black hat®
USA 2016

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

What's the **DFIR**ence for ICS?

Chris Sistrunk, PE
Senior Consultant, FireEye
@chrissistrunk

Josh Triplett
Senior Reverse Engineer, FireEye

Agenda

- Digital Forensics and Incident Response Overview
- DFIR for ICS
    - What’s the DFIRence?
- Embedded Devices
    - What to Collect
    - What to Analyze
- RTU Examples
    - GE D20MX
    - VxWorks DFIR Tool
    - SEL-3530 RTAC

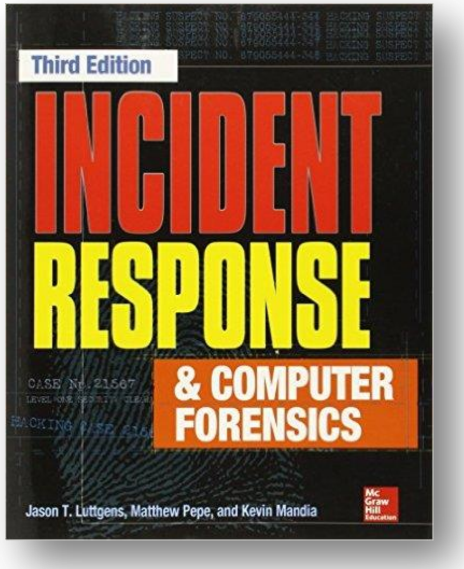
Incident Response Overview
"Find Evil"

- Assess the situation
- Define objectives
- Collect evidence
- Perform analysis
- Communicate
- Develop remediation plan
- Document findings

http://www.cumbriafire.gov.uk/about/photo/engines/incident-response.asp

Digital Forensics Overview

- Data Collection
  - Data Files
  - OS (volatile and non-volatile)
  - Network Traffic
  - Applications
- Examination
- Analysis
- Reporting



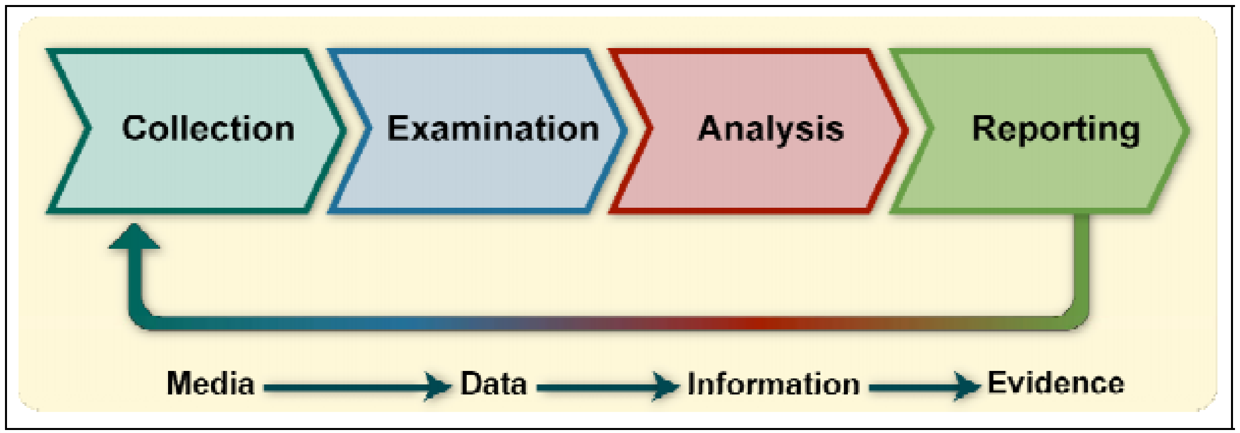


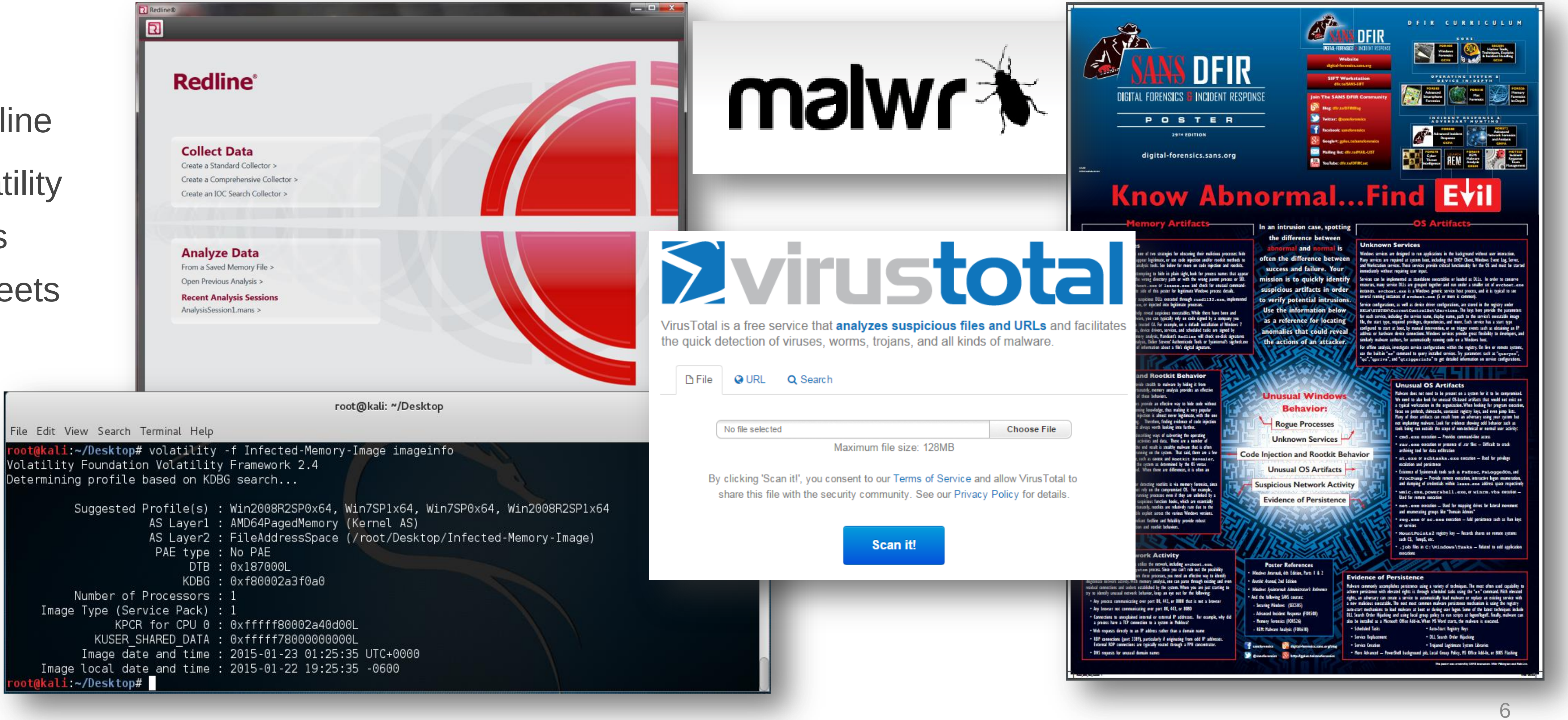
Figure 3-1. Forensic Process

NIST SP 800-86

Traditional DFIR tools

Mature

- Tools
  - Redline
  - Volatility
- Websites
- Cheatsheets
- Books



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

In an intrusion case, spotting the difference between abnormal and normal is often the difference between success and failure. Your mission is to quickly identify suspicious artifacts in order to verify potential intrusions. Use the information below as a reference for locating anomalies that could reveal the actions of an attacker.

root@kali: ~/Desktop

File Edit View Search Terminal Help

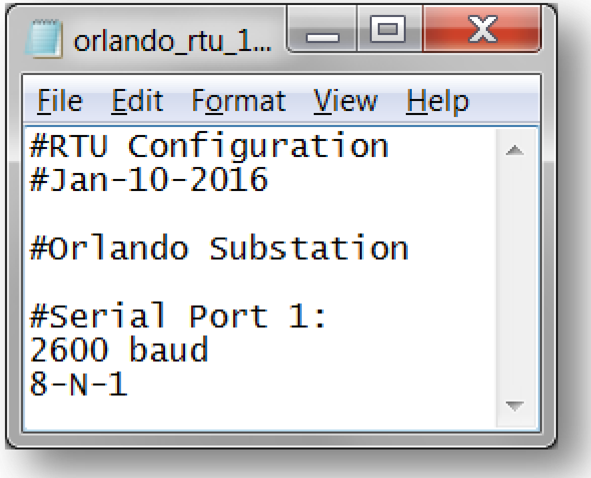
```
root@kali:~/Desktop# volatility -f Infected-Memory-Image imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

          Suggested Profile(s) : Win2008R2SP0x64, Win7SP1x64, Win7SP0x64, Win2008R2SP1x64
                     AS Layer1 : AMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Desktop/Infected-Memory-Image)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002a3f0a0
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002a40d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2015-01-23 01:25:35 UTC+0000
     Image local date and time : 2015-01-22 19:25:35 -0600
root@kali:~/Desktop# 
```

What’s the DFIRence for ICS?

		IT/OT Differences
Assess the situation	• When/Where/How is the ICS affected?	✓ Similar
Define objectives	• Return the ICS to normal quickly and safely	! Physical Processes
Collect evidence	• ICS devices have RTOS and ICS protocols	! Must be collected manually
Perform analysis	• Analysis must be done to verify anomalies	! No ICS-specific DFIR tools
Communicate	• Regularly report status to management	✓ Similar
Develop remediation plan	• How/When to regain control of the ICS	! ICS devices have constraints
Document findings	• Write a report of what exactly happened	✓ Similar

ICS anomaly → incident?

- An anomaly of some kind has occurred
  - Increased network activity, strange behavior, failure
- Now we need to **investigate** the anomaly
- Is it known bad?
- Is it unknown bad?
- Do we **escalate** this to a security incident?
- Who do we call?
  - Engineers, Admins, PR, Safety
  - Vendors

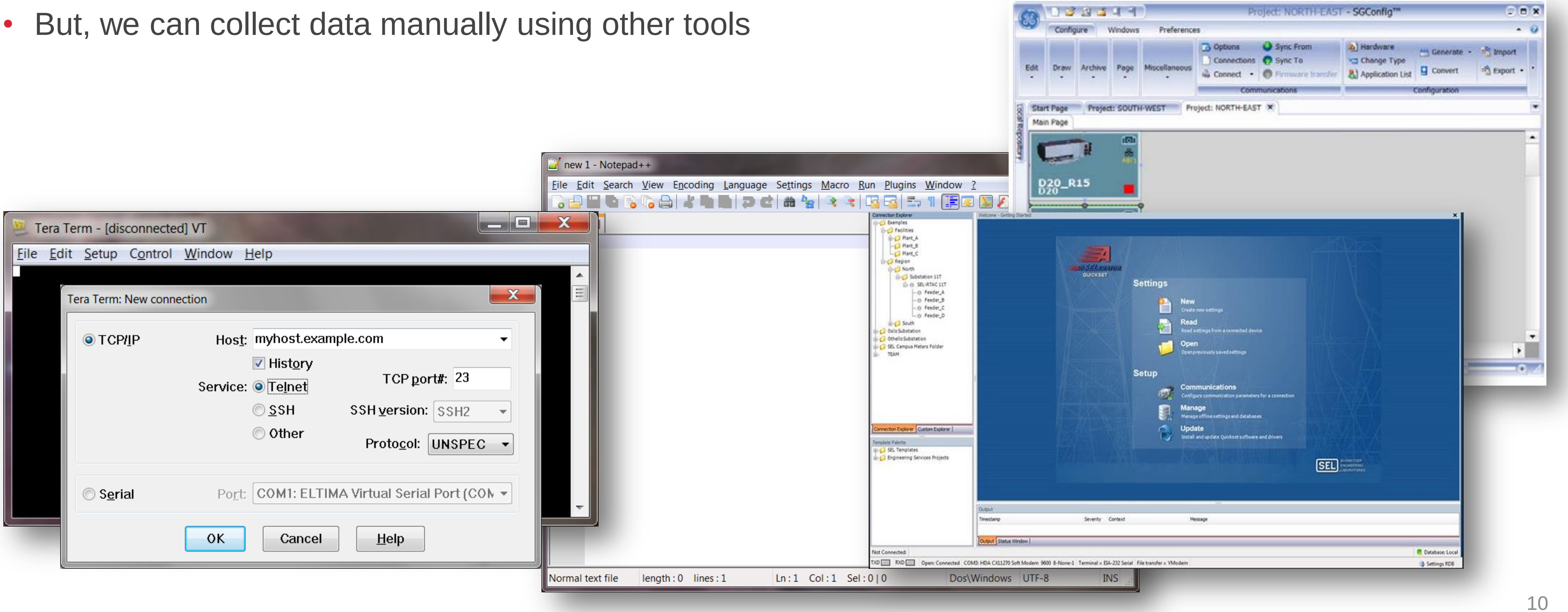


```
#RTU Configuration
#Jan-10-2016

#Orlando Substation

#Serial Port 1:
2600 baud
8-N-1
```

Don’t!

