

# 하드웨어 해커가 되어보자!

정구홍(mongii)

GRAYHASH 수석연구원

cybermong@grayhash.com

<https://www.facebook.com/goohong.jung>

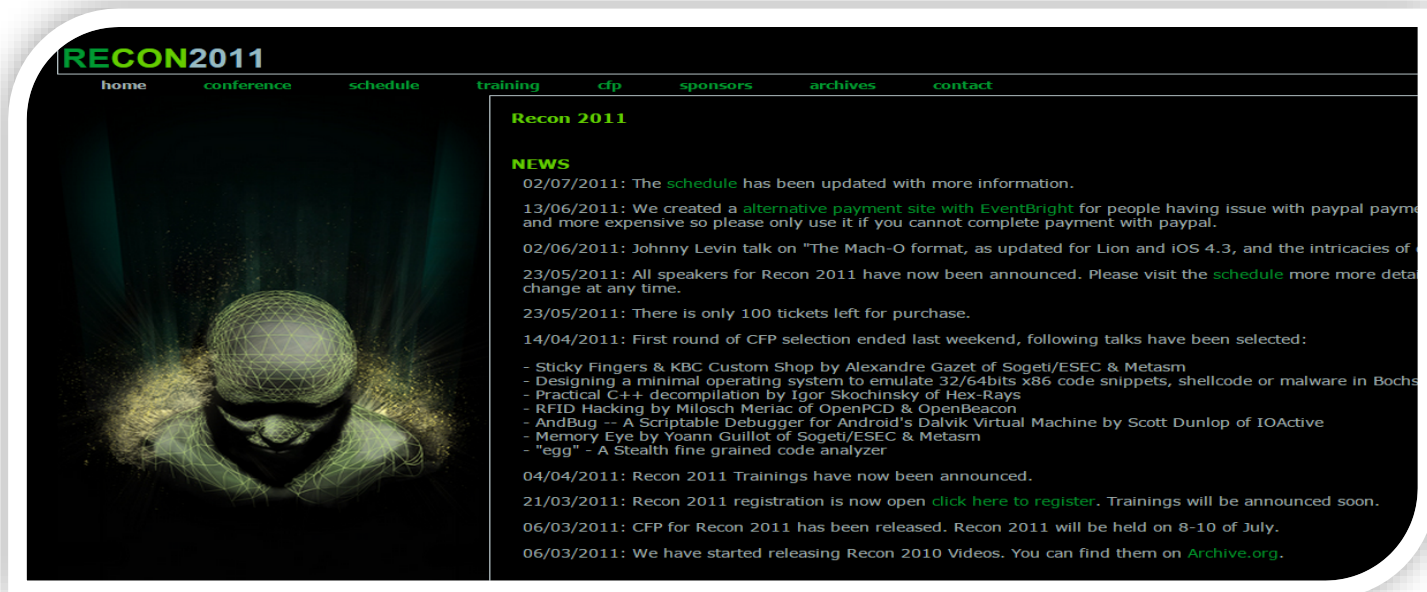
# 발표자 소개

- 보안 커뮤니티 해커스쿨 운영자
- 정보보안업체 GRAYHASH 수석 연구원
- BoB 보안인재 양성 프로그램 멘토
- 발표 내용
  - 다양한 하드웨어 해킹 기술들을 단계별로 정리
  - 하드웨어 해킹 공부 방법 소개



# Hardware Hacking을 공부하게 된 계기

- 2011 Recon(Reverse Engineering Conference)
- Montreal, Canada



# Recon 2011의 발표 주제들

- Abusing Hardware Defined Radios
- RFID Hacking
- How to develop a rootkit for Broadcom NetExtreme network cards
- Sticky Fingers & KBC Custom Shop
- Ghetto Tools for Embedded Analysis
- Hardware Stuff for Software People
- ...

# Recon 2011의 발표 주제들

- Abuse
- RFID
- How
- Sticky
- Ghet
- Hard
- ...



ork cards

# After that...

- 하드웨어 그룹스터디 진행
- 하드웨어 기초
  - 납땜부터..
- AVR Programming
- RC Car 제작 실습
- MP3 player 제작 실습





# After that...

Recon 2011 - Hardware Stuff for Software People By Stephen Ridley Recon

## Bus Pirate

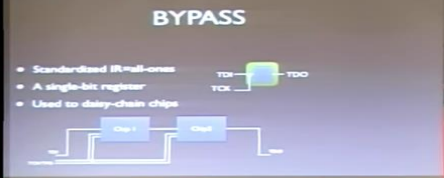
- An "interface" Swiss Army Knife
- Built-in "terminal" that you can connect to
- or Python/C libraries for programmable control
- Interfaces your computer via USB to:
  - I-Wire, I-ART, I2C, SPI, raw 3-wire, MIDI, PC Keypads, JTAG
- Lots of features like I2C sniffer!



1 | 52 S. Ridley 42:34

Prefer flash? • Embed • Questions/Feedback?

외국의 하드웨어 해킹 자료들을  
열심히 열심히 공부



## BYPASS

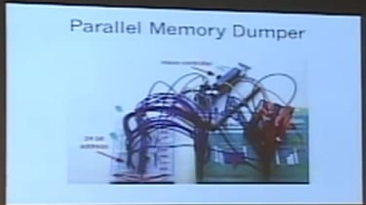
- Standardised IR-mail-ones
- A single-bit register
- Used to duty-chain chips

Chip 1 Chip 2

TDO TCK TDO

26:39 / 56:38

Blackbox JTAG Reverse Engineering [26C3]



## Parallel Memory Dumper

23:12 / 56:12

[27C3] (en) JTAG/Serial/FLASH/PCB Embedded Reverse Engineering Tools and Techniques

# After that...

- 유무선 공유기 해킹
- 스마트폰 UART/JTAG 해킹
- 스마트 TV 해킹
- CCTV 해킹
- 프린터 해킹
- 홈 네트워크 해킹
- 무선 해킹
- 도어락 해킹
- 자동차 해킹
- ...



# 하드웨어 해킹 레벨 분류

- Level-1 : 용기를 가지고 분해해 보기
- Level-2 : Datasheet를 읽어 보기
- Level-3 : Debug Port에 연결해 보기
- Level-4 : 전기 신호 분석해 보기
- Level-5 : Desoldering
- Level-6 : Side Channel Attack
- Level-7 : Decapping & Imaging
- Level-8 : Glitching Attack
- Level-9 : FIB(Focused Ion Beam) Attack
- Level-10 : IC Chip Reversing

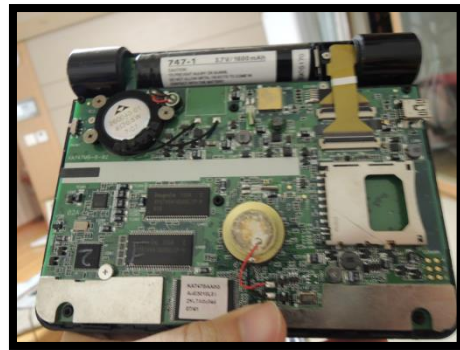
\* 발표자의 주관적인 견해에 따라 분류되었습니다.

