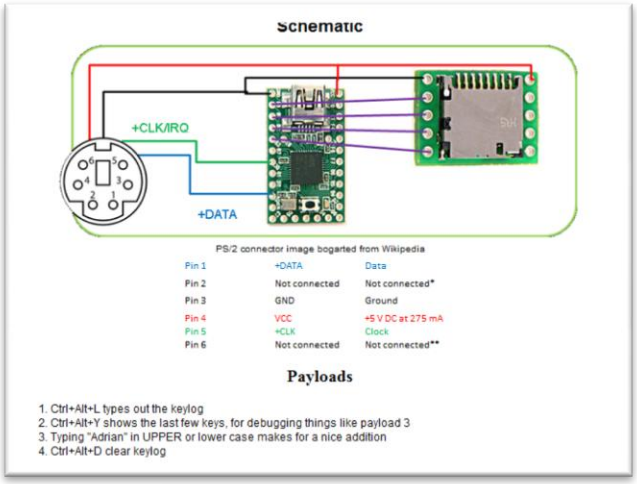
하드웨어 기반의 키보드 스니퍼 제작기 (1)

2012-05-10 몽이@해쿨

작년 말쯤 재미로 만들었던 "하드웨어 기반의 키보드 스니퍼" 제작 과정을 정리해 보려고 합니다. 제가 키보드 스니퍼를 만들게 된 계기는 어샤인(@beistlab.ashine)이 페이스북에 올린 한 포스팅을 읽고 나서였습니다.

http://www.irongeek.com/i.php?page=security/homemade-hardware-keylogger-phukd



골자는 약 $24 정도만 있으면 하드웨어 기반 키로거를 만들 수 있다이며, 이 해커가 PS/2 기반의 키로거 뿐만 아니라, HID USB, 블루투스 무선 키보드에 대한 키로거까지 만들었다는 내용입니다.

저는 마침 Logic Analyzer라는 무시무시한 하드웨어 분석도구를 질러놓은 상태였고, 이 것을 이용하면 나도 만들 수 있겠다 싶어서 시작을 해보았습니다.

[신비의 Logic Analyzer]

이 Logic Analyzer에 대해 간략하게 말씀 드리자면, 해외 사이트 http://www.saleae.com에서 판매하는 오실로스코프 대용으로 쓸 수 있는 소프트웨어+하드웨어 기반의 전기신호 분석 도구입니다. 한마디로 디지털 오실로스코프라고 생각하면 되며, 차이점은 캡쳐 된 전기신호를 분석하여 HEX 파일로 변환해주는 기능이 있다는 점입니다.

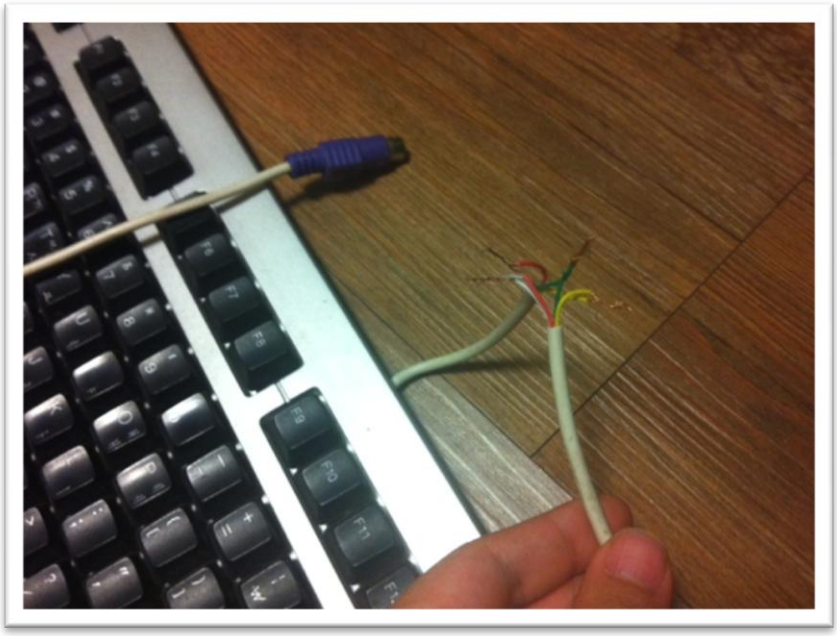
Logic Analyzer 구매에 앞서 이미 아날로그 오실로스코프를 가지고 있긴 했으나, 한 번 지나간 신호는 다시 볼 수 없는 후진 모델이어서 Logic Analyzer에 급 땡기게 되었던 것입니다.

