Embedded System의 Firmware 획득하기

mongii@grayhash

펌웨어를 획득하는 7가지 방법

1. 제조사에서 공개하는 펌웨어 다운로드

2. 자동/수동 업데이트가 될 때 패킷 스니핑

3. UART 포트 접속

4. 논리적 취약점을 이용하여 Shell 접근 권한 획득 후 추출 (partition dump, /dev/mtdblock)

5. Flash Memory 덤프

6. JTAG 포트 접속

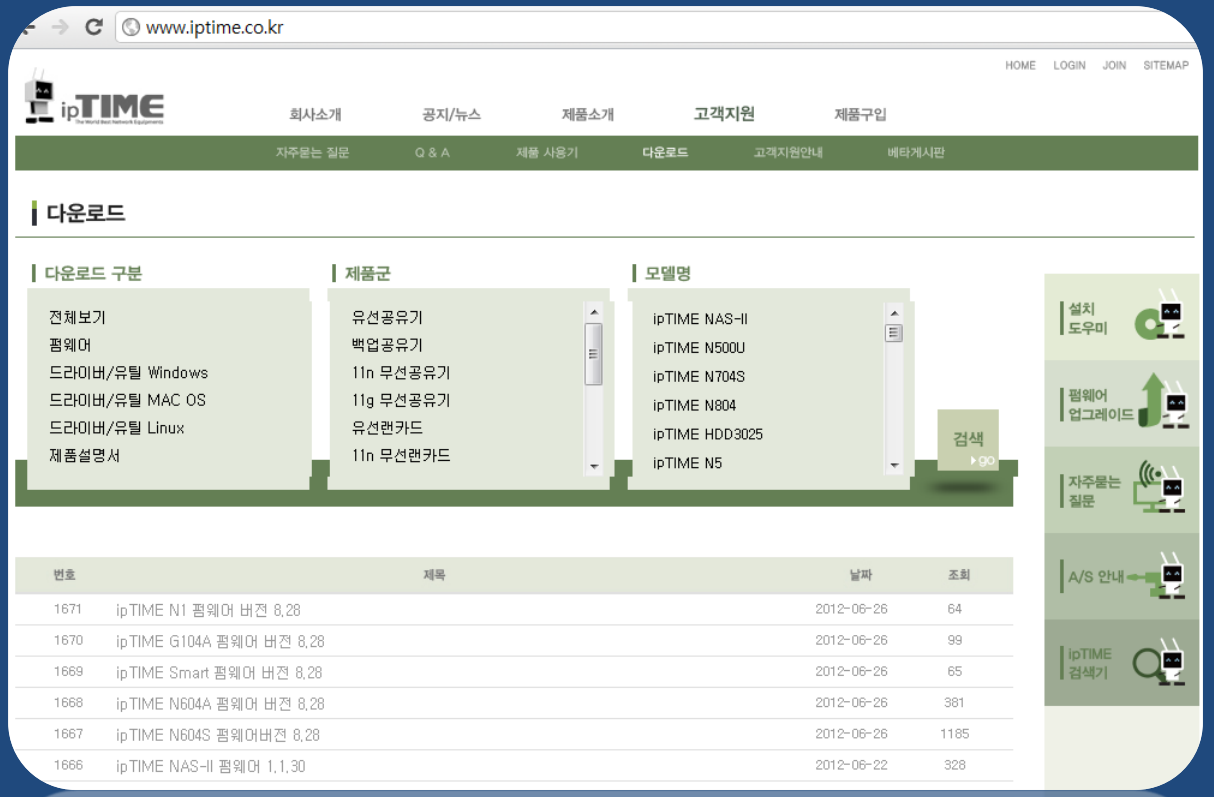
7. Programming Interface(ISP, ICSP)를 이용하여 추출

Firmware만 획득하면..

- 그 다음은..
- Software Hacking과 크게 다르지 않다!

