



# 한국디지털포렌식학회

Ⓢ 서울특별시 서대문구 미군동 209 경찰청 사이버테러대응센터 1307호  
(사) 한국디지털포렌식학회 회장 양근원 담당자 오소정 (E-mail : kdfs.manager@gmail.com)

문서번호 협조 제2024-071호

시행일자 2024. 12. 23.

공개여부

경유 :

수신 : 세종대학교

선결			지시	
접수	일자		결재	
	시간			
	번호		·	
처리부서	사무국		공	
담당자	오소정		람	

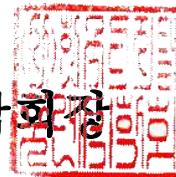
제목 : 2024년 한국디지털포렌식학회 동계학술대회 참가 사실 확인(조배근)

- 귀 기관의 무궁한 발전을 기원합니다.
- 한국디지털포렌식학회는 디지털증거의 증거능력을 위해 필요한 다양한 기술과 법·제도를 연구하여 국가경쟁력을 확보하기 위해 노력하고 있습니다.
- 우리학회가 주최하고 경찰청, 한국저작권보호원에서 공동주최하는 아래 학술행사에 귀 기관 소속의 조배근연구원이 논문 제출 및 발표한 사실을 확인합니다.

- 다 음 -

- 가. 행사명: 2024년 한국디지털포렌식학회 동계학술대회
- 나. 일시장소: 2024년 12월 16일 (월), 한성대학교 낙산관 대강당 9:00 ~ 19:00
- 다. 주최: (사)한국디지털포렌식학회, 경찰청, 한국저작권보호원
- 라. 주관: 한성대학교
- 마. 확인사항
  - 제출 논문명: 인공위성 포렌식에 관한 고찰
  - 발표 세션: 세션2, 2번 트랙. 끝.

(사) 한국디지털포렌식학회



# 인공위성 포렌식에 관한 고찰

조 배 근\*, 박 기 응\*\*

세종대학교 정보보호학과(대학원생)\*, 세종대학교 정보보호학과(교수)

## Considerations on Satellite Forensics

Bae Geun Cho\*, Ki-Woong Park\*\*

Dept. of Computer and Information Security, Sejong University (Graduate Student)\*

Dept. of Computer and Information Security, Sejong University (Professor)\*\*

### 요 약

위성은 현대 사회에서 통신, 내비게이션, 기상 관측 등 핵심적 역할을 한다. 위성 시스템이 사이버 공격, 오작동, 물리적 제약 또는 보안 위협에 노출되면 치명적 영향을 미칠 수 있다. 본 논문은 위성 디지털 포렌식의 필요성과 복잡성을 고찰하고, 이를 효과적으로 구현하기 위한 방법론을 제시한다. 위성의 구조와 임무, 위성 시스템의 주요 위협, 디지털 포렌식의 중요성, 도전 과제, 적용 가능한 기술을 분석한다. 위성 디지털 포렌식 발전이 시스템 신뢰성 및 안전성을 강화하고, 위협 대응의 기반이 됨을 제시한다.

주제어 : 인공위성, 위성 시스템, 보안 위협, 디지털 포렌식, 인공위성 포렌식

### ABSTRACT

Satellites play a crucial role in modern society, particularly in communication, navigation, and weather observation. However, satellite systems are vulnerable to cyberattacks, malfunctions, physical constraints, or other security threats, which could lead to catastrophic consequences. This paper examines the necessity and complexity of satellite digital forensics and proposes methodologies for its effective implementation. It analyzes satellite structures and missions, major threats faced by satellite systems, the importance of digital forensics, challenges, and applicable technologies. The study highlights that advancements in satellite digital forensics enhance system reliability and safety, providing a robust foundation for responding to various threats.