ICS forensics collection tools

- No ICS-specific DFIR tools…especially embedded devices
- But, we can collect data manually using other tools



Tera Term - [disconnected] VT

Tera Term: New connection

● TCP/IP Host: myhost.example.com

☑ History

Service: ● Telnet TCP port#: 23

○ SSH SSH version: SSH2

○ Other Protocol: UNSPEC

○ Serial Port: COM1: ELTIMA Virtual Serial Port (COM

new 1 - Notepad++

Normal text file length : 0 lines : 1 Ln : 1 Col : 1 Sel : 0 | 0 Dos\Windows UTF-8 INS

Project: NORTH-EAST - SGConfig™

Settings

New — Create new settings

Read — Read settings from a connected device

Open — Open previously saved settings

Setup

Communications — Configure communication parameters for a connection

Manage — Manage offline settings and databases

Update — Install and update Quickset software and drivers

OK
Cancel
Help
File Edit Setup Control Window Help
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Configure Windows Preferences
Edit Draw Archive Page Miscellaneous
Options Connections Connect Sync From Sync To Firmware transfer
Communications
Hardware Change Type Application List Generate Convert Import Export
Configuration
Start Page Project: SOUTH-WEST Project: NORTH-EAST
Main Page
D20_R15
Connection Explorer
Template Palette
SEL
Output
Timestamp Severity Context Message

Embedded devices: What to collect?

Physical data

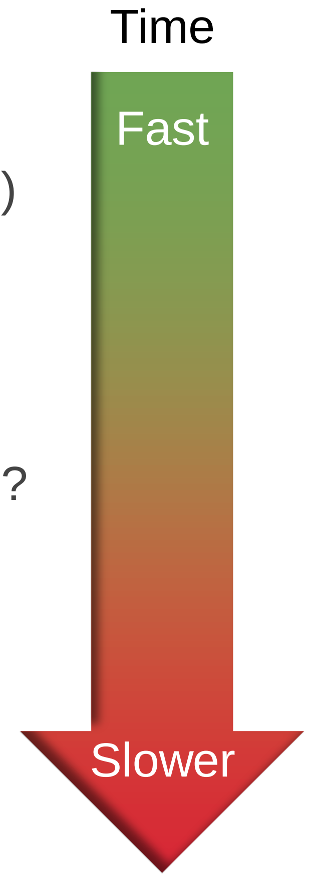
- Exact location of device
- Device description
- Identifying info (manufacturer, S/N, P/N, name)
- Connections (serial, ethernet, USB)
- Front/back panel LED status
- Power consumption
- Temperature (if running hot)
- Evidence of tampering

Digital data

- Running configuration (including user accounts)
- Last-known good configuration
- Running firmware, approved firmware
- CPU usage %, Memory usage % (RAM, Storage)
- Running processes
- Active ports (serial, ethernet, USB, etc)
- Logs (security, events)
- Memory dump (if possible)

Embedded devices: What to analyze?

Find Evil…or ways for evil to do evil



First Responders: ICS Engineer or Technician, Network Engineer, Vendor

- What do the user and event logs reveal? (these need to be viewed first as they may rollover)
- Does the configuration match the firmware? Is the firmware approved from FAT/SAT?
- Running config / last known good config / standard config
- Is the configuration and logic correct for the process?
- Are communications (serial, ethernet, USB, wireless) normal as compared with known good?

Vendor, Digital Forensics Specialist, Embedded Systems Analyst

- Analyze embedded OS files, captured data at rest, captured data in transit
- Volatile memory if possible (to look for code injection and potential rootkits)

Let’s do DFIR on two substation RTUs

SEL
RTAC SEL-3530 REAL-TIME AUTOMATION CONTROLLER
SCHWEITZER ENGINEERING LABORATORIES
RTAC
SEL-3530
REAL-TIME AUTOMATION CONTROLLER
ETH F
USB A
USB B

Time to…RTFM

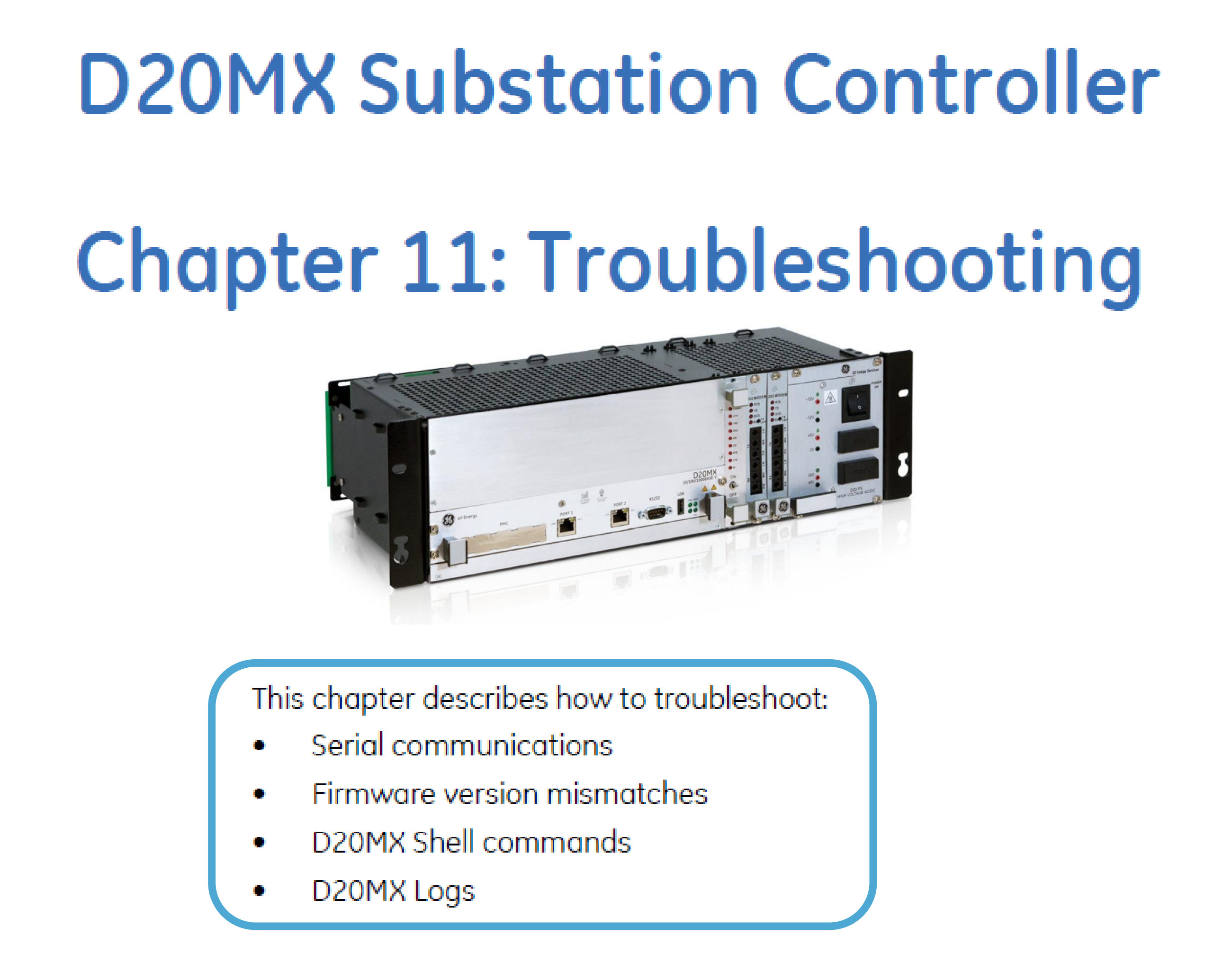
Data Collection: D20MX

Specs

- 667 MHz embedded PowerQUICC II Pro
- 1024 MB of 266 MHz DDR2 RAM with ECC
- 16 MB NVRAM for persistent event storage
- 8 MB boot flash, 256 MB firmware flash
- VxWorks RTOS

Tools to use

- *D20MX Product Documentation Binder.pdf*
- GE SGconfig software
- Terminal (Tera Term, PuTTY)
- WinSCP



D20MX Substation Controller

Chapter 11: Troubleshooting

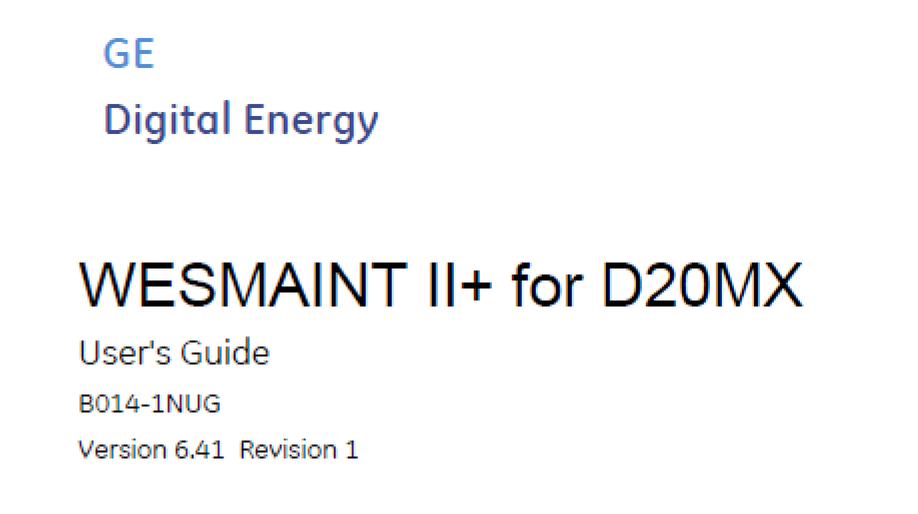
This chapter describes how to troubleshoot:

- Serial communications
- Firmware version mismatches
- D20MX Shell commands
- D20MX Logs

Data Collection: D20MX

You will need three manuals from the binder pdf:

1. **994-0140** D20MX Substation Controller Instruction Manual
   - Chapter 11: Troubleshooting
2. **B014-1NUG** Westmaint II+ for D20MX User's Guide
   - Shows how to use the D20 console interface, menus, error and user logs
3. **SWM0080** D20MX Shells User's Guide



GE

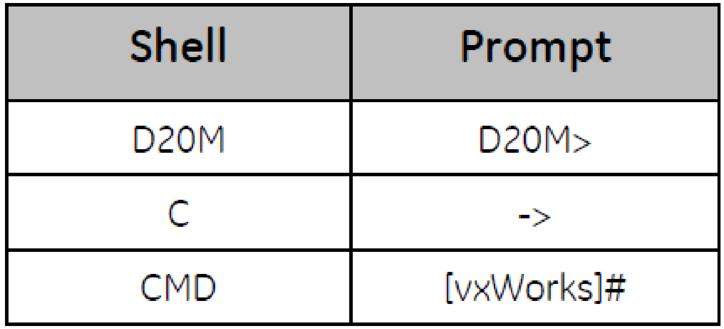
Digital Energy

WESMAINT II+ for D20MX

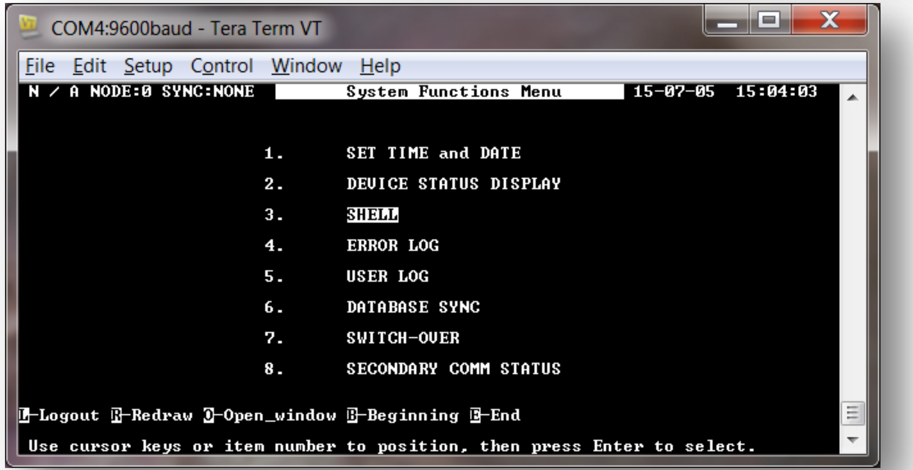
User's Guide

B014-1NUG

Version 6.41 Revision 1



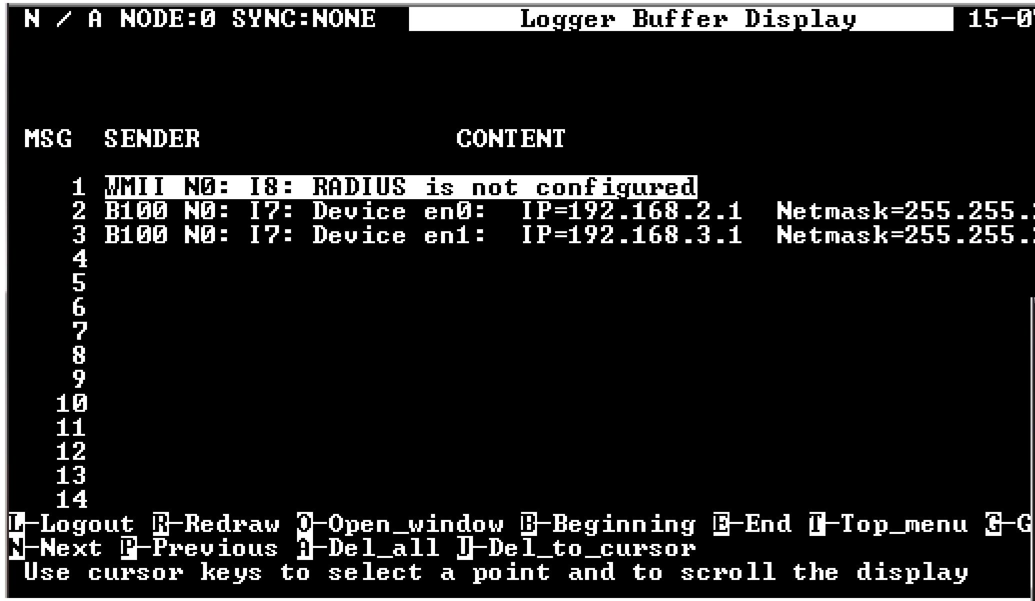
Shell	Prompt
D20M	D20M>
C	->
CMD	[vxWorks]#