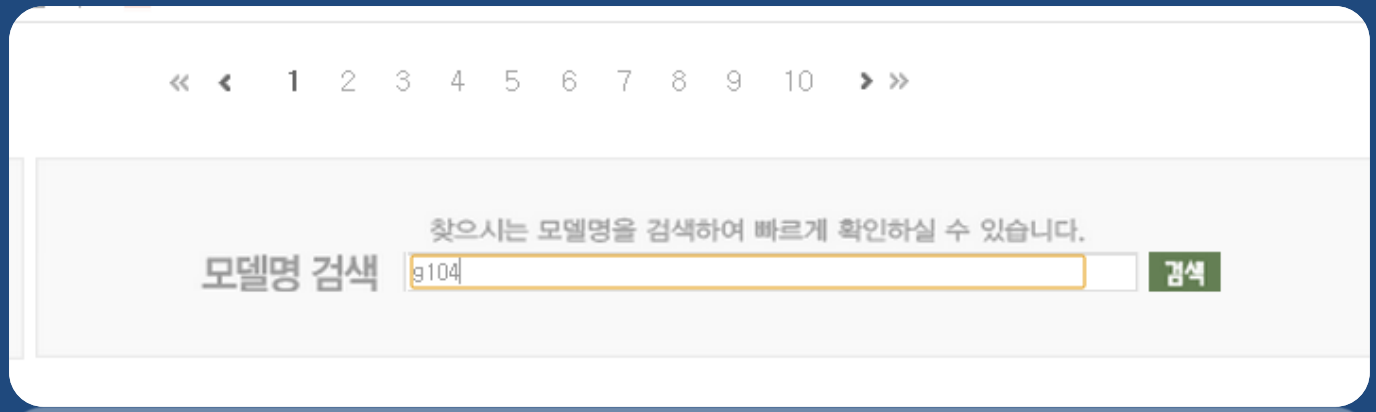
1. 제조사에서 공개하는 펌웨어 다운로드

업데이트 파일 다운받기



- http://www.iptime.co.kr/~iptime/bbs/zboard.php?id=sw_download

업데이트 파일 다운받기



번호	제목	날짜	조회
123	ipTIME **g104** 펌웨어 버전 8.46	2012-11-14	10896
122	ipTIME **g104** 펌웨어 버전 8.44	2012-11-07	2666
121	ipTIME **g104**i 펌웨어 버전 8.38	2012-09-06	1993
120	ipTIME **g104**M 펌웨어 버전 8.38	2012-09-06	6006
119	ipTIME **g104**BE 펌웨어 버전 8.38	2012-09-06	4293
118	ipTIME **g104**A 펌웨어 버전 8.38	2012-09-05	2098
117	ipTIME **g104**A 펌웨어 버전 8.32	2012-07-18	1069
116	ipTIME **g104**A 펌웨어 버전 8.30 (ipTIME 모바일 앱 지원)	2012-07-05	892

업데이트 파일 다운받기

다운로드

제 목	:	ipTIME G104 펌웨어 버전 8.46
다운로드 #1		g104_kr_8_46.bin (1.87 MB), Download : 8972

펌웨어 정보

- 펌웨어 버전: 8.46
- 펌웨어 상태: 정식 버전(자동 업그레이드 적용됨)

문제점 해결

- 8.44 버전에서 VPN서버 접속이 안되는 문제 해결

주의 사항

- 예기지 못한 상황으로 인하여 업그레이드가 실패할 경우, 아래의 문서를 참조하여 펌웨어를 복구할 수 있습니다.
  참조> [펌웨어 복구 하기]

업데이트 파일의 구성

- Boot-loader
- Kernel
- Ram Disk (initrd)
- Root File System (applications)

- 위와 같은 파일들이 하나의 파일로 덩어리져있다.
- 업데이트 파일의 성격에 따라 구성이 다를 수 있다.

업데이트 파일 관련 팁

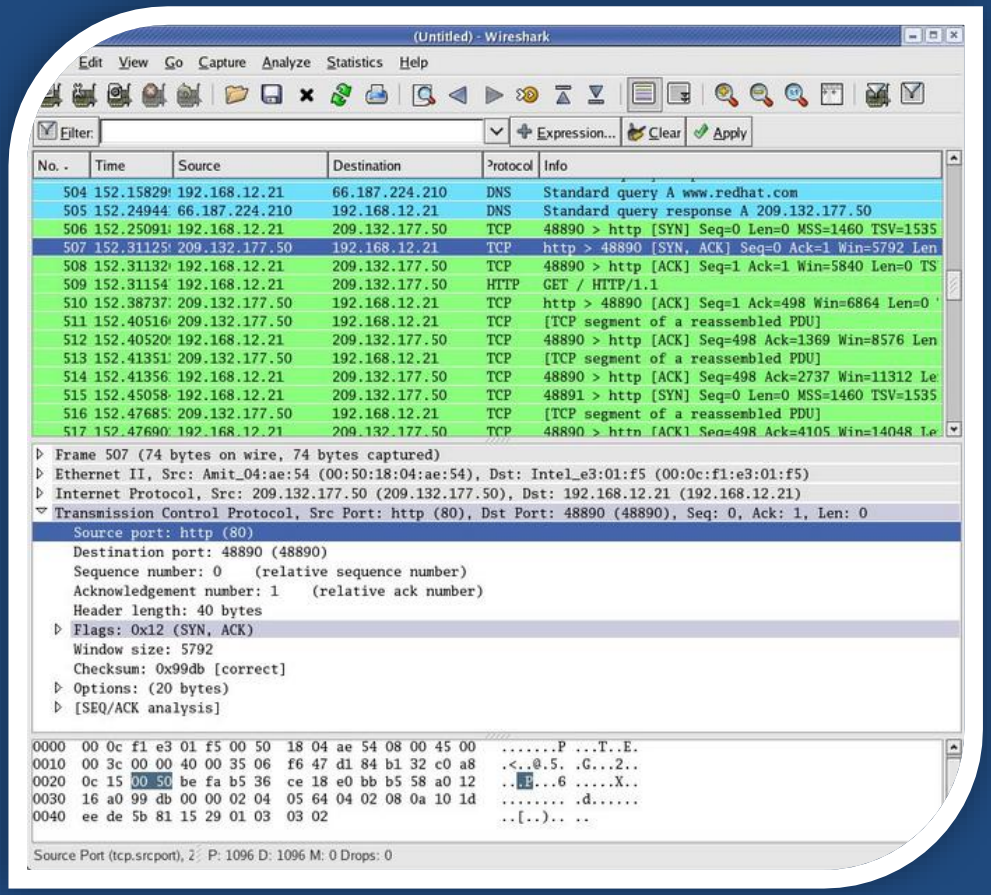
- 만약 최신 버전을 통해 펌웨어를 획득할 수 없었다면 (ex. 암호화) 오래된 버전으로부터 펌웨어 추출 후 취약점 분석을 한다.

