网络安全创新大会
Cyber Security Innovation Summit

工控设备数字取证破冰之战

高剑　绿盟科技 工控安全研究员

高 剑

- 绿盟科技，格物实验室
- 工控安全研究员
- 主要方向：工控系统及设备漏洞挖掘与分析、工控业务场景风险评估与测试
- 已获得数十个CVE、CNVD、CICSVD编号（ Siemens、Codesys、Schneider、组态王等）
- 看雪 SDC 2020 演讲嘉宾

目录

网络安全创新大会
Cyber Security Innovation Summit

背景概述

VS

个人或者小团体犯罪行为

对象为IT领域软件或硬件

有成熟的流程或者工具、方法

……

敌对势力、恐怖组织、国家力量等

对象为OT领域各种复杂、多样的专用设备与系统

目前没有明确的提法，更没有工具、方法与流程……

ICS数字取证挑战与流程

ICS系统的连续运行

- 是否有实时取证的措施？
- 如何处理易失性内存类设备的证据？

ICS系统设备与软件多样、复杂

- 厂区内包含控制设备种类多、品牌多、设计各不相同，如何取证？
- 软件及专用系统不同于IT领域，也存在多个厂家的不同种类，如何取证？

快速处理，快速恢复生产

- 如何在证据未被冲刷前保障取证时效性？
- 快速处理整个事件，确保恢复生产降低损失？

ICS缺失DFIR（数字取证与事件应急响应）的流程与工具

- ICS领域缺失专业的分析流程与指导方法；
- ICS领域更缺乏专业工具集，现阶段只能依靠人工分析，急需专业的设备与工具；

流量取证分析更困难、易失性内存取证壁垒高……

ICS数字取证挑战与流程

及时认识ICS的异常状况；
按规程处置与上报事件；

识别受影响区域、组件、进程、设备……；
受影响事务的隔离处理；

设备数据源：内存、存储卡、日志等；
网络数据源：历史流量、ARP表、相关日志……

异常或者事件调查结果总结、事件线串接、取证不足点讨论……

预处理 → 准备 → 识别 → 分类 → 采集 → 分析 → 报告 → 跟踪

资料：ICS系统组成、网络拓扑、资产列表……；
相关人员访谈、记录；……

受影响系统、设备、软件等分门别类；
按照关键性、可获取性、证据驻留时间排优先级……

文本化日志分析：归一化处理、事件线梳理……
二进制文件分析：恶意文件查找……

不足之处的补充，综合人员访谈和电子证据，得出结论，进行汇报……

工控设备实时取证方案及实践

本议题关注 ICS领域工控设备数字取证技术：

- 立足**预防角度**——提出实时取证的解决方案；
- **抓重点、强聚焦**——以西门子工控设备为研究对象；
- **不同技术方向**的尝试——设备类日志取证实践、设备类特殊取证工具实践。