Logic Analyzer의 가격은 한화로 약 17만원($149)!!.. 이며, 해외배송비가 $22가 추가됩니다. 홈페이지상엔 해외 배송 시 10일정도 소요된다고 나와있는데, 생각보다 빨리(한 5일 후) 받았던 것으로 기억합니다. 결제는 VISA 카드로 했었습니다. 저는 요즘엔 잘 안 쓰므로 혹시 써보고 싶으신 분이 계시면 1주일 정도 빌려드릴 수 있습니다. 해쿨이나 페북(@goohong.jung)으로 쪽지 주세요 ㅋ

다음으로 필요했던 것은 PS/2 기반의 키보드였습니다. 요즘엔 대부분 USB 키보드를 쓰기 때문에.. 집안 창고를 뒤적인 결과 겨우 하나를 발견할 수 있었습니다.

PS/2 커넥터 부분을 보았는데, PS/2가 생각보다 핀이 많았더군요... 무려 여섯 개!

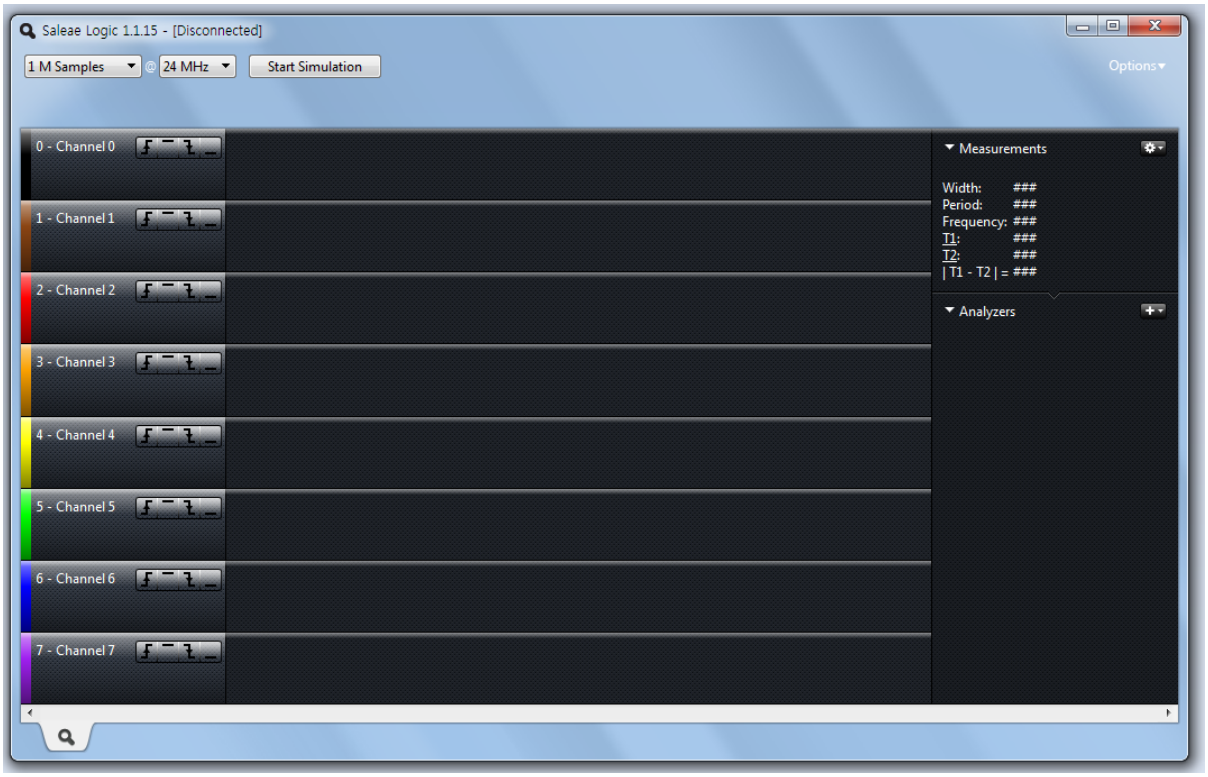
여튼 이 걸 보면서 이 커넥터와 PC의 커넥터 사이에 뭔가 프락시 역할을 하는 물건이 있어야겠다라고 생각하다가... 성격이 급해서 케이블 중간을 걍 짤라버립니다ㅋㅋ =_=



그런데 막상 속을 들여다 보니 실제 전선은 네 가닥뿐이었습니다. 즉, PS/2의 여섯 핀들 중 실제로 사용되는 것은 네 핀이었습니다. 그 중 두 개는 전원을 공급하는 VCC와 GND일테니, 그렇다면 결국 키보드 신호 송신에 사용되는 전선은 단 두 개일 뿐!!