COM4:9600baud - Tera Term VT
File Edit Setup Control Window Help

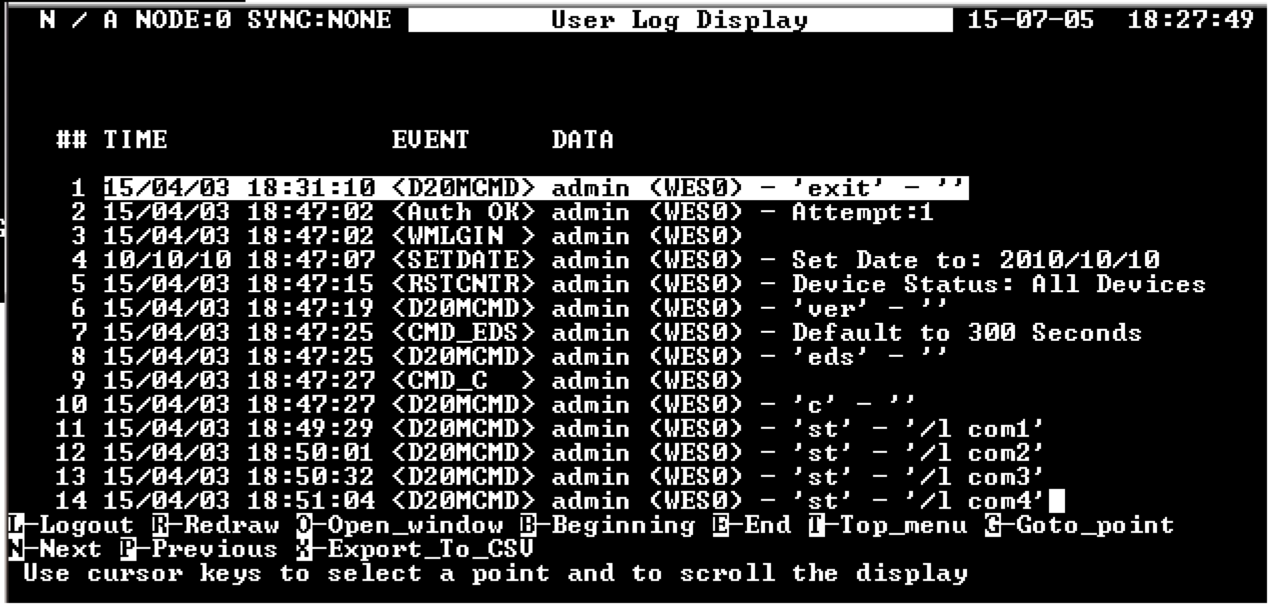
```
N / A NODE:0 SYNC:NONE          System Functions Menu          15-07-05   15:04:03


                          1.        SET TIME and DATE

                          2.        DEVICE STATUS DISPLAY

                          3.        SHELL

                          4.        ERROR LOG

                          5.        USER LOG

                          6.        DATABASE SYNC

                          7.        SWITCH-OVER

                          8.        SECONDARY COMM STATUS

L-Logout R-Redraw O-Open_window B-Beginning E-End
 Use cursor keys or item number to position, then press Enter to select.
```

Data Collection: D20MX
Error Log and User Log



```
N / A NODE:0 SYNC:NONE          Logger Buffer Display          15-07-05   18:29:10



MSG  SENDER                 CONTENT

   1 WMII N0: I8: RADIUS is not configured
   2 B100 N0: I7: Device en0:  IP=192.168.2.1  Netmask=255.255.255.0
   3 B100 N0: I7: Device en1:  IP=192.168.3.1  Netmask=255.255.255.0
   4
   5
   6
   7
   8
   9
  10
  11
  12
  13
  14
L-Logout R-Redraw O-Open_window B-Beginning E-End T-Top_menu G-G
N-Next P-Previous A-Del_all D-Del_to_cursor
 Use cursor keys to select a point and to scroll the display
```

The **error log** tells what's wrong with the configuration.

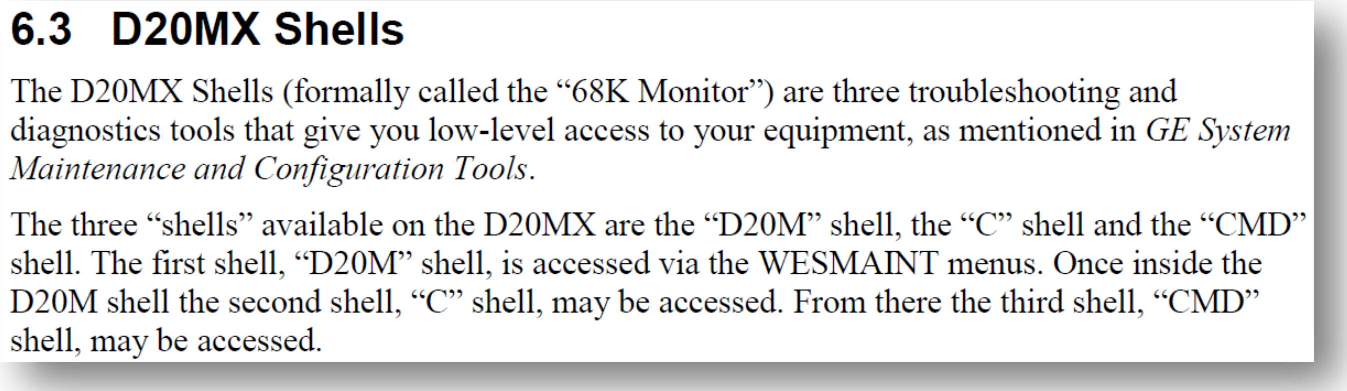


```
 N / A NODE:0 SYNC:NONE           User Log Display            15-07-05   18:27:49



   ## TIME               EVENT      DATA

    1 15/04/03 18:31:10 <D20MCMD> admin (WES0) - 'exit' - ''
    2 15/04/03 18:47:02 <Auth OK> admin (WES0) - Attempt:1
    3 15/04/03 18:47:02 <WMLGIN > admin (WES0)
    4 10/10/10 18:47:07 <SETDATE> admin (WES0) - Set Date to: 2010/10/10
    5 15/04/03 18:47:15 <RSTCNTR> admin (WES0) - Device Status: All Devices
    6 15/04/03 18:47:19 <D20MCMD> admin (WES0) - 'ver' - ''
    7 15/04/03 18:47:25 <CMD_EDS> admin (WES0) - Default to 300 Seconds
    8 15/04/03 18:47:25 <D20MCMD> admin (WES0) - 'eds' - ''
    9 15/04/03 18:47:27 <CMD_C  > admin (WES0)
   10 15/04/03 18:47:27 <D20MCMD> admin (WES0) - 'c' - ''
   11 15/04/03 18:49:29 <D20MCMD> admin (WES0) - 'st' - '/l com1'
   12 15/04/03 18:50:01 <D20MCMD> admin (WES0) - 'st' - '/l com2'
   13 15/04/03 18:50:32 <D20MCMD> admin (WES0) - 'st' - '/l com3'
   14 15/04/03 18:51:04 <D20MCMD> admin (WES0) - 'st' - '/l com4'
L-Logout R-Redraw O-Open_window B-Beginning E-End T-Top_menu G-Goto_point
N-Next P-Previous X-Export_To_CSV
 Use cursor keys to select a point and to scroll the display
```

The **user log** shows logins, logouts, and all user activity. Can be exported to CSV. This data also gets put into the **syslog**.

The power of the 3 Shells

- You can access the shell remotely with SSH, but the most powerful access is through the front serial port.
- Some of these commands require assistance from GE unless you really know what you are doing.



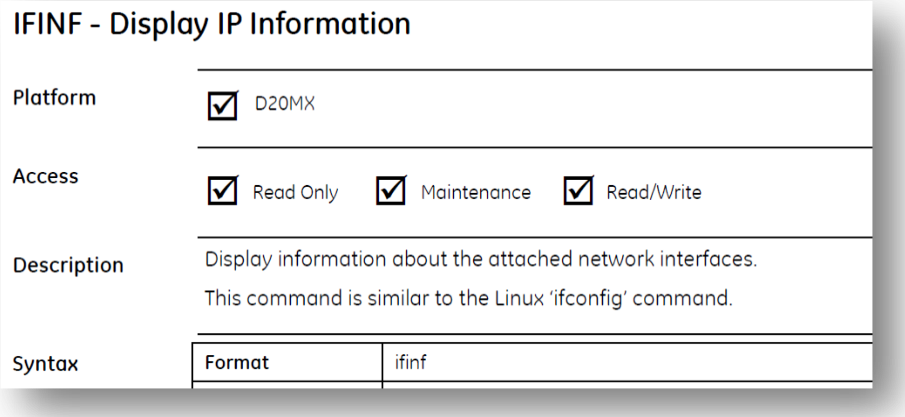
6.3 D20MX Shells

The D20MX Shells (formally called the "68K Monitor") are three troubleshooting and diagnostics tools that give you low-level access to your equipment, as mentioned in *GE System Maintenance and Configuration Tools*.

The three "shells" available on the D20MX are the "D20M" shell, the "C" shell and the "CMD" shell. The first shell, "D20M" shell, is accessed via the WESMAINT menus. Once inside the D20M shell the second shell, "C" shell, may be accessed. From there the third shell, "CMD" shell, may be accessed.

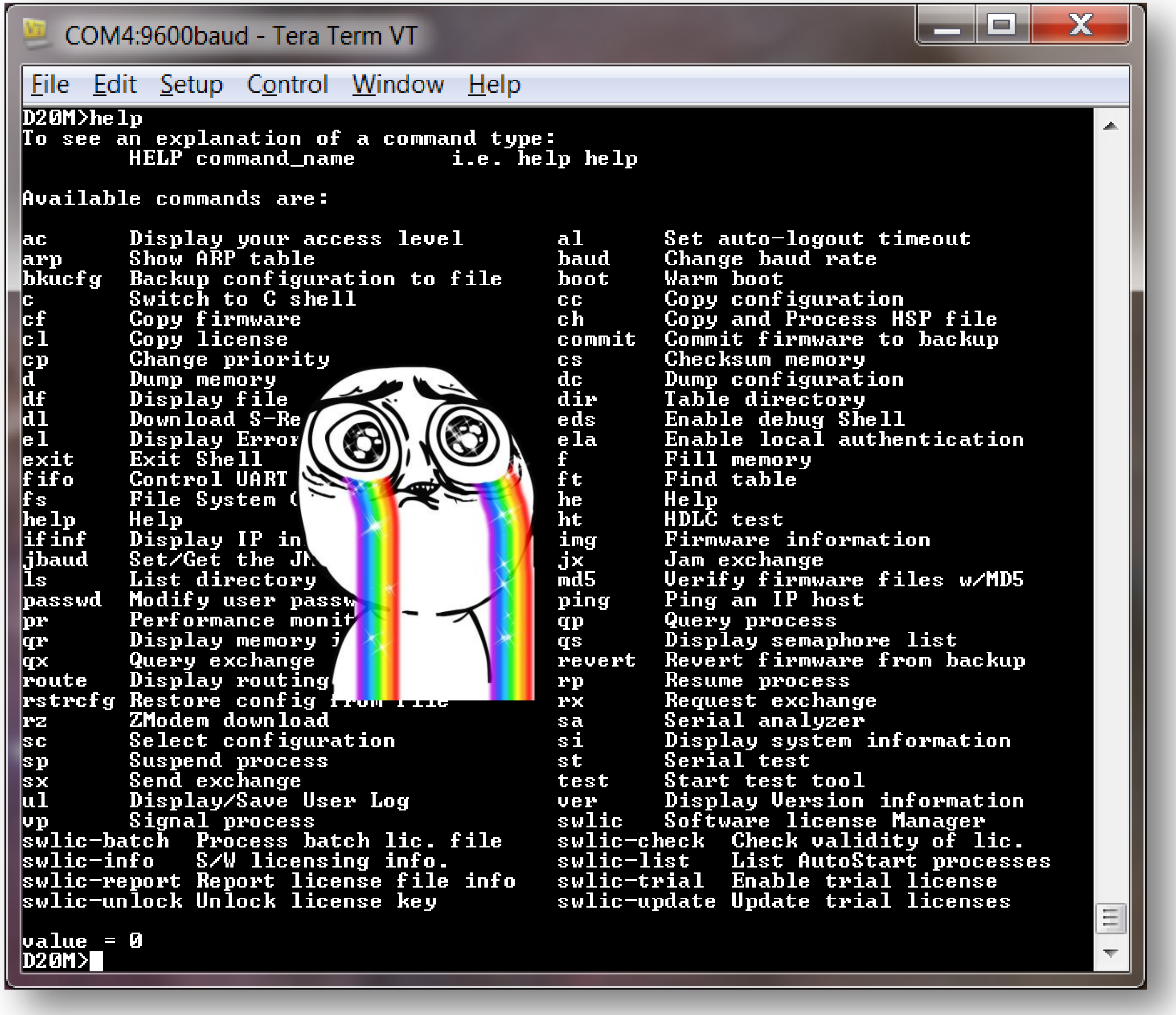
The main shell

- D20M Shell is the main shell
- Very similar to 68k monitor shell in older D20s
- Incident Responders will want to collect data from this shell
- All of the commands are explained in detail in the D20MX Shells UG