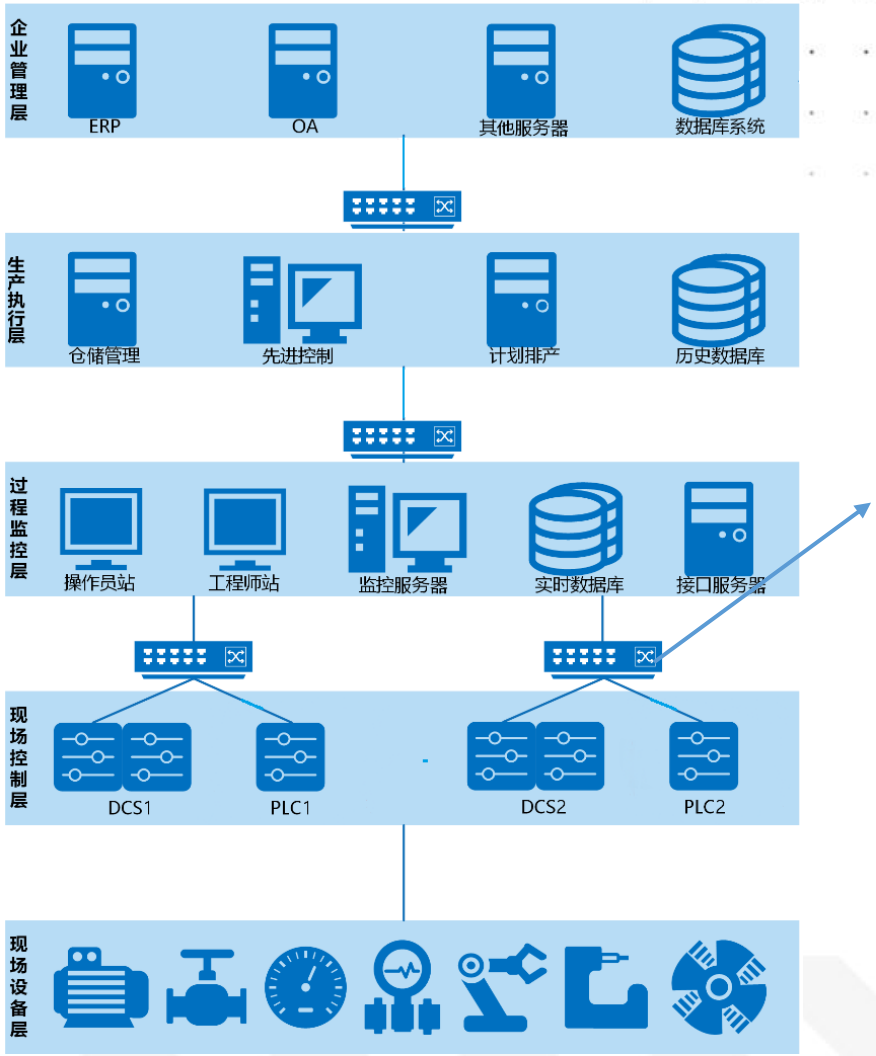
工控设备实时取证方案及实践

事后取证弊端：

- 流量未做记录，或者被冲刷、无法在庞杂流量中定位
- 由于工控设备内存小，记录的日志条目有限，不能保证所有恶意行为均被记录
- 不易从设备中提取日志记录……

现有安全审计类产品弊端：

- 审计的范围与动作有限，不能识别出所有的操作，无法解析业务强相关的动作；
- 重点在审计行为，而不是构建证据场景，功能单一；

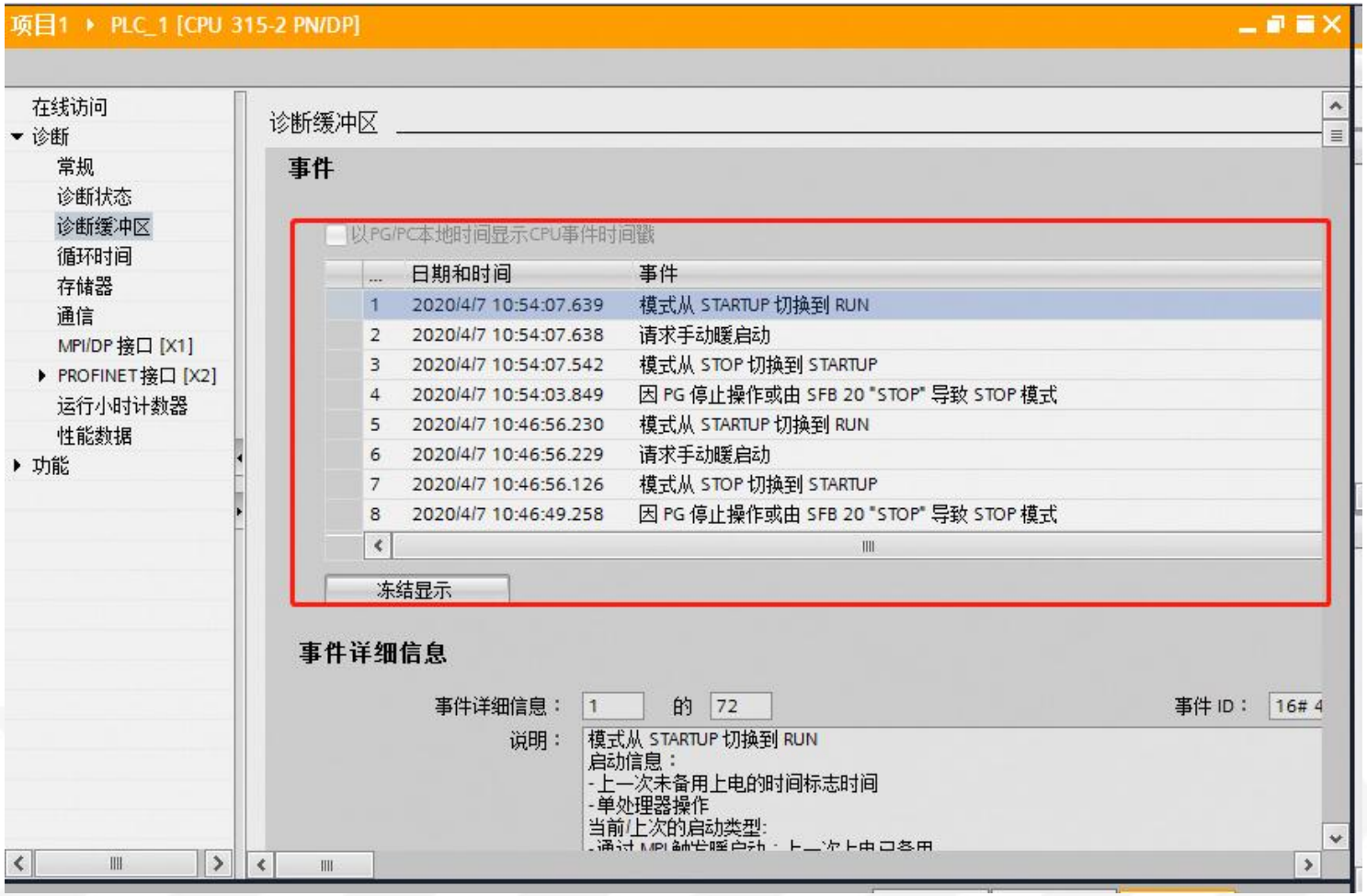


- 取证模块处理流量记录特定区域；
- 用户设定周期**采集不同设备日志信息；**
- 预置点表与逻辑映射文件，记录业务关键操作证据；
- 与情报系统连接，融合威胁信息；
- 编排组件。融合信息串接为时间线形成报告；
- ……

工控设备实时取证方案及实践

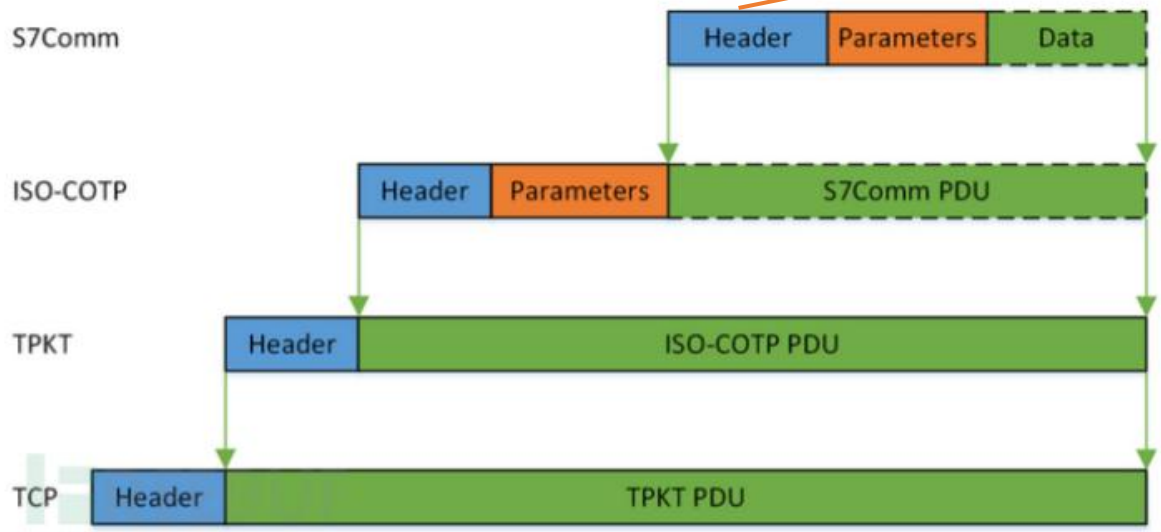
研究对象：Siemens S7 PLC

研究内容：采集分析PLC内部记录日志信息



- 西门子PLC内部有诊断缓冲区，该部分包含有错误事件、模式改变和其它对用户重要的操作事件、用户定义的诊断事件（诊断事件包括模块故障、过程写错误、CPU中的系统错误、CPU运行模式的切换、用户程序的错误等）等，这类事件的记录比较完善可以反映外部输入对控制器的操作和控制器本身的大部分故障原因；
- 以上作为取证数据最为恰当
- 诊断缓冲区为PLC的固有功能不依赖与用户的程序或者配置。

