련한 사항을 검사하는 기능에 중점을 두고 있는 관계로 막상 국가 간 분쟁이 발생하였을 경우 제공되는 자료로서는 부족함이 많다.

현재 선박은 SOLAS(해상인명안전협약: International Convention for the Safety of Life at Sea 1974)규정에 따라 일정한 수준이상의 선박에 대하여 안전항해에 관한 규정 장비의 장착을 의무화 하고 있으며, 이는 디지털저장장치에 운항거리와 운항관련 자료를 저장하게 됨으로써 이러한 분쟁에 대한 자료를 제출할 수 있다.

이때 제출되는 디지털자료는 임의적으로 훼손되거나 변조 되는 것을 방지하여야 하는바, 이를 데이터의 무결성 이라고 하고, 디지털 자료의 추출에서부터 필요에 의하여 제출하는 과정을 해상 디지털 포렌식 이라고 한다.

본 논문에서는 SOLAS에서 규정한 장비에 대한 설명과 함께 디지털 자료를 저장하는 방식을 살펴보고, 이러한 디지털 자료를 디지털 포렌식을 이용하여 추출하고 무결성을 입증하는 방법과 함께 분쟁에 대비하는 방안을 제시 한다.

본 논문의 연구를 통해 공해상에서 발생할 수 있는 국가 간 분쟁에 대처하고, 아울러 디지털 포렌식을 통한 디지털 증거의 무결성을 입증함으로써 해상 범죄에 대한 명확한 증거를 확보하고, 해상 범죄의 증거자료의 공정성을 유지하여 디지털시대에 발맞춰가는 해상 범죄 및 재판에 대한 컴퓨터 기술을 확보하고자 한다.

II. 선박용 디지털 장비

SOLAS협약에 의하여 선박에 장착이 의무화된 장비들은 모두 디지털 장비라고 해도 과언이 아니다. 디지털화된 항해자동화 장비에 대한 개요와 데이터의 전달체계 및 디지털 자료를 추출하여 증거의 무결성을 보장하는 연계방안을 제시하기 위하여 선박항해장비와 해상교통안전용 디지털장비는 어떤 것이 있는지 검토해보고, 해상 디지털 포렌식의 정의·유형·절차에 관하여 살펴본다.

2.1. 선박 항해 장비

2001년 2월에 개정된 SOLAS 협약 제5장에 의해 모든 선박에 구비하여야 할 항해장비는 전세기위성항법장치(GPS: Global Positioning System), 선박자동식별장치(AIS: Automatic Identification System), 항해자동기록기(VDR: Voyage Data Recorder), 전자해도(ECDIS: Electronic Chart Display and Information System) 등이 있으며, 선박회사에서는 선박용 블랙박스, 선박 항해 제어 시스템 등으로 단일 제품화하여 과거 종이 해도 상에서 수행하던 모든 업무들을 자동화, 디지털화 하고 있다[3].

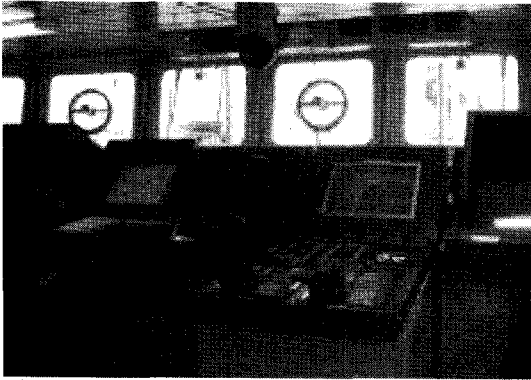


그림 1 선박의 브릿지
Fig. 1. Bridge of Vessel

가) 전 세계 위성항법장치(GPS)

현재 대부분의 선박에는 위성항법장치가 설치되어 있다. 그러나 이러한 장비는 현재까지 강제화 된 설비는 아니며 선주가 자기 선박의 안전을 위하여 자발적으로 설치하여왔다. 하지만 SOLAS 협약 본문에 강제되었다.

나) 선박자동식별장치(AIS)

본래 항공용으로 개발된 것으로 1993년도 영국연안에서 유조선의 좌초사건을 계기로 도입이 논의되기 시작하였고, 이는 선박의 충돌방지 및 관제를 목적으로 선박명세, 타입, 위치, 항로, 선속 및 기타 항행안전정보의 송수신이 가능하도록 되어있다.

다) 항해자동기록기(VDR)

비행기의 블랙박스에 해당하는 것으로 선박의 운행 중 각종 데이터의 실시간 기록의 유지 및 관리를 하는 장치다. 항해데이터, 엔진의 상태, 운항정보, 기상정보 등을 신호변환장치가 인식할 수 있도록 디지털 신호로 변환하여 메인 시스템에 전송하고 자료를 원하는 형태로 출력할 수 있도록 구성된다. 이는 사고를 예방하는 차원이 아니고 사고 후 다른 선박에 대한 교훈을 삼으려는 기기이므로 유럽과 미국에서는 여객선 및 3,000톤 이상의 모든 선박에 설치하지는 의견과 일본을 위시한 국가들은 모든 선박을 대상으로 하지 않고 여객선을 탑재대상으로 하자는 의견이 팽배하다가 중재안을 채택하였다.