그렇다면 과연 어느 것이 VCC, GND이며, 또 어느 것이 신호 라인인지 확인하기 위해 신비의 Logic Analyzer를 물립니다.

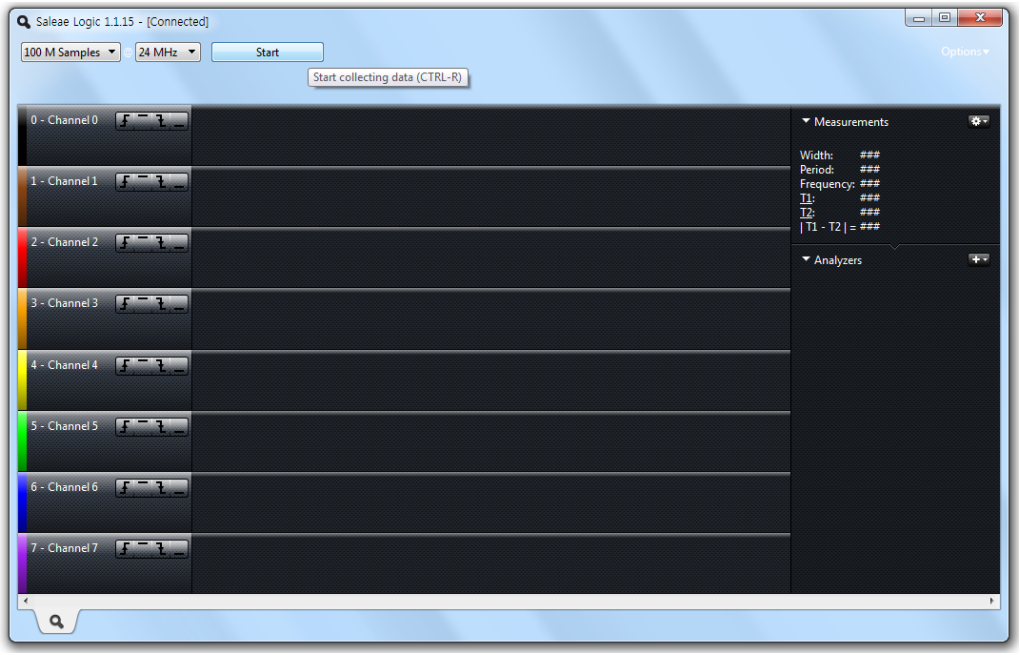
우선 Logic Analyzer의 사용법을 간단하게 설명 드리자면, 장비에 연결된 갈고리처럼 생긴 커넥터 전기신호를 스니핑하고자 하는 곳에 물리고, Logic Analyzer 전용 소프트웨어를 다운받아 PC에서 실행하면 끝입니다. 장비와 PC는 USB로 연결되며, 전용 드라이버는 소프트웨어와 함께 깔립니다.