**Key Words** : Satellites, satellite systems, Security Threats, Digital Forensics, Satellite Forensics

## 1. 서 론

Space X의 발사체 재사용 기술로 인해 기존보다 낮은 단가로 우주산업에 진출하는 뉴 스페이스 시대가 도래함에 따라 초소형 위성, 군집위성 등 다양한 위성 개체가 빠르게 증가하고 있다. 위성 기술은 지구상의 통신과 정보 전달을 혁신적으로 변화시켰으며, 세계 경제와 안보에 필수적인 인프라로 자리 잡았다. 그러나 위성 시스템이 사이버 공격의 표적이 되거나 내부적인 오류로 인해 오작동할 경우, 그 영향은 치명적일 것이다. 상대적으로 사이버 공격 사례는 민감한 정보로 잘 공개되지 않지만, 발표된 내용을 보면 미국 위성 해킹사건(2007-2008)은 Landsat-7과 Terra AM-1의 지상국 해킹으로 위성 통제권을 가로챈 사건이고, 2022년 러시아-우크라이나 전쟁 중 미국의 위성 서비스 업체인 Viasat의 KA-SAT 위성 네트워크를 지상국 해킹을 통해 유럽 전역의 인터넷 통신이 손상된 사건이다. 같은 시기 SpaceX의 starlink 공격도 발생하였는데 우크라이나 군의 전술 통신망을 무력화 하기 위함이었다고 한다. 이러한 상황에서 위성에 대한 보안을 강화하고 문제의 원인을 규명하고 재발을 방지하는 데 중요한 역할을 하는 디지털 포렌식에 대해 고찰하고자 한다. 본 연구의 목적은 우주에 있는 위성에 대한 디지털 포렌식의 필요성과 그 복잡성을 이해하고, 효과적인 포렌식 절차와

방법론을 제시한다. 본 논문의 구성은 2장에서 위성에 대한 전반적인 구성, 3장에서 위성 디지털 포렌식의 중요성, 4장에서 위성 디지털 포렌식 방법론, 5장에서는 결론으로 구성되어 있다.

## II. 인공위성

### 2.1 인공위성의 분류

인공위성은 크기에 따른 분류[표1], 궤도에 따른 분류[표2], 임무에 따른 분류[표3]와 같이 분류한다[1].

〈표 1〉 크기에 따른 분류

Class	Mass
Large-size	1000 (Kg)
Medium-size	500~1000
Mini-satellite	100~500
Micro-satellite	10~100
Nano-satellite	1~10
Pico-satellite	0.1~1
Femto-satellite	0.1
Nano, Pico, Femto는 초소형 위성으로 분류	

〈표 2〉 궤도에 따른 분류

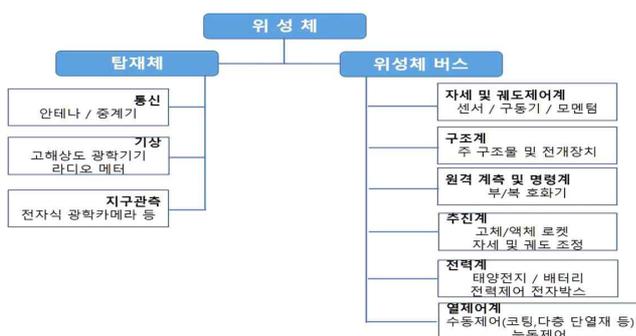
궤도	특징
저궤도(LEO) (Low Earth Orbit)	고도 500km~1500km
중궤도	고도 5000~15000km
정지궤도(GEO) (Geosynchronous Orbit)	고도 35786 km, 궤도 공전주기와 지구 자전주기가 일치하여 해당 지역에서 볼 때 항상 고정된 위치에 있는 것으로 보인다.
몰니아 궤도 (Molniya)	원지점 약 4000km, 근지점 약 600km의 이심률이 대단히 큰 타원궤도로 궤도면이 적도면에 대해 약 63도의 경사를 이루고 있다.
태양동기궤도	궤도면의 회전방향과 주기가 지구의 궤도주기와 동일하여 위성 궤도면과 태양이 항상 동일한 각도를 유지하게 된다.