IFINF - Display IP Information

Platform	☑ D20MX
Access	☑ Read Only ☑ Maintenance ☑ Read/Write
Description	Display information about the attached network interfaces. This command is similar to the Linux 'ifconfig' command.
Syntax	Format: ifinf

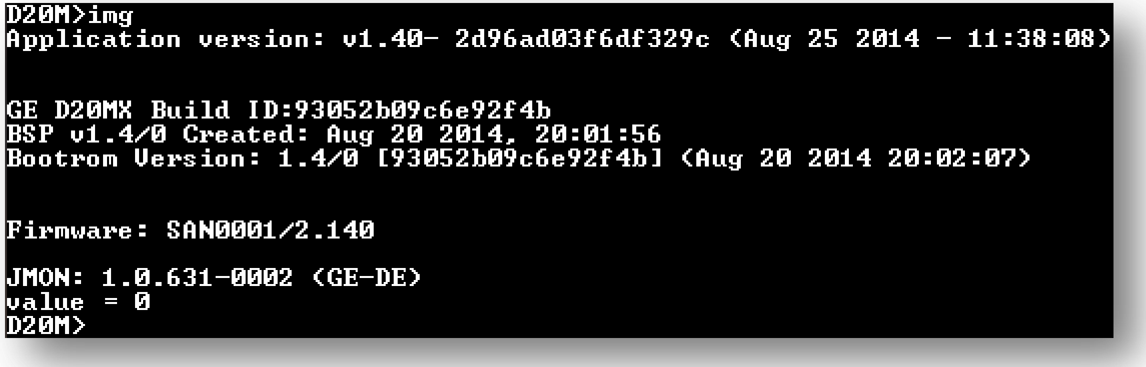


COM4:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
D20M>help
To see an explanation of a command type:
        HELP command_name       i.e. help help

Available commands are:

ac      Display your access level       al      Set auto-logout timeout
arp     Show ARP table                  baud    Change baud rate
bkucfg  Backup configuration to file    boot    Warm boot
c       Switch to C shell               cc      Copy configuration
cf      Copy firmware                   ch      Copy and Process HSP file
cl      Copy license                    commit  Commit firmware to backup
cp      Change priority                 cs      Checksum memory
d       Dump memory                     dc      Dump configuration
df      Display file                    dir     Table directory
dl      Download S-Re                   eds     Enable debug Shell
el      Display Error                   ela     Enable local authentication
exit    Exit Shell                      f       Fill memory
fifo    Control UART                    ft      Find table
fs      File System (                   he      Help
help    Help                            ht      HDLC test
ifinf   Display IP in                   img     Firmware information
jbaud   Set/Get the J                   jx      Jam exchange
ls      List directory                  md5     Verify firmware files w/MD5
passwd  Modify user passw               ping    Ping an IP host
pr      Performance monit               qp      Query process
qr      Display memory i                qs      Display semaphore list
qx      Query exchange                  revert  Revert firmware from backup
route   Display routing                 rp      Resume process
rstrcfg Restore config from file        rx      Request exchange
rz      ZModem download                 sa      Serial analyzer
sc      Select configuration            si      Display system information
sp      Suspend process                 st      Serial test
sx      Send exchange                   test    Start test tool
ul      Display/Save User Log           ver     Display Version information
vp      Signal process                  swlic   Software license Manager
swlic-batch  Process batch lic. file    swlic-check  Check validity of lic.
swlic-info   S/W licensing info.        swlic-list   List AutoStart processes
swlic-report Report license file info   swlic-trial  Enable trial license
swlic-unlock Unlock license key         swlic-update Update trial licenses

value = 0
D20M>
```

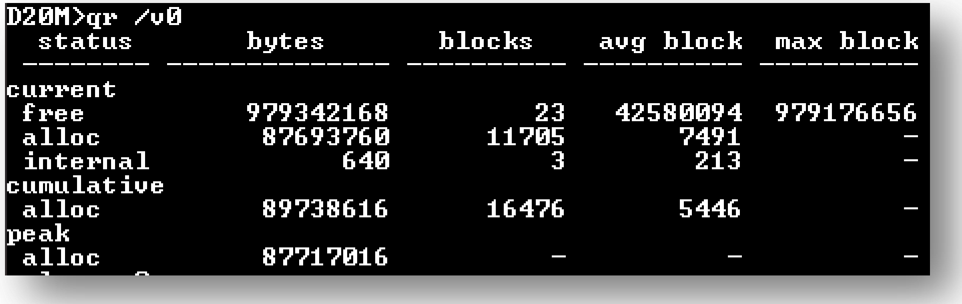
Data Collection: D20MX

- Running configuration
  - ✓ Use SGConfig, ConfigPro, or TeraTerm
  - ✓ Very common task
- Last-known good configuration
  - ✓ Look in email, config database, engineer’s laptop, or it may be on a USB in the cabinet
- Running firmware - **img**



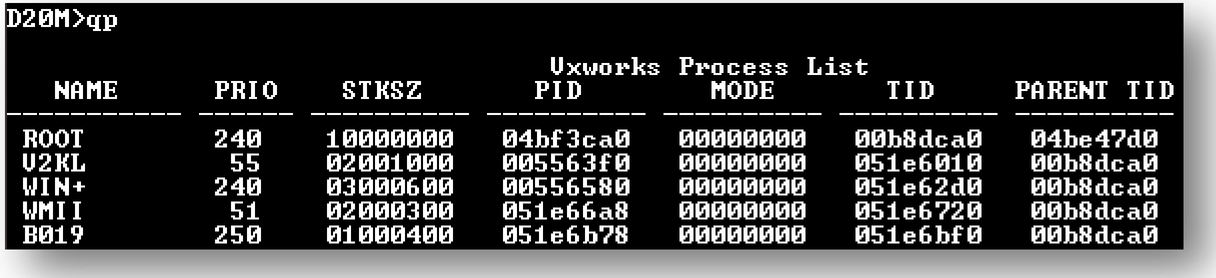
```
D20M>img
Application version: v1.40- 2d96ad03f6df329c (Aug 25 2014 - 11:38:08)


GE D20MX Build ID:93052b09c6e92f4b
BSP v1.4/0 Created: Aug 20 2014, 20:01:56
Bootrom Version: 1.4/0 [93052b09c6e92f4b] (Aug 20 2014 20:02:07)


Firmware: SAN0001/2.140

JMON: 1.0.631-0002 (GE-DE)
value = 0
D20M>
```

- CPU usage %, Memory usage %
  - ✓ **pr** – performance monitor
  - ✓ **qr** – query ram (volatile and nvram)



```
D20M>qr /v0
  status       bytes       blocks    avg block  max block
 -------- -------------- ---------- ---------- ----------
current
 free          979342168         23   42580094  979176656
 alloc          87693760      11705       7491          -
 internal            640          3        213          -
cumulative
 alloc          89738616      16476       5446          -
peak
 alloc          87717016          -          -          -
```

- Running processes - **qp**

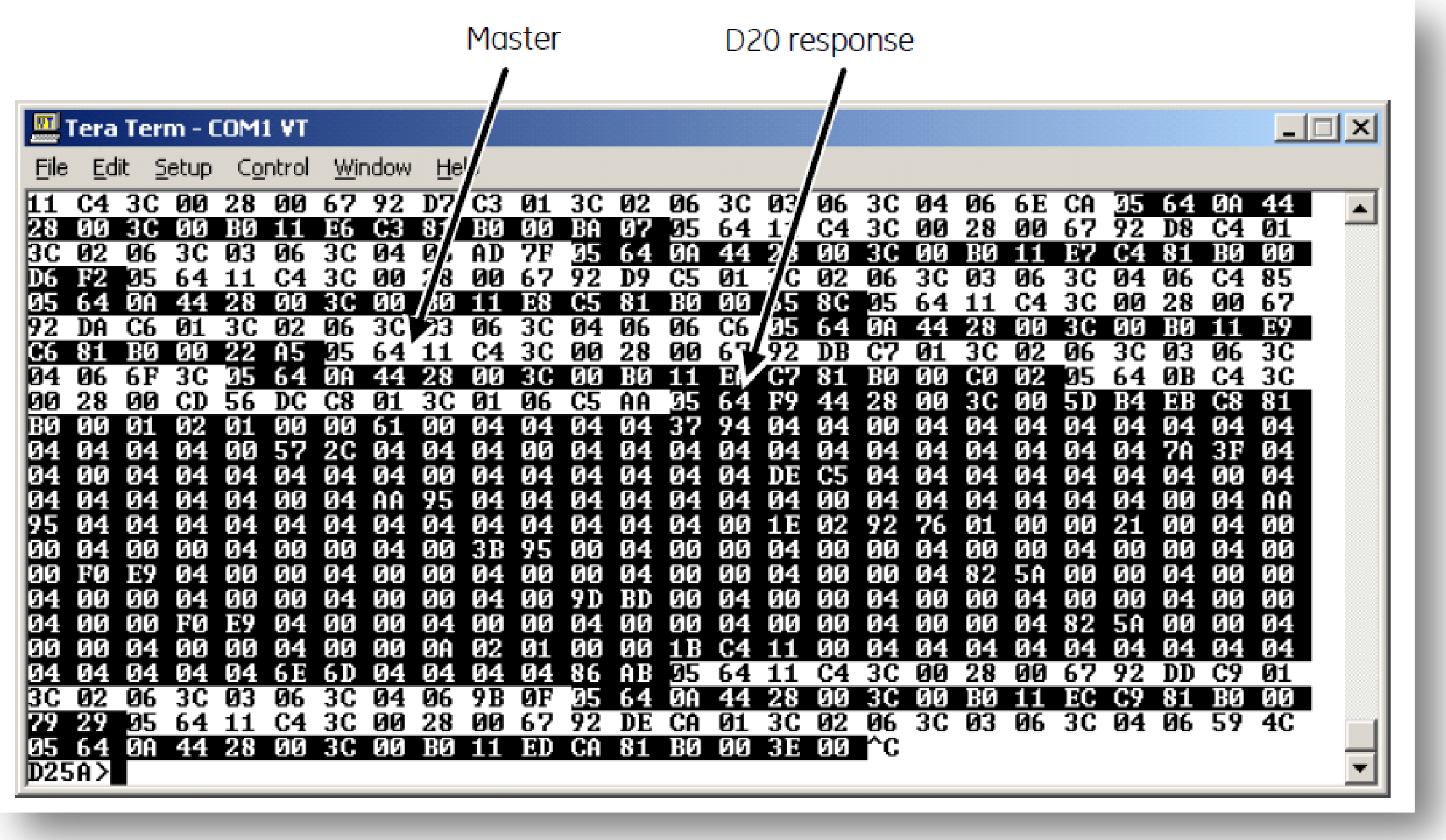