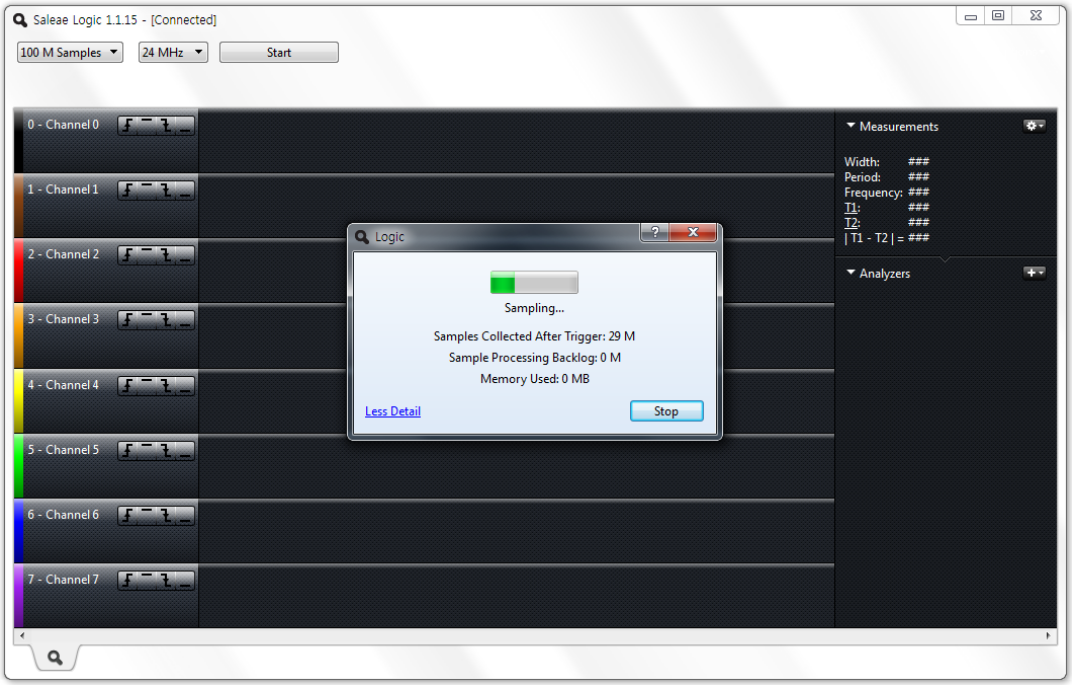


다음은 키보드의 네 가닥 전선에 Logic Analyzer를 물리는 모습입니다.

이제 PS/2 키보드를 PC의 PS/2의 커넥터에 연결하는데.. 아차..! PS/2는 USB와는 달리 부팅 시에만 인식이 됩니다. 그러므로 리부팅을 해줍니다 =_=

이제 다시 Logic Analyzer 소프트웨어를 실행하고, 캡쳐 할 신호의 용량을 선택한 후 Start 버튼을 누르면 캡쳐가 시작됩니다. 캡쳐 할 용량을 100M 정도로 정해주니 약 4초간 캡쳐가 진행되었습니다.

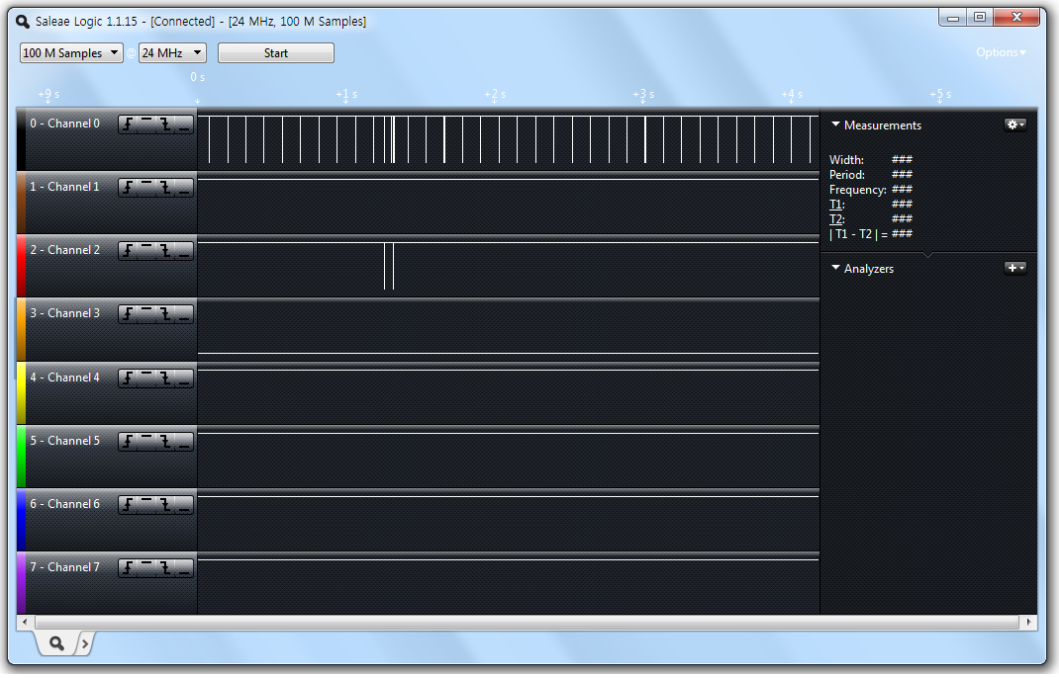




[전기신호 캡쳐가 진행되는 모습]