研究方法：通信协议分析与实现




```
S7 Communication
  Header: (Userdata)
    Protocol Id: 0x32
    ROSCTR: Userdata (7)
    Redundancy Identification (Reserved): 0x0000
    Protocol Data Unit Reference: 3328
    Parameter length: 8
    Data length: 8
  Parameter: (Request) ->(CPU functions) ->(Read SZL)
  Data (SZL-ID: 0x0011, Index: 0x0000)
```

```
S7 Communication
  Header: (Userdata)
  Parameter: (Request) ->(CPU functions) ->(Read SZL)
    Parameter head: 0x000112
    Parameter length: 4
    Method (Request/Response): Req (0x11)
    0100 .... = Type: Request (4)
    .... 0100 = Function group: CPU functions (4)
    Subfunction: Read SZL (1)
    Sequence number: 0
  Data (SZL-ID: 0x0132, Index: 0x0004)
```

0x01：JOB
即作业请求，如，读/写存储器，读/写块，启动/停止设备，设置通信
0x02：ACK
即确认，这是一个没有数据的简单确认
0x03：ACK_DATA
即确认数据的响应，一般是响应JOB的请求
0x07：USERDATA
即扩展协议，其参数分段包含请求/响应ID，一般用于编程/调试，**读取SZL等**

系统状态列表（德语：System-ZustandsListen，英语：System Status Lists）用于描述PLC的当前状态，系统状态列表的内容只能读取不能修改。

工控设备实时取证方案及实践

The following table lists all the possible partial lists with the number contained in the SSL-ID.

Partial List	SSL-ID
Module identification	W#16#xy11
CPU characteristics	W#16#xy12
User memory areas	W#16#xy13
System areas	W#16#xy14
Block types	W#16#xy15
Interrupt status	W#16#xy22
Assignment between process image partitions and OBs	W#16#xy25
Communication status data	W#16#xy32
H CPU group information	W#16#xy71
Status of the module LEDs	W#16#xy74
Switched DP slaves in the H-system	W#16#xy75
Module status information	W#16#xy91
Rack / station status information	W#16#xy92
Rack / station status information	W#16#0x94
Extended DP master system / PROFINET IO system information	W#16#xy95
Module status information, PROFINET IO and PROFIBUS DP	W#16#xy96
Tool changer information (PROFINET IO)	W#16#xy9C
Diagnostic buffer of the CPU	W#16#xyA0
Module diagnostic information (data record 0)	W#16#00B1
Module diagnostic information (data record 1), geographical address	W#16#00B2
Module diagnostic information (data record 1), logical address	W#16#00B3
Diagnostic data of a DP slave	W#16#00B4

```
S7 Communication
  > Header: (Userdata)
  > Parameter: (Request) ->(CPU functions) ->(Read SZL)
  v Data (SZL-ID: 0x00a0, Index: 0x547f)
      Return code: Success (0xff)
      Transport size: OCTET STRING (0x09)
      Length: 4
    v SZL-ID: 0x00a0, Diagnostic type: CPU, Number of the partial list extract: All entries possible in the current mode, Nu
        0000 .... .... .... = Diagnostic type: CPU (0x0)
        0000 0000 1010 0000 = Number of the partial list extract: All entries possible in the current mode (0x00a0)
        .... .... 1010 0000 = Number of the partial list: Diagnostic buffer of the CPU (0xa0)
      SZL-Index: 0x547f
```

```
S7 Communication
  > Header: (Userdata)
  > Parameter: (Response) ->(CPU functions) ->(Read SZL)
  v Data (SZL-ID: 0x00a0, Index: 0x0000)
      Return code: Success (0xff)
      Transport size: OCTET STRING (0x09)
      Length: 214
    v SZL-ID: 0x00a0, Diagnostic type: CPU, Number of the partial list extract: All entries possible in the current mode,
        0000 .... .... .... = Diagnostic type: CPU (0x0)
        0000 0000 1010 0000 = Number of the partial list extract: All entries possible in the current mode (0x00a0)
        .... .... 1010 0000 = Number of the partial list: Diagnostic buffer of the CPU (0xa0)
      SZL-Index: 0x0000
      SZL partial list length in bytes: 20
      SZL partial list count: 87
    v SZL data tree (list count no. 1)
      v CPU diagnostic message: Event='STOP caused by PG STOP operation or by SFB 20 STOP'
        > Event ID: 0x4304, Event class: Mode transitions, Event entering state, Entry in diagnostic buffer
          Priority class: 255
          OB number: 132
          DatID: 0x0000
          INFO1 Additional information 1: 0x0000
          INFO2 Additional information 2: 0x00000000
        > S7 Timestamp: Apr 23, 2020 14:53:21.705
```

事件总数

事件描述

事件代码

时间戳

报文解析与归一化处理：

```
43 01 ff 46 c7 72 43 04   00 14 77 14 20 03 19 14    C··F·rC·  ··w· ···
51 49 66 55 43 04 ff 84   00 00 00 00 00 00 00 00    QIfUC···  ········
```

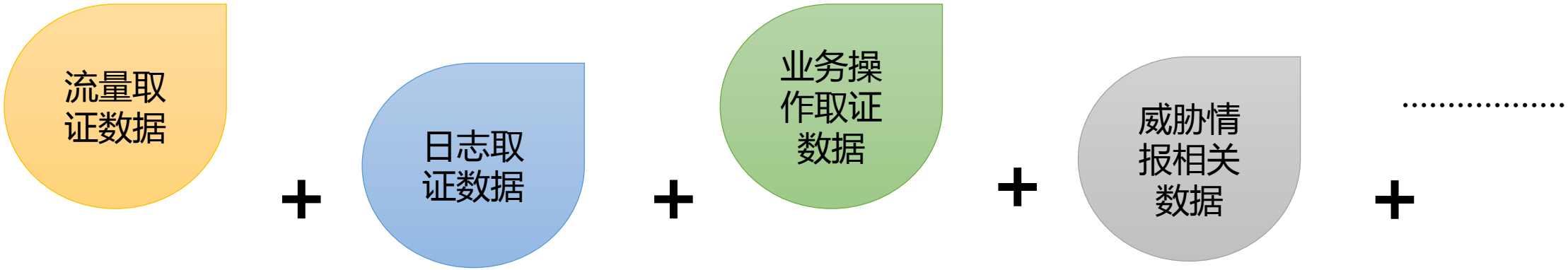
什么时间？针对Siemens S7 PLC的什么位置？做了什么事情？产生了什么结果？.....

```
0x4001 :'''模式从 STOP 切换到 STARTUP''' ,
0x4002 :'''模式从 STARTUP 切换到 RUN''' ,
0x4003 :'''激活停止开关导致 STOP 模式''' ,
0x4004 :'''因 PG 停止操作或由 SFB 20 "STOP" 导致 STOP 模式''' ,
0x4005 :'''HOLD：到达断点''' ,
0x4006 :'''HOLD：退出断点''' ,
0x4007 :'''由 PG 操作启动存储器复位''' ,
0x4008 :'''通过开关设置启动存储器复位''' ,
0x4009 :'''自动启动存储器复位''' ,
0x400a :'''退出 HOLD, 切换到 STOP''' ,
```