- 업데이트 파일에 따라 구성이 다를 수 있다.
  - 부트로더, 커널, 디렉토리의 구성 등

- Strip이 되지 않은 업데이트 파일이 있을 수 있다!

2. 자동/수동 업데이트가 될 때 패킷 스니핑

자동 업데이트가 될 때 패킷 스니핑



자동 업데이트가 될 때 패킷 스니핑

- 언제 업데이트가 되는가?
  - 기기를 재부팅 할 때 => 최신 버전 체크
  - 특정 기간이 지났을 때 ex> 매월 1일
  - 특수한 방법으로 기기를 켤 때 ex> 파워키+리셋키

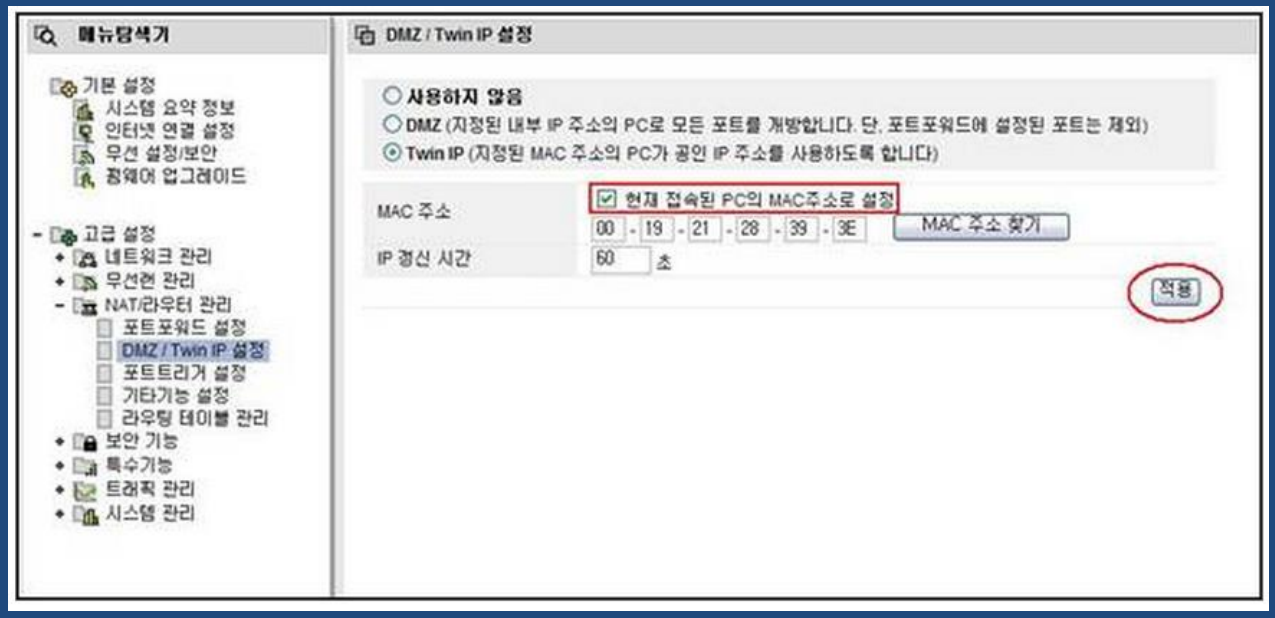
- 패킷 스니핑 방법들
  - 포트 미러링
  - TWIN IP
  - ARP Spoofing

포트 미러링

- 공격 대상 장비를 랜선에서 분리시킨 후,
- 그 랜선에 해커의 공유기를 연결
- 공유기에 대상 장비를 연결
- 공유기에 해커의 노트북을 연결
- “포트미러링” 기능을 이용하여 공유기로 오가는 모든 패킷을 해커의 노트북으로 전달