# LEVEL-1 : 용기를 가지고 분해해 보기

- 주변의 전자장비들을 무작정 뜯어본다!
- 다양한 IC칩들의 모델명을 구글에서 검색해 본다.
  - 특히 CPU, Flash, RAM이 무엇인지 찾아본다.
- 연결이 가능해 보이는 포트들을 찾아본다.
  - USB, UART, JTAG, ISP ...
- 분해하고 살펴보는 과정에서 고장이 날 수도 있다.
  - 뒤통수는 고장이 난 다음에 생각한다.



# 일단 무조건 뜯어 본다.

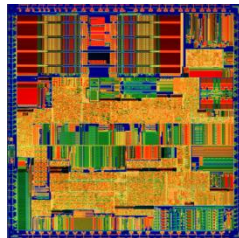


# 유용한 도구들

- 디지털 멀티 테스터
  - 전압, 전류, 저항 테스트
  - 통전 테스트

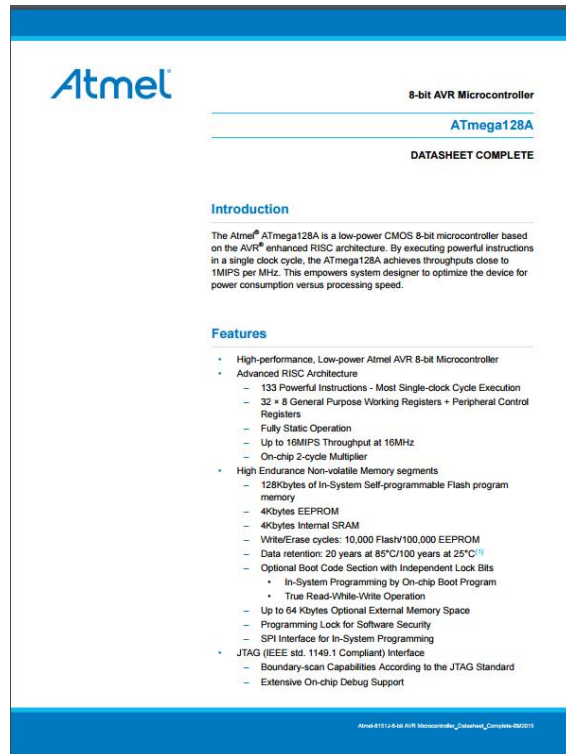


- USB 현미경
  - IC 칩, 소자 확대, 회로 패턴 분석
  - 500배율, 3만원대 제품 정도면 적합

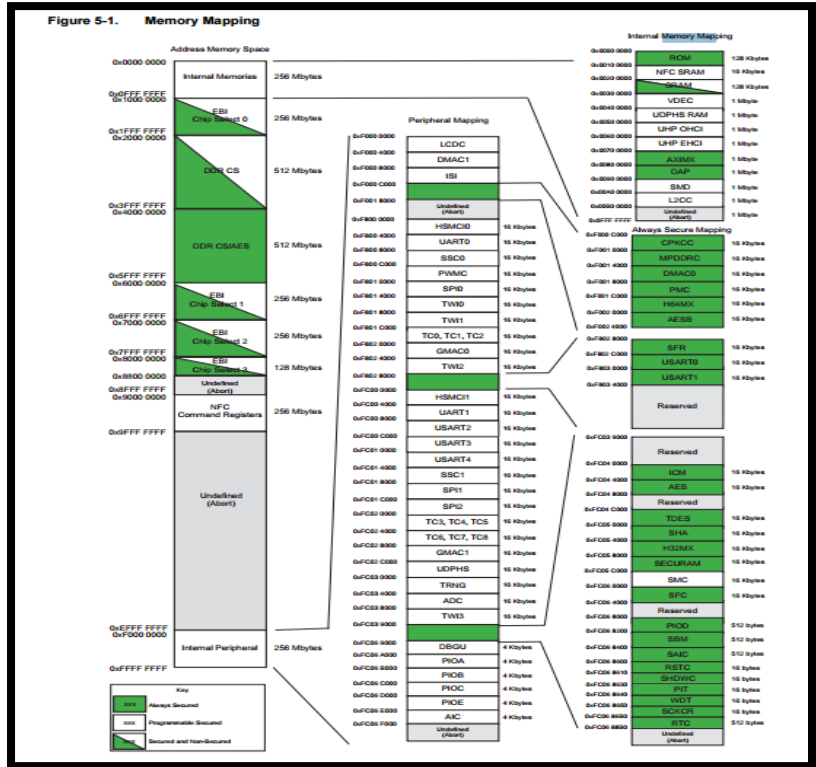
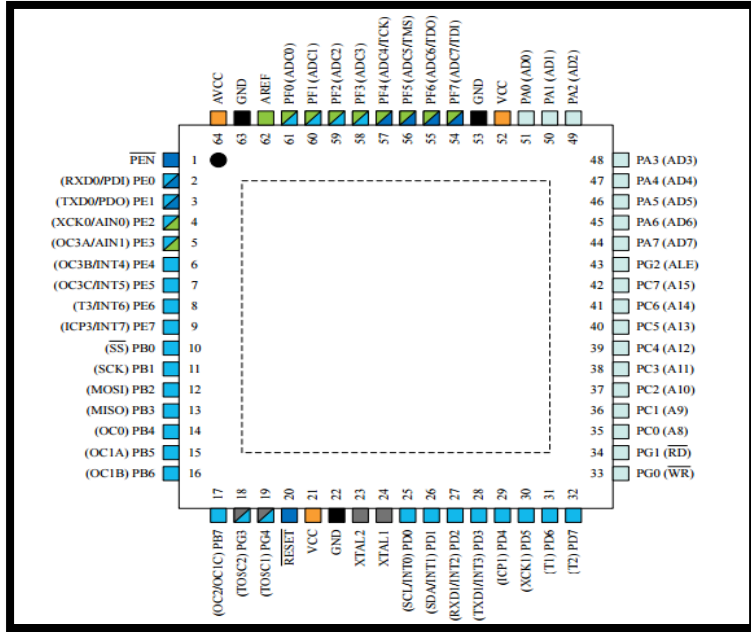


# LEVEL-2 : Datasheet 읽어 보기

- IC칩 모델명 검색 시 “datasheet” 단어를 추가하여 구글 검색
- CPU, Flash memory 위주로 datasheet 읽어 보기
- 처음엔 잘 모르겠어도 여러 번 반복해서 읽어 본다.
- 특히 Pin Map과 Memory Map 부분을 자세히 본다.



