Live Forensic Analysis on an ICS / SCADA

Jorge Kamlofsky, Raúl Oscar Romero. *Universidad Abierta Interamericana. Centro de Altos Estudios en Tecnología Informática. Buenos Aires, Argentina.*

***Abstract*--The production of goods on a large scale is carried out in industrial control systems (ICS according to its acronym in English). They consist of a network of industrial automata that control the equipment that executes the production processes. They are supervised in computer terminals called SCADA. ICS are very robust systems, designed for continuous operation, but they are not designed to be safe. Therefore, connect them to corporate networks and also to the Internet, leaving their vulnerabilities exposed. In the face of cybersecurity incidents, computer forensics is presented as a tool that allows the analysis of events, but the background on these systems is very scarce. In addition, since continuous operation is important in these systems, the analysis must be carried out without stopping their operation. This paper details the performance of a forensic analysis on these systems, through live acquisition and without stopping the system's operation. The results are promising.**

***Index Terms*--forensics, SCADA. Live-forensic SCADA. Forensic on ICS.**

I Introducción

LUEGO de recorrer tres revoluciones industriales, la humanidad ha atravesado cambios paradigmáticos. Algunos efectos ya observados en la primera revolución industrial y que se repiten en las dos siguientes son [1]: la producción de bienes de mejor calidad a menor costo, cambios revolucionarios en la producción de alimentos, mayor demanda de mano de obra en las ciudades, crecimiento económico logró la disminución de la pobreza [2], avances en sanidad y medicina lograron aumentar la expectativa de vida y con ello, un marcado aumentos de la población. Mientras que la primera revolución industrial se basó en la mecanización de la producción, la segunda, se caracterizó por el uso intensivo de energía (eléctrica y petróleo).

La tercera revolución industrial (estimada desde 1970 hasta la actualidad) se basó en la incorporación de dispositivos electrónicos, informáticos y redes de comunicaciones para la automatización y control de la producción [3]: los sistemas de control industrial (ICS según sus siglas en inglés). Integran las tecnologías operacionales (OT según sus siglas en inglés). En general se componen por redes de autómatas industriales o PLCs (siglas del inglés Programable Logic Controller) supervisados en tiempo real por terminales denominados SCADA (siglas del inglés Supervisory Control and Data Acquisition): son muy robustas y aptas para funcionamiento continuo. Y por ello se los utiliza en las infraestructuras críticas de las naciones [3].

Hoy se presenta una nueva etapa que promete cambios revolucionarios en la producción de bienes: La Industria 4.0. Este concepto presentado en Alemania [4], se basa en la integración de OT con tecnologías disruptivas y probadas en el mundo IT (iniciales en inglés de Tecnologías de la Información) como ser: Inteligencia artificial, Internet de las Cosas, Realidad Aumentada, interconexión de redes, entre otros. Plantea como desafío las necesidades de investigación en ciberseguridad [4].

Los crecientes ataques a sistemas ICS / SCADA utilizando malware como Stuxnet, Havex, BlackEnergy exigen una investigación forense para determinar la causa de la intrusión y también para prevenir ataques cibernéticos [5].

Frente a un incidente de ciberseguridad, y debido a que los sistemas OT normalmente no se pueden detener, en general, se intenta restaurar el servicio tan pronto como se pueda, lo que muchas veces implica la pérdida de evidencias digitales. En el caso que se desee averiguar las causas del incidente, es importante comprender cuáles son sus consecuencias forenses digitales, qué procedimientos o protocolos, herramientas y técnicas se necesitan usar durante la investigación, y de dónde se pueden recopilar los datos forenses y cómo. En forensia, en tecnologías OT, existe un gran vacío en la literatura para responder a estas cuestiones [6],

Sin embargo, tras un incidente, en caso de decidirse la recopilación de evidencia forense, pueden recopilarse tanto datos volátiles como datos persistentes [7], en vivo o post-mortem [8]. Las herramientas existentes para el monitoreo de red son de gran utilidad para las aplicaciones forenses, pero se diseñaron para la adquisición en tiempo real, lo cual no es aplicable para el análisis post-mortem (o en frío) de los datos adquiridos de manera forense [9].