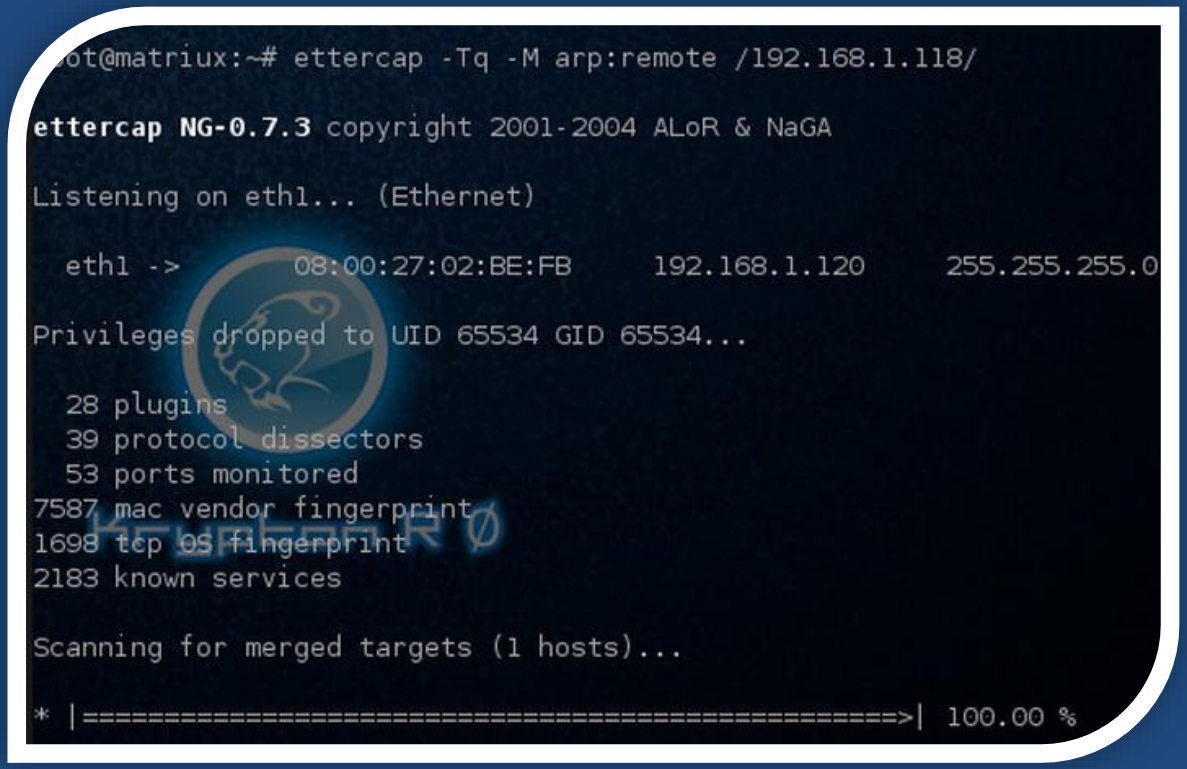
TWIN IP

- 공유기의 IP주소를 NAT로 물린 특정 MAC의 내부 기기와 동일시 하는 기능
- 즉, 마치 공유기가 없는 것 같은 효과를 얻게 됨
- 대상 기기가 특정 IP 상에서만 통신이 가능할 경우에 유용



ARP Spoofing

- Ettercap 툴 추천
  - ettercap -T -M arp /192.168.0.1/ /192.168.0.10/
    - 192.168.0.1 : 라우터, 192.168.0.10 : Sniffing 대상



3. UART PORT 접속

UART 포트 접속

UART PORT 접속

- Shell 접근이 가능할 시 파티션 덤프
- 부트로더 접근이 가능할 시 memory reading

4. 논리적 취약점 이용

논리적 취약점 이용

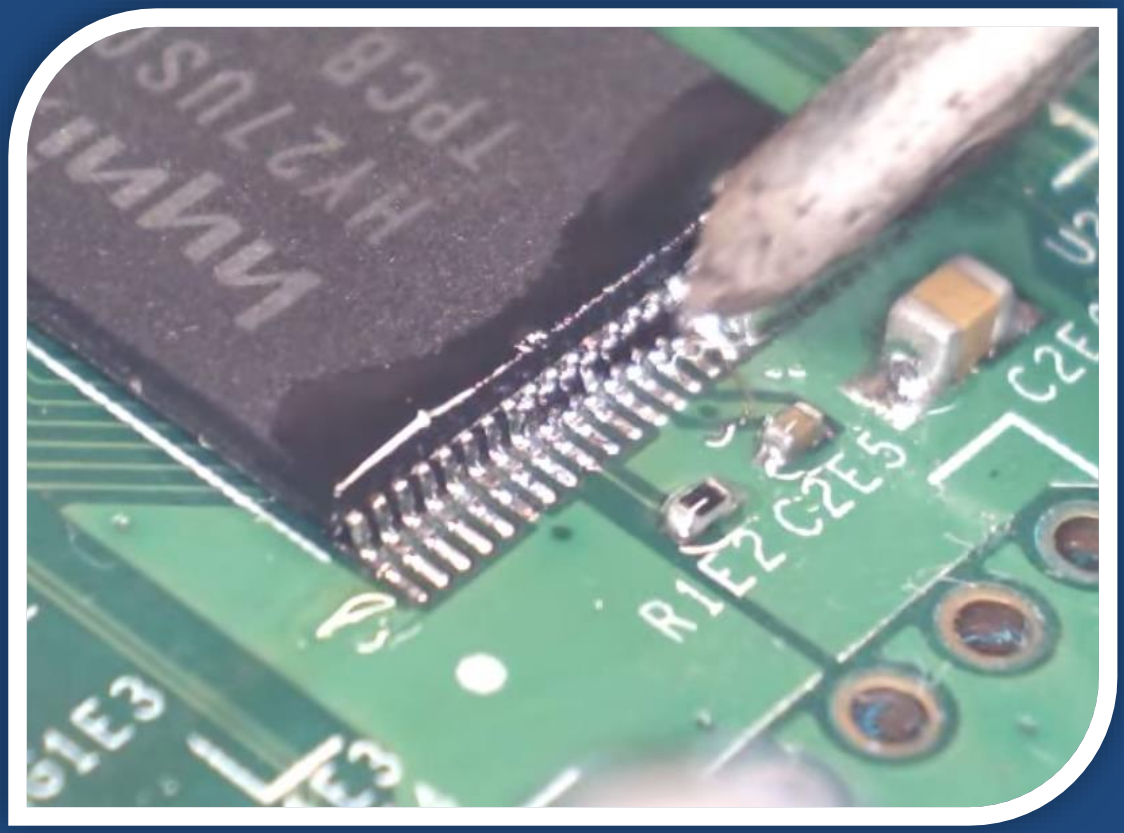
- 원격 백도어, Shell command execution 등의 단순한 취약점을 이용하여 Shell 획득
- /dev/에 접근하여 파티션 덤프