라) 전자 해도(ECDIS)

전자해도 시스템은 선박의 항해와 관련된 정보, 즉 해도 정보, 위치정보, 선박의 침로, 속력, 측심자료 등을 종합하여 컴퓨터 스크린에 도시하는 시스템으로서 자선의 위치확인, 최적항로 선정, 좌초 및 충돌예방조치를 신속하

고 안전하게 수행하는 것을 보조하는 것이다(4)(5).

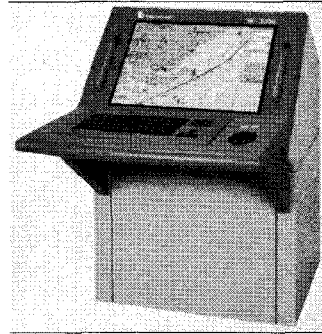


그림 2 전자해도장치
Fig. 2. Electronic Chart Display and information System

2.2. 해상 교통안전용 디지털 장비

가) 선박모니터링시스템(VMS: Vessel Monitoring System)

선박위치 및 항적추적, 안전보안감시를 위한 장비로서 SOLAS 협약에 의하여 연근해 및 원영해역에 항행하는 선박에 장착하는 장비다. 이러한 모니터링시스템의 활용을 위하여 육상에서는 모니터링 장치로서 전자해도가 필요하고, 선박에는 AIS, SSB, 위성 송수신 장치 등이 필요하지만 이는 SOLAS 협약에 의하여 선박에 탑재가 강제된 기기로서 추가로 장착을 요구하지는 않는다. 현재 해양수산부 해양안전종합포털서비스로 Web VMS가 구축되어 활용중이다(6).

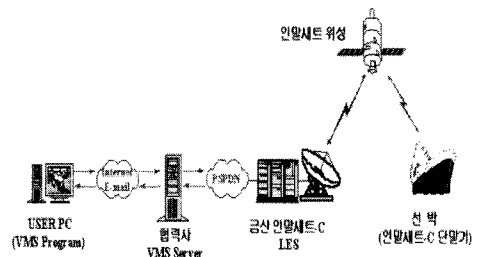


그림 3. VMC 통신망
Fig. 3. VMS Network

나) 선박자동식별시스템(AIS: Automatic Identification System) 항만 내 혹은 연안 해역으로 육지에서 약50해리를 반경으로 선박통항관계 및 항적추적을 위한 장비로서 현재 AIS기지국이 전국적으로 22개소가 개설되었고, 선박에는 AIS단말기 장착을 의무화한다. 이는 국제 항해 선박은 2004. 12. 31까지, 국내 항해선박으로 여객선은 2005. 12. 31까지, 150톤 이상 예선과 유조선은 2007. 7.1까지 장착을 의무화 한다. 관제는 VTS 센터에서 병행하도록 하였으며 전국 통합망이 구축되어 운영 중에 있다.

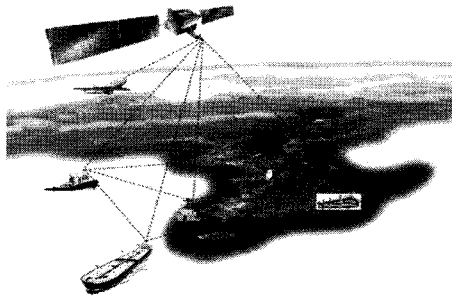


그림 4. AIS 통신망
Fig. 4. AIS Network

다) 선박통항관제서비스(연안VTS: Vessel Traffic Service) 연안 해역 선박의 통항을 관제하기 위한 시스템으로 항적추적을 목적으로 하고 있다. 해상교통 밀집해역에 대한 선박의 운행을 통제함으로써 안전 운항을 지원한다. 선박에는 VHF 무선전화를 장착하여야 하고, 육상에는 Radar 기지국과 CCTV, VHF 무선전화를 비치하여 선박의 운행과정을 추적하며, 비상시 혹은 수시로 연락을 주고받는다. 현재 진도, 외나라도, 육지도에 설치하여 연안해역의 항행추적을 실시하면서 문제점을 파악하고 차후 여수 마산권으로 확대추진 할 예정이다.

라) 해상교통관제서비스(VTS: Vessel Traffic Service) 개항 질서법에 의하여 항만 내 선박의 입출항관계 및 항적추적을 위하여 지원되는 시스템으로 선박에는 VHF 무선전화를 장착하여야 하고, 육상 관제센터는 RADAR, CCTV, VHF 무선전화를 장착하여야 한다. 현재 부산, 인천, 마산, 울산 등 14개소에 대한 지원을 하고 있고, 부산신항에도 시스템을 구축하여 지원하고 있다.

이러한 항해장비속에 저장된 디지털자료들은 법적다툼에서 중요한 자료가 될 수 있는데, SOLAS 협약 제5장 제 28조 규칙에 의하면 국제 항해에 종사하는 모든 선박은 항해안전에 영향을 미치는 주요사건은 모두 기록을 남기

도록 하는 내용의 규정을 삽입하였으며, 기재하여야 하는 구체적인 내용들은 현재 항해안전소위원회에서 지침작업을 진행하였다[7][8].