〈표 3〉 임무에 따른 분류

임무 명칭	주요임무
방송/통신	- TV, 라디오, 전화, 데이터 중개 - 정지궤도 위성의 경우 커버할 수 있는 영역은 넓으나 시간 지연이 큰 단점이 있다. 이동통신의 경우 주로 중궤도, 저궤도 위성이 사용되나 커버 영역이 좁아 여러 대의 위성을 연계하여 사용한다.
기상	- 날씨 정보 제공 (일기예보) - 허리케인, 홍수, 산불, 해일 등 재난 정보 제공, 예방 및 구호에 활용
지구관측	- 지표면: 지표면 영상 촬영, 자원 탐사, 농작물 작황 정보 파악, 측량, 지도 제작 - 해양: 해수면 온도, 해류 상태 관측 - 대기: 대기 성분, 기온, 습도 등 관측
항법/위치정보	- NAVSTAR GPS(미국), Galileo (유럽), GLONASS (러시아, 인도), Beidou (중국)
과학기술연구	- 행성 탐사 - 천체 관측 (예: 허블망원경) - 각종 실험 - 진보된 기술을 이용한 장치를 탑재, 우주 환경상에서 동작 확인, 성능 시험
군사목적	- 정찰 영상 제공 - 기상 정보 제공 - 통화, 교신 내용 도청

### 2.2 인공위성의 구조

〈그림 1〉 위성 구조도



인공위성은 위성 본체인 버스의 각 서브시스템과 탑재체(payload)로 구성되어 있으며, 이는 [그림 1]에 나타나 있다[2]. 일반적으로 위성은 버스에 해당하는 각 서브시스템과 탑재체(payload)에 따라 임무를 결정하고 명칭을 부여한다. 위성에 탑재되어 부여된 임무를 수행하고, 위성과 지상국 간의 명령 전달 및 위성의 상태를 전송하는 핵심 소프트웨어를 위성 비행 소프트웨어(FSW: Satellite Flight Software)라고 한다. 이 소프트웨어는 위성의 다양한 상태를 모니터링하며, 이상

상황 발생 시 정해진 절차를 자동으로 실행하여 위성을 최대한 안전한 상태로 유지한다. 이러한 위성 비행 소프트웨어는 임무와 환경의 특수성 때문에 고도의 안전성과 신뢰성이 요구된다. 또한 탑재체에 따라 위성의 지상국 시스템 구성이 달라지며, 이는 다음 2.3 인공위성 시스템에서 자세히 설명한다.

### 2.3 인공위성 시스템

관제 시스템의 구성과 절차를 정리하면 다음[표4]과 같다[2].

〈표 4〉 관제 시스템 명칭

영문	국문
SGS(Satellite Ground Station)	위성지상국
MOC(Mission Operation Center)	임무운영센터
MPS(Mission Planning Subsystem)	임무계획팀
FDS(Flight Dynamics Subsystem)	궤도역학팀
ROS(Real-time Operating Subsystem)	위성운영팀

〈그림 2〉 관제 시스템 운영도



[그림2]와 같이 관제시스템이 운영된다. FDS는 궤도 결정 및 필요한 기동량 계산, 연료추정, 각종 이벤트 예측을 하여 MPS에 전달한다. MPS는 FDS에서 전달된 정보를 이용하여 위성의 궤도 및 자세 보정을 위한 기동을 준비하고 임무를 통합하여 실시간 운영에 전달한다. ROS는 MPS에서 전달된 임무계획 정보를 미리 정의된 위성운영 절차서(FOP: Flight Operation Procedure)를 이용해 TC(Telecommand)를 전송하고, 전송된 FOP에 따라 임무 실행상태 및 위성의 상태 등을 TM(Telemetry)을 통해 지상 관제시스템에 연동하여 각 서브시스템의 기능 동작을 확인할 수 있다.[2] 또한 위성별 탑재체에 따라 광학위성 및 기상위성의 경우 위성으로부터 원시데이터의 영상을 수신받고 해당 데이터의 처리 및 가공을 통해 적절히 활용한다. 이처럼 위성은 우리 삶에 꼭 필요한 인프라로 자리매김 하였다. 다양한 목적으로 위성에 대한 사이버 공격 및 물리적인 공격이 날로 증가함에 따라 디지털 포렌식의 중요성이 부각되고 있다. 따라서 다음 장에서 위성 디지털 포렌식을 다루겠다.

## III. 위성 디지털 포렌식의 중요성

### 3.1 디지털 포렌식 절차와 역할

디지털 포렌식은 일반적으로 사전 준비 → 증거 수집 → 정보 저장매체 운반 → 증거 분석 → 결과 보고서 작성 → 보존 및 증거 관리의 절차로 진행되며, 이는 초기의 DFRWS 조사 모델을 따른다.[3] 최근에는 다양한 모델들이 등장하고 있지만, 위성 분야에서는 특히 원인 규명과 보안 강화를 우선시해야 한다.