En caso de análisis forense en sistemas ICS / SCADA, la cantidad de referencias documentadas es muy reducida. Entre ellas, es de interés el análisis del caso de una planta de tratamiento de aguas residuales [5] donde se utilizó FTK Imager para el volcado de memoria (datos volátiles). En el trabajo de Van der Knijff [9] se destaca la forma constante y predecible en la que normalmente se comportan los ICS para facilitar la detección de anomalías. El trabajo de Haris Iskandar Mod [10] se especializa en las redes de suministro energético conocidas como Redes Inteligentes. En general, utilizan tecnología OT, ICS, SCADA. Varios ataques sobre estos sistemas utilizan malware diseñado para evitar ser rastreados por procedimientos forense utilizando la fragilidad de la evidencia digital como ventaja para lanzar un ataque sin dejar rastros. En su trabajo se realiza una revisión de los procedimientos Forenses y propone un procedimiento específico para ambiente de redes inteligentes.

En este trabajo, basado en [11] se presentan detalles de un análisis forense realizado sobre un ICS / SCADA tras adquisición de información en vivo.

I.A Objetivos de este Trabajo

El objetivo principal de este trabajo es presentar un abordaje de análisis forense sobre tecnologías operacionales, el cual puede ser aplicado tanto a industrias como a infraestructuras críticas industriales.

Un objetivo secundario es mostrar las ventajas en el uso de herramientas forenses para la adquisición de datos en vivo en estas tecnologías, donde normalmente se requiere continuidad operacional.

I.B Contribuciones de este Trabajo

El análisis Forense en ICS / SCADA aporta al mejoramiento de las condiciones de ciberseguridad de los entornos operacionales. Además de Industrias, las tecnologías OT se usan en muchas de las Infraestructuras Críticas de las naciones. Así, estos resultados contribuyen a la mejora de la ciberseguridad de las naciones.

I.C Motivación y Alcance

La forensia informática brinda herramientas para la identificación y el estudio de ataques informáticos. Pero en los ICS / SCADA, sus técnicas están muy poco difundidas. Motiva la redacción de este trabajo la reducción de esta brecha.

Las experiencias que soportan los resultados aquí presentados se basan en una experiencia realizada sobre un banco experimental compuestos por elementos de hardware y software de uso en la industria que simulan una planta de producción. Gracias a ello, los resultados que se presentan son limitados. Así y todo, son de gran interés por presentar evidencia respecto de acciones específicas de los dispositivos de control industrial.

I.D Estructura de este Trabajo

En la sección 2 se presenta el marco teórico con conceptos fundamentales sobre los que se basa este desarrollo. La sección 3 presenta detalles de la experiencia. La sección 4 se enfoca en los resultados. En la sección 5 se presentan las conclusiones.

II Marco Teórico

II.A Tecnologías de la Operación

La automatización de la producción a gran escala se realiza mediante los ICS (del inglés: Industrial Control Systems): Son sistemas de tele-mando y tele-control de procesos compuestos por redes de autómatas industriales: RTU (siglas en inglés de Unidad de Transmisión Remota), PLC (siglas en inglés de Controlador Lógico Programable), DCS (siglas en inglés de Sistemas de Control Distribuido), etc. Estos poseen procesadores de pequeño porte y lógica determinista, lo cual favorece a la alta disponibilidad, esencial en el ambiente industrial. Controlan los elementos de Campo: entradas y salidas, discretas y/o analógicas como ser: micro-switches, sensores de temperatura, actuadores para encendido de motores, llaves, etc. Las componentes de los ICS poseen exigencias propias de un ambiente más agresivo por vibraciones, ruido eléctrico, temperatura y tensión con rangos más amplios a los convencionales. Los ICS se supervisan y controlan en tiempo real desde sistemas informáticos llamados SCADA [3].

A los sistemas de automatización y control industrial ICS, a los SCADA, a los DCSs, normalmente se los denomina Tecnología Operacional (según sus siglas en inglés: OT). Gracias a su robustez, estos sistemas son usados para monitorear y controlar infraestructuras críticas tales como plantas de distribución de energía, de tratamiento y distribución de agua, de alcantarillado, entre otras [3, 12].

Muchas veces, al conjunto de los sistemas de campo, control y supervisión se lo denomina como SCADA [13].

La primer generación de SCADA presenta tres niveles: El nivel de campo, el nivel de control y el de supervisión.

En el nivel de campo se puede hallar a los diferentes equipos que intervienen directamente en el proceso de producción: sensores analógicos como ser: de temperatura y/o nivel en tanques, caudalímetros, sensores de presión (que en general por su confiabilidad usan el estándar 4 – 20mA [14]); digitales (que usan diferencias de potencial) como ser: micro-switches, sensores de fin de carrera, sensores ópticos [15], actuadores para encendido de motores o bombas, apertura o cierre de válvulas, etc. que generalmente se conectan a relés. Las Salidas a relé son generalmente las más utilizadas, libres de tensión, de modo de poder accionar cualquier actuador, ya sea a corriente continua o alterna [16].