마) 해양안전종합정보시스템(GICOMS: General Information Center on Maritime Safety & Security)

해양수산부는 정보기술을 활용하여 국가적으로 해난안전 종합관리체계를 구축하므로 선박모니터링을 통한 소형선박과 어선 등에 대한 긴급 조난 등에 대비하고 인명을 구조하기 위한 일환으로 선박모니터링 시스템 등을 구비한 해양안전종합서비스를 2006. 1월부터 시작하였다. 이는 기존의 선박모니터링 시스템을 기반으로 분산된 해양안전 관련 정보시스템을 연계·통합함으로써 선박 조난 등 재해에 대비하는 예방적 차원과 안전·재난관련 정보를 수집하고 공개하므로 사후 처리를 지원하는 정보시스템이다. 아울러 해양안전종합정보시스템은 기관·부서별로 분산되어 신속한 정보수집과 확산의 어려움 등을 해결하고자 행정자치부, 국가정보원등과 연계하여 선박등록, 검사, 무선국, 사업자, 선원정보 등 선박관련 정보를 일괄 조회할 수 있도록 지원하는 정보 기술의 활용을 극대화 하고있다[9].

GICOMS 구성도

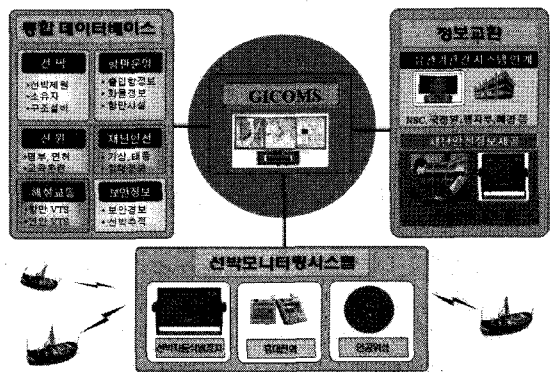


그림 5. GICOMS의 구성도
Fig. 5. GICOMS Structure

III 해상 디지털 포렌식

3.1 해상 디지털 포렌식의 정의

증거법칙과 적법절차에 따라 증거의 무결성을 유지하면

서 선박에 설치된 각종 컴퓨터 시스템, 저장매체 등으로부터 디지털증거를 수집, 보존, 분석하여 국가 간 분쟁 혹은 법정에 증거를 제출하는 일련의 과정을 의미한다.

3.2 해상 디지털 포렌식의 주요내용

가) 증거수집(Aquisition)

원본 디지털 저장매체로부터 필요한 증거를 추출하기 위하여 원본 데이터와 동일한 내용을 가진 복사본을 만드는 작업으로 이때 원본 데이터의 변형이나 훼손을 막기 위하여 쓰기방지장치를 하는 등 보호조치를 취해야 한다.

나) 분석(Exams)

복사본 저장매체로부터 필요한 데이터를 추출하여 가시적인 정보로 변환하는 작업을 말한다. 이때 저장된 데이터의 파일시스템과 저장방식을 구분하여 적절한 분석도구를 사용하기도 한다.

다) 추적(Tracking)

데이터가 브릿지에 있는 장비에 저장되기는 하였지만 작성되거나 전송된 데이터라면 원 발신지등을 추적하여 증거를 검색하는 것이다. 이때는 선박의 항행장비간의 원활한 운행에 지장을 주지 않도록 포트등 의 구성에 주의하여야 한다.

라) 데이터복구(Data Recovery)

삭제되거나 덮여 씌어진 데이터라면 원본 복구 프로그램을 이용하여 원본 파일을 복구하여야 한다. 삭제된 파일 등 복구하기도 하고 삭제된 네트워크 관련 로그 파일 복구하여 데이터의 출처를 파악한다.

마) 조사과정의 문서화

조사과정의 기록(Examination Documentation)하여 특이한 사항이나 변동된 사항, 기타 문제가 될 만한 사항들은 문서로 보존하여야 한다. 또 데이터가 추출되어 증거로 활용되고 종결되는 때까지 그 과정에 대한 보관의 연속성(Chain of Custody)을 유지하기 위하여 문서화하는 것은 매우 중요하다.

바) 증거의 무결성 유지

추출된 데이터가 본인 혹은 제3자에 의하여 변질되거나 훼손되지 않았다고 하는 것을 입증하는 것을 말한다. 이를 위하여 해쉬값을 이용하기도 하고, 디지털 타임 스탬핑(Digital time stamping)을 이용하여 운영시간을 남기기도 하고, 동영상·사진을 촬영하거나 1회용 부작 태일을 사용한다[10].

3.3 해상 디지털 포렌식의 요구사항

해상에서 사용하는 자동 항행 장비 등의 디지털증거 분석에 디지털 포렌식을 적절하게 사용하기 위하여 3가지 요소가 상호 지원되어야 한다.

가) 전문 인력 : 해상 특성 잘 이해하고 국제법등을 교육받은 후, 포렌식 관련 이론과 실무가 겸비한 전문가가 필요하다. 이를 위하여 선박항행장비 뿐만 아니라 디지털장비의 특성을 이해하고 이러한 장비가 선박에서 운영되는 과정을 분석하여 필요한 정보를 추출할 수 있는 전문 인력을 양성해야 한다.