.....
"time":"2019-12-17 07:25:56" "event":"所有模块都做好运行准备"
"time":"2019-12-17 07:25:55" "event":"模块监视时间已启动"
"time":"2019-12-17 07:25:54" "event":"备用上电"
"time":"2019-12-17 06:21:18" "event":"电源故障"
"time":"2019-07-09 15:44:18" "event":"模式从 STARTUP 切换到 RUN “
"time":"2019-07-09 15:44:18" "event":"请求手动暖启动 “
"time":"2019-07-09 15:44:18" "event":"模式从 STOP 切换到 STARTUP"
.....

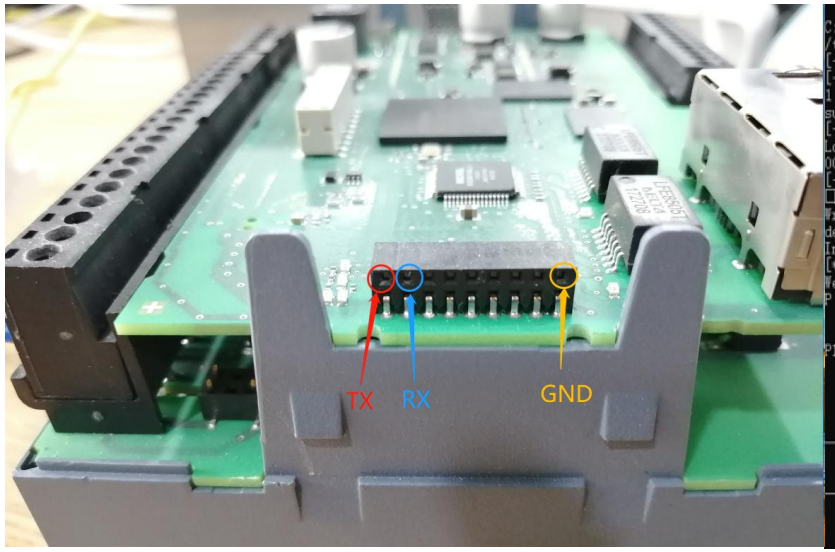
工控设备实时取证方案及实践

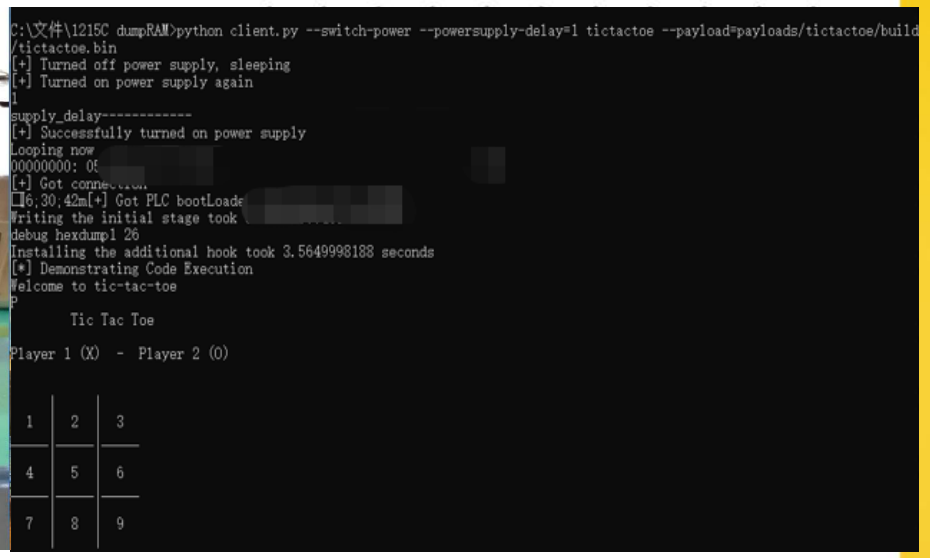
事件线融合：



2020-05-18 02:25:36 IP:10.60.67.54 对ENG1: 10.60.67.79 利用 “永恒之蓝”漏洞发起攻击
2020-05-19 11:21:32 IP:10.60.67.79 对PLC1：10.60.60.129 执行“停止”操作。
2020-05-19 11:21:35 IP:10.60.67.79 对PLC1：10.60.60.129 执行“下装工程”操作。
2020-05-19 11:21:52 IP:10.60.67.79 对PLC1：10.65.60.129 执行“将阀岛3-1变量置为0”操作。
……