(CPU 예제)



# Pin Map / Instruction Set (Flash Memory 예제)

## 3. PIN CONFIGURATION SOIC 150 / 208-MIL

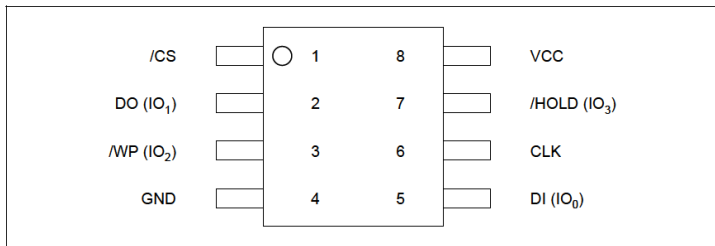


Figure 1a. W25Q16BV Pin Assignments, 8-pin SOIC 150 / 208-mil (Package Code SN & SS)

## 11.2.4 Instruction Set Table 3 (ID, Security Instructions)

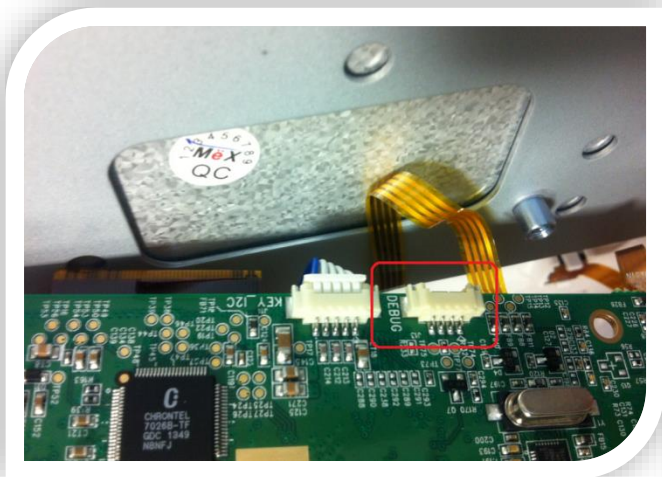
INSTRUCTION NAME	BYTE 1 (CODE)	BYTE 2	BYTE 3	BYTE 4	BYTE 5	BYTE 6
Release Power down / Device ID	ABh	dummy	dummy	dummy	(ID7-ID0) <sup>(1)</sup>	
Manufacturer/ Device ID <sup>(2)</sup>	90h	dummy	dummy	00h	(MF7-MF0)	(ID7-ID0)
Manufacturer/Device ID by Dual I/O	92h	A23-A8	A7-A0, M[7:0]	(MF[7:0], ID[7:0])		
Manufacture/Device ID by Quad I/O	94h	A23-A0, M[7:0]	xxxx, (MF[7:0], ID[7:0])	(MF[7:0], ID[7:0], ...)		
JEDEC ID	9Fh	(MF7-MF0) Manufacturer	(ID15-ID8) Memory Type	(ID7-ID0) Capacity		
Read Unique ID	4Bh	dummy	dummy	dummy	dummy	(ID63-ID0)



# Level-3: Debug Port에 연결해 보기

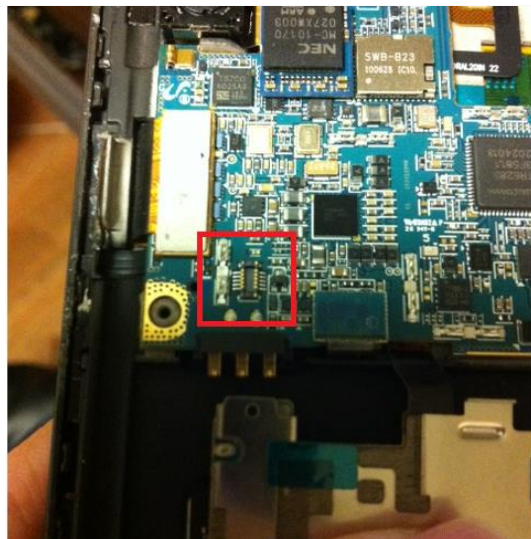
- UART
  - Universal asynchronous receiver/transmitter
  - 하드웨어 통신 규약의 한 종류
  - 각종 디버그 메시지를 보거나, shell access 권한을 획득할 수 있다.
- JTAG
  - Joint Test Action Group
  - 하드웨어 디버깅의 국제 표준
  - 대상 장비를 실시간 디버깅하거나, 펌웨어를 획득할 수 있다.
- USB
  - adb shell, USB2TTL(UART), 저장장치
  - PC에 usb 케이블 연결 시 인식되는 장치를 확인한다.

# 다양한 연결 Port들을 찾아본다.



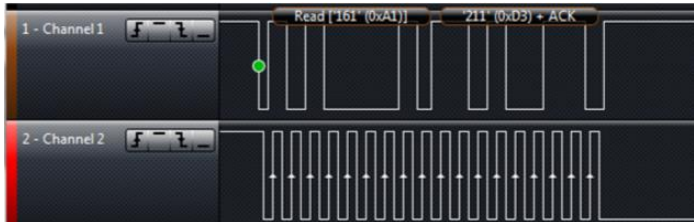
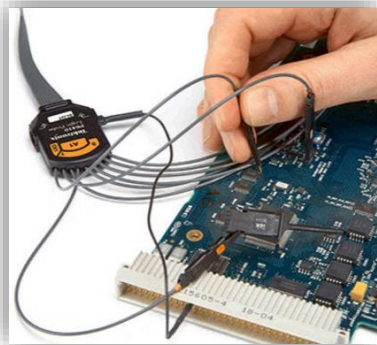
Wallpad UART

Smartphone JTAG

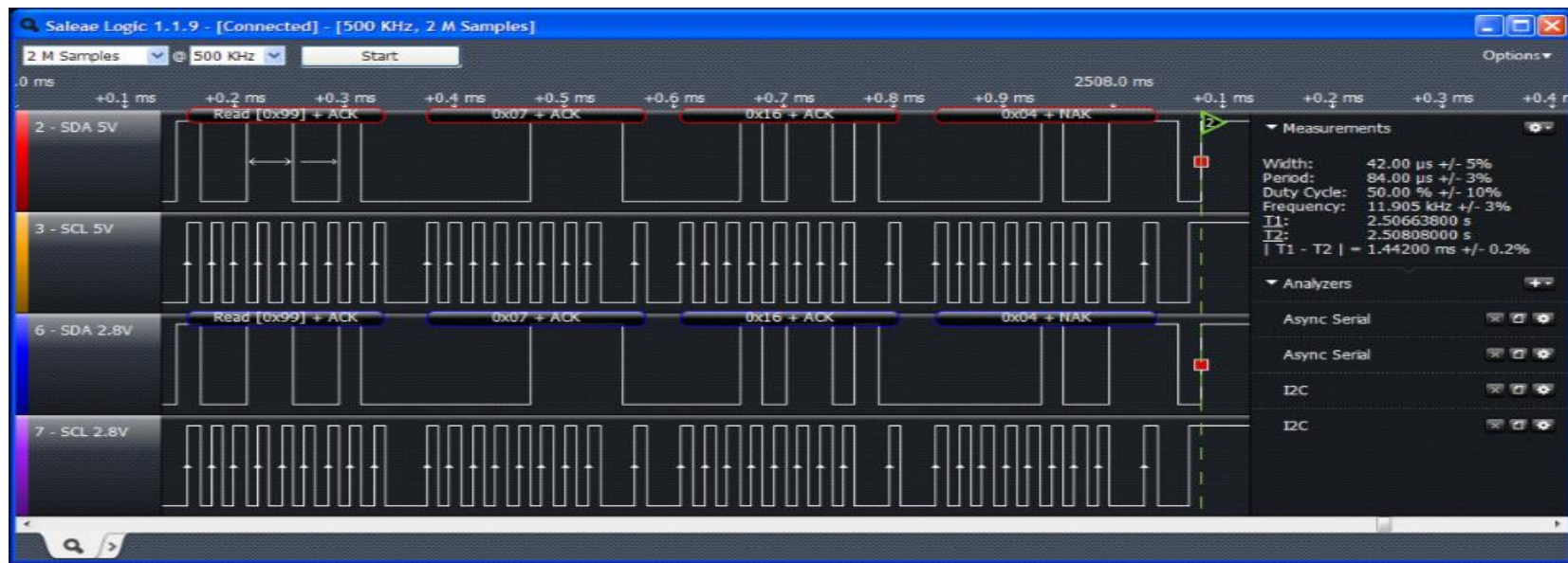


# Level-4 : 전기 신호 분석해 보기

- 신호분석기(Logic Analyzer), 오실로스코프(oscilloscope) 이용
- 하드웨어 통신 신호 캡처/디버깅이 가능하다.
- 특정 핀의 용도 파악, 민감 데이터 유출 시 유용하다.
- 하드웨어의 세계에 대해 더욱 잘 이해할 수 있게 된다.
  - Clock 및 Rising/Falling edge에 대한 이해