나) 전문장비 : 해상용 디지털 포렌식 장비가 있어야 한다. 현재 디지털 해상용 포렌식 장비뿐만 아니라 해상용 디지털 포렌식 이라는 용어 마저 생소한 현실에서 통상 쓰이는 디지털 포렌식 장비의 대부분이 외산장비로서 국내 실정에 맞지 않을 뿐만 아니라 막대한 외화유출의 한 원인이 되고 있다. 외제 장비의 경우 컴퓨터 장비의 발전에 따른 업그레이드가 지연 혹은 지원되지 않는 경우도 발생하고 전달교육의 부실 등으로 효과적인 장비활용의 걸림돌이 되고 있다.

다) 지침 : 해상용 디지털 포렌식의 표준 지침의 미비로서 관련기관에서 어떠한 표준을 제시하지 못하고 있다.

라) 무결성 : 자동해상장비 등에서 디지털 증거가 수집되어 보관, 분석되는 과정에서 부당한 수정(Alteration), 변경(Modification), 손상(Damage or Destruction)이 없도록 유지하는 과정이다.

이를 위하여 해상관련 장비의 컴퓨터데이터를 안전하게 보존하고 원본데이터와 사본데이터가 동일하다는 것을 검증할 수 있어야 한다. 검증이란 원본 증거와 현재 증거로 제출하는 증거사본이 동일하다는 것을 입증하는 것을 말한다.

3.4 해상 디지털 포렌식의 적용사항

가) 선박 디스크 포렌식(Vessel Disk Forensics)

디스크 포렌식은 물리적인 저장매체인 하드디스크, 플로피디스크, 각종 보조기억장치에서 증거를 수집하고 분석하는 포렌식 분야로서 디스크 포렌식은 포렌식의 여러분야중에서 가장 발전되어 있다.

디스크 포렌식은 디스크를 검색하여 삭제된 파일을 복구하고, 패스워드나 암호가 설정되어 있는 파일의 경우 패스워드나 암호키를 복구하여 증거를 찾아내는 작업을 말

한다. 여러 가지 종류의 파일을 파일 확장자, 부서, 작성자, 작성일시, 사용일시 등을 기준으로 분류하고, 검색 키워드를 사용하여 단서를 추출하는 작업을 병행한다. 이때 주의하여야 할 점은 원본데이터를 사용하지 않는다. 복사본을 사용하여야 하며, 부득이 원본데이터를 사용해야 하는 경우에는 디스크의 변경을 방지하기 위하여 그림 5와 같이 쓰기방지장치를 사용하여 디스크를 분석 한다.

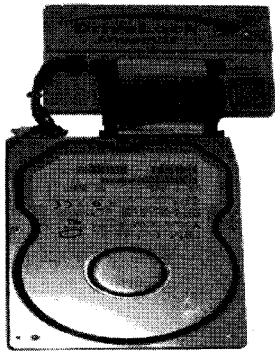


그림 6. 쓰기방지가 부착된 하드디스크

Fig. 6. Hard Disk Equipped with an Anti-writing Device

나) 선박 네트워크 포렌식(Vessel Network Forensics)
네트워크 포렌식은 네트워크를 통하여 전송되는 데이터나 패스워드 등 데이터 트래픽을 분석하거나, 접근·에러 로그, 네트워크 환경 등을 조사하여 단서를 찾아내는 분야이다. 네트워크를 통하여 데이터가 전송되는 과정에서 생성되는 자동 로그 기록을 분석하여 증거를 획득할 수 있다. 대부분의 네트워크는 사용자의 행위를 감시하고 추적하기 위한 장치를 가지고 있다. IP 헤더는 발신자 및 최종 목적지 IP주소 정보를 포함하고 있으며, 데이터 링크 헤더는 하드웨어 주소 정보를 포함하고 있다. 네트워크의 관문 역할을 하는 라우터에는 routing table, arp cache table, login해 있는 사용자, TCP connection과 관련된 정보, NAT translation과 관련된 정보가 존재하기 때문에 여기에 저장된 데이터를 분석한다면 운영에 관계된 자료를 수집할 수 있다. 또한 IMMASAT을 통하여 서비스되는 월드 와이드 웹, ftp, Usenet 등 인터넷 응용 프로토콜에서 증거를 수집하고 분석할 수 있다. 웹 히스토리(WWW history)분석, 전자우편 헤더분석, 전자우편 수신자 추적(E-Mail Tracking), WHOIS 검색 및 IP 추적 등이 선박의 항해경로나 혹은 일정에 관한 보고문등을 포함할 수 있기 때문에 중요 내용이 된다.