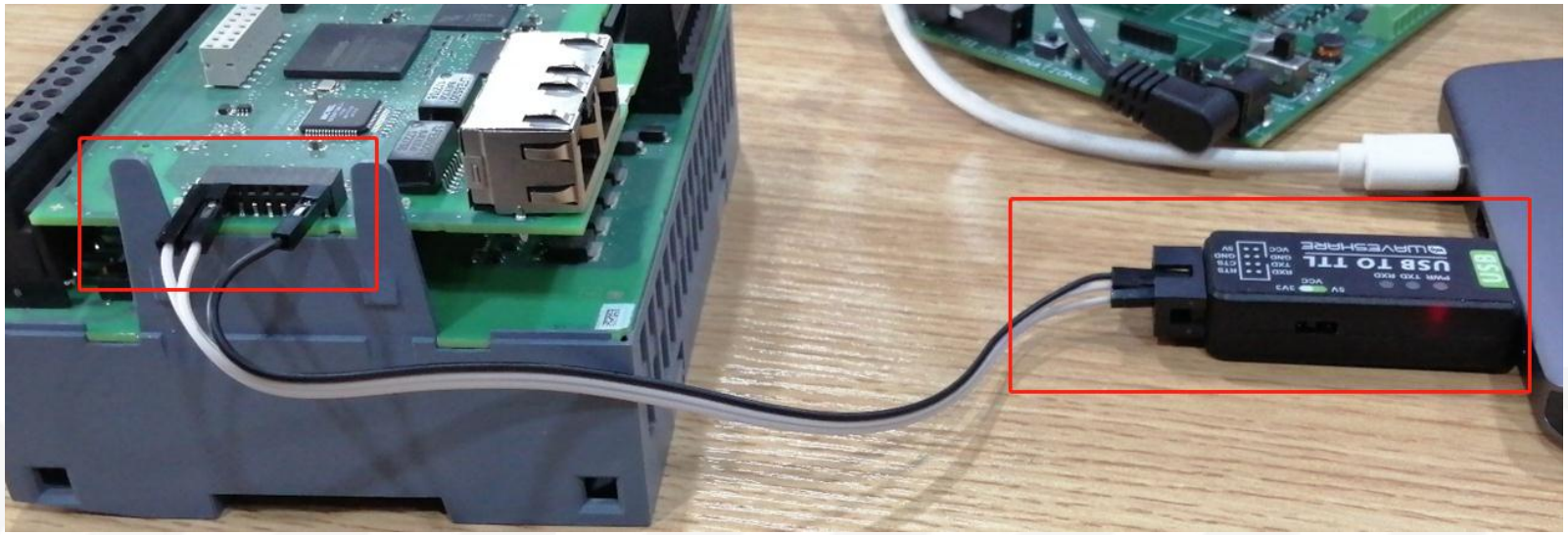
工控设备特制取证工具实践



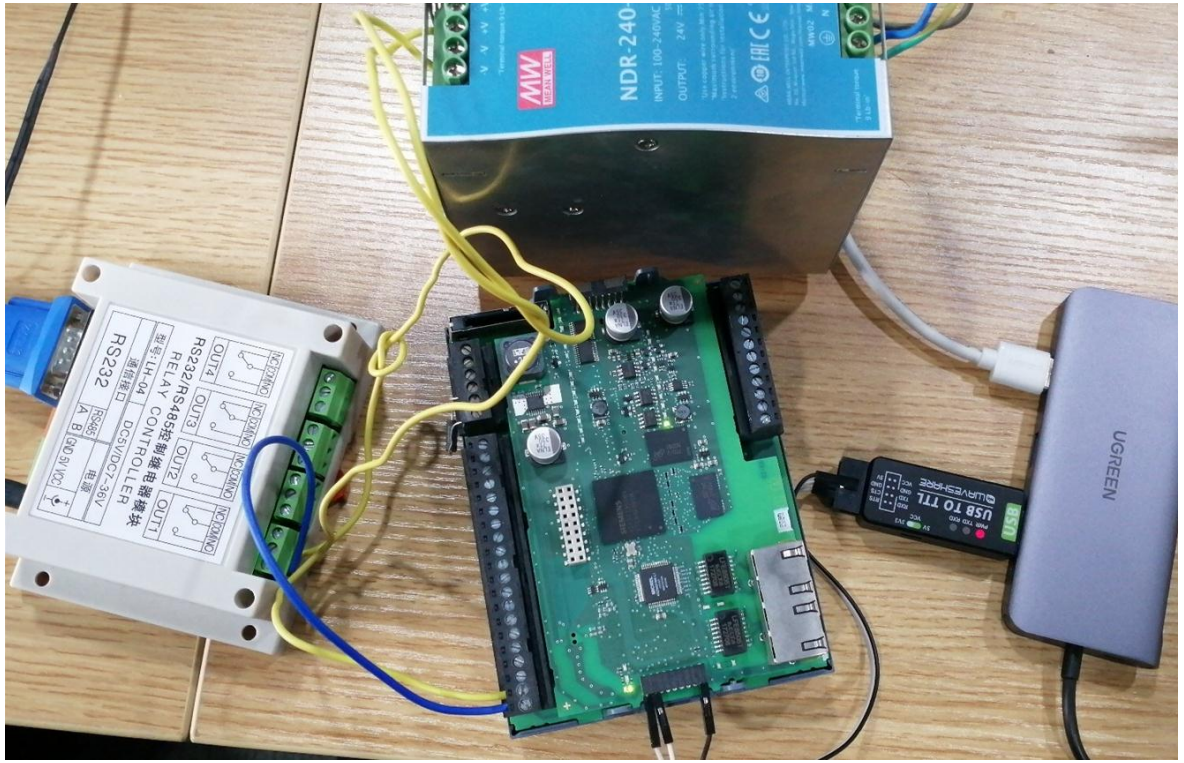


内存取证硬件工具

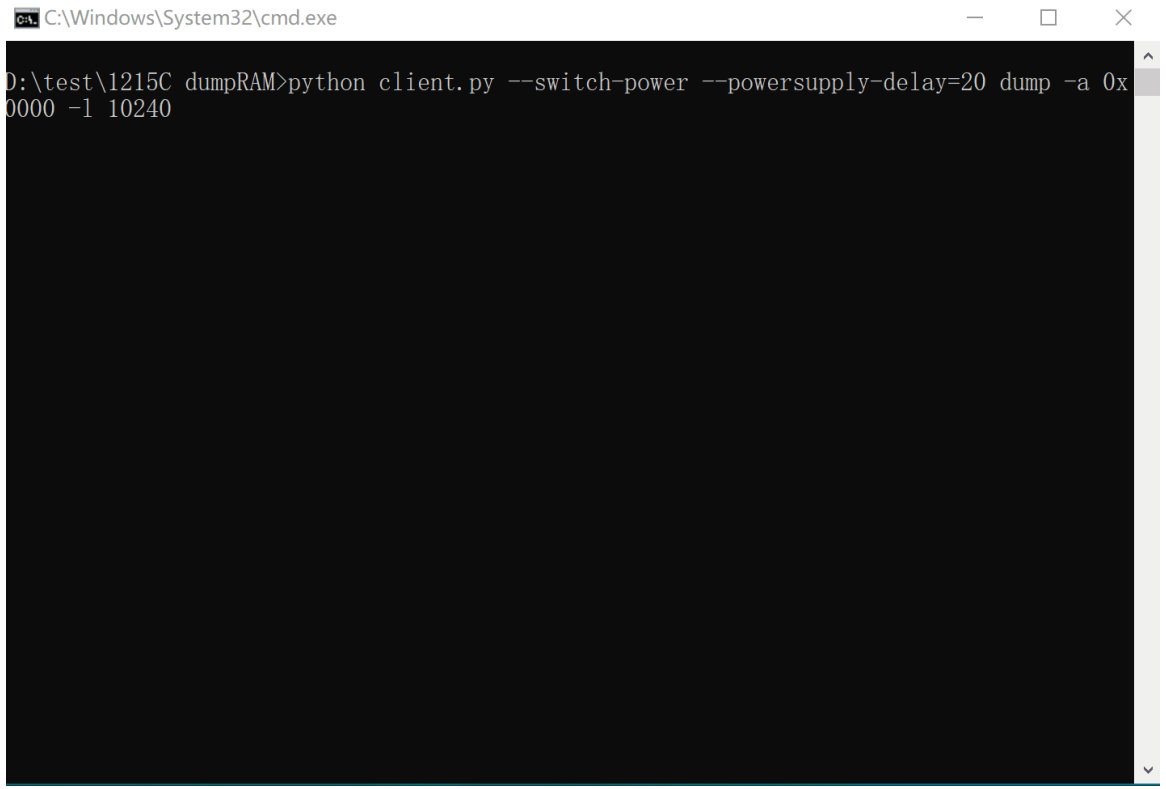
内存取证客户端



工控设备特制取证工具实践



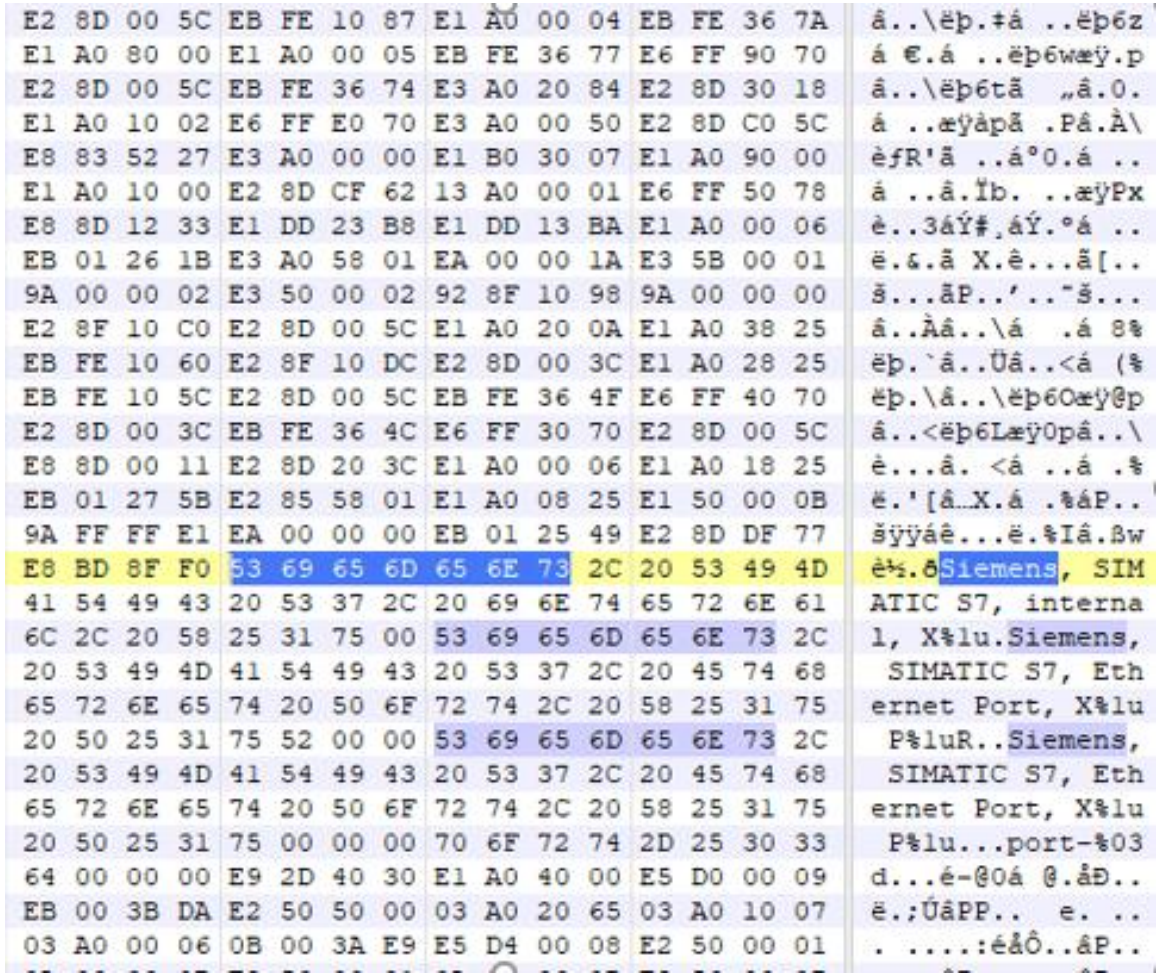
Demo版 S7-1200系列 特制取证工具



Dump内存动态效果示意图

可dump出PLC内存所有数据（包含代码段、数据段、只读数据段等）

工控设备特制取证工具实践



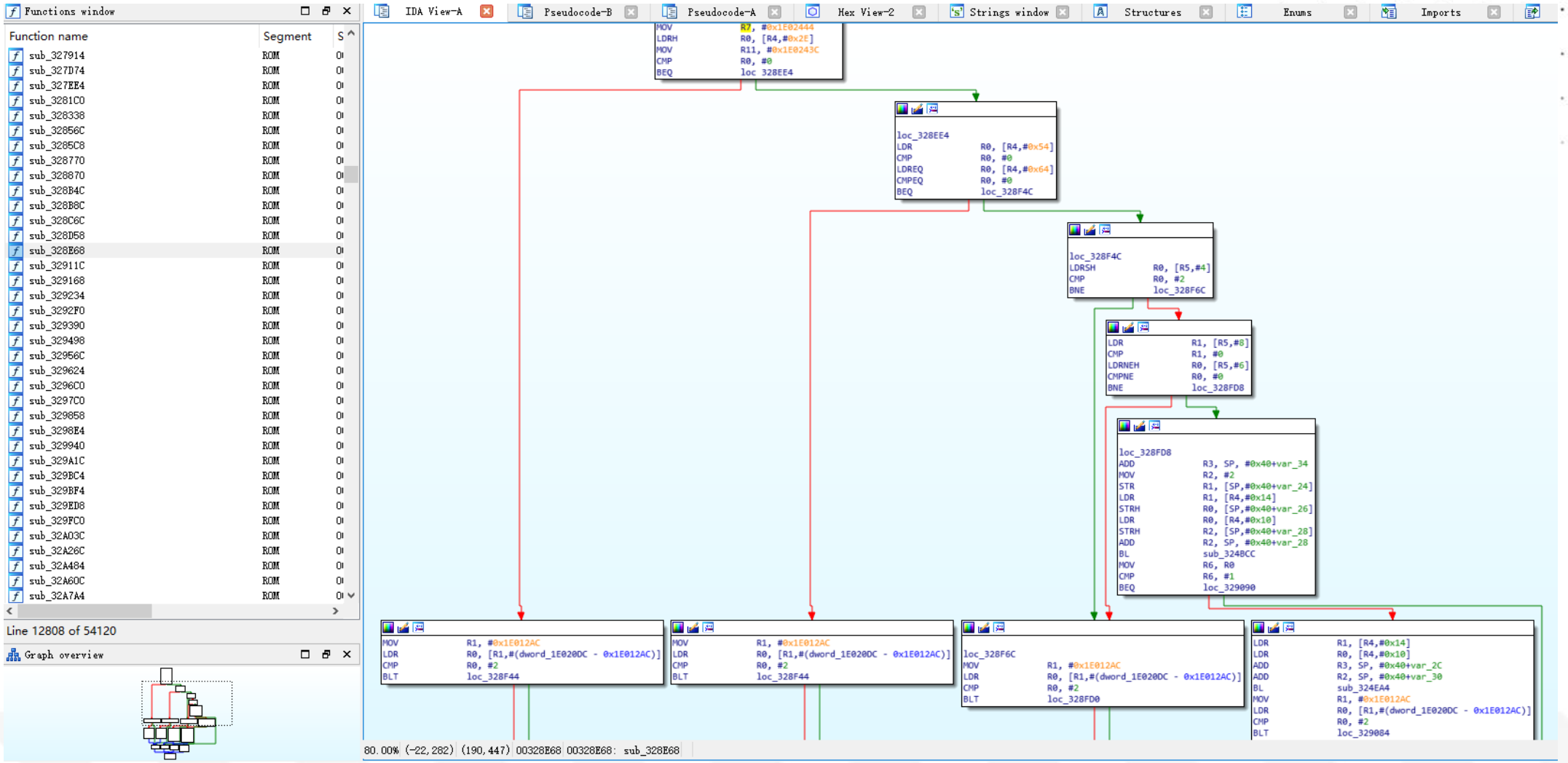
```
E2 8D 00 5C EB FE 10 87 E1 A0 00 04 EB FE 36 7A  â..\ëþ.‡á ..ëþ6z
E1 A0 80 00 E1 A0 00 05 EB FE 36 77 E6 FF 90 70  á €.á ..ëþ6wæÿ.p
E2 8D 00 5C EB FE 36 74 E3 A0 20 84 E2 8D 30 18  â..\ëþ6tã „â.0.
E1 A0 10 02 E6 FF E0 70 E3 A0 00 50 E2 8D C0 5C  á ..æÿàpã .Pâ.À\
E8 83 52 27 E3 A0 00 00 E1 B0 30 07 E1 A0 90 00  èƒR'ã ..á°0.á ..
E1 A0 10 00 E2 8D CF 62 13 A0 00 01 E6 FF 50 78  á ..â.Ïb. ..æÿPx