```
D20M>qp

                                  Vxworks Process List
   NAME      PRIO    STKSZ      PID         MODE       TID       PARENT TID
----------- ------ ---------- ---------- ---------- ---------- ----------
 ROOT        240    10000000   04bf3ca0   00000000   00b8dca0   04be47d0
 V2KL         55    02001000   005563f0   00000000   051e6010   00b8dca0
 WIN+        240    03000600   00556580   00000000   051e62d0   00b8dca0
 WMII         51    02000300   051e66a8   00000000   051e6720   00b8dca0
 B019        250    01000400   051e6b78   00000000   051e6bf0   00b8dca0
```

Data Collection: D20MX

Serial analyzer

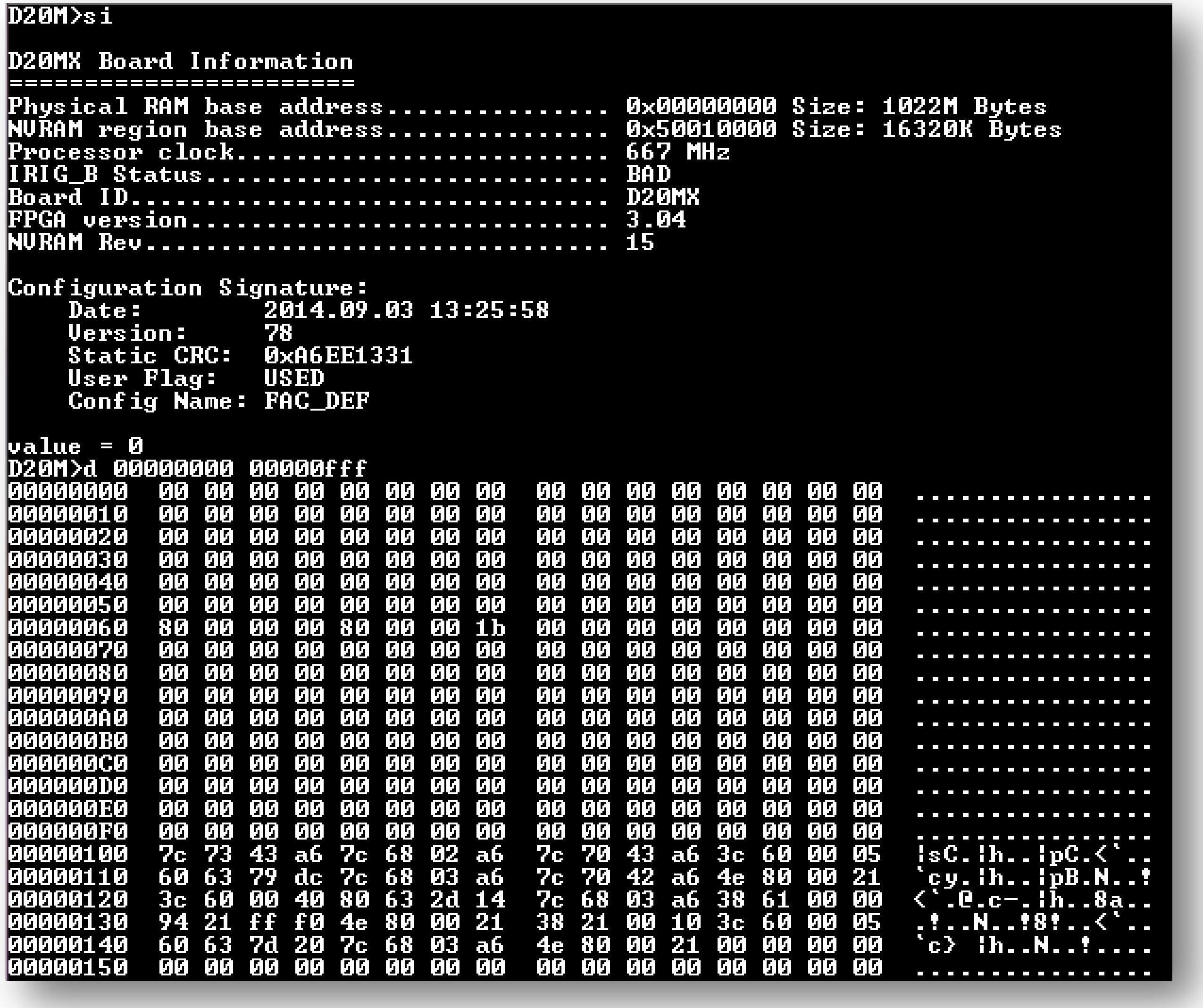
- Very popular shell command (what’s Wireshark?)
- In the D20M shell, use
  - ✓ **sa com#**
    where # is the port number
  - ✓ Turn on logging in TeraTerm beforehand to save the traffic
  - ✓ This example is DNP3



```
11 C4 3C 00 28 00 67 92 D7 C3 01 3C 02 06 3C 03 06 3C 04 06 6E CA 05 64 0A 44
28 00 3C 00 B0 11 E6 C3 81 B0 00 BA 07 05 64 11 C4 3C 00 28 00 67 92 D8 C4 01
3C 02 06 3C 03 06 3C 04 06 AD 7F 05 64 0A 44 28 00 3C 00 B0 11 E7 C4 81 B0 00
D6 F2 05 64 11 C4 3C 00 28 00 67 92 D9 C5 01 3C 02 06 3C 03 06 3C 04 06 C4 85
05 64 0A 44 28 00 3C 00 B0 11 E8 C5 81 B0 00 05 8C 05 64 11 C4 3C 00 28 00 67
92 DA C6 01 3C 02 06 3C 03 06 3C 04 06 06 C6 05 64 0A 44 28 00 3C 00 B0 11 E9
C6 81 B0 00 22 A5 05 64 11 C4 3C 00 28 00 67 92 DB C7 01 3C 02 06 3C 03 06 3C
04 06 6F 3C 05 64 0A 44 28 00 3C 00 B0 11 EA C7 81 B0 00 C0 02 05 64 0B C4 3C
00 28 00 CD 56 DC C8 01 3C 01 06 C5 AA 05 64 F9 44 28 00 3C 00 5D B4 EB C8 81
B0 00 01 02 01 00 00 61 00 04 04 04 04 37 94 04 04 00 04 04 04 04 04 04 04 04
04 04 04 04 00 57 2C 04 04 04 00 04 04 04 04 04 04 04 04 04 04 04 04 7A 3F 04
04 00 04 04 04 04 04 04 00 04 04 04 04 04 04 DE C5 04 04 04 04 04 04 04 00 04
04 04 04 04 04 00 04 AA 95 04 04 04 04 04 04 04 00 04 04 04 04 04 04 00 04 AA
95 04 04 04 04 04 04 04 04 04 04 04 04 04 00 1E 02 92 76 01 00 00 21 00 04 00
00 04 00 00 04 00 00 04 00 3B 95 00 04 00 00 04 00 00 04 00 00 04 00 00 04 00
00 F0 E9 04 00 00 04 00 00 04 00 00 04 00 00 04 00 00 04 82 5A 00 00 04 00 00
04 00 00 04 00 00 04 00 00 04 00 9D BD 00 04 00 00 04 00 00 04 00 00 04 00 00
04 00 00 F0 E9 04 00 00 04 00 00 04 00 00 04 00 00 04 00 00 04 82 5A 00 00 04
00 00 04 00 00 04 00 00 0A 02 01 00 00 1B C4 11 00 04 04 04 04 04 04 04 04 04
04 04 04 04 04 6E 6D 04 04 04 04 86 AB 05 64 11 C4 3C 00 28 00 67 92 DD C9 01
3C 02 06 3C 03 06 3C 04 06 9B 0F 05 64 0A 44 28 00 3C 00 B0 11 EC C9 81 B0 00
79 29 05 64 11 C4 3C 00 28 00 67 92 DE CA 01 3C 02 06 3C 03 06 3C 04 06 59 4C
05 64 0A 44 28 00 3C 00 B0 11 ED CA 81 B0 00 3E 00 ^C
D25A>
```

Data Collection: D20MX

- Dump memory
  - ✓ **si** – shows system information including the memory base addresses
  - ✓ **d** – dumps memory, but you have to tell it where to start and stop (only available over serial connection)
- Hand the output to someone who understands VxWorks for analysis
- Look for strings, injected code, or rootkits



```
D20M>si

D20MX Board Information
=======================
Physical RAM base address............... 0x00000000 Size: 1022M Bytes
NVRAM region base address............... 0x50010000 Size: 16320K Bytes
Processor clock......................... 667 MHz
IRIG_B Status........................... BAD
Board ID................................ D20MX
FPGA version............................ 3.04
NVRAM Rev............................... 15

Configuration Signature:
    Date:         2014.09.03 13:25:58
    Version:      78
    Static CRC:   0xA6EE1331
    User Flag:    USED
    Config Name:  FAC_DEF

value = 0
D20M>d 00000000 00000fff
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000060  80 00 00 00 80 00 00 1b  00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000100  7c 73 43 a6 7c 68 02 a6  7c 70 43 a6 3c 60 00 05  ¦sC.¦h..¦pC.<`..
00000110  60 63 79 dc 7c 68 03 a6  7c 70 42 a6 4e 80 00 21  `cy.¦h..¦pB.N..!
00000120  3c 60 00 40 80 63 2d 14  7c 68 03 a6 38 61 00 00  <`.@.c-.¦h..8a..
00000130  94 21 ff f0 4e 80 00 21  38 21 00 10 3c 60 00 05  .!..N..!8!..<`..
00000140  60 63 7d 20 7c 68 03 a6  4e 80 00 21 00 00 00 00  `c} ¦h..N..!....
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

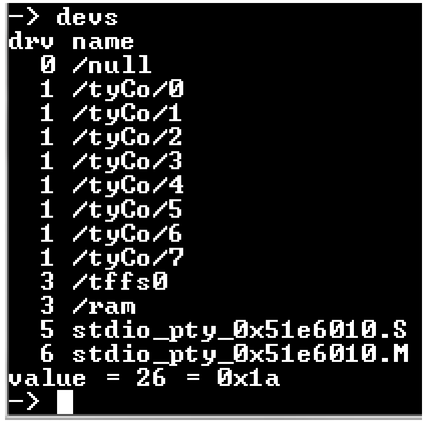
Data Collection: D20MX

VxWorks C Shell

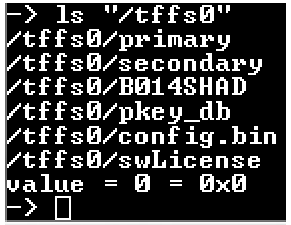
- OS level shell only accessible from the RS-232 port (access is denied from SSH)
- Mainly used by GE customer support for troubleshooting

VxWorks CMD Shell

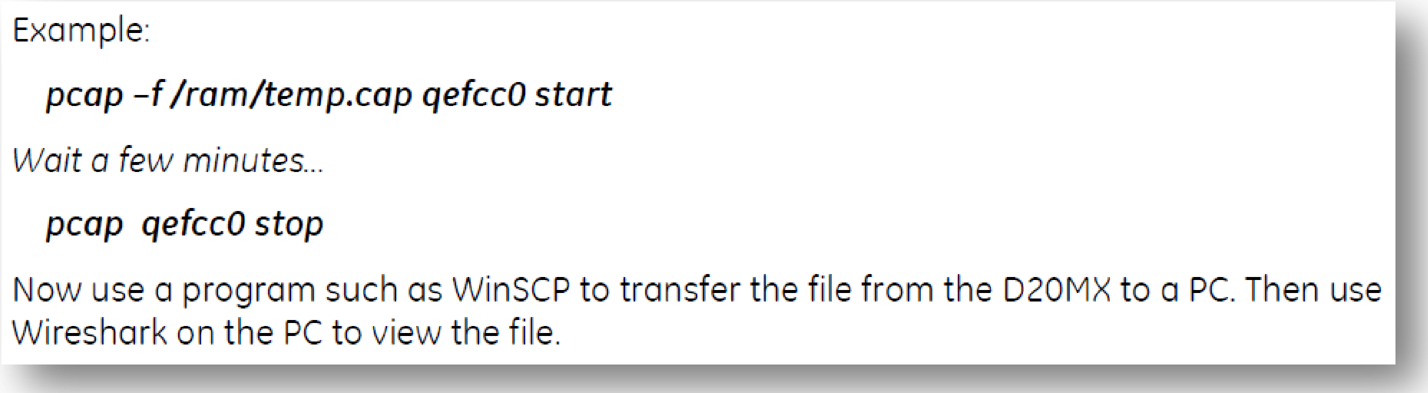
- OS 2nd level shell, accessed by typing **cmd**
- VxWorks Kernel Shell Command Reference 6.9
- We can use some commands for forensics
  - ✓ **d** (dump), **netstat**, **ipf** (firewall), **syslog**, **show devices**, **show drivers**, **show history, ifconfig, route,** and even **pcap!**



```
-> devs
drv name
  0 /null
  1 /tyCo/0
  1 /tyCo/1
  1 /tyCo/2
  1 /tyCo/3
  1 /tyCo/4
  1 /tyCo/5
  1 /tyCo/6
  1 /tyCo/7
  3 /tffs0
  3 /ram
  5 stdio_pty_0x51e6010.S
  6 stdio_pty_0x51e6010.M
value = 26 = 0x1a
->
```



```
-> ls "/tffs0"
/tffs0/primary
/tffs0/secondary
/tffs0/B014SHAD
/tffs0/pkey_db
/tffs0/config.bin
/tffs0/swLicense
value = 0 = 0x0
->
```



Example:

pcap –f /ram/temp.cap qefcc0 start

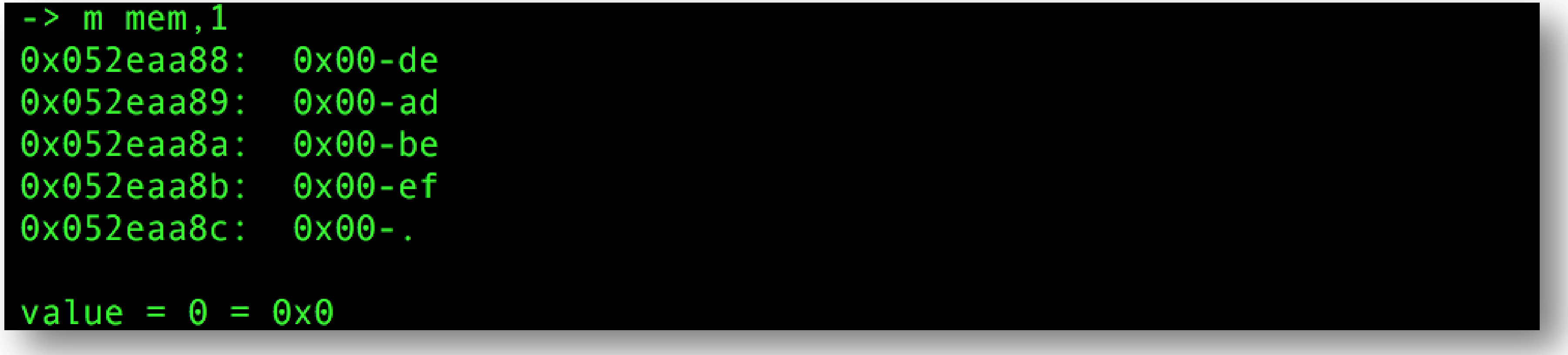
Wait a few minutes…

pcap qefcc0 stop

Now use a program such as WinSCP to transfer the file from the D20MX to a PC. Then use Wireshark on the PC to view the file.