다) 선박 무선 포렌식(Vessel Radio Forensics)

모바일 포렌식은 PDA, Laptop, 전자수첩, 휴대폰, 디지털 카메라, MP3 플레이어, 휴대용 메모리카드, USB 저장장치 등 휴대용 기기에서 필요한 정보를 입수하여 분석하는 포렌식 분야다. 선박에서도 휴대폰 및 PDA의 보급이 급속도로 늘어나고 선수와 선미간의 통신을 위하여 무선통신장비 및 모바일 장비의 사용이 활성화 되면서 다양한 종류의 멀티미디어 기기가 개발되어 보급되고 있다. PDA는 선장을 비롯한 항해사들의 일상적인 업무에 관한 자료가 저장되기도 하지만, 입출항시 필요한 서류 및 관련 사항, 운항 기록 시 주의사항 등을 기록하기도 한다. 로밍을 이용한 휴대폰의 사용이 증가하게 되면서, 모바일 포렌식은 법정다툼의 증거자료로서 매우 중요한 시점에 와 있다.

3. 5 해상 디지털 포렌식 절차

가) 증거확보

디지털 저장장치에 저장된 정보의 유형과 형태를 확인하는 확인단계로, 증거자료 확보가 관건이다.

이를 위하여 브릿지에 설치되어 있는 항해장비에 대한 목록이 필요하며, 이는 선박에 비치된 계기목록을 참조하여 디지털자료가 저장된 장비와 운영상의 주의점에 대하여 충분히 파악한 다음 자료를 백업받거나 제출받도록 해야 한다. 이때 선원들은 이러한 장비에 대한 풍부한 지식과 경험이 필요한 것이 아니고, 운영상의 기술만을 습득하였을 경우가 많으므로 기술적인 부분을 담당하는 전문가의 도움을 받거나 수사관이 이에 상당한 기술과 경험이 있어야 한다.

나) 증거입증

보존단계로서 디지털로 저장된 자료를 확인 한 후, 변경되지 않도록 보존하는 단계이다. 만약 변경이 될 경우에는 법적 절차에 따라 변경된 원인을 설명해야 한다. 이것은 자료뿐만 아니라 자료를 읽을 수 있는 기기의 변경도 포함한다.

다) 증거분석

디지털자료를 추출, 처리, 판단하는 단계로 분석용 도구를 이용하여 디지털자료를 분석하는 단계이다. 자료 분석 시에는 검사대상 자료가 변경되지 않도록 주의해야 한다.

라) 증거제출

마지막 단계로서 법정제출을 의미한다. 법정에서 진술방법, 발표자의 전문적인 기술과 위의 세 가지 단계가 법적

증거자료로서, 신빙성 있게 서술될 수 있도록 체계적으로 준비하는 것을 의미한다.

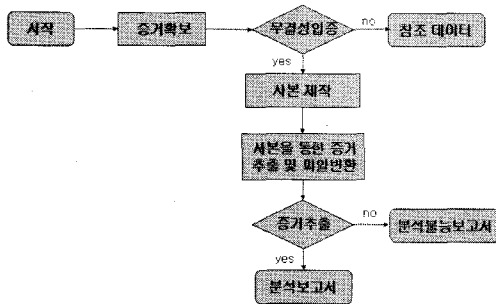


그림 7. 해상 디지털 포렌식의 절차
Fig. 7. Marine Digital Forensic Procedure

IV. 해상 디지털 포렌식 적용

4. 1 해상 디지털 포렌식이 필요한 사례연구

가) 선박 충돌 사례

2006. 9. 28. 06:00경 일본 북해도 남남동 24마일 해상에서 일본어선 제3신행호(어선 19톤)과 국적불명의 선박이 충돌하여 선원7명이 사망하고 1명은 구조되었으나 충돌선박은 도주하는 사고가 발생하였다. 이에 일본 해상 보안청은 도주한 선박의 항로를 분석하여 위 선박이 부산항에 입항하였을 것이라는 판단을 가지고 해양경찰청에 국제공조수사를 의뢰한 바, 부산해양경찰청 수사과에서는 부산항에 입항중인 이스라엘 선적 컨테이너 ZIM ASIA(41,507톤)호의 사고당일 당직자인 2등 항해사와 타수 등을 대상으로 충돌사실을 추궁하였으나 국구 부인하였다. 이 선박은 미국, 한국, 중국 등을 있는 정기선으로 일본국에 입항예정이 없는 것으로 체계적인 과학수사를 위하여 선박의 좌현 선미등에서 충돌한 흔적을 발견하고, 선장 입회하에 선체에 붙어있는 FRP 조각으로 추정되는 이물질을 채취하고, 조타실 내의 전자해도, GPS 자료, 항해일지, 항적도 등으로 다수의 증거를 확보하여 일본 해상보안청에 인계하였다.

2001. 9. 26. 07:50경 부산선적 소형기선저인망 어선 동진호(25톤)와 일본 수산청 소속 어업지도선 하쿠마루(1,000톤)이 충돌해 동진호가 침몰 하고 선원4명이 물에 빠졌으나 인근 해역에서 조업 중이던 다른 선박 태창호에 의해 모두 구조되는 사건이 발생하였다. 이 사고는

일본 수산청 어업 지도선이 동진호가 일본 영해를 침범했다며 배를 세우고 검문 받을것을 요구했지만, 동진호가 이를 불복, 한국영해로 달아나자 뒤쫓아와 동진호를 들이받아 일어난 것으로 추측되고, 사고 후 이 지도선은 일본 해상보안청 소속 경비정의 호위를 받고 일본 영해로 뒤 돌아 가는 바람에 울산해양경찰서 소속 경비정 215호는 사고 선박 선원들을 대상으로 경위를 조사하였다(11).