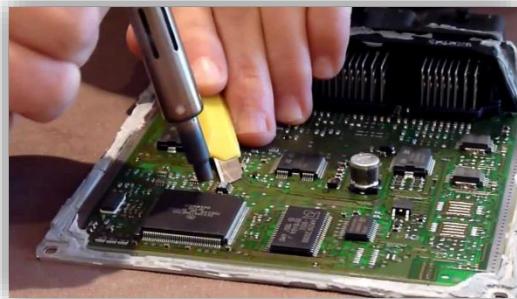


무엇보다 이런 화면을 보고 있으면 친구들이  
나를 진짜 하드웨어 해커라고 생각하게 됨



# Level-5 : Desoldering

- IC 칩을 PCB에서 분리해 내는 작업을 의미
- IC 칩 교체 작업 시 필요함. (수리, Upgrade)
- Flash Memory dump 시 필요함.
  - 떼어 낸 Flash Memory 칩을 아두이노 등에 연결하여 READ Command 전송
- IC Pin Hijacking 시 필요함.
  - Ex> CPU와 Modem 사이에 통신하는 AT Command 신호 변조

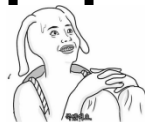


# iPhone Storage Upgrade





주의 : 만약 레고나 퍼즐 조립을 끝까지  
못 한다면 성격 상 안 맞을 수도..





# Level-6 : Side Channel Attack

- 간접적인 정보들을 기반으로 중요한 데이터를 획득해 내는 기술
- 소비 전력(Power analysis) 분석, 소요 시간 분석(Timing Attack), 방출되는 전자기파/소리 분석 등의 방법들이 사용 됨
- 쉬운 것에서부터 매우 어려운 것까지 다양한 기술들이 존재함



