Challenge 2 - write up

Scenario:
We sniffed this capture between a microcontroller and various eeproms. Unfortunately, the capture was cutoff before we could see the results of the read. Could you figure out what would have come out from the read?

Solution:

> We load the .logicdata file on Logic and see there is a synchronous pattern.
> Based on the scenario, we assume we will need an I2C protocol analyzer, as the microcontroller behaves as the master and the eeproms as slaves.
> So, we load an I2C analyzer with the following settings:

SDA -->Channel 1
SCL --> Channel 0
Address Display --> 8-bit R/W bit included

So, we recieve a list of Decoded Protocols, that we now need to arrange. Firstly, we export the details as a .csv file. Now we need to arrange the data that the eeproms receive by the microcontroller, based on the Internal Register Address.

For this reason, I have written a script that consists of the following steps (the script appears at the end of the page):

• Opens the .csv file (default name: "untitled.csv") and creates a string with all the Decoded Protocols.
• Find all the eeproms addresses (Spoiler Alert: They are 4).
• For every eeprom it:
  ‣ Finds all the Internal Register Addresses and Data and categorizes them in pairs
  ‣ Sorts them based on the Internal Register Address
  ‣ Converts the Data from hexadecimal values to ascii ones
  ‣ Prints a corresponding message, to show what every eeprom received as a message

After running the script, we get the following message:

> Eeprom with the address 0x0E received the following message:
>
> **flap{p37eR_m4n!_tURn_0n_ch4nN3l_8!}**
>
> Eeprom with the address 0x0C received the following message:
>
> **f1ag{b3cUZ_5eV3n_n1ne}**
>
> Eeprom with the address 0x12 received the following message:
>
> **flog{7ry_4n0tHeR_C4s7Le}**
>
> Eeprom with the address 0x10 received the following message:
>
> **flag{ii_c_y0U_Kn0w_uR_5er1aL}**

So we understand that the flag is the Data that the eeprom with Device Address 0x10 has received,
flag{ii_c_y0U_Kn0w_uR_5er1aL}

The script is the following:

```
import csv;

c = ''
eeproms = []
with open('untitled.csv') as csvfile:
    spamreader = csv.reader(csvfile, delimiter=' ', quotechar='|')
    i = 0
    for row in spamreader:
        if len(str(i)) == 1:
            c += '00'
        elif len(str(i)) == 2:
            c += '0'
        c += str(i)+' '
        c += ', '.join(row)
        c += '\n'
        i += 1

for line in c.splitlines():
    d = int(line[0]+line[1]+line[2])
    if d % 3 == 1:
        eep = line[45]+line[46]+line[47]+line[48]
        if eep not in eeproms:
            eeproms.append(eep)

lines = c.splitlines()
eepromsData = []

for eep in eeproms:
    u = []
    tempList = []
    for line in range(0,len(lines)):
        d = int(lines[line][0]+lines[line][1]+lines[line][2])
        if d % 3 == 1:
            e = lines[line][45]+lines[line][46]+lines[line][47]+lines[line][48]
            if e == eep:
                p = (lines[line+1])[26]+(lines[line+1])[27]+(lines[line+1])[28]+(lines[line+1])[29]
                t = (lines[line+2])[26]+(lines[line+2])[27]+(lines[line+2])[28]+(lines[line+2])[29]
                tempList.append([int(p,16),int(t,16)])
    tempList.sort(key=lambda x: x[0])
    for inArr in tempList:
        inArr[1] = chr(inArr[1])
        u.append(inArr[1])
    print "------------------------------------------------------------"
    print "Eeprom with the address "+ eep + " received the following message:\n" + "".join(u)

print "------------------------------------------------------------"
```