디지털 포렌식은 문제 발생 시 정확한 원인을 파악하여 대응책을 마련하는 사건 원인 규명, 법적 분쟁이나 국제적인 분쟁에서 활용될 수 있는 증거 확보, 그리고 취약점을 식별하고 보안정책을 개선하여 미래의 위협에 대비하는 보안 강화 등의 중요한 역할을 수행한다.

따라서 수사의 목적을 효율적으로 달성하기 위해 디지털 포렌식 절차에 대한 연구가 필요하며, 이것이 바로 디지털 포렌식 절차 모델이다. 이 모델은 기술적인 측면뿐만 아니라 법률적인 측면도 포함한다. 각국의 디지털 포렌식 현실, 특히 법률적인 현실에 따라 절차는 달라질 수밖에 없기 때문에, 이러한 요소들을 종합적으로 고려해야 한다.

디지털 포렌식 절차 모델은 문제의 원인을 정확히 규명하고, 법적 증거를 확보하며, 보안 강화를 통해 미래의 위협에 대비하는 것을 목표로 한다. 이는 위성 분야에서도 동일하게 적용되며, 위성 시스템의 특수성을 반영한 디지털 포렌식 절차의 개발과 적용이 필수적이다.

그러나 위성 시스템은 지구 전역을 대상으로 운영되며, 물리적 접근이 어렵고 실시간 데이터 수집이 제한되는 등 일반적인 디지털 포렌식과는 다른 취약점과 제약사항이 존재한다. 이러한 어려움을 극복하기 위해서는 위성 포렌식의 제약사항을 면밀히 분석하고, 이에 대한 해결 방안을 모색해야 한다.

다음 장에서는 위성 포렌식의 제약사항을 살펴보고, 이러한 제약을 극복하기 위한 방안을 논의하고자 한다.

### 3.2 위성 포렌식 제약사항

위성 포렌식은 위성의 복잡한 구성과 우주 환경의 특수성으로 인해 다양한 취약점과 제약사항에 직면했다. 위성은 수많은 구성요소로 이루어져 있어 하드웨어 결함이나 소프트웨어 버그가 발생할 가능성이 높다. 특히 우주라는 예측하기 어려운 환경에서 운영되기 때문에 장애를 사전에 예측하거나 대응하기가 더욱 어렵다. 물리적 제약은 위성 포렌식의 가장 큰 한계이다. 위성은 우주 공간에서 작동하기 때문에 탑재된 펌웨어, 메모리 덤프, 저장장치 등을 회수하여 분석하거나 수리하는 것이 사실상 불가능하다. 이러한 물리적 접근의 불가능성으로 인해 하드웨어 고장이 발생하면 수리나 교체가 거의 불가능하며, 복구 작업도 매우 어렵다. 또한 우주 방사선, 전자기장, 극한의 온도 변화 등 우주 환경의 특이 사항은 하드웨어 손상을 유발하여 내부 시스템의 오작동 가능성을 높인다. 이러한 환경적 요인들은 위성의 안정적인 운영을 위협하며, 예측하지 못한 시스템 장애를 발생시킬 수 있다. 통신의 제약도 위성 포렌식에 큰 영향을 미친다. 지상국과 위성 간의 통신은 제한된 대역폭에서 암호화되어 짧은 시간 동안만 이루어진다. 지구와의 거리에 따른 통신 지연은 항상 존재하며, 이는 실시간 대응을 어렵게 한다. 또한 전파간섭으로 인해 통신이 불안정해지고, 이는 데이터 전송과 명령 수행에 부정적인 영향을 미친다. 위성은 태양에너지와 배터리를 기반으로 전력을 공급받기 때문에 에너지 자원이 제한적이며, 이는 시스템 운영과 통신에 많은 제약을 가한다. 최근 들어 위성에 대한 사이버 공격이 증가하고 있다. 이는 위성 자체뿐만 아니라 위성을 운영하는 지상 시스템에 대한 공격도 포함된다. 이러한 공격은 위성의 운영을 방해하거나 정보를 탈취하려는 의도를 가지며, 전체 위성 네트워크의 안전성과 신뢰성을 위협한다.