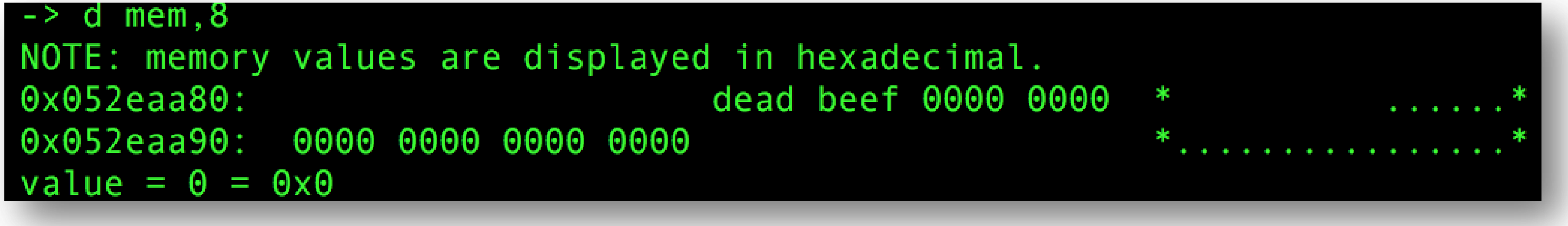
Example of live memory code injection & mem dump on the D20MX

- Inject code via VxWorks C shell memory edit command **m** to simulate a rootkit



```
-> m mem,1
0x052eaa88:  0x00-de
0x052eaa89:  0x00-ad
0x052eaa8a:  0x00-be
0x052eaa8b:  0x00-ef
0x052eaa8c:  0x00-.

value = 0 = 0x0
```

- Collect volatile memory using the dump memory command **d**



```
-> d mem,8
NOTE: memory values are displayed in hexadecimal.
0x052eaa80:                      dead beef 0000 0000  *          ......*
0x052eaa90:  0000 0000 0000 0000                      *................*
value = 0 = 0x0
```

Data Collection: VxWorks DFIR Tool – Problem

- We need tools that enable us to perform DFIR on ICS and embedded devices.

Data Collection: VxWorks DFIR Tool - Solution

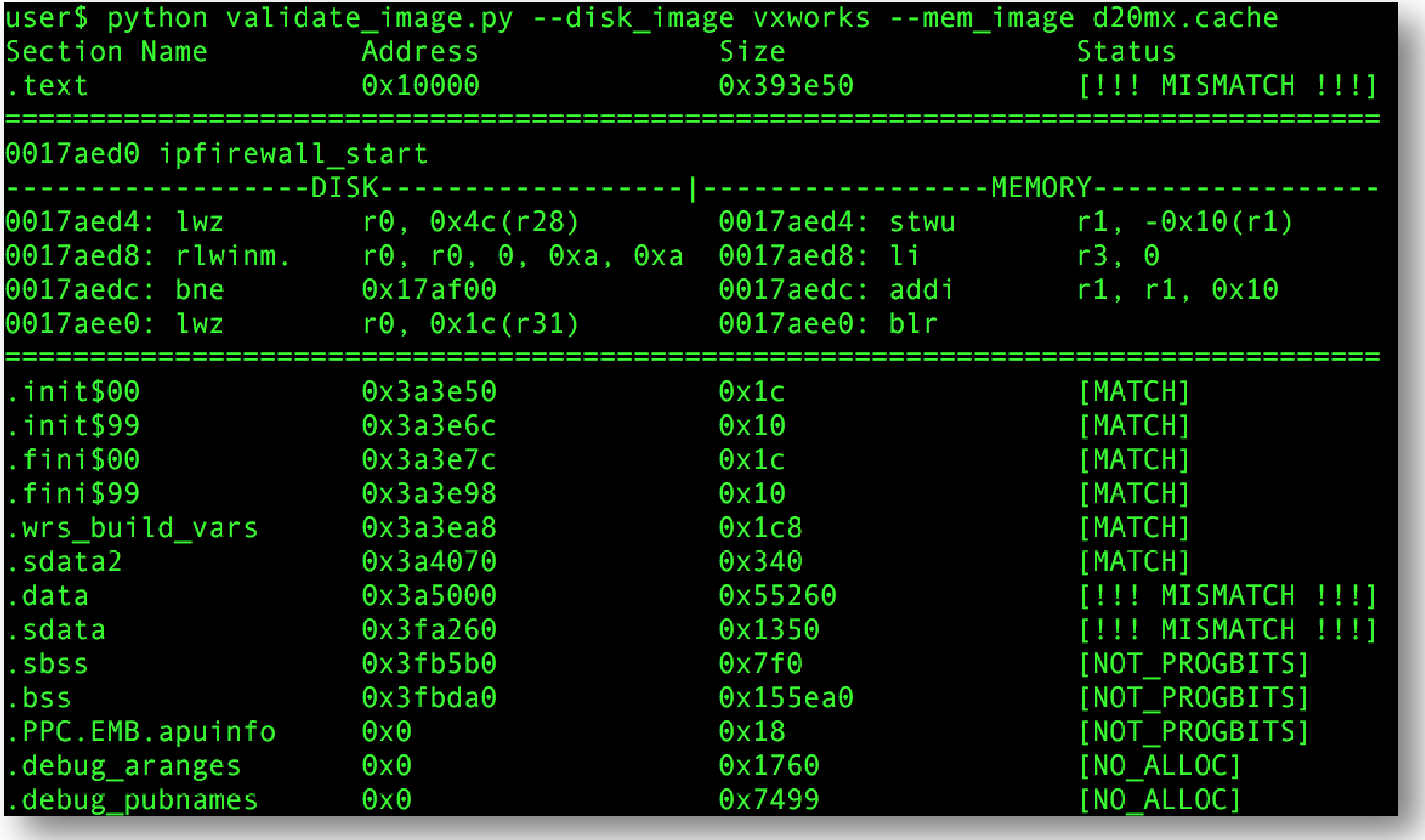
A collection of utilities that enable us to:

- Read (and write) to memory on the device programmatically
  - We don’t want to have do dump memory manually
- Cache the live memory locally
  - We shouldn’t need to fetch the same memory twice to check for different issues.
- Compare the system image
  - Knowing the image is good is the first step toward looking somewhere else.
- Provide the ability to read/write and cache device data to other tools
  - Tools can be written more generically when they don’t need to worry about how to get the data

Data Collection: VxWorks DFIR Tool - Cool Features

- Can easily accommodate different transport mechanisms
  - Serial
  - TCP/Serial bridges
  - Protocols specific to other dumping utilities
- Supports caching
  - Allows resuming if connectivity is lost
  - Sparse memory dumping
- Comparative analysis works on
  - Anything that looks like a seek-able Python File Object
    - Cache Files
    - Memory Dumps
    - Sparse Memory Maps
    - Special Objects that request live memory

Data Collection: VxWorks DFIR Tool – Validating the host image



```
user$ python validate_image.py --disk_image vxworks --mem_image d20mx.cache
Section Name         Address              Size                 Status
.text                0x10000              0x393e50             [!!! MISMATCH !!!]
=================================================================================
0017aed0 ipfirewall_start
------------------DISK------------------|-----------------MEMORY-----------------
0017aed4: lwz        r0, 0x4c(r28)        0017aed4: stwu       r1, -0x10(r1)
0017aed8: rlwinm.    r0, r0, 0, 0xa, 0xa  0017aed8: li         r3, 0
0017aedc: bne        0x17af00             0017aedc: addi       r1, r1, 0x10
0017aee0: lwz        r0, 0x1c(r31)        0017aee0: blr
=================================================================================
.init$00             0x3a3e50             0x1c                 [MATCH]
.init$99             0x3a3e6c             0x10                 [MATCH]
.fini$00             0x3a3e7c             0x1c                 [MATCH]
.fini$99             0x3a3e98             0x10                 [MATCH]
.wrs_build_vars      0x3a3ea8             0x1c8                [MATCH]
.sdata2              0x3a4070             0x340                [MATCH]
.data                0x3a5000             0x55260              [!!! MISMATCH !!!]
.sdata               0x3fa260             0x1350               [!!! MISMATCH !!!]
.sbss                0x3fb5b0             0x7f0                [NOT_PROGBITS]
.bss                 0x3fbda0             0x155ea0             [NOT_PROGBITS]
.PPC.EMB.apuinfo     0x0                  0x18                 [NOT_PROGBITS]
.debug_aranges       0x0                  0x1760               [NO_ALLOC]
.debug_pubnames      0x0                  0x7499               [NO_ALLOC]
```

Data Collection: VxWorks DFIR Tool - Cool Projects We Used

- CLE Loads Everything – (angr/CLE)
  - Loads our system image and provides an abstraction to a process memory space
  - Identifies architecture, endianness, etc.
  - Will soon support relocatable images (important for modules like appl.out)

- Capstone - Nguyen Anh Quynh
  - Easy access to disassemble exactly what we needed

Data Collection: VxWorks DFIR Tool – Plans for the Future

- Documentation
- Expand the tool to work on other devices
- Refine the scripts into easy-to-use modules
- Moving the code to GitHub
- Allow for feedback / feature requests / bug submissions

Data Collection: SEL-3530 RTAC

<u>Specs</u>

- 533 MHz Power PC
- 1024 MB DDR2 ECC RAM
- 2GB Storage
- Embedded SEL Linux

<u>Tools to use</u>

- *SEL-3530 RTAC Instruction Manual*
- *SEL-5033 Instruction Manual*
- SEL-5033 software
- Web Browser (Chrome, FireFox, etc)
- Terminal for SSH (Tera Term, PuTTY)

SEL-3530

Real-Time
Automation Controller
(RTAC)

Instruction Manual

20150904

SEL SCHWEITZER ENGINEERING LABORATORIES, INC.

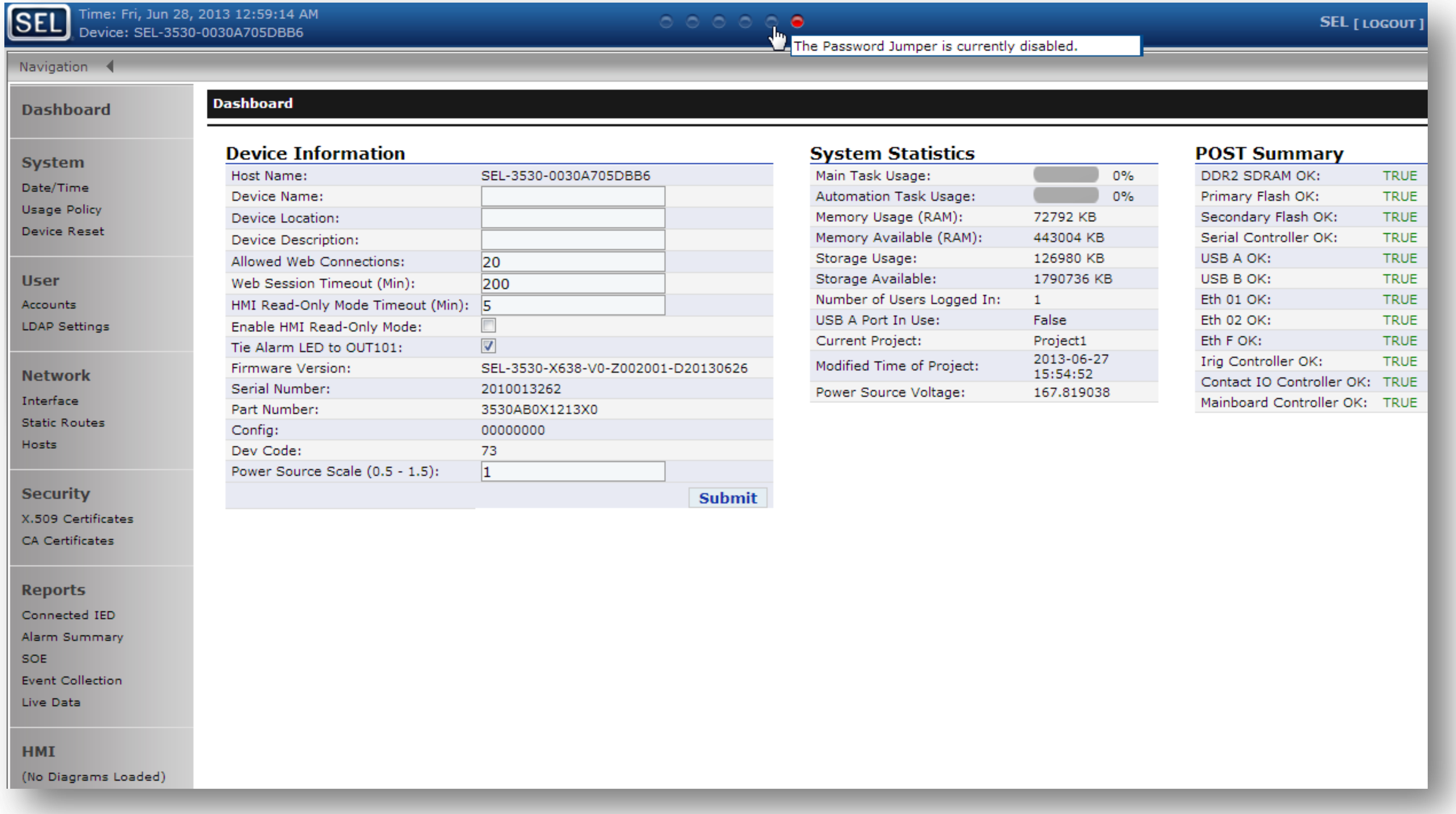
Data Collection: SEL-3530

Digital data

- Running configuration
- User Accounts
- Running firmware
- CPU usage %
- Memory usage %
- POST checks
- Reports (several)

Physical Data

- Password jumper



Time: Fri, Jun 28, 2013 12:59:14 AM
Device: SEL-3530-0030A705DBB6

The Password Jumper is currently disabled.