2007. 5. 12. 04:05경 중국 남동쪽에서 38해리 떨어진 보하이 해역에서 한국국적의 골든 로즈호와 중국국적의 진성호가 충돌한 직후 진성호가 구조나 신고도 하지 않은 채 곧바로 사고현장을 떠나 중국으로 입항한 후 신고 처리가 되고, 이에 대한 외교통상부나 해경의 처리도 미숙하여 문제가 되고 있다. 심지어 사고지점이 중국의 해역으로 구조선박을 출동하는 과정에서부터 구조헬기의 공중수색, 그리고 침몰사고경위에 대한 조사도 주목구구 식으로 이루어져 국가 간 분쟁의 소지는 더욱 커지는 실정이다. 정부에서는 사고조사 전문가를 중국으로 보내 사고경위를 조사한다는 계획이다(12).

나) 디지털 증거 제출 미비 사례

일본해역에서 도주한 이스라엘소속 ZIM ASIA의 경우 당직선원의 부인에 따라 영사관 직원의 입회하에 수사를 진행하였으며 당시 필요한 증거 서류 중 전자해도, GPS 자료 등에 대한 디지털증거자료는 추출되지 않았다. 이는 영사관 직원의 참여하에 신속한 공조수사를 위한 임의 제출형식의 방편으로 전자해도 및 GPS의 동작 상태를 모니터에 동작 시킨 다음 그 장면을 사진 촬영하여 증거물로 일본 해상 보안청에 송부하였다. 또 우리나라 어선과 일본 어업 지도선 간의 충돌사건에서도 우리나라 어선의 GPS플로터를 이용한 분석(당시는 침몰로 분석이 어려울 수 있음)을 하거나 일본 어업 지도선의 경우에는 비디오 데이터 레코더 등이 장착되어 있으므로 이를 분석한다면 하쿠마루의 운행위치와 충돌위치에 대한 정확한 증거가 제출되어 국가 간 분쟁해결에 도움이 되었을 것이다. 이때 일본해역을 침해하였다는 증거로 GPS 위치표시가 디스플레이 되는 장면을 일반 비디오 촬영을 실시하여 테잎 등을 증거물로 제출하였다. 또한 중국국적의 진성호와 같은 화물선의 경우 SOLAS 규정에 의하여 선박에 장착된 GPS, AIS, VDR, ECDIS등의 자료를 요청을 하였다면 디지털 자료의 원본을 제출받아 당사국간의 분쟁을 해결 할 수 있음에도 불구하고 해상 디지털 포렌식의 미비로 디지털 증거의 수집에 실패하였다고 볼 수 있다.

4. 2 선박 디스크 포렌식 적용 사례 연구

가) 선박 디스크 포렌식

선박의 안전항해를 지원하기 위하여 장착된 장비의 저장 장치로는 대용량의 저장 공간을 필요로 하는 전자해도, 항해자동기록기 등은 일반적인 디스크에 저장되기도 하고 일부는 플래쉬 메모리 등의 저장장치를 이용한다. 이러한 저장장치에 저장된 데이터는 시간이 지남에 따라 저장 공간의 확보를 위하여 삭제와 쓰기를 반복하게 되는데 분쟁시의 데이터 복구 및 추출을 위하여 국내에서 사용 중인 EnCase, DEAS2 등 디지털 데이터 복구전문프로그램을 이용하여 삭제되거나 은닉된 자료를 추출하면 된다. 추출된 데이터는 장치별로 포맷을 달리하는 저장형식을 취하므로 XML로 변환하여 보일 수 있도록 하며, 특수한 파일 포맷을 사용하는 경우에는 그 파일을 볼 수 있는 뷰를 설치한다. 즉 한글을 보기위한 프로그램으로 한글 뷰를 설치하거나 마이크로소프트사의 워드를 보기위해서 워드 뷰를 설치하는 것처럼 뷰 프로그램을 설치하며 이런 경우에도 지적재산권의 침해행위가 일어나지 않도록 주의할 하여야 수집된 디지털 증거의 무결성을 보장할 수 있다. 설치된 뷰를 통하여 선박 상호간의 항행증거와 이동경로, 기타 증거가 추출되면 가시적으로 보일 수 있도록 조치하고, 이러한 진행사항을 모두 기록하여 증거의 무결성에 대한 다듬에 대비하여야 한다.