E8 8D 12 33 E1 DD 23 B8 E1 DD 13 BA E1 A0 00 06  è..3áÝ#¸áÝ.ºá ..
EB 01 26 1B E3 A0 58 01 EA 00 00 1A E3 5B 00 01  ë.&.ã X.ê...ã[..
9A 00 00 02 E3 50 00 02 92 8F 10 98 9A 00 00 00  š...ãP..'..˜š...
E2 8F 10 C0 E2 8D 00 5C E1 A0 20 0A E1 A0 38 25  â..Àâ..\á  .á 8%
EB FE 10 60 E2 8F 10 DC E2 8D 00 3C E1 A0 28 25  ëþ.`â..Üâ..<á (%
EB FE 10 5C E2 8D 00 5C EB FE 36 4F E6 FF 40 70  ëþ.\â..\ëþ6Oæÿ@p
E2 8D 00 3C EB FE 36 4C E6 FF 30 70 E2 8D 00 5C  â..<ëþ6Læÿ0pâ..\
E8 8D 00 11 E2 8D 20 3C E1 A0 00 06 E1 A0 18 25  è...â. <á ..á .%
EB 01 27 5B E2 85 58 01 E1 A0 08 25 E1 50 00 0B  ë.'[â…X.á .%áP..
9A FF FF E1 EA 00 00 00 EB 01 25 49 E2 8D DF 77  šÿÿáê...ë.%Iâ.ßw
E8 BD 8F F0 53 69 65 6D 65 6E 73 2C 20 53 49 4D  è½.ðSiemens, SIM