# 전류 소모량은 작업량에 따라 다르다.

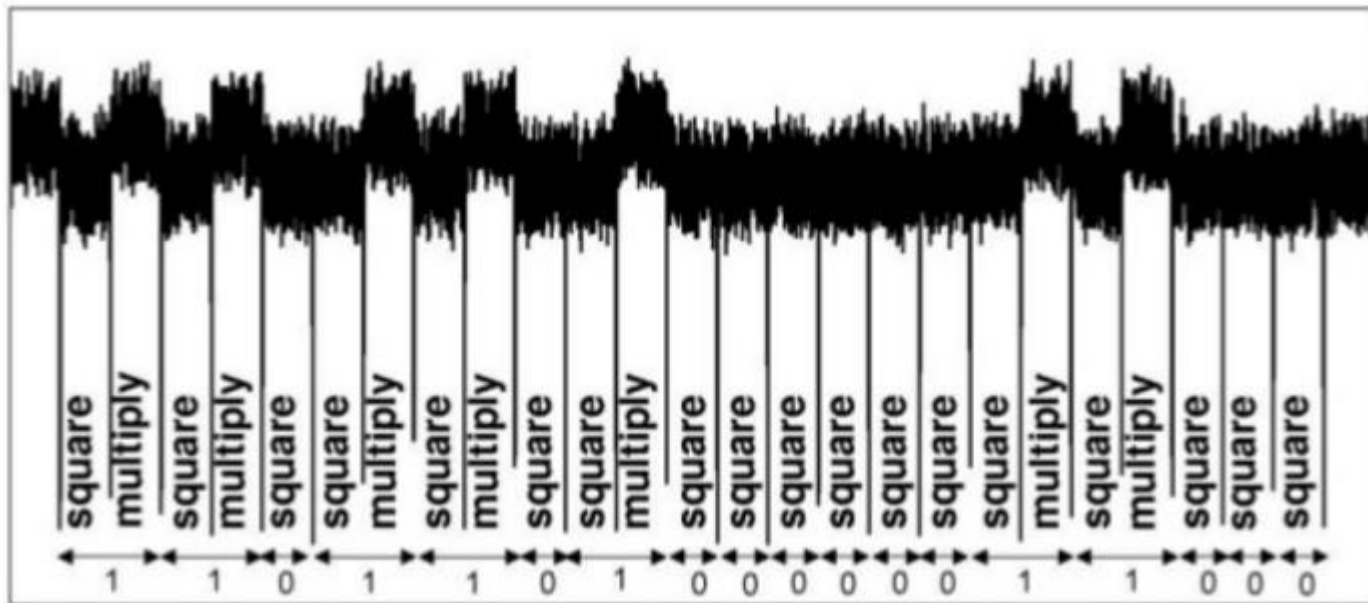


VS



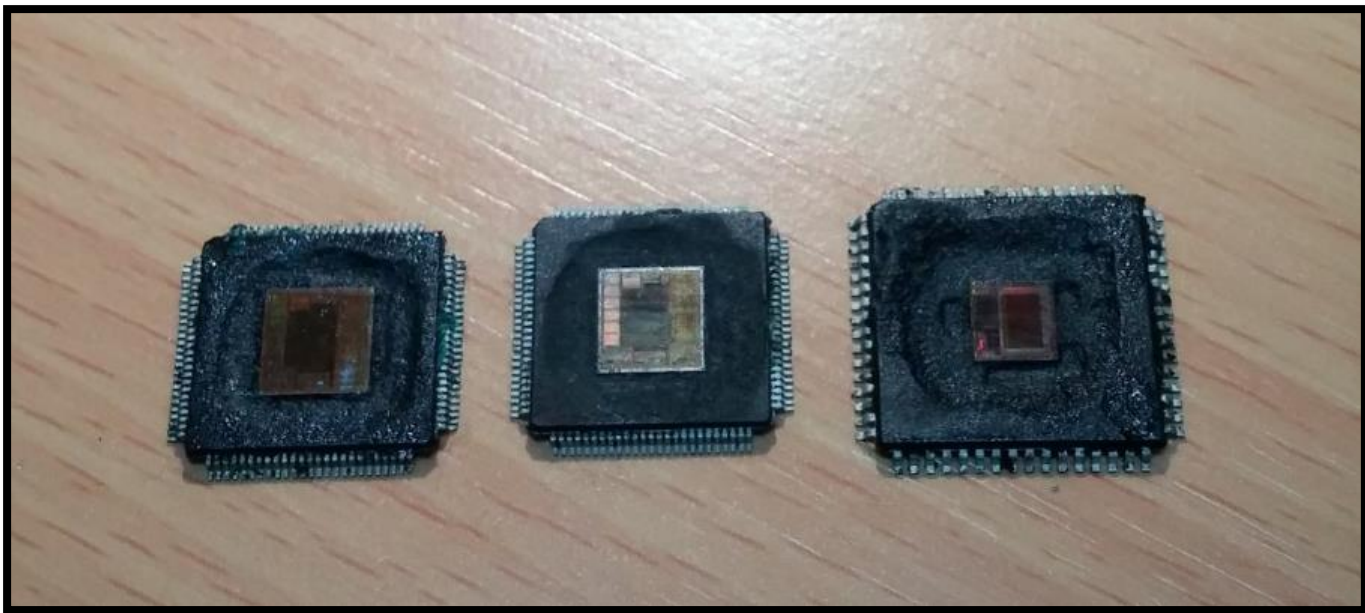
# Instruction에 따른 전력 소모

- Secret Exponent value of RSA



# Level-7 : Decapping & Imaging

- 칩의 Package를 제거한 후, IC 회로를 분석하는 작업

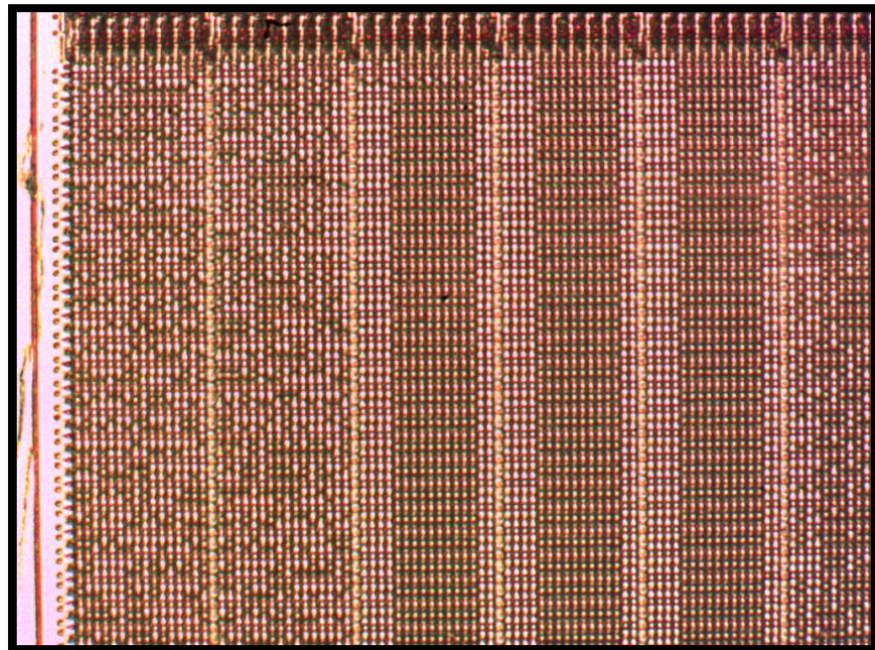
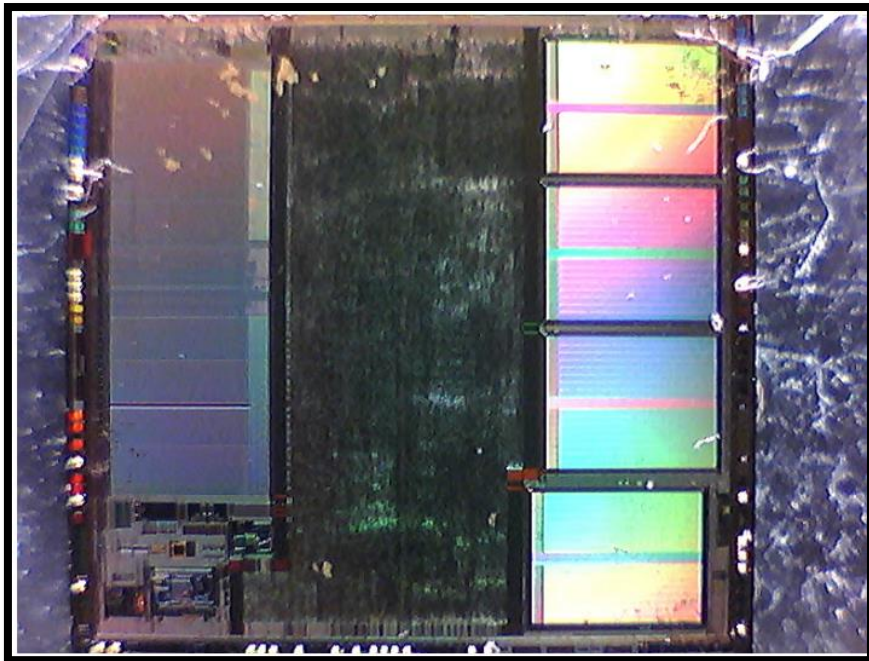