여기서 중요한 점은, 캡쳐가 진행되는 동안 PS/2 키보드의 A키를 한 번 눌러주는 것입니다. 그래야 신호가 발생해서 분석을 할 수 있기 때문입니다. 만약 키를 여러 번 누르면 분석이 복잡해지니 **딱 한 번만 누릅니다.**

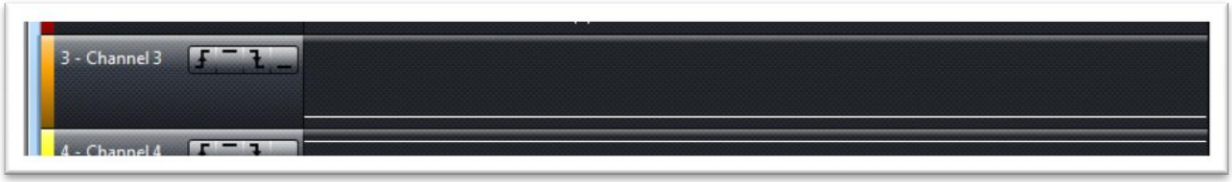
이제 캡쳐가 완료되면..



이와 같이 0과 1로 이루어진 디지털 신호들이 보이게 됩니다.

[신호 분석]

일단 가장 확실한 건 3번 채널입니다.



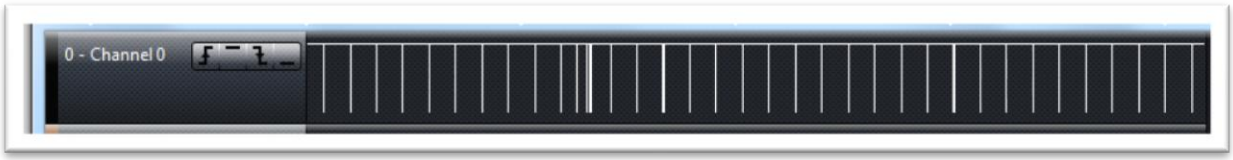
신호가 밑바닥을 기고 있는 이 곳은.. 바로 그라운드(GND)입니다. LOW 신호가 잡힌 것입니다.
그리고 다음은 1번 채널,

그라운드와는 반대로 HIGH 신호를 고수하고 있는 이 채널은 바로 VCC입니다.
이렇게 해서 VCC와 GND를 찾았습니다.

다음은 2번 채널,

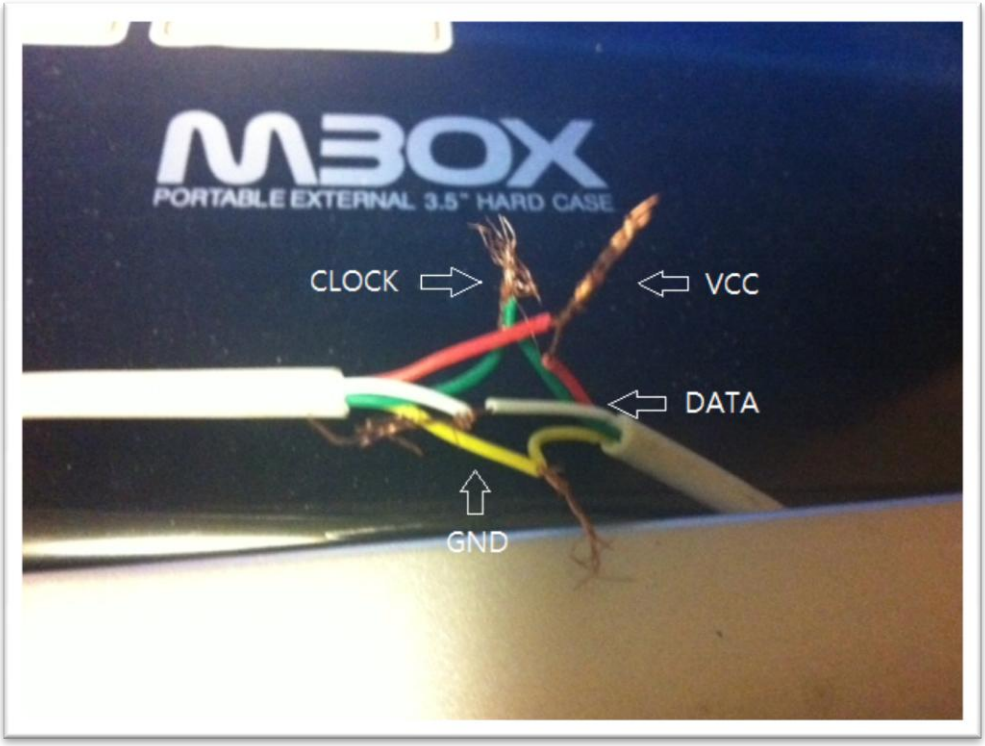
HIGH로 일정하던 신호가 어느 한 시점에서 변하게 됩니다.
이 시점은 바로 우리가 키보드 A 키를 눌렀을 때입니다. 그러므로 이 채널을 DATA라고 지칭하겠습니다.