41 54 49 43 20 53 37 2C 20 69 6E 74 65 72 6E 61  ATIC S7, interna
6C 2C 20 58 25 31 75 00 53 69 65 6D 65 6E 73 2C  l, X%1u.Siemens,
20 53 49 4D 41 54 49 43 20 53 37 2C 20 45 74 68   SIMATIC S7, Eth
65 72 6E 65 74 20 50 6F 72 74 2C 20 58 25 31 75  ernet Port, X%1u
20 50 25 31 75 52 00 00 53 69 65 6D 65 6E 73 2C   P%1uR..Siemens,
20 53 49 4D 41 54 49 43 20 53 37 2C 20 45 74 68   SIMATIC S7, Eth
65 72 6E 65 74 20 50 6F 72 74 2C 20 58 25 31 75  ernet Port, X%1u
20 50 25 31 75 00 00 00 70 6F 72 74 2D 25 30 33   P%1u...port-%03
64 00 00 00 E9 2D 40 30 E1 A0 40 00 E5 D0 00 09  d...é-@0á @.åÐ..
EB 00 3B DA E2 50 50 00 03 A0 20 65 03 A0 10 07  ë.;ÚâPP..  e. ..
03 A0 00 06 0B 00 3A E9 E5 D4 00 08 E2 50 00 01  . ....:éåÔ..âP..
```