# Decapping 작업





# Optical Imaging 작업



출처 : <http://zacsblog.aperturelabs.com/>

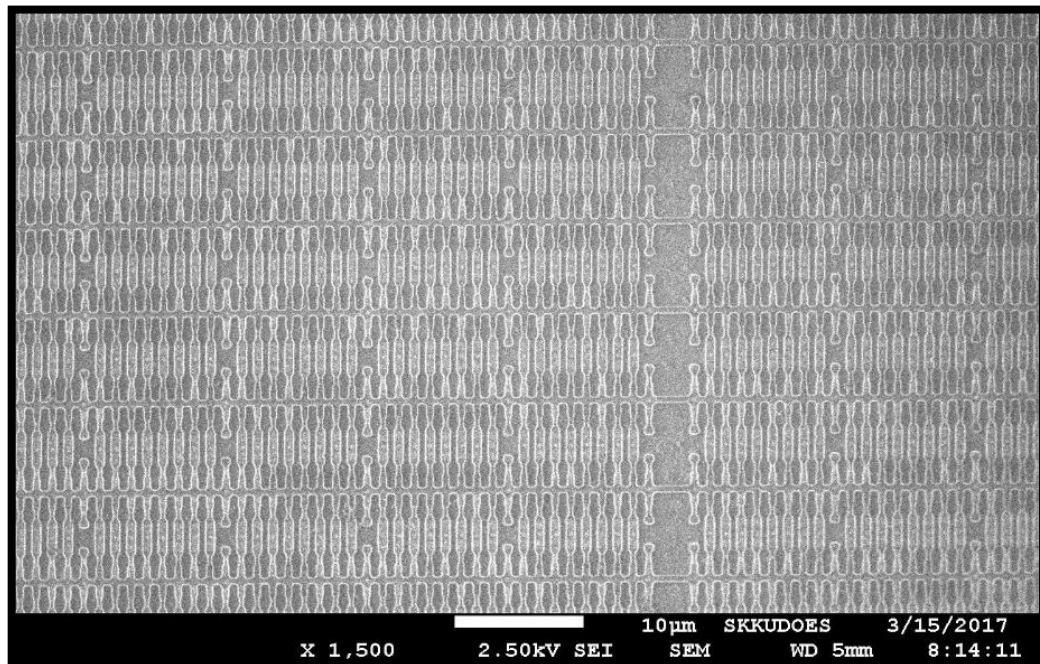
# SEM Imaging 작업





# SEM Imaging 결과

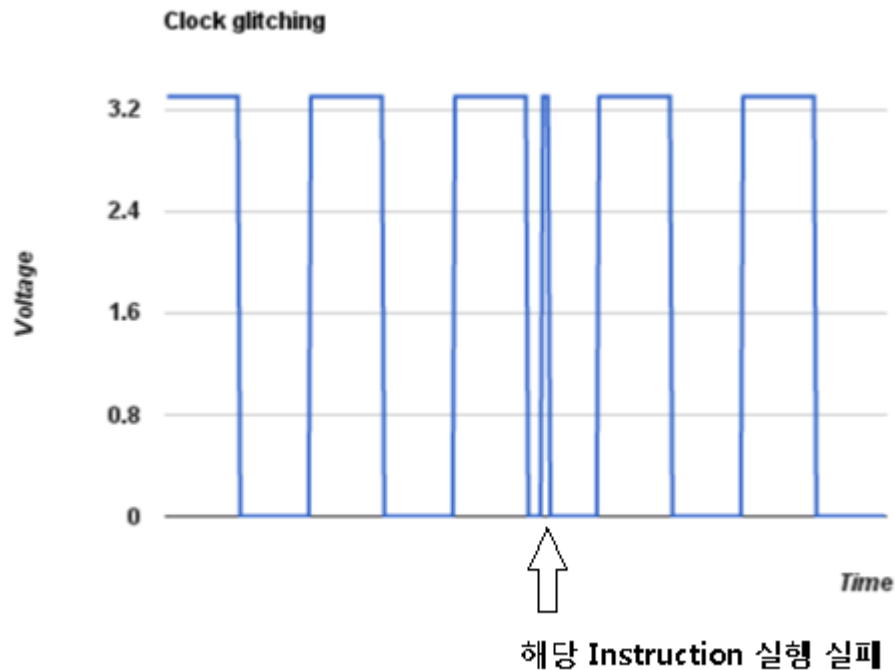
- 자아알 보면 메모리셀간의 차이점이!



# Level-8 : Glitching Attack

- IC 칩에 의도적인 오류를 발생시켜 오작동을 유발하는 기술
  - 이 오류가 때로는 좋은 "버그"가 되어 돌아온다.
  - Glitching의 뜻 : 프로그램 오류, bug, exploit, 어지러운
- 대표적인 Glitching attacks
  - Clock glitching : 비정상적인 clock을 인가하여 오작동 유발
  - Voltage glitching : 전압을 순간적으로 올리거나 내려서 오작동 유발
  - Thermal glitching : 정상 범위를 벗어나는 온도(hot or cold)로 오작동 유발
- 효과
  - Firmware dump, crypto break, bypass secure-boot or some checks

# Clock Glitching Attack 예시



# Clock Glitching Attack 예시

## - Bypass secure booting

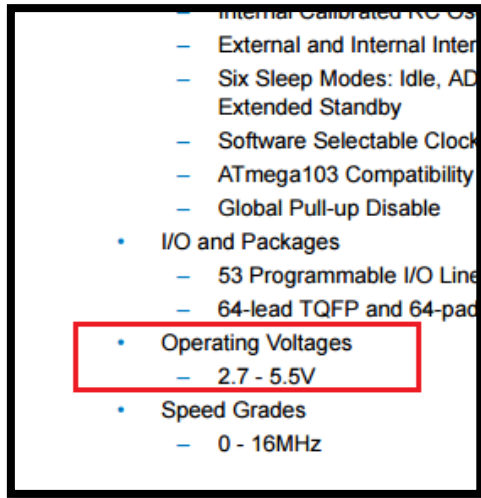
```
      LDA    #01h
      AND    $0100           ;the contents of the first byte of EEPROM is checked
loop:  BEQ    loop           ;endless loop if bit 0 is zero
      BRCLR  4, $0003, cont  ;test mode of operation
      JMP    $0000           ;direct jump to the preset address
cont:  LDA    #C0h
      STA    $000D           ;initialize the serial asynchronous port
      CLR    $000E
      BSET   2, $000F
      LDX    #50h
wait:  BRCLR  5, $0010, wait  ;upload user code
      LDA    $0011
      STA    , x
      INCX
      DEC    $0050
      BNE    wait
      JMP    $0051           ;jump to the user code
```

Figure 41. Example of the bootloader code responsible for security in MC68HC05B6 microcontroller

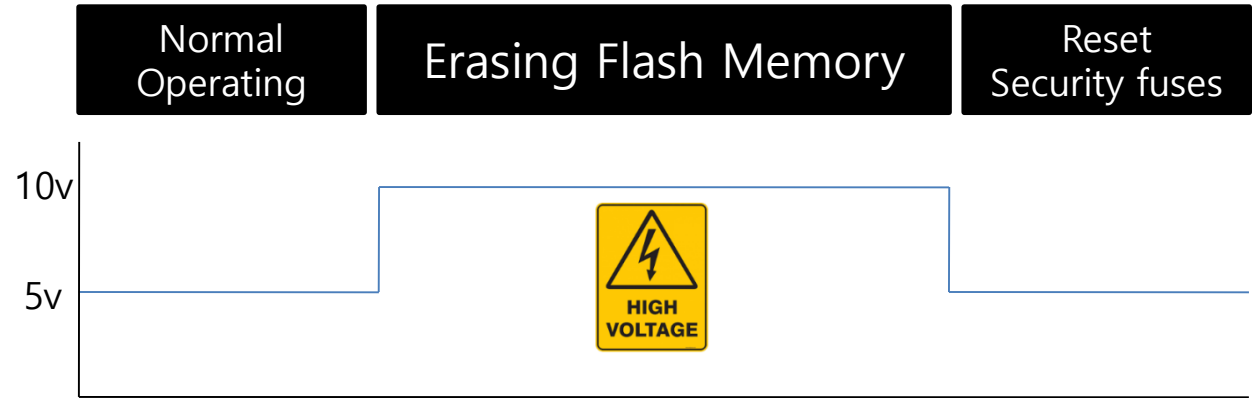
1. Secure Boot 관련 코드
2. User code loading 루틴
3. EEPROM에 저장된 security bit 체크
4. 만약 0이라면, 더 이상 진행하지 않음 (endless loop)
5. Clock Glitching을 통해 해당 Instruction이 Fail되게 만들면 Endless loop 탈출 가능