## IV. 위성 디지털 포렌식 방법론

### 4.1 기존 위성의 문제 분석 방법

위성에 이상이 발생하였을 경우, 텔레메트리를 통해 위성의 상태정보를 분석한다. 일반적으로 위성비행소프트웨어(FSW: Satellite Flight Software)는 지상에서 요청받은 특정 메모리 위치의 내용을 전송하는 메모리 덤프(Memory Dump) 기능을 포함하며, 발사 전 위성 성능 검증 환경에서는 이 기능을 활용하여 덤프 결과를 수작업으로 분석해 소프트웨어 내부의 상태를 파악해왔다. 문제가 발생하거나 또는 사이버공격을 당했을 경우에도 텔레메트리와 OBC(위성 컴퓨터)의 저장 데이터 덤프를 통해 언제 통신이 이루어졌는지, 어떤 작업이 수행되었는지, 무엇이 변경되고 작동되었는지를 확인할 수 있다. 그러나 위성에서 지상으로 전송되는 데이터 속도의 한계로 인해 FSW 내부의 모든 내용을 텔레메트리로 전송하기는 어렵다. 또한 문제에 따라 FSW의 기능을 수정할 수 있는 온보드 리프로그래밍(On-Board Re-programming) 기능을 사용하기도 하지만, 이러한 수정은 매우 제한적이며 극히 드물게 이루어진다[4]. 따라서 문제의 징후를 파악하기 위해 비정상적인 데이터 전송, 명령 실행 오류, 시스템 재부팅 등의 패턴을 분석하는 것이 핵심이다. 이러한 분석은 일반적으로 위성이 상태 이상이나 기능 이상으로 인해 안전 모드로 진입했을 때 상세하게 이루어진다. 하지만 이 방법은 많은 인력과 시간이 소요되는 작업으로, 최근에는 AI를 활용한 자동화된 분석 및 대응 연구가 지속되어 이러한 한계를 극복하고자 한다.

### 4.2 최신 위성의 문제 분석 방식

근래에 운영되는 국내 중대형 위성은 다음과 같은 방식들을 개발하고 실제로 위성복구에 사용되며 효율적으로 적용되었다. 바로 결함 관리시스템[4]과 한국항공우주연구원 위성연구본부 위성비행소프트웨어 팀에서 특허로 등록한 “위성 상태를 기록하는 장치 및 방법”으로 다목적 실용위성에서는 CODA(Contingency Operation Data Area)로 불리우며, 정지궤도 복합위성에서는 Context 라 불리우는 기법이다[5].

먼저 결함관리시스템은 NASA 프로젝트로부터 시작되었고, 위성 시스템의 임무 복잡성과 자동화 요구 증가로 인해 결함 관리 시스템과 함께 시스템 상태 관리로 확장되고 있다. 결함 관리는 위성 시스템의 위험을 감소시키는 핵심 요소로서, 시스템이 이상 현상이나 고장 상태에 대해 제한, 감지, 고립, 진단, 대응할 수 있도록 기능을 구성한다. 이는 전체 시스템 관점에서 기능의 확장된 조합 형태로 구현되며, 고장 감지, 고립, 복구(FDIR, Failure Detection, Isolation, and Recovery)로도 알려져 있다. 결함(Fault)과 고장(Failure)은 원인과 결과의 관계로서, 시스템 내에서 원인과 결과의 순환 관계를 이룬다. 따라서 결함 관리