En el nivel de control se encuentra principalmente a los dispositivos de control (básicamente PLC y RTU) e interfaces hombre-máquina (HMI según sus siglas en inglés). Estos elementos se encuentran distribuidos dentro de la planta de producción, y conectados entre sí mediante red de comunicaciones. Un PLC es una computadora industrial que usa la ingeniería para la automatización de procesos. Controlan las entradas y salidas de manera segura, poseen una programación compatible con distintos lenguajes, interfaz amigable que facilita la comunicación con el usuario, conexión a sistemas de supervisión, ejecutan la programación de forma continuada [17]. Un HMI, por otro lado, es un software diseñado específicamente para ICS. Utiliza datos en red para proporcionar a los operadores una interfaz gráfica que permite monitorear el rendimiento de muchas partes y equipos y emitir comandos y configuraciones de proceso desde una pantalla [18].

El nivel de supervisión se compone por equipos de cómputo con software específico. Allí puede hallarse el software SCADA de supervisión, terminales de ingeniería y mantenimiento. Los SCADA permiten que los operadores de los ambientes de producción tengan un informe resumido de cada uno de los equipos conectados a la red. Las soluciones SCADA permiten monitorear con precisión, controlar y visualizar cada aspecto de la operación de manera centralizada. Así, a simple vista, el operador puede visualizar qué es lo importante que necesita conocer [18]. Los SCADA tradicionales no se conectaban con otros sistemas ni otras redes de computadoras. Sus mecanismos de comunicación y protocolos se acercaron a esquemas del tipo propietario [13]. En [19] se presentan los últimos productos desarrollados para

el protocolo Modbus (uno de los más usados en los SCADA).

La segunda generación de sistemas SCADA integró sistemas de gestión con los sistemas de control dentro de un empresa o una empresa conectando las redes del sistema de control SCADA a las redes del Sistema de gestión pasando a conformar la Intranet de una empresa [13]. A esta generación de SCADA se lo llama sistema MES (iniciales en inglés de Administración de Sistemas de Ejecución). Gracias a los sistemas MES se pueden conectar todas las áreas de trabajo de una empresa y gestionarla de forma integral. Los sistemas MES agregan las siguientes funcionalidades: proporcionar ordenes de producción ayudando a su eficiencia, calcular el rendimiento y busca su eficiencia, medir y reducir los costos de producción y anticipación a los posibles imprevistos y/o errores [20]. Puede datarse al inicio de esta generación de SCADA a fines de la década de 1990.

Los sistemas SCADA de hoy integran los MES a Internet. Se corresponden con la denominada tercer generación de SCADA o SCADA basados en Internet. Se integran los SCADA con el sistema ERP (iniciales en inglés de planificación de recursos empresariales). Los SCADA de tercer generación tienen una integración total con las redes corporativas que están interconectadas con Internet. Para este nivel de integración se requiere la apertura de los SCADA lo que se manifiesta en las técnicas comunes adoptadas, plataformas, instalaciones, software, etc. En los sistemas SCADA de tercera generación. Los datos en tiempo real en los sistemas de control y monitoreo se transfieren a través de Intranet o incluso Internet [13].

La figura 1 presenta un esquema que muestra los diferentes niveles de integración de los SCADA.

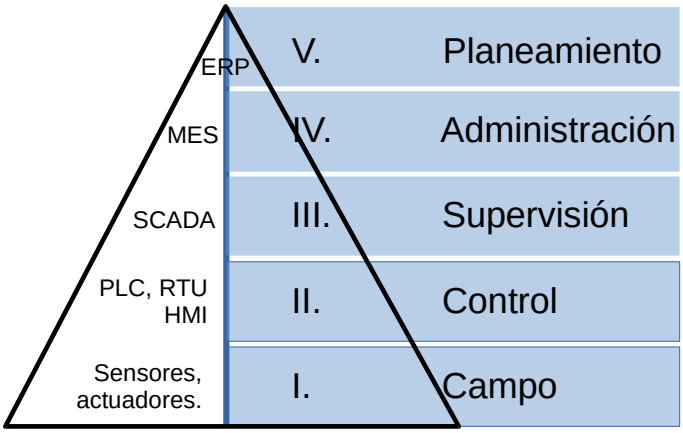

Fig. 1. Pirámide de los niveles SCADA

Puede fecharse el inicio de la tercer generación de SCADA a inicios de la década pasada (es decir a inicios de 2010).

Hoy, el concepto de Industria 4.0 propone la interconexión de los SCADA de tercera generación con otros sistemas y otras tecnologías [4].