Device Information

Host Name:	SEL-3530-0030A705DBB6
Device Name:	
Device Location:	
Device Description:	
Allowed Web Connections:	20
Web Session Timeout (Min):	200
HMI Read-Only Mode Timeout (Min):	5
Enable HMI Read-Only Mode:	☐
Tie Alarm LED to OUT101:	☑
Firmware Version:	SEL-3530-X638-V0-Z002001-D20130626
Serial Number:	2010013262
Part Number:	3530AB0X1213X0
Config:	00000000
Dev Code:	73
Power Source Scale (0.5 - 1.5):	1

Submit

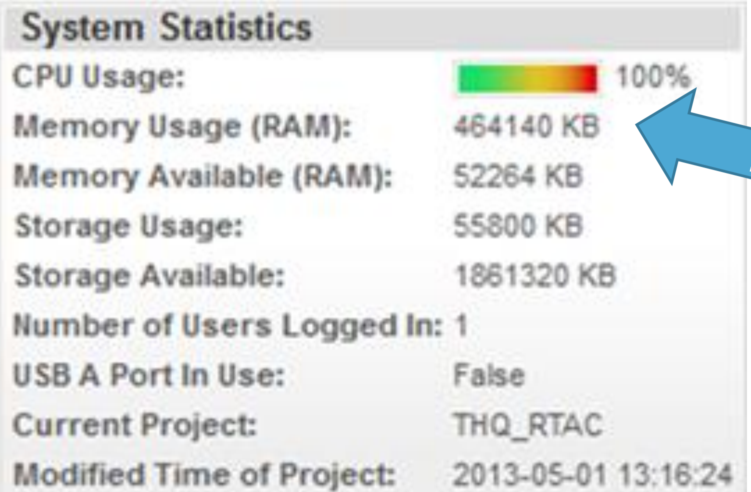
System Statistics

Main Task Usage:	0%
Automation Task Usage:	0%
Memory Usage (RAM):	72792 KB
Memory Available (RAM):	443004 KB
Storage Usage:	126980 KB
Storage Available:	1790736 KB
Number of Users Logged In:	1
USB A Port In Use:	False
Current Project:	Project1
Modified Time of Project:	2013-06-27 15:54:52
Power Source Voltage:	167.819038

POST Summary

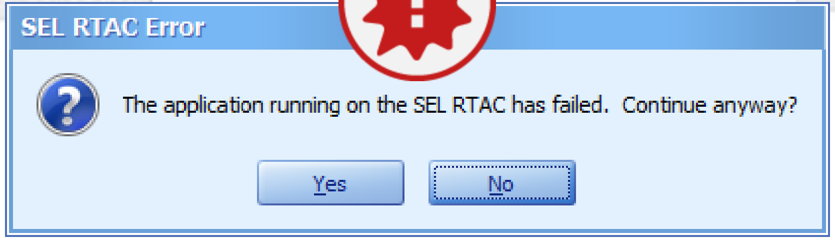
DDR2 SDRAM OK:	TRUE
Primary Flash OK:	TRUE
Secondary Flash OK:	TRUE
Serial Controller OK:	TRUE
USB A OK:	TRUE
USB B OK:	TRUE
Eth 01 OK:	TRUE
Eth 02 OK:	TRUE
Eth F OK:	TRUE
Irig Controller OK:	TRUE
Contact IO Controller OK:	TRUE
Mainboard Controller OK:	TRUE

Data Collection: SEL-3530



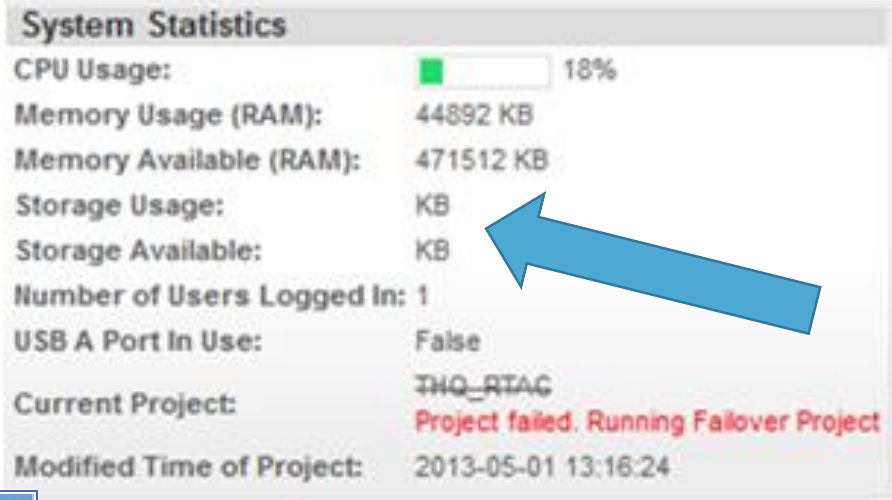
System Statistics

CPU Usage:	100%
Memory Usage (RAM):	464140 KB
Memory Available (RAM):	52264 KB
Storage Usage:	55800 KB
Storage Available:	1861320 KB
Number of Users Logged In:	1
USB A Port In Use:	False
Current Project:	THQ_RTAC
Modified Time of Project:	2013-05-01 13:16:24



SEL RTAC Error

The application running on the SEL RTAC has failed. Continue anyway?



System Statistics

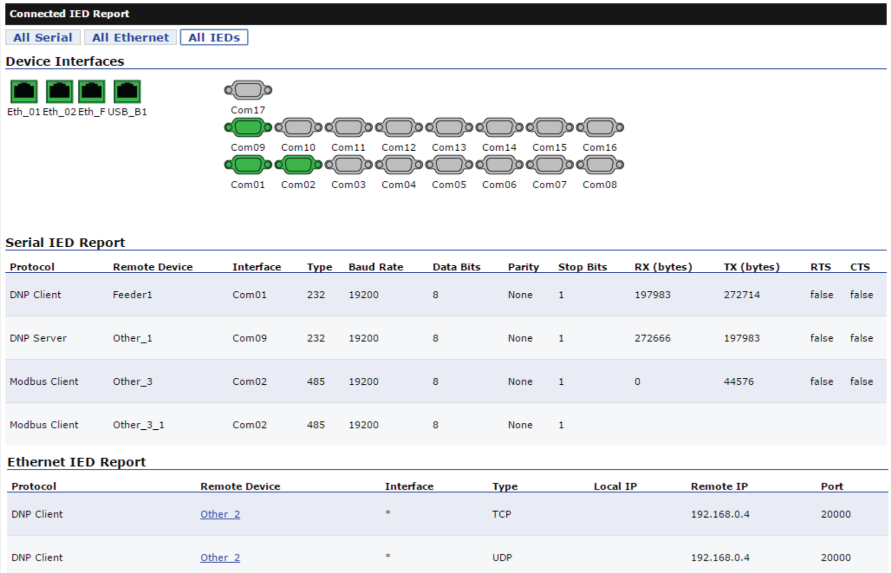
CPU Usage:	18%
Memory Usage (RAM):	44892 KB
Memory Available (RAM):	471512 KB
Storage Usage:	KB
Storage Available:	KB
Number of Users Logged In:	1
USB A Port In Use:	False
Current Project:	~~THQ_RTAC~~ Project failed. Running Failover Project
Modified Time of Project:	2013-05-01 13:16:24

These are the screenshots from when I sent a malformed DNP3 message that caused the RTAC to lose the configuration.

https://ics-cert.us-cert.gov/advisories/ICSA-13-219-01

Data Collection: SEL-3530

- Section 3: Testing and Troubleshooting
- Section 5: Web HMI and Logging
- Section 6: Security
- There are tags in the RTAC database that are assigned to help troubleshoot but are also useful for forensics as well.
- Several log types
    - SOE report
    - IED report
    - **syslog**



Connected IED Report

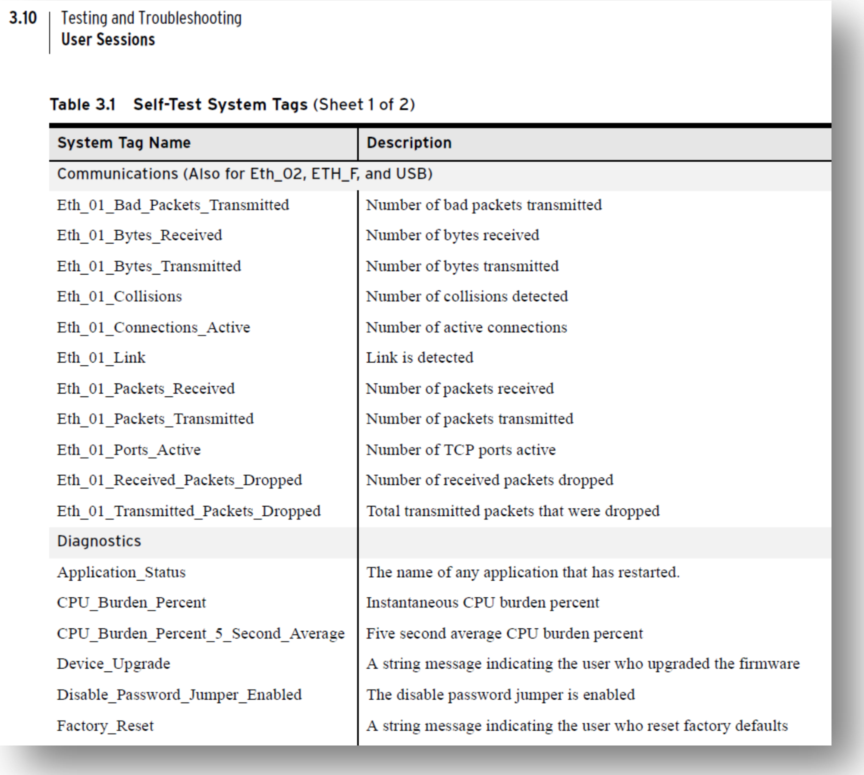
Device Interfaces

Serial IED Report

Protocol	Remote Device	Interface	Type	Baud Rate	Data Bits	Parity	Stop Bits	RX (bytes)	TX (bytes)	RTS	CTS
DNP Client	Feeder1	Com01	232	19200	8	None	1	197983	272714	false	false
DNP Server	Other_1	Com09	232	19200	8	None	1	272666	197983	false	false
Modbus Client	Other_3	Com02	485	19200	8	None	1	0	44576	false	false
Modbus Client	Other_3_1	Com02	485	19200	8	None	1				

Ethernet IED Report

Protocol	Remote Device	Interface	Type	Local IP	Remote IP	Port
DNP Client	Other_2	*	TCP		192.168.0.4	20000
DNP Client	Other_2	*	UDP		192.168.0.4	20000