# Voltage Glitching Attack 예시

## - Bypass code protection



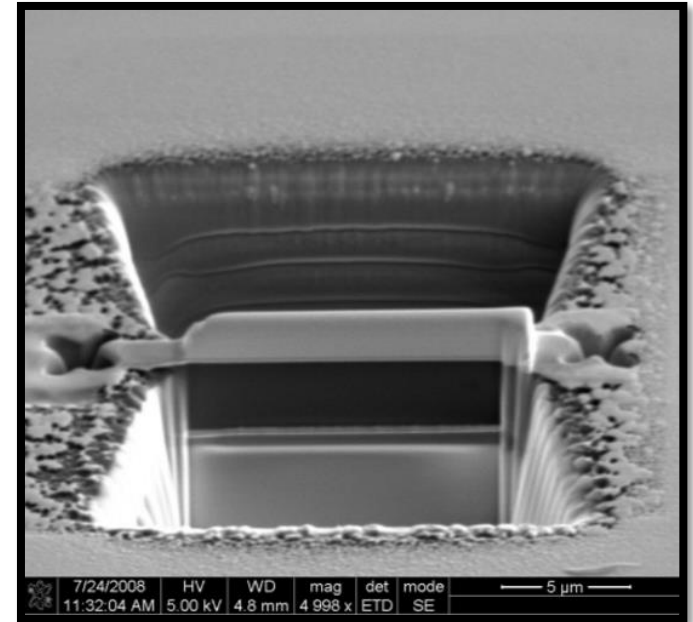
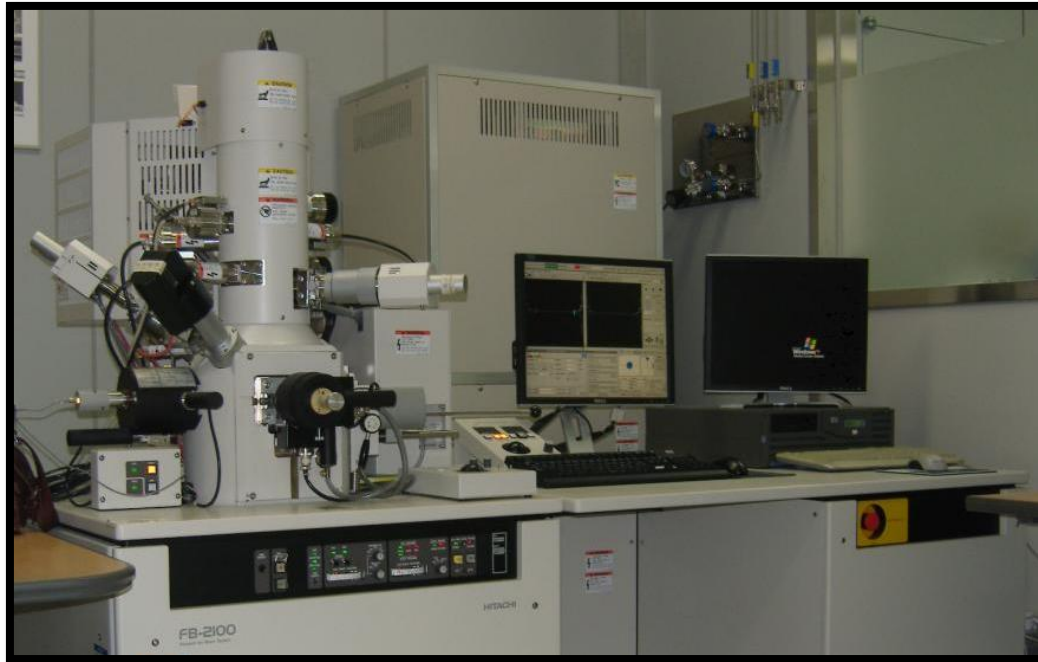
Datasheet



# Level9 : FIB attack

- FIB = 집속이온빔시스템(Focused ion beam system)
- Ga이온 빔을 회로 내의 원하는 위치에 집속(Focus)시켜, 회로를 식각/증착 할 수 있는 장비
  - 식각 : 회로 패턴을 제거
  - 증착 : 회로 패턴을 추가 (기체 -> 고체)
- 회로에 수정을 가할 수 있음!
- Code Protection을 break할 수 있음
  - Security bit에 해당하는 메모리 소자의 출력을 GND나 VCC로 강제 연결시킴

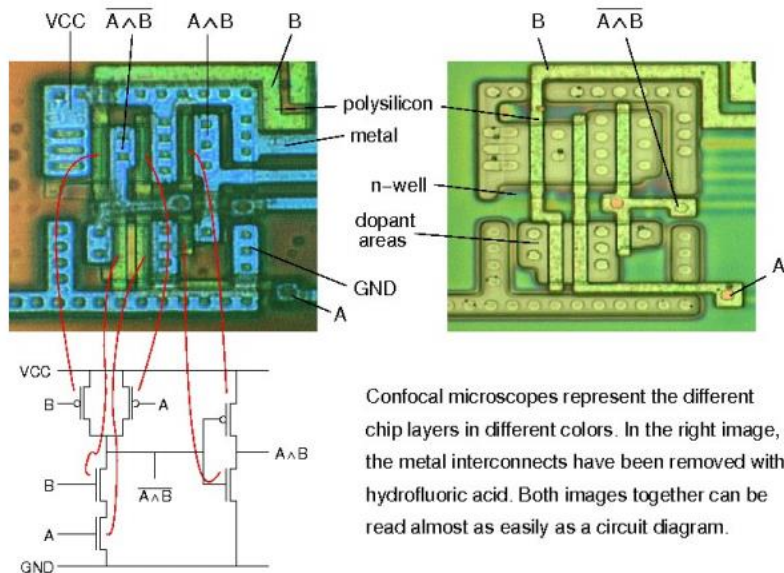
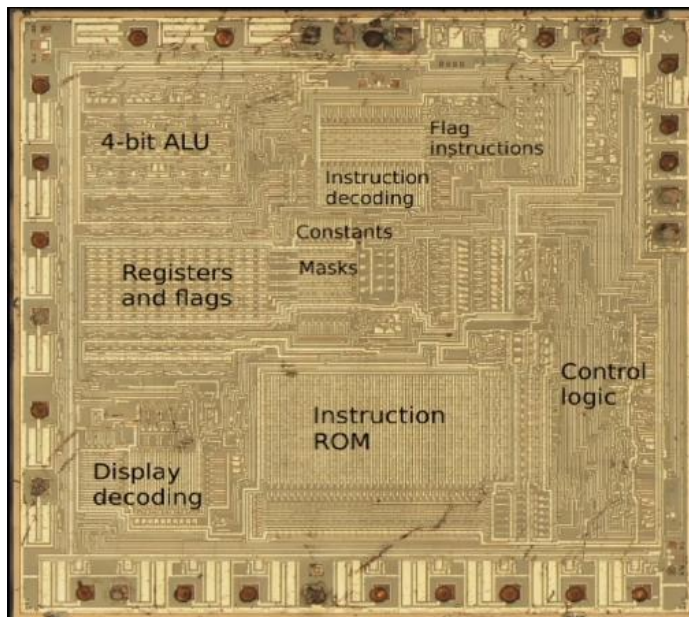
# FIB 장비 예시