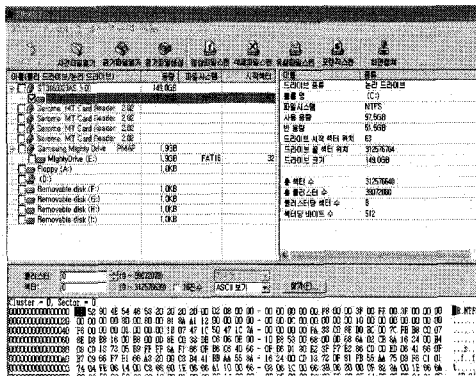


그림 8. 디스크 포렌식 툴인 DEAS2
Fig. 8. DEAS2 of Disk Forensic Tool

가) 선박 네트워크 포렌식

선박의 네트워크는 육상의 네트워크와 크게 다른 점이 2가지가 있다. 그 중 하나는 선박 내부의 네트워크를 반경으로 하는 소형 네트워크이므로 대형 네트워크의 구성이

필요하지 않으나 해상 특성상 염분, 주기적인 진동, 철제구조에 의한 설치 후 네트워크의 변경, 유지보수의 어려움 등이 존재한다는 것과, 데이터의 송수신을 위하여 인공위성 통신방식 INMASAT 통신방식을 이용한다는 것이다. 이는 선박의 네트워크를 조사하고자 할 경우에 특히 기관실에 설치된 기관 룸의 네트워크에 주의하여야 하며, 인공위성 네트워크를 차단하기 위해서는 인공위성 통신을 기본적으로 이해하여야 한다. 인공위성 통신에는 이를 리셋하지 않는다면 차후 선박안전항해에 커다란 영향을 주게 되어 조난 등 긴급한 상황에 대처할 수 없게 되므로 필요한 자료 등을 추출한 다음에 원상회복을 하여 운영에 지장이 없도록 조치하여야 한다.

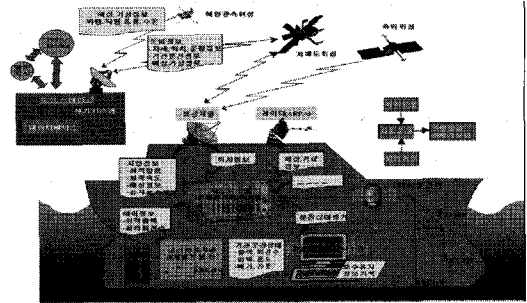


그림 9. 해상 안전장비 네트워크 구성
Fig. 9. Marine Safe-equipment Network Structure

4. 3 육상 디지털 포렌식과 해상 디지털 포렌식의 차이

현재 디지털자료는 선박에만 국한되어 저장되는 것은 아닙니다. 선박의 안전항해를 지원하는 해양안전종합포탈처럼 육상에서도 디지털자료는 보관하고 있으며 이를 분석하는 것은 육상의디지털 포렌식 절차에 의하면 된다. 하지만 육상에서 해상안전을 지원하는 기관마다 디지털자료의 보존기간의 상이함으로 인하여 표준절차가 없다는 것이 큰 문제라고 할 수 있다. 물론 서버 저장장치의 용량이나 비용 등을 고려하지 않을 수는 없지만 이번 골든 로즈호의 사고처럼 당사국 간의 분쟁이 발생하는 경우를 대비하여 적절한 보존기간을 명시함이 타당하다. 해상 디지털 포렌식의 경우에도 각 장비별로 별도의 저장장치 혹은 선박네트워크를 통한 통합 백업장치가 설치되고 보존기간이 필요하다. 이는 규정이나 강제라는 절차를 떠나서 선박의 안전을 위한 최소한의 기준으로 규정하여야 하며, 이미 신조되는 선박이나 일정 톤수이상의 선박은 SOLAS 규정에 의하여 디지털장비가 장

착되어 있으므로 백업장치만 추가 장착을 하면 되고, 최소한의 사양으로 비행기의 블랙박스처럼 방수기능과 상당기간 자동 전파 송신기능이 있으면 족하다 할 것이다. 이러한 디지털 자료를 분석하기 위한 육상디지털 포렌식과 해상디지털 포렌식을 비교하면 다음과 같다.

표 2. 육상 디지털 포렌식과 해상디지털 포렌식의 비교표
Table. 2. Comparison of Ground Digital Forensic & Marine Digital Forensic

	육상디지털포렌식	해상디지털포렌식	차이점
디스크	-저장용량 대형화 -저장장치 소형화	-특화된 저장매체 -분석의 난해성	-해도등 단순분석보다는 연계분석
네트워크	-웹서버등 사용 -DB와 연동	-IMMASAT사용 -선박장기와 연동	-선박특성상 폐쇄된 네트워크
이동성	-휴대폰등 분석 -전자파차단 주의	-소형무전기 분석 -염분부식등 주의	-휴대폰의 다양성으로 해상사용증가
기타	-각종 연구로 분석이 용이	-파일시스템 다양성으로 분석난해	-선박 데이터 분석의 다양성존재

V. 결론

본 논문은 3면이 바다로 둘러싸인 우리나라의 해역 또는 공해상에서 발생할 수 있는 선박 간 충돌사고나 조업으로 인하여 영해침범을 다투는 경우에 필요한 증거를 해상용 디지털 포렌식을 수행함으로써 분쟁의 해결을 찾고자 하였다. 해상이라는 특수한 환경 속에서 급변 한국선적의 골든 로즈호와 중국선적의 진성호 충돌사고에서 그 문제점이 나타난 것처럼 일방은 침몰로 인하여 사고에 대한 증거가 소실되고 다른 선박은 자국으로 도주하여 사고대응이 미흡하게 된다면 분쟁은 국제 재판으로까지 이어질 수밖에 없고, 사고 피해자는 엄청난 육체적 정신적 고통을 받게 된다. 이러한 경우 현재 선박에는 많은 디지털 장치가 장착되었고 중국선적의 진성호 또한 5천 톤급 상선으로 디지털장비에 대한 해상 디지털 포렌식으로 사고 수사를 진행 한다면 디지털 수사는 진일보 하게 되고 해상 뺑소니 등으로 사고를 부인하는 사례는 사라질 것이다.