설계자는 발생 가능한 고장뿐만 아니라 이상 현상의 잠재력도 함께 고려해야 한다. 특히 위험 임계 시간 이내에 고장 대응을 완료하여 위험 고장 영향이 발생하기 전에 문제를 해결하는 것이다. 이를 위해 구성품 단계에서 고장을 조기에 감지하여 시스템 고장으로의 확장을 막는 것이 중요하다. 일반적으로 결합 관리의 설계 범주는 위성체의 강건성, 서브시스템 수준의 FDIR, 시스템 수준의 FDIR, 그리고 지상 운영으로 나눌 수 있다. 다음으로 위성의 문제 발생 시 원인 분석을 위한 자료를 제공하는 '위성 상태를 기록하는 장치 및 방법'은 위성비행소프트웨어가 운영 중 발생하는 문제에 대처하고 해당 원인을 분석하기 위해 위성의 상태 정보를 기록하여 활용하는 기술이다. 기존의 다목적 실용위성에서는 CODA(Contingency Operation Data Area)를 이용하여 소프트웨어가 주기적으로 위성의 주요 상태 정보를 기록하고, 소프트웨어가 문제를 인지할 경우 시스템 리셋 이전에 해당 상태 정보를 저장한 후 시스템을 초기화한다. 정지궤도복합위성의 경우에도 Context라는 이름으로 SRAM의 특정 영역을 상태 저장을 위해 사용하며, Reconfiguration과 같은 위성의 상태 변화 시 문제의 원인을 기록하고 자동 복구 과정에 활용한다[5].

#### 4.3 위성 디지털 포렌식을 위한 방향성

위성의 고장진단을 위한 메모리 덤프 방식 외에 위성에도 표준화된 맞춤형 포렌식 도구를 탑재하는 것이 필요하다고 생각한다. 제한된 통신환경에서 효율적인 데이터 수집을 위해 데이터 압축 및 최적화를 수행하도록 스크립트를 탑재한다면 포렌식 분석에 도움이 될 것이다. 또한 메모리 및 파일시스템 분석도구를 통해 수집된 데이터에서 증거를 추출하여 침해에 대응할 수 있을 것이며, 나아가 테스트베드 또한 구축된다면 각종 시나리오 기반으로 시뮬레이션을 통한 위협에 대응하고 분석 및 검증 할 수 있을 것이다.

## V. 결 론

우주에 있는 위성에 대한 디지털 포렌식은 물리적 접근의 불가능성, 제한된 통신 환경, 강력한 보안 조치 등으로 인해 지상에서의 포렌식보다 훨씬 복잡하고 도전적일 것이다. 그러나 위성 시스템의 중요성과 잠재적인 위협을 고려할 때, 효과적인 포렌식 절차와 기술을 개발하는 것은 필수적일 것이다. 이를 위해 위성 원격 데이터 수집 기술의 발전, 맞춤형 분석 도구의 개발 및 국제표준 확립이 필요하다. 향후 연구에서는 이러한 도전과제를 해결하기 위한 기술적 혁신과 국제 협력의 강화가 요구될 것이다.

## 참 고 문 헌 (References)

- [1] [https://satrec.kaist.ac.kr/02\\_01.php](https://satrec.kaist.ac.kr/02_01.php)
- [2] Bae Geun Cho. "Conceptual Design of a Universal Simulator for Satellite Operations." Proceedings of the Korean Society for Aeronautical and Space Sciences Conference (2023): 1171-1172.
- [3] Kim, Ji-Hong. *A New Approach to the Digital Forensic Procedure Model*. Seoul National University Graduate School of Convergence Science and Technology, 2015.
- [4] Kim, Jongah, and Choi, Jaedong. "The Technical Trends of Spacecraft Fault Management System Development." Current Industrial and Technological Trends in Aerospace, 12(2), 66-74, 2014.
- [5] Shin, Hyun-Kyu. "New Technologies on Satellite Flight Software with Patents." Current Industrial and Technological Trends in Aerospace, 15(2), 142-151, 2017.

## 저 자 소 개



### 조 배 근 (Bae Geun Cho)

준회원

2014년 2월 : 한양사이버대학교 컴퓨터공학과 졸업

2021년 9월 ~ 현재 : 세종대학교 일반대학원 정보보호학과 석사과정

관심분야 : 인공위성, 디지털 포렌식, 정보보호



### 박 기 응 (Ki-Woong Park)

정회원

연세대학교 Computer Science 학사

KAIST Electrical Engineering 석사

KAIST Electrical Engineering 박사

2009년 10월: Microsoft Research, Graduate Research Fellow

2012년 8월: 국가보안기술연구소 연구원

2016년 8월: 대전대학교 정보보안학과 교수

2016년 9월~현재: 세종대학교 정보보호학과 교수

관심분야 : 클라우드 시스템 보안, 초고속 보안 시스템, 시스템 인스펙션, 디지털포렌식