갤럭시S 파티션 덤프 예제

- 부트로더
  - dd if=/dev/block/bml1 of=/sdcard/boot.bin bs=512
- 커널
  - dd if=/dev/block/bml7 of=/sdcard/zImage bs=4096
- 파일시스템
  - dd if=/dev/block/stl9 of=/sdcard/factoryfs.rfs bs=4096

5. Flash Memory Dump

Flash Memory 덤프

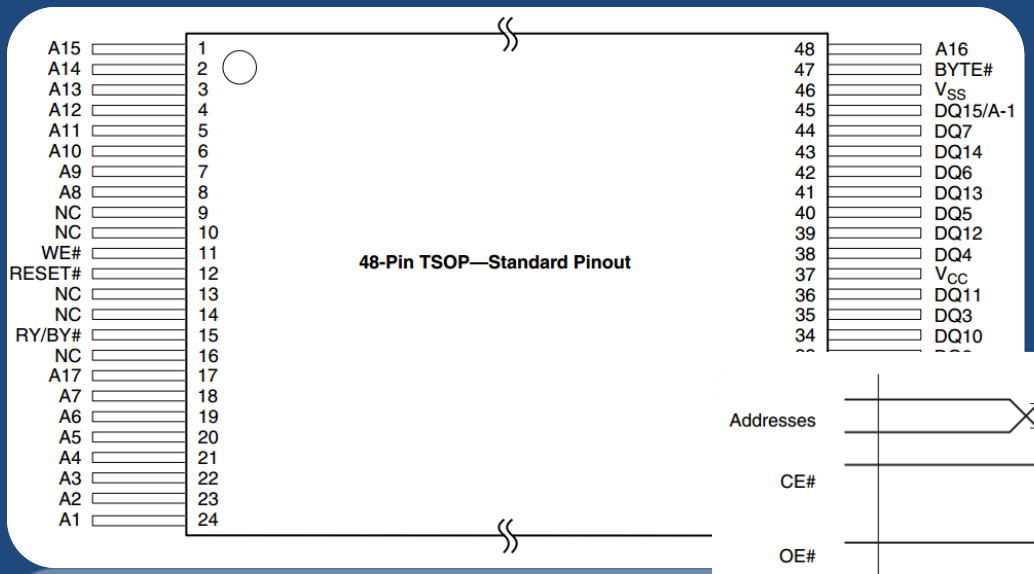


Flash Memory 덤프

- Socket Adaptor

Flash Memory 덤프

- DataSheet 학습



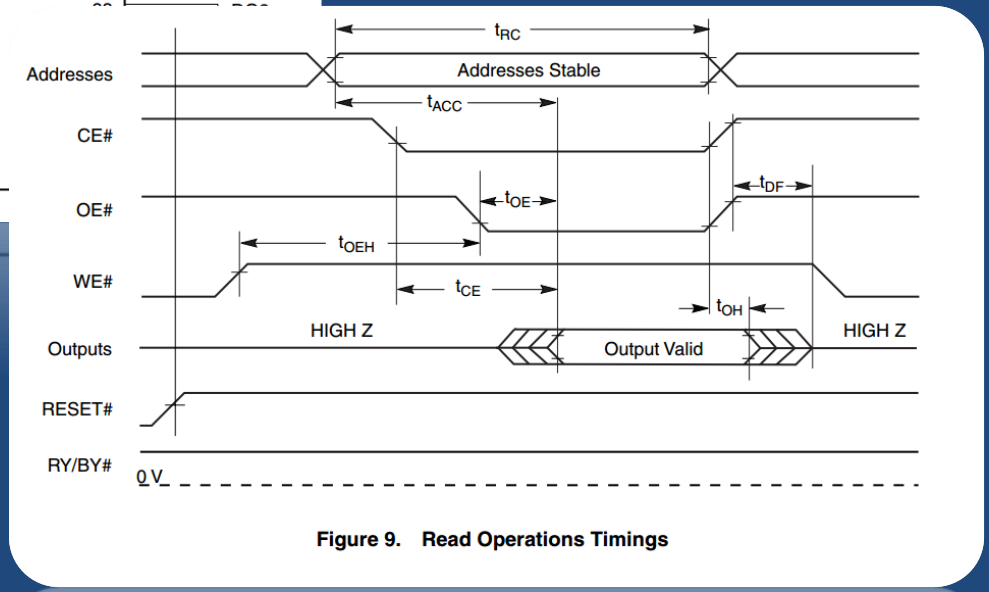
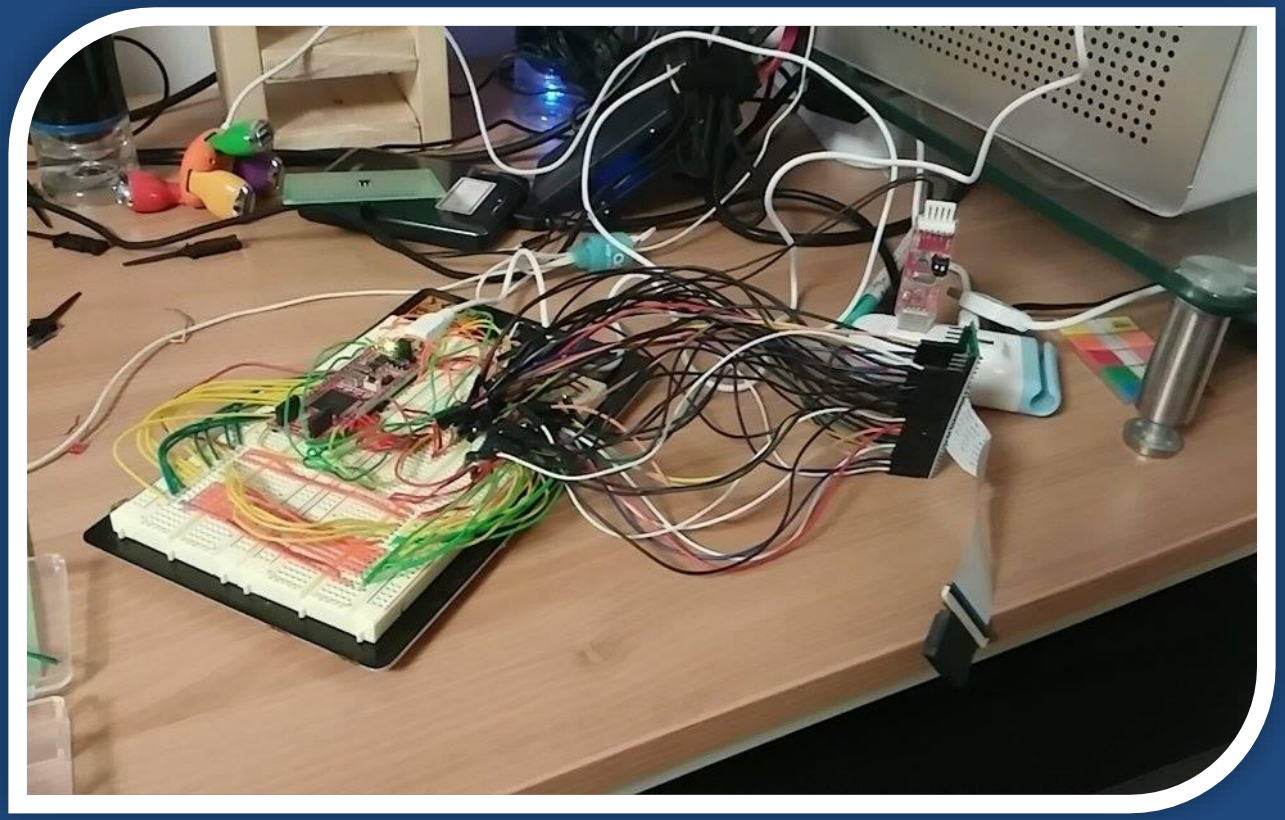


