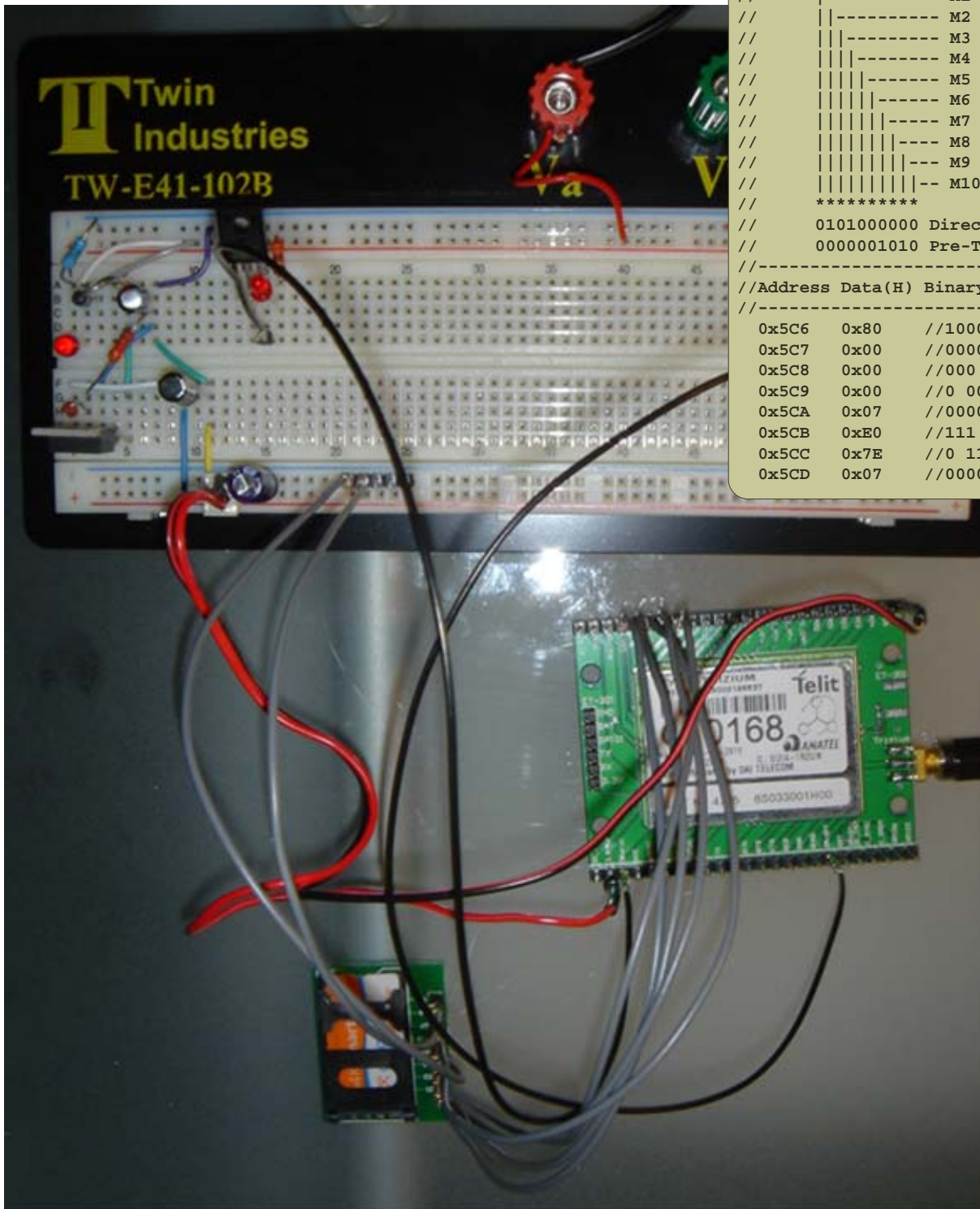


# SIM Sniffer

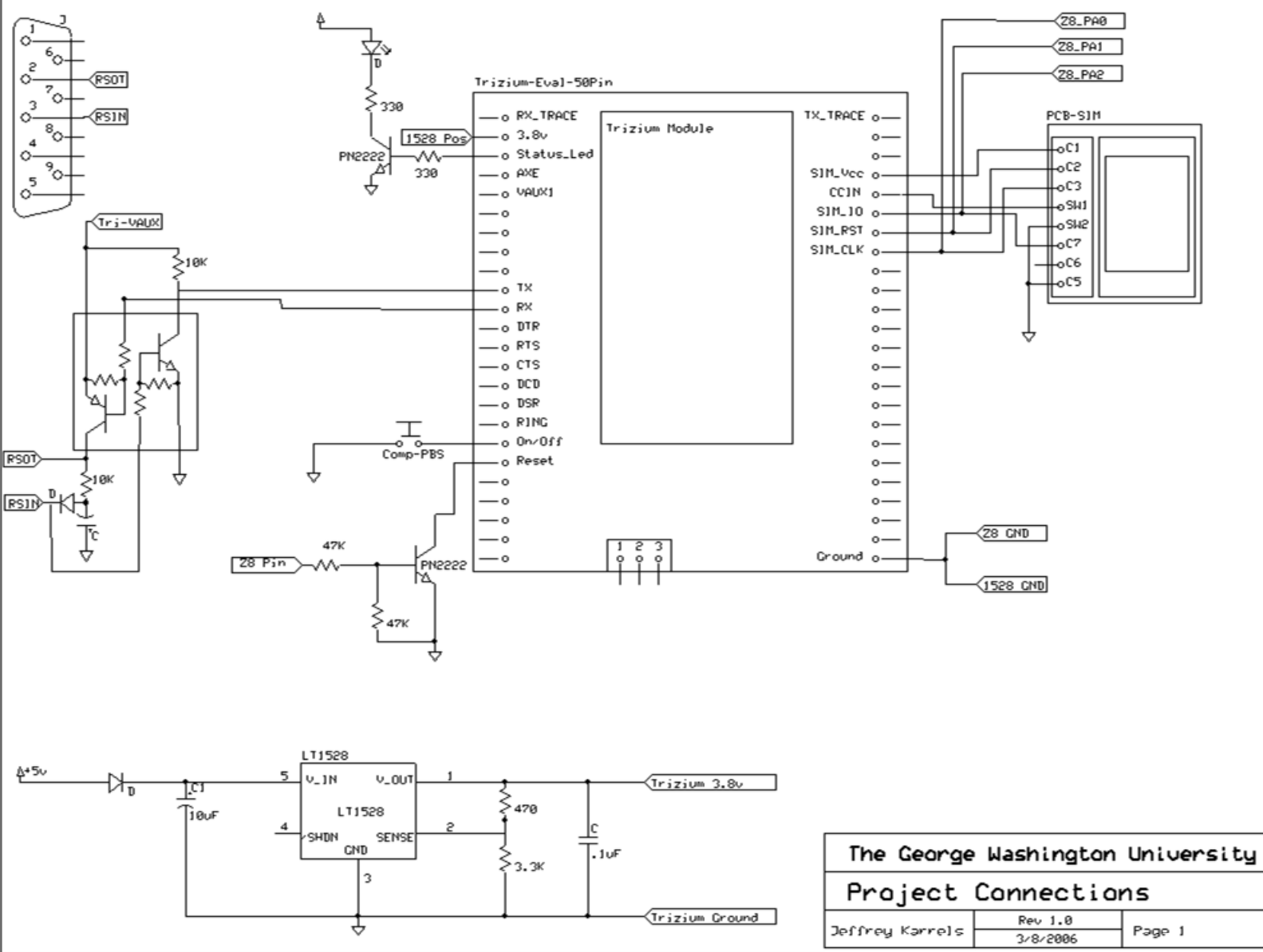
The George Washington University  
Jeffrey Karrels ([karrels@gwu.edu](mailto:karrels@gwu.edu))  
Real-Time Embedded Systems  
Spring 2006

## Project Abstract:

The project goal was to be able to sniff the I/O line of the SIM card (the card that a GSM network uses for authentication and other actions). The resulting project was able to capture the data coming across the I/O line of the SIM card, store it to RAM, and at a later time transfer that data to a host machine. The data could then be parsed to get the desired information from it.



```
// Recorded Class byte of an APDU
// -----
//
// |----- M1 Start Bit
// |----- M2 B8
// |----- M3 B7
// |----- M4 B6
// |----- M5 B5
// |----- M6 B4
// |----- M7 B3
// |----- M8 B2
// |----- M9 B1
// |----- M10 Parity
// *****
// 0101000000 Direct Convention -> CLASS [A0]
// 0000001010 Pre-Transformation
// -----
//Address Data(H) Binary(b) Bit
//-----
0x5C6 0x80 //1000000 0 0
0x5C7 0x00 //00000 000 0
0x5C8 0x00 //000 00000 0
0x5C9 0x00 //0 000000 0 00
0x5CA 0x07 //00000 111 0
0x5CB 0xE0 //111 00000 1
0x5CC 0x7E //0 111111 0 01
0x5CD 0x07 //00000 111 0
```



# Lessons Learned

- 3.25Mhz is really fast
- GSM does not like to stick to specifications
- Bottom Up Design