II.B Ciberseguridad en las Tecnologías de la Operación

Los SCADA se diseñaron para supervisar y actuar sobre los procesos industriales. No se diseñaron para ser seguros. El aislamiento de los procesos de producción les dio por muchos años una sensación de seguridad ilusoria gracias al ocultamiento. Con el tiempo surgió la necesidad de vincularlos a la red corporativa e incluso a internet. Su interconexión dejó a los ICS expuestos a amenazas y riesgos, los que suponen serias consecuencias [21]. Los casos documentados de ataques a sistemas SCADA comenzaron a incrementarse significativamente desde 1998 [13], coincidiendo con la evolución de los SCADA a su segunda generación y su interconexión con la red corporativa.

En el año 2010 las plantas nucleares de Irán fueron atacadas por un virus informático llamado Stuxnet, lo que desconcertó a analistas estratégicos de todo el mundo. La comunidad internacional mostró preocupación por la seguridad [21]. Desde esa fecha fueron varios los ataques documentados contra sistemas ICS. Muchos de ellos pueden consultarse en las bases de datos públicas RISI[1] y en las del ICS Cert de EEUU[2].

En el ámbito IT (siglas en inglés de Tecnologías de la Información), se posee conocimientos amplios y experiencias en ciberseguridad. Se destacan las normas ISO/IEC 27000:2018 [22] y la NIST SP800-128 [23]. Entre otras cosas, ellas se presentan definiciones y propuestas de buenas prácticas que ayudan a evitar incidentes y/o ataques cibernéticos. Componen un ambiente completo de ciberseguridad. Se dispone también, de dispositivos y equipos y su uso práctico para la defensa contra cibercrimen: antivirus, sistemas de detección de intrusiones, firewalls, entre otros.

Sin embargo, en el ámbito OT también se dispone de amplia y completa normativa específica de ciberseguridad, entre ellas se destacan: ISO/IEC 62443 [24] y NIST SP 800-82 [25], Sin embargo, en OT la prioridad se centra en la disponibilidad de los sistemas, los cuales deben funcionar en forma continua. La seguridad de la información no es prioridad. Es por ello, quizás, que habiendo normativa completa y de gran calidad, sus recomendaciones no se despliegan en todo el mundo OT.

La forensia informática brinda herramientas para la identificación y el estudio de ataques informáticos. En el ámbito IT la informática forense posee varios estándares que las regula. Entre ellas: La informática forense cuenta con varias normas que las regula, ellas: NIST SP800-86, ISO / IEC 27037:2012, ISO / IEC 27042:2015, RFC 3227, RFC 4810, RFC 4998, RFC 6283 [11].

Sin embargo, en el ambiente OT no se presenta normativa específica de Informática Forense para ICS / SCADA.

II.C Nociones Básicas de Informática Forense

La delincuencia ha encontrado en la cibernética una herramienta muy útil para la comisión de distintos tipos de delitos. También la justicia reconoce la utilidad de las pruebas digitales que pueden ser obtenidas a través de las herramientas informáticas. El procesamiento de la evidencia digital debe realizarse asegurando la integridad de modo de no poder ser refutada [11].

1 Vínculo a la Base de Datos RISI: https://www.cybersecurityintelligence.com/repository-of-industrial-security-incidents-risi-3024.html

2 Vínculo a ICS Cert de EEUU: https://www.cisa.gov/uscert/ics/alerts

Según Rodney McKemmish, la Informática Forense *"es el proceso de identificación, conservación, análisis y presentación de pruebas digitales de forma legalmente aceptable"* [26].

En [11] se presentó una definición más actual y amplia: *"es la aplicación de técnicas científicas y analíticas especializadas en infraestructura tecnológica que permiten la identificación, preservación, análisis y presentación de datos que sean válidos dentro de procesos preventivos, legales o particulares"*.

Existen varias modalidades para realizar un análisis informático forense, algunos de los cuales son [27]: análisis forense de equipos de cómputo (computadoras personales, notebooks, netbooks, memoria RAM), análisis forense de dispositivos móviles (teléfonos celulares, Smartphones, tablets), análisis forense de software (software enlatado, software a medida, sistemas operativos), análisis forense de dispositivos extraíbles (disco rígido magnético, disco estado sólido, pendrive, memorias flash, medios ópticos como ser CD, DVD, Blue Ray, Mini-Disc, medios magnéticos como ser tape backup o diskettes), análisis forense de redes (redes alámbricas e inalámbricas).

Para la adquisición de datos pueden destacarse la adquisición de datos en vivo o adquisición de datos persistentes en frío [7, 8].