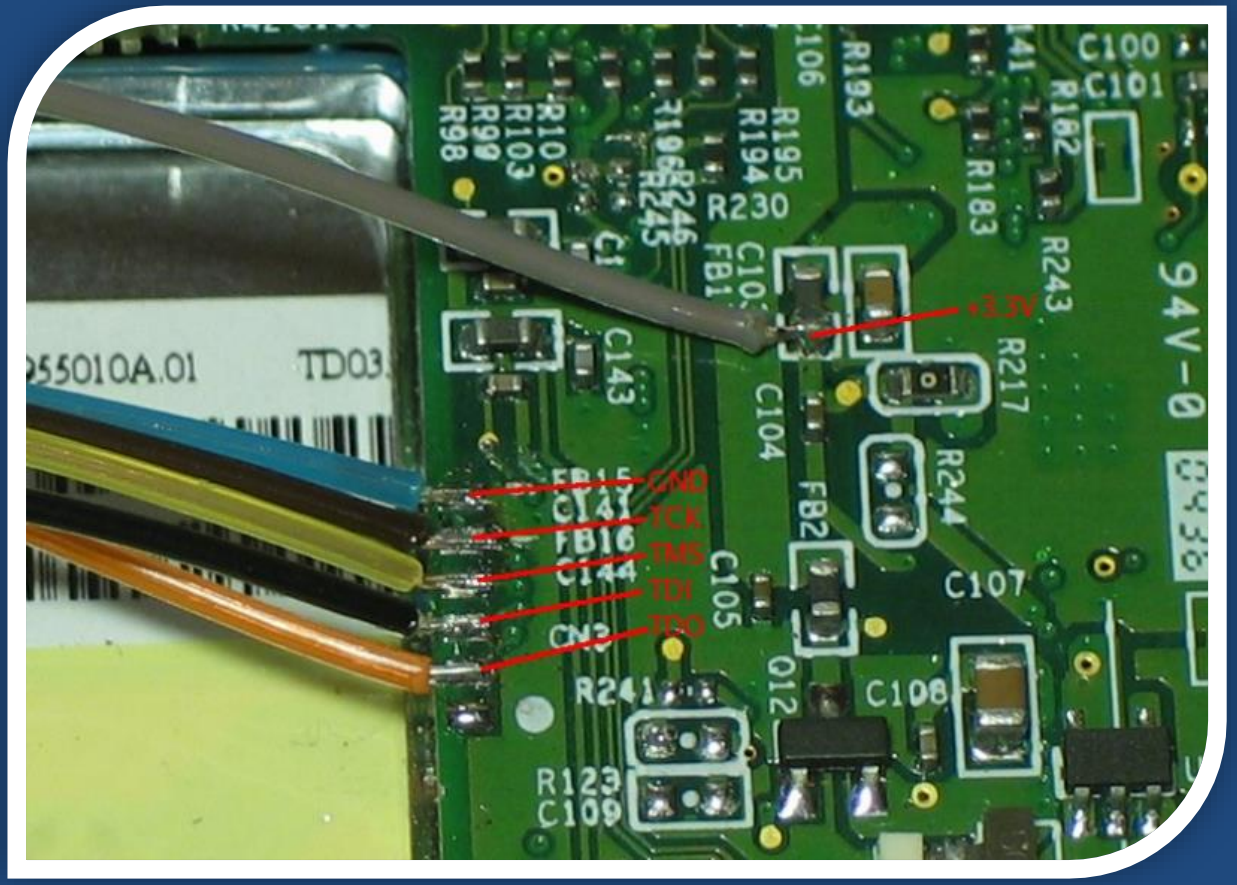
Figure 9. Read Operations Timings

Flash Memory 덤프

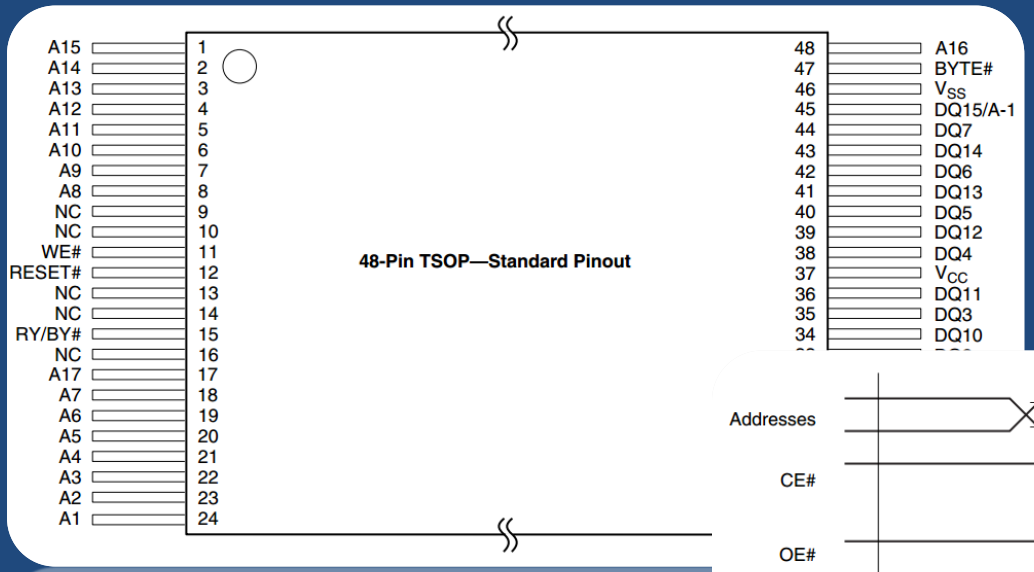


6. JTAG 포트 접속

CPU의 JTAG 포트 접속



JTAG을 통해 Flash Memory 제어



48-Pin TSOP—Standard Pinout

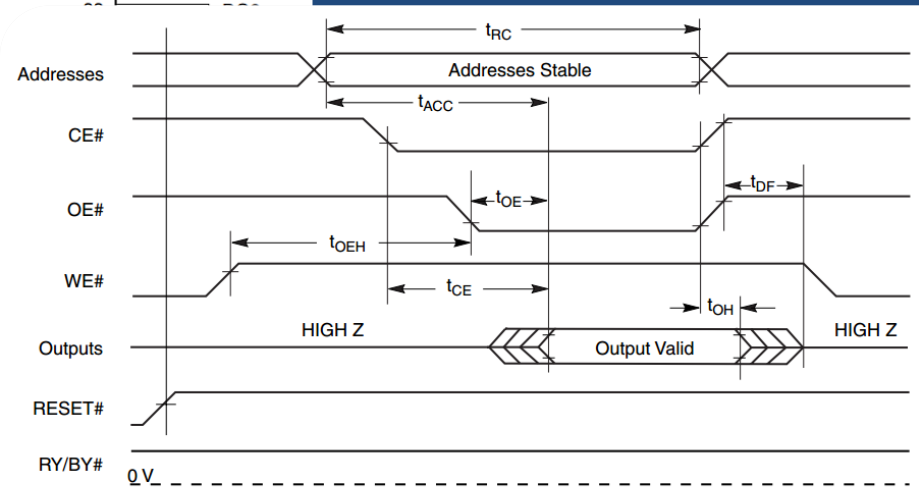


Figure 9. Read Operations Timings

7. Programming Interface (ISP, ICSP)를 이용하여 추출