# Level10 : IC Chip Reversing

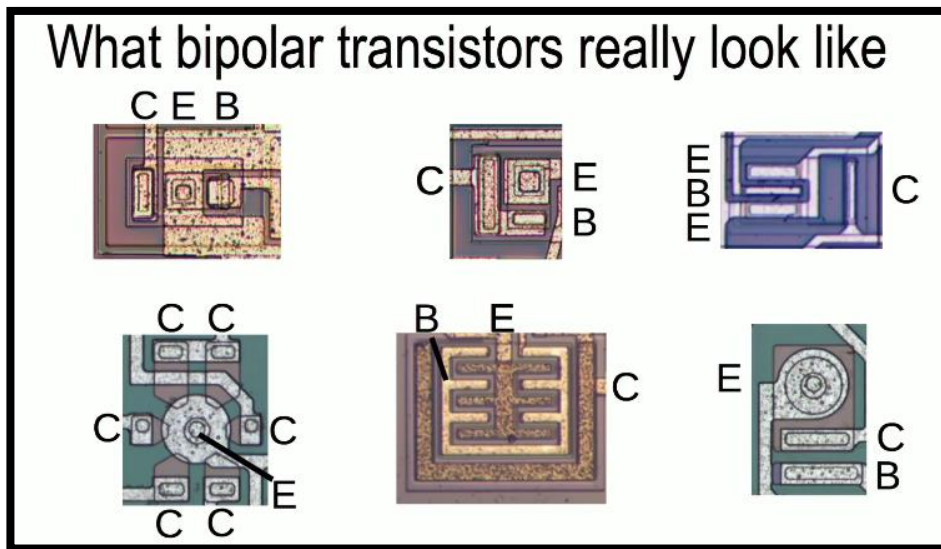
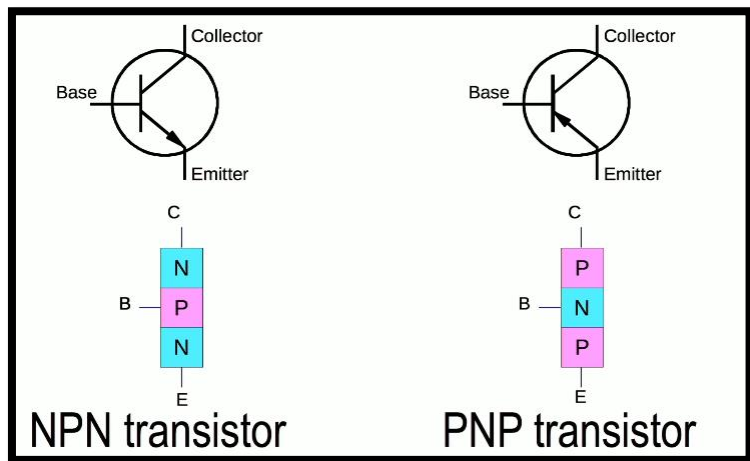
- IC Chip의 회로를 분석하여 용도를 attack point를 파악하는 작업
- 반도체공정 및 회로이론에 대한 지식이 뛰어나야 함



Confocal microscopes represent the different chip layers in different colors. In the right image, the metal interconnects have been removed with hydrofluoric acid. Both images together can be read almost as easily as a circuit diagram.

Picture courtesy of Dr Markus Kuhn

# Book VS Real World



출처 : <https://www.youtube.com/watch?v=aHx-XUA6f9g>

# 하드웨어 해킹을 통해 얻을 수 있는 것들

- 임베디드 장비(공유기, CCTV 등) 0-day 취약점 헌팅
  - KISA 신규 취약점 신고포상제로 제보, 컨퍼런스 발표 등
- 컴퓨터 작동에 대한 더욱 깊은 이해
  - Clock, Transistor, Logic Gate, Interrupt,
- Fun! Fun!!
  - DIY : 하드웨어 지식이 쌓이면 원하는 장난감, 아이디어 제품을 직접 만들 수 있다.

# 하드웨어 해킹 사례들

스마트폰

스마트 카드

드론

충전기

도어락

EGG

스마트카

CCTV

인터넷 폰

스카다

스마트  
TV

공유기

로봇청소기

가전기기

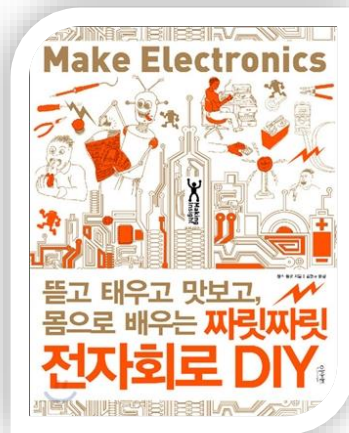
의료기기

현금인출기

인공위성

# 하드웨어 해킹 공부 방법 추천

- 추천 서적 for newbies
  - 뇌를 자극하는 하드웨어 입문
  - 만화로 쉽게 배우는 전기
  - 짜릿짜릿 전자회로 DIY
  - 당근이의 AVR 갖고 놀기
  - 일렉트릭 유니버스
  - 임베디드 레시피
- 추천 사이트
  - Youtube.com은 진리다!
  - 당근이의 AVR 갖고 놀기 커뮤니티
    - <http://cafe.naver.com/carroty>
  - HACKADAY
    - <http://hackaday.com>



# 장비 사용 실습 - 공용기기지원

- 고려대 <https://medicine.korea.ac.kr>
- 경희대 <https://crf.khu.ac.kr>
- 나노종합기술원 <https://www.nnfc.re.kr>
- 동국대 <https://equips.dongguk.edu>
- 서울대 <http://irf.snu.ac.kr>
- 성균관대 <http://ccrf.skku.edu>
- 세종대 <http://rfc.sejong.ac.kr>
- 아주대 <http://cmcm.ajou.ac.kr>
- 인천대 <http://www.uirf.or.kr>
- 조선대학교 <http://www.chosun.ac.kr>
- 충남대 <http://www.cnucrif.re.kr>
- 한국산업기술대학교 <http://cec.kpu.ac.kr>

**장비 및 담당자 안내**

HOME > NNFC서비스안내 > 장비 및 담당자 안내

전체 Nanodevice MEMS Sensor Nano-Bio Nanomaterial **Measurement & Analysis** Simulation Tool

장비별 적용 가능한 Wafer(시편) 규격 정보 안내 | 장비책자 바로가기

전체 검색어를 입력하세요.

장비	담당자	연락처	이메일
Thickness Measurement system(Nanospec 9100) by Nanometrics	손우식	042-366-1708	✉
Micro Raman Spectrometer(FEX) by NOST, Korea	현문섭	042-366-1706	✉
UHR FE-SEM(SU8230) by Hitachi High-Technologies Corp., Japan	현문섭	042-366-1706	✉
X-ray Photoelectron Spectrometer (XPS) System by ThermoFisher Scientific	김경태	042-366-1711	✉
Cs-Corrected Scanning Transmission Electron Microscopy by JEOL	박윤창	042-366-1705	✉
FE-TEM (Tecnai G <sup>2</sup> F30 S-TWIN) by FEI	박윤창	042-366-1705	✉
In-situ TEM (JEM-3011 HR) by JEOL	유정호	042-366-1703	✉
FE-TEM (JEM-2100F HR) by JEOL	유정호	042-366-1703	✉
Ion Milling System (PIPS™) by Gatan	유정호	042-366-1703	✉
Precision Etching Coating System (PECS™) by Gatan	유정호	042-366-1703	✉

실験신청 및 관리  
NNFC서비스 신청  
신청 서비스 상태확인

NNFC 기술소개

이용절차 안내  
보유장비 및 연락처  
이용절차 및 수가 등

원스톱하이라인서비스  
공정부문 리셉션

# 마지막으로..

- 공부를 진짜 열심히 해야 한다!
  - 노력 없이 얻어지는 것은 없다.
- 즐겁게 공부하는 방법을 터득해야 한다.
  - 그룹 스터디, 컨퍼런스 발표, 업무로 경험할 수 있는 업체 취직 등
- 영어 공부는 필수다.
  - 100배 이상의 정보들을 흡수할 수 있다.





QnA

**감사합니다.**