마지막으로 0번 채널,

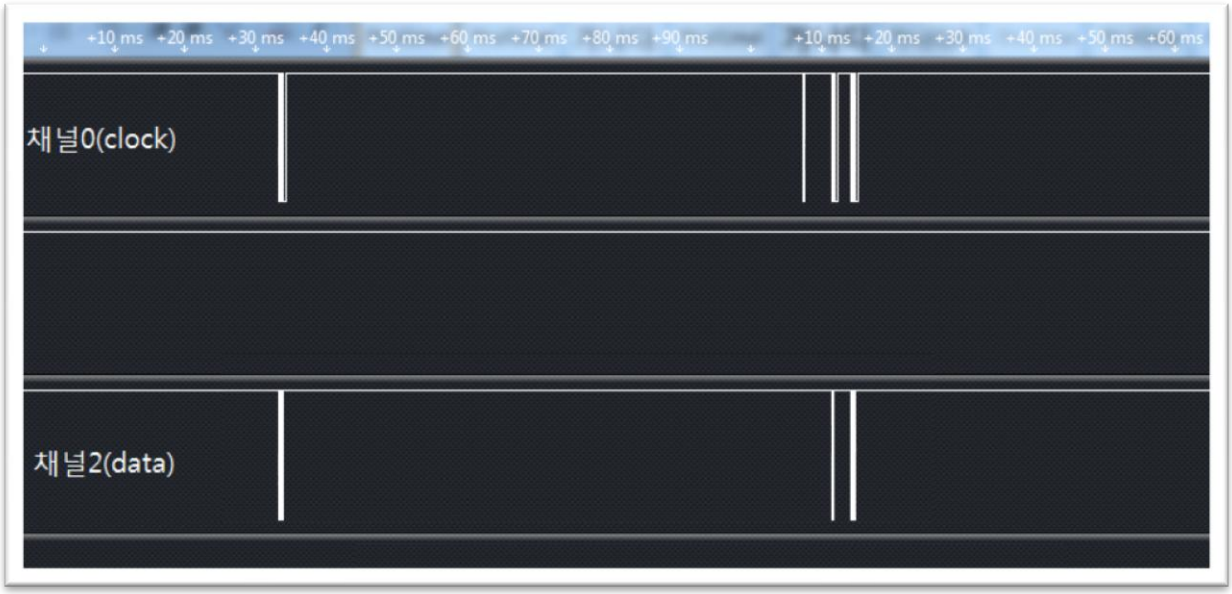


어떤 일정한 파형이 반복되고 있습니다. 이 같은 형태는 신호의 동기화를 위한 CLOCK 라인의 특징입니다. 이 채널은 CLOCK이라고 지칭하겠습니다. 중간에 규칙적이지 않은 부분이 살짝 존재하는데, 잘 보면 DATA 채널의 A 키 입력 시점과 일치합니다. 조금 이따가 이 부분을 더 확대해서 보겠습니다.

이렇게 해서 키보드의 네 가닥 선들에 대한 비밀이 풀렸습니다.