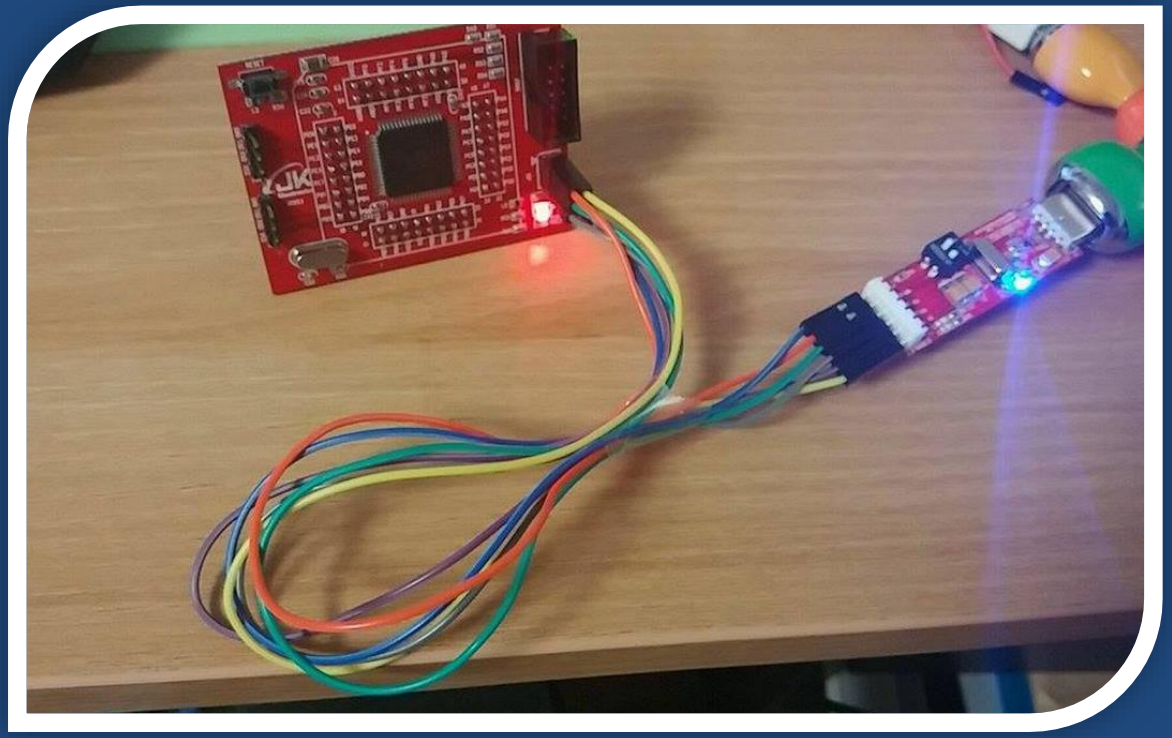
ISP란?

- In-System Programming
  - 플래쉬롬을 탈착하지 않고 프로그램 기록 가능한 형태를 의미
- 컴파일된 프로그램을 AVR 칩에 기록하는 작업을 "다운로딩" 이라고 부르며, 이를 퓨징(Fusing), 플래싱(Flashing), 혹은 프로그래밍(Programming)이라고 부르기도 함

AVR용 ISP 장비

USB-ISP 도구 연결

- VCC
- GND
- MOSI
- MISO
- SCK
- RST



- 해당하는 IDE 실행 후 firmware download

감사합니다.