Dump内存片区总大小为128M，起始部分为BootLoader，随后为固件代码数据

Module=1215C DC/DC/DC FW Version=V4.4.1			
段信息	起始地址	长度	
.text	0x00043400	0xEE8A1C	代码段
.rodata	0x00F2BE80	0x42AF7C	只读数据
.data	0x01356E00	0x0763EC	数据段
.tls.cond.data	0x013CD1EC	0X00	
.bss	0x01E01040	0x9DAC18	
.tls.cond.bss	0x027DBC58	0X00	
.uninitialized	0x03641040	0x03F11D10	
.cc_memory	0x075F0000	0X00600000	
open_bsd_mem_pool	0x07BF0000	0X00400000	
MAP_MAC_MEM	0x07ff0000	0x061c	
.iram0	0x10030000	0x7aa0	
.iram1	0x10040000	0xC474	
.crctable	0x1004f400	0x0400	
.softboot	0x1004f800	0x0700	
.bootinfo	0x1004ff00	0x001c	
.dtcm	0x10010000	0x2DC4	

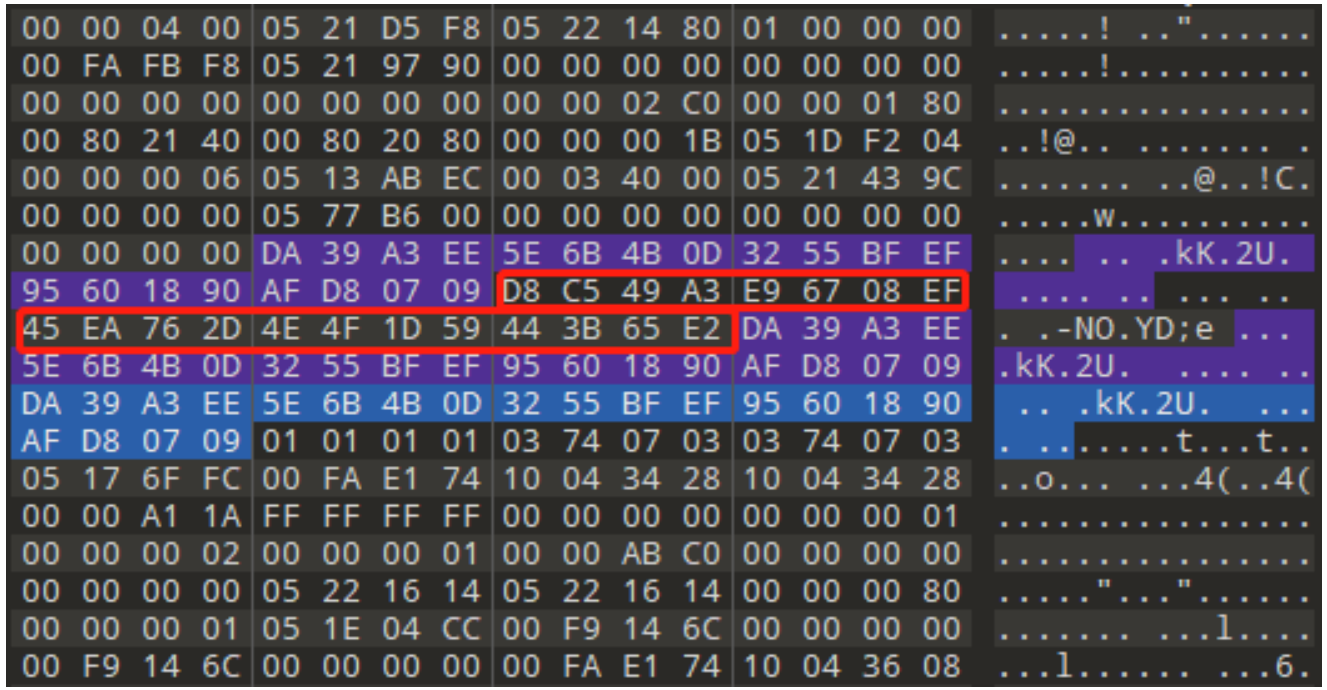
内存中包含了控制器的固件代码和工程数据等

工控设备特制取证工具实践



代码分析——通过IDA加载内存内容，分析出固件是否存在恶意代码

工控设备特制取证工具实践



00	00	04	00	05	21	D5	F8	05	22	14	80	01	00	00	00
00	FA	FB	F8	05	21	97	90	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	02	C0	00	00	01	80
00	80	21	40	00	80	20	80	00	00	00	1B	05	1D	F2	04
00	00	00	06	05	13	AB	EC	00	03	40	00	05	21	43	9C
00	00	00	00	05	77	B6	00	00	00	00	00	00	00	00	00
00	00	00	00	DA	39	A3	EE	5E	6B	4B	0D	32	55	BF	EF
95	60	18	90	AF	D8	07	09	D8	C5	49	A3	E9	67	08	EF
45	EA	76	2D	4E	4F	1D	59	44	3B	65	E2	DA	39	A3	EE
5E	6B	4B	0D	32	55	BF	EF	95	60	18	90	AF	D8	07	09
DA	39	A3	EE	5E	6B	4B	0D	32	55	BF	EF	95	60	18	90
AF	D8	07	09	01	01	01	01	03	74	07	03	03	74	07	03
05	17	6F	FC	00	FA	E1	74	10	04	34	28	10	04	34	28
00	00	A1	1A	FF	FF	FF	FF	00	00	00	00	00	00	00	01
00	00	00	02	00	00	00	01	00	00	AB	C0	00	00	00	00
00	00	00	00	05	22	16	14	05	22	16	14	00	00	00	80
00	00	00	01	05	1E	04	CC	00	F9	14	6C	00	00	00	00
00	F9	14	6C	00	00	00	00	00	FA	E1	74	10	04	36	08

原本均未设置密码保护的PLC，被勒索病毒设置了密码，导致用户无法访问PLC，不能执行修改程序逻辑等操作

数据分析——在整个内存二进制文件中寻找取证需要的敏感数据，比如勒索病毒修改后的密码hash

ICS领域数字取证展望

近期

1. 基于应急响应体系建设的要求——主要集中在应急事件的处置流程上，对于技术点的深入探究有限；
2. 取证技术主要由设备或者系统软件厂商支援；
3. 单点突破的取证方法会出现，但是整体取证架构的建立欠缺；

长远

1. 顶层设计跟进——建立完善有监督、有记录、有监管的ICS事件调查取证流程与法规；
2. 参考传统的取证框架建立ICS领域数字取证技术框架，经过实践修改后推广使用；
3. ICS取证通用工具集及产品，特定设备取证工具及产品等。

网络安全创新大会
Cyber Security Innovation Summit

THANKS