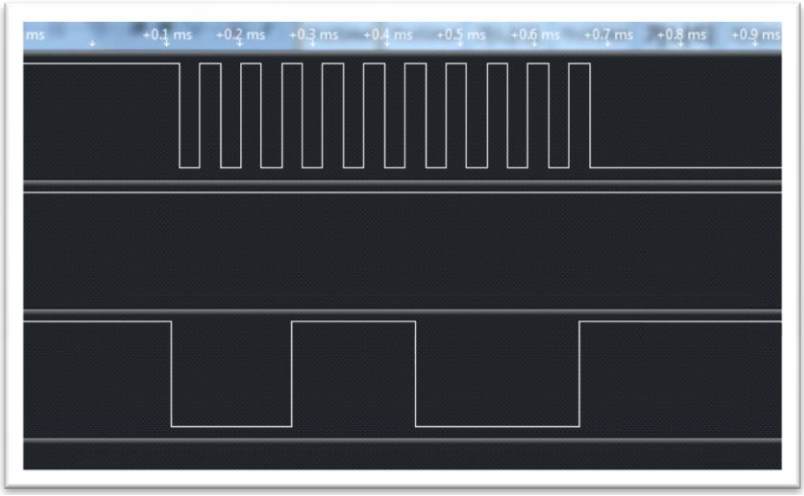


이제 A키를 눌렀을 때에 해당하는 부분을 확대하여 살펴보겠습니다.
마우스의 wheel을 움직이면 캡쳐된 신호를 확대하거나 축소할 수 있습니다.



캡쳐 중 A 키를 딱 한 번 눌렀을 뿐인데, 총 세 개의 data 신호가 발생한 것을 볼 수 있습니다.

이들 세 개의 data 신호 중, 첫 번째 것을 더 확대해서 보겠습니다.

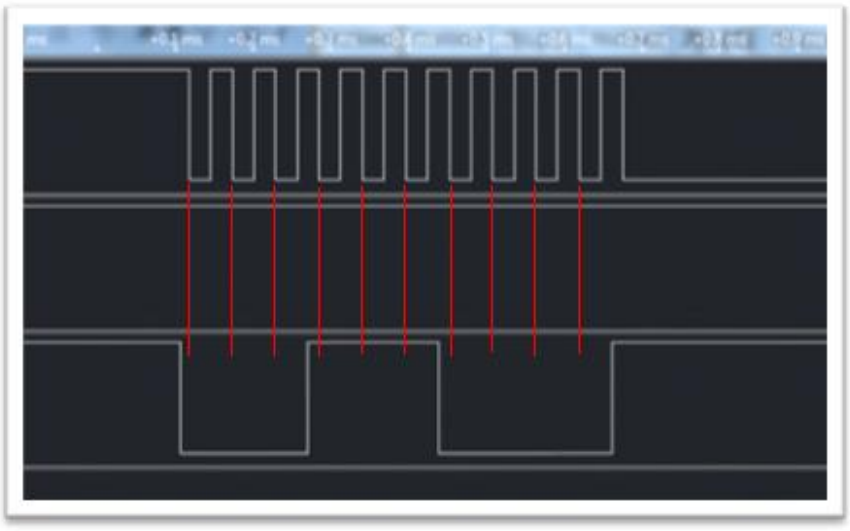


확대를 하기 전에는 잘 보이지 않았지만, 확대를 하고 나면 CLOCK 신호가 규칙적임을 알 수 있습니다. 그리고 CLOCK의 횟수를 세어보면 총 10개입니다. 혹시 시리얼 통신을 분석해보신 경험이 있으시다면, 이처럼 10비트의 데이터의 경우 시작비트 1비트, 종료비트 1비트, 그리고 그 사이에 8비트의 실제 데이터 비트가 존재하는 형태가 아닐까?하고 추측할 수 있을 것입니다.
저 또한 이렇게 추정하고 분석을 시작해 보았습니다.