3.10 | Testing and Troubleshooting
User Sessions

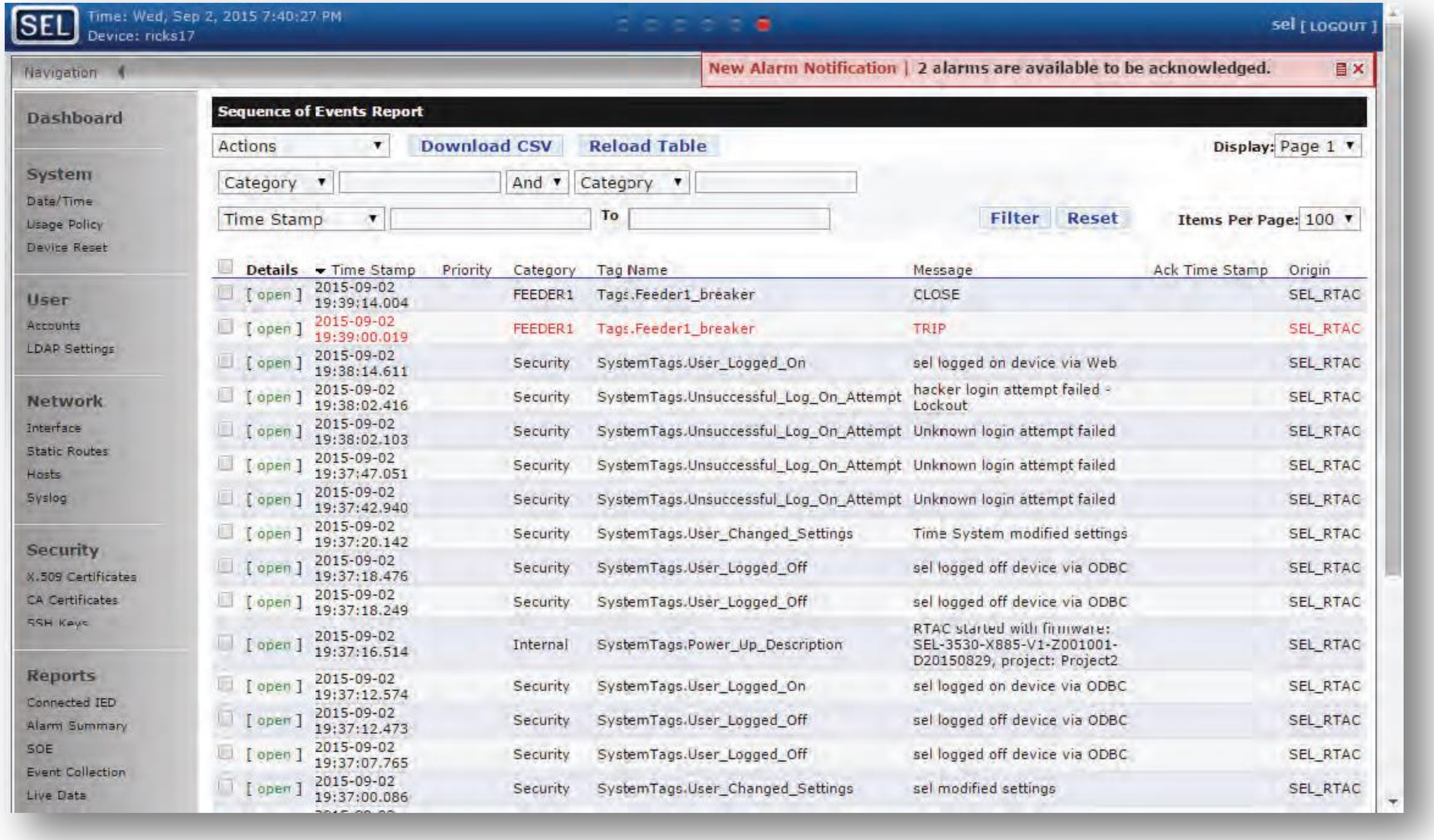
Table 3.1 Self-Test System Tags (Sheet 1 of 2)

System Tag Name	Description
Communications (Also for Eth_02, ETH_F, and USB)	
Eth_01_Bad_Packets_Transmitted	Number of bad packets transmitted
Eth_01_Bytes_Received	Number of bytes received
Eth_01_Bytes_Transmitted	Number of bytes transmitted
Eth_01_Collisions	Number of collisions detected
Eth_01_Connections_Active	Number of active connections
Eth_01_Link	Link is detected
Eth_01_Packets_Received	Number of packets received
Eth_01_Packets_Transmitted	Number of packets transmitted
Eth_01_Ports_Active	Number of TCP ports active
Eth_01_Received_Packets_Dropped	Number of received packets dropped
Eth_01_Transmitted_Packets_Dropped	Total transmitted packets that were dropped
Diagnostics	
Application_Status	The name of any application that has restarted.
CPU_Burden_Percent	Instantaneous CPU burden percent
CPU_Burden_Percent_5_Second_Average	Five second average CPU burden percent
Device_Upgrade	A string message indicating the user who upgraded the firmware
Disable_Password_Jumper_Enabled	The disable password jumper is enabled
Factory_Reset	A string message indicating the user who reset factory defaults

Data Collection: SEL-3530

- Example of IED Report
- Can be accessed via web or ODBC (MS Access)

- **No Linux Shell**
- **Pros & cons**
- No SSH Interface with RTAC
    - SSH used for engineering remote access to relays



Time: Wed, Sep 2, 2015 7:40:27 PM
Device: ricks17

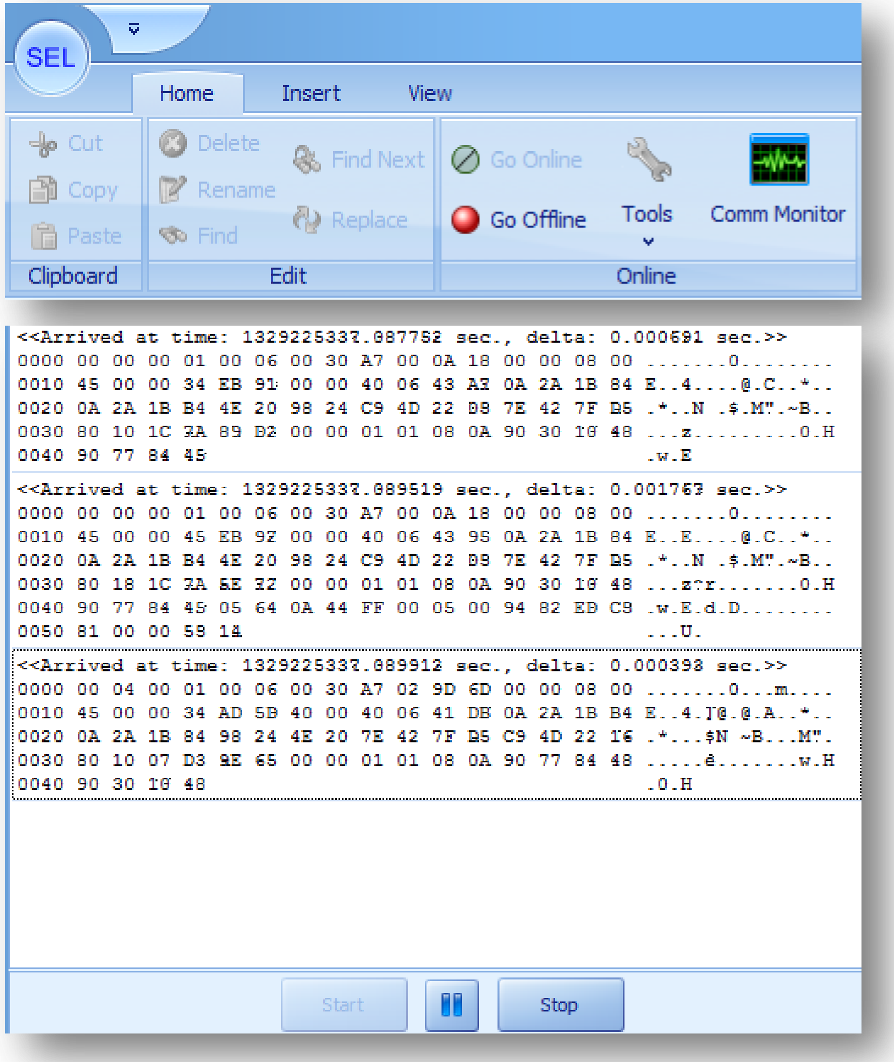
New Alarm Notification | 2 alarms are available to be acknowledged.

Sequence of Events Report

Details	Time Stamp	Priority	Category	Tag Name	Message	Ack Time Stamp	Origin
[open]	2015-09-02 19:39:14.004		FEEDER1	Tags.Feeder1_breaker	CLOSE		SEL_RTAC
[open]	2015-09-02 19:39:00.019		FEEDER1	Tags.Feeder1_breaker	TRIP		SEL_RTAC
[open]	2015-09-02 19:38:14.611		Security	SystemTags.User_Logged_On	sel logged on device via Web		SEL_RTAC
[open]	2015-09-02 19:38:02.416		Security	SystemTags.Unsuccessful_Log_On_Attempt	hacker login attempt failed - Lockout		SEL_RTAC
[open]	2015-09-02 19:38:02.103		Security	SystemTags.Unsuccessful_Log_On_Attempt	Unknown login attempt failed		SEL_RTAC
[open]	2015-09-02 19:37:47.051		Security	SystemTags.Unsuccessful_Log_On_Attempt	Unknown login attempt failed		SEL_RTAC
[open]	2015-09-02 19:37:42.940		Security	SystemTags.Unsuccessful_Log_On_Attempt	Unknown login attempt failed		SEL_RTAC
[open]	2015-09-02 19:37:20.142		Security	SystemTags.User_Changed_Settings	Time System modified settings		SEL_RTAC
[open]	2015-09-02 19:37:18.476		Security	SystemTags.User_Logged_Off	sel logged off device via ODBC		SEL_RTAC
[open]	2015-09-02 19:37:18.249		Security	SystemTags.User_Logged_Off	sel logged off device via ODBC		SEL_RTAC
[open]	2015-09-02 19:37:16.514		Internal	SystemTags.Power_Up_Description	RTAC started with firmware: SEL-3530-X885-V1-Z001001-D20150829, project: Project2		SEL_RTAC
[open]	2015-09-02 19:37:12.574		Security	SystemTags.User_Logged_On	sel logged on device via ODBC		SEL_RTAC
[open]	2015-09-02 19:37:12.473		Security	SystemTags.User_Logged_Off	sel logged off device via ODBC		SEL_RTAC
[open]	2015-09-02 19:37:07.765		Security	SystemTags.User_Logged_Off	sel logged off device via ODBC		SEL_RTAC
[open]	2015-09-02 19:37:00.086		Security	SystemTags.User_Changed_Settings	sel modified settings		SEL_RTAC

Data Collection: SEL-3530

- The RTAC can capture ethernet and serial traffic
  - ✓ SEL-5033 software and the Comm Monitor
- AG2012-15 *Using Wireshark® to Troubleshoot Protocol Communications Issues on an RTAC*
  - ✓ DNP3 example
- AG2015-15 *Using Wireshark® to Decode RTAC Serial Line Messages and SEL Protocols*
  - ✓ SEL Fast Messaging example
- SEL published several serial Wireshark dissectors
  - ✓ SELFM, Telegyr 8979



```
<<Arrived at time: 1329225337.087752 sec., delta: 0.000691 sec.>>
0000 00 00 00 01 00 06 00 30 A7 00 0A 18 00 00 08 00 ........0.......
0010 45 00 00 34 EB 91 00 00 40 06 43 A3 0A 2A 1B 84 E..4....@.C..*..
0020 0A 2A 1B B4 4E 20 98 24 C9 4D 22 D9 7E 42 7F B5 .*..N .$.M".~B..
0030 80 10 1C 7A 89 B2 00 00 01 01 08 0A 90 30 1E 48 ...z.........0.H
0040 90 77 84 45                                     .w.E

<<Arrived at time: 1329225337.089519 sec., delta: 0.001767 sec.>>
0000 00 00 00 01 00 06 00 30 A7 00 0A 18 00 00 08 00 ........0.......
0010 45 00 00 45 EB 97 00 00 40 06 43 95 0A 2A 1B 84 E..E....@.C..*..
0020 0A 2A 1B B4 4E 20 98 24 C9 4D 22 D9 7E 42 7F B5 .*..N .$.M".~B..
0030 80 18 1C 7A 5E 72 00 00 01 01 08 0A 90 30 1E 48 ...z^r.......0.H
0040 90 77 84 45 05 64 0A 44 FF 00 05 00 94 82 ED C9 .w.E.d.D........
0050 81 00 00 58 14                                  ...U.

<<Arrived at time: 1329225337.089912 sec., delta: 0.000393 sec.>>
0000 00 04 00 01 00 06 00 30 A7 02 9D 6D 00 00 08 00 ........0...m....
0010 45 00 00 34 AD 5B 40 00 40 06 41 DB 0A 2A 1B B4 E..4.]@.@.A..*..
0020 0A 2A 1B 84 98 24 4E 20 7E 42 7F B5 C9 4D 22 16 .*...$N ~B...M".
0030 80 10 07 D3 9E 65 00 00 01 01 08 0A 90 77 84 48 .....ê.......w.H
0040 90 30 1E 48                                     .0.H
```

For Further Reading…

- HD Moore’s blogpost on VxWorks from 2010.
  - https://community.rapid7.com/community/metasploit/blog/2010/08/02/shiny-old-vxworks-vulnerabilities
  - Metasploit module for VxWorks remote memory dump (**wdbrpc_memory_dump**)

- David Odell’s blogpost on QNX from 2012.
  - https://www.optiv.com/blog/pentesting-qnx-neutrino-rtos

- ICS-CERT recommended practices for ICS forensics
  - https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Forensics_RP.pdf

For Further Reading…

- Travis Goodspeed’s embedded device work on the MSP430 family
  - http://travisgoodspeed.blogspot.com/2007/11/ti-ez430-in-linux-with-iar-kickstart.html
  - http://travisgoodspeed.blogspot.com/2008/08/repurposing-ti-ez430u-part-3.html
- Ralph Langner’s forensics work on Stuxnet payloads for Siemens PLCs
  - http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
- The Dec 23, 2015 Ukrainian Power Grid attack included writing over firmware of embedded Ethernet-serial converters.
  - https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

QUESTIONS?