현재 조난통신장비가 왜 동작하지 않았는지 등 디지털 장비에 대한 하드웨어적인 미비점은 본 논문에서 논하지 않더라도 해상안전협약에 장착을 의무화한 장비의 기본 장착은 물론이고 육상에서도 선박의 이동 및 입출항에 대한 설

비를 구비함으로써 안전한 항해와 조업을 지원해야 한다.

아울러 이러한 장비를 잘 활용하면 국가 간 분쟁에 대하여 증거주의에 입각하여 좋은 결과를 기대할 수 있다.

이에 따라 남해지방해양경찰청에서도 2007. 4. 24일 과학수사팀을 창설하여 해상에서 일어나는 범죄에 대한 해양 관련범죄에 대처하고 있다. 과학수사팀은 컴퓨터 관련 사이버 범죄 수사 등 과학수사에 대한 지원과 드러나지 않는 범죄에 대한 추적을 하는 등 날로 지능화되고 과학화 되는 범죄에서 증거를 추출하고 대처하는 해상용 디지털 포렌식의 한 축이 될 것이다[13].

현재 해난사고에 디지털 자료가 증거로 입증된 사례는 없다. 하지만 본 논문에서 연구하고 제시한 바와 같이 디지털 자료는 언제나 존재하므로 육상에서 활용중인 디지털 포렌식에 대한 개념을 도입하고, 활용한다면 작게는 선박의 안전운항과 각종 해상 범죄에 대한 예방과 증거의 증명력의 차원에서 그 활용도 더욱 증가될 것이다.

참고문헌

- [1] 최중화, 신흥호사건이 남긴 과제와 대책, 통일한국, 2005.7.
- [2] 이종근, 어선위치추적시스템의 도입 필요성에 관한 고찰, 한국해양수산개발원논문지, 2003. 12.
- [3] 삼성중공업 <http://www.shi.samsung.co.kr/kor/2007.3.12>
- [4] 구자윤, 새로운 항해장비의 국제적 동향과 대응방안, IMO기술정보, 2002.
- [5] 박종민, 오세웅, 서상현, 전자해도품질관리절차설계연구, 선박해양기술, 2005. 11.
- [6] 해양수산부. http://www.momaf.go.kr/news/momaf/N_momaf_category_view.asp?ID=70063628&Code=b_sec_1, 2007. 5.14.
- [7] http://www.imo.org/Conventions/contents.asp?topic_id=257&doc_id=647#dec2006
- [8] 강창구, 공인영, "해난방지를 위한 과학적인 대처방안" 한국기계연구원 선박해양공업연구소, 1998.
- [9] 해양수산부, http://www.momaf.go.kr/doc_kyulje/union_kyulje. 2007. 5. 14.
- [10] 이규안, 박대우, 신용태, "포렌식자료의 무결성확보를 위한 수사현장의 연계관리 방법 연구". 한국컴퓨터정보학회 논문지, 제11권 제6호, pp175-184, 2006.12.

- [11] 최중화, 박재영. "동북아 신국제어업질서하에서의 어업 분쟁 발생가능성과 그 해결방법." STRATEGY21, 제 3권2호, 2001.
- [12] 한겨레뉴스, http://www.hani.co.kr/arti/society/society_general/209053.html, 2007. 5. 13.
- [13] 해사신문, <http://www.haesanews.com>. 2007. 4. 24.

저자 소개



이 규 안

2006년 숭실대학교 정보과학대학원 정보통신학과 졸업 (공학석사)
 2007년 숭실대학교 컴퓨터과학과 (박사과정)
 2000년 벽산대학 정보통신과 겸임교수
 2002년 대검찰청 중앙수사부 컴퓨터 수사과 근무
 2005년 대검찰청 과학수사2담당관 실 근무
 2007년 대검찰청 디지털수사담당관 실 근무
 <관심분야> 유비쿼터스 보안, 디지털 포렌식, 해상 디지털 포렌식, 이동통신 보안



박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)
 2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)
 2000년 매직캐슬정보통신연구소 소장, 부사장
 2004년 숭실대학교 정보과학대학원 정보보안학과 겸임조교수
 2006년 정보보호진흥원 선임연구원
 2007년 호서대학교 벤처전문대학원 조교수
 <관심분야> 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality



신 용 태

1985년 한양대학교 산업공학과 학사
 1990년 Univ. of Iowa 전산학과 석사
 1994년 Univ. of Iowa 전산학과 박사
 1994년 ~ 1995년 Michigan State Univ. 전산학과 객원교수
 1995년 ~ 현재 숭실대학교 컴퓨터학부 교수
 <관심 분야> 멀티캐스팅, 실시간통신, 이동통신, DRM 등