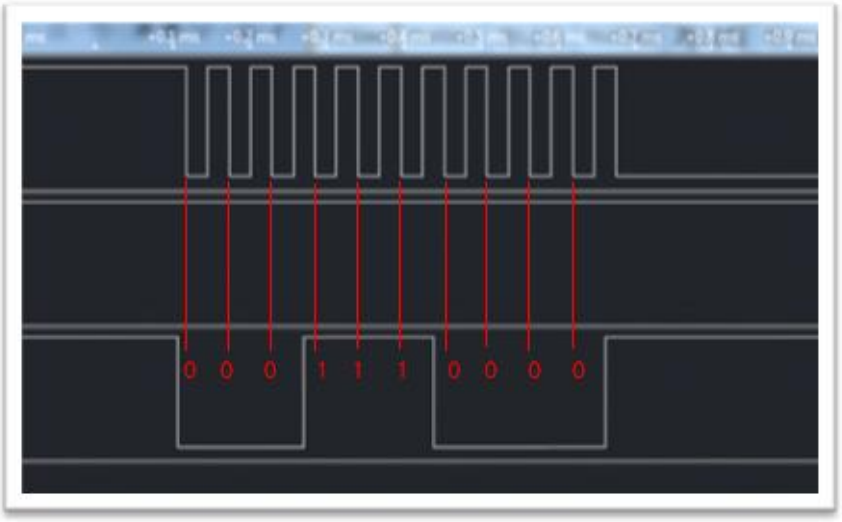
CLOCK을 기반으로 데이터를 추출하는 방법은, CLOCK의 움직임이 변하는 시점에서의 DATA가 HIGH인지 LOW인지를 판별하는 것입니다. 만약 CLOCK이 HIGH에서 LOW로 변하는 시점을 기준으로 한다면 FALLING EDGE, 반대로 LOW에서 HIGH로 변하는 시점을 기준으로 한다면 RISING EDGE라고 부릅니다.

PS/2 키보드의 CLOCK 신호를 보면, 평상시엔 HIGH로 유지되다가 키보드가 눌렸을 때, LOW로 떨어지는 것을 알 수 있습니다. HIGH에서 LOW로 떨어졌으므로 FALLING EDGE 방식일 거라 가정하고 DATA를 추출해 보겠습니다.

우선 FALLING EDGE 시점과 DATA를 서로 맞추어 놓고, (그림판을 이용해 선을 그었습니다.)

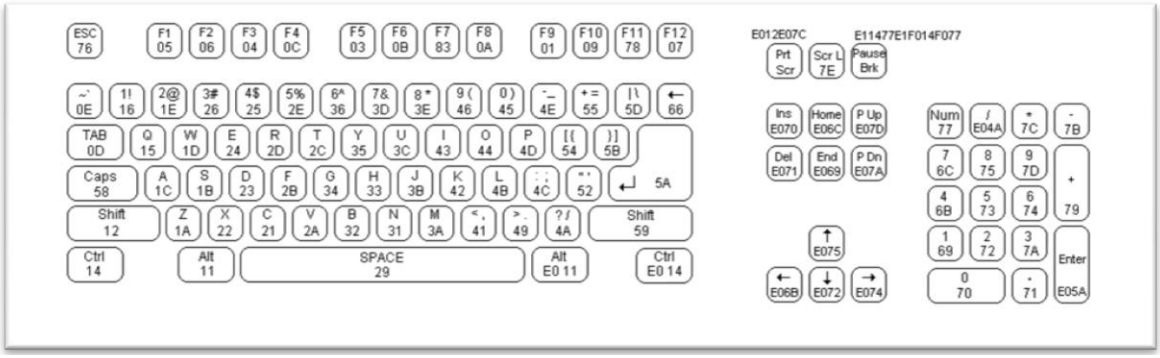


해당 시점에서의 DATA가 0인지 1인지를 판별합니다.

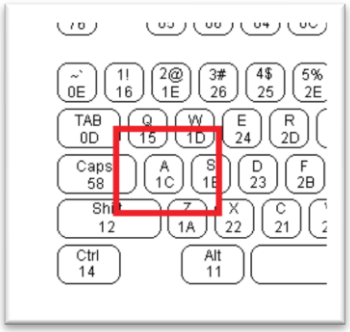


첫 번째와 마지막은 시작, 종료 비트라고 가정했으므로, 가운데 8비트만 빼서 모으면, 00111000이 됩니다. 근데 우리는 이 비트의 배열이 MSB 먼저인지 LSB 먼저인지를 아직 모릅니다. 그러므로 실제 데이터는 00111000일 수도, 아니면 반대로 00011100일 수도 있을 것입니다.

이 둘을 각각 16진수로 변환해 보면, 0x38, 0x1C가 됩니다.
자.. 이쯤에서 구글의 도움을 받아 키보드 스캔 코드표를 찾아봅니다.



A = 0x1C!! 다행히도 예상한 값 중 하나가 나타나 주었습니다. 역시 첫 비트와 마지막 비트는 중요하지 않고, 중간의 8비트만 반대 순서로 뒤집어서 1바이트로 변환하면 되는 것이었습니다.



2편에서 계속됩니다...