En instancias de un allanamiento, elegir la adquisición en vivo o en frío implica considerar o no el corte de energía eléctrica. Un sistema de adquisición en vivo permite recopilar información de un sistema que está en funcionamiento donde la información puede modificarse a medida que los datos se procesan continuamente. Hay mucha información de gran valor probatorio que puede hallarse tras una adquisición en vivo como ser: procesos en ejecución, conexiones a redes y sistemas de archivos montados. Esta información se pierde si los equipos se apagan. Por otro lado, dejar la computadora encendida puede causar la alteración o eliminación de la evidencia. Aquí, el investigador debe decidir por la alternativa con mejor relación costo-beneficio [8].

En el sistema forense muerto o de adquisición en frío, para crear una imagen forense de un disco completo, las mejores prácticas sugieren que la creación de imágenes forenses no debe alterar ningún dato en el disco, y que además, se incluyan todos los datos, metadatos y espacios no asignados. Los investigadores forenses conectan los discos (desconectados del sistema y protegidos contra escritura) a una estación de trabajo forense para crear la imagen. Esto se conoce como imágenes muertas [8].

Un enfoque mixto consiste en utilizar herramientas especializadas para extraer datos volátiles de la computadora antes de apagarla para luego extraerle los datos mediante una adquisición en frío [8].

III El Experimento

III.A Resumen

El experimento consiste en la adquisición de datos forenses en vivo obtenidos de un ICS / SCADA portable montado en laboratorio para su posterior análisis y presentación de los resultados.

III.B Herramientas y Equipos

El ICS / SCADA portable usado en esta experiencia consiste en un conjunto de hardware adecuadamente interconectado y con los correspondientes drivers instalados. El listado de hardware consiste en: una notebook donde se instaló el SCADA, un PLC montado sobre un gabinete, con un proceso programado, un switch y cables UTP categoría 5 para la conexión física de la red.

Para el análisis forense se utilizó la herramienta Bento[3] Toolkit1, un conjunto de herramientas para la informática forense incluida dentro del paquete Tsurugui. Bento se instaló y se usó desde un pen drive.

La notebook es marca HP modelo Pavilion[4] dv5 Notebook PC con procesador Intel(R) Core(TM) i5 CPU[5] M 4503 @ 2.40GHz, 2048MB de memoria RAM y disco rígido de 465.8GB. El PLC consiste en un PLC marca DELTA modelo DVP[6]-12SP. El switch es marca Cisco[7].

El PLC Delta se instaló dentro de un gabinete estanco conteniendo un riel DIN donde se montaron los módulos del PLC: fuente, PLC y bornera. Sobre el mismo, además, se instaló una llave térmica de seguridad. En la puerta del gabinete se instalaron llaves, botones, y lámparas para el comando del PLC desde el exterior. En el interior, se incluyó el diagrama de cableado. La figura 2 muestra una imagen del PLC instalado dentro del gabinete.

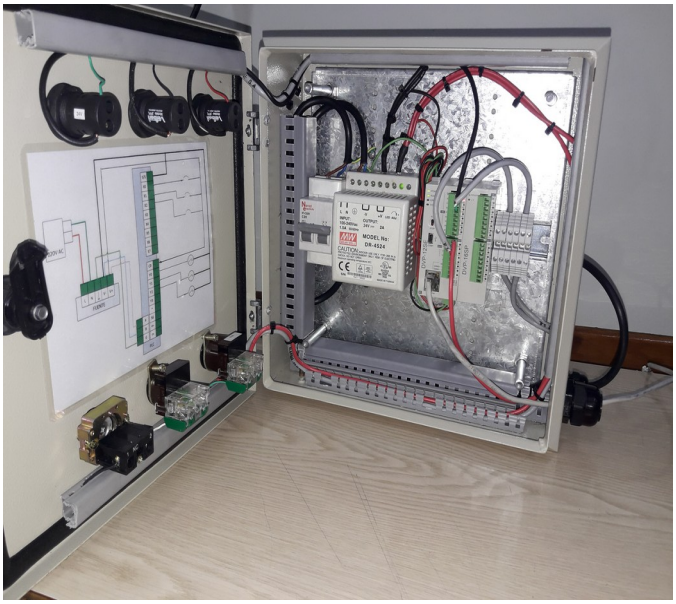

Fig. 2. PLC Delta instalado dentro del gabinete

3 Bento: https://tsurugi-linux.org/documentation_bento_toolkit.php

4 Sitio oficial HP: https://www.hp.com/ar-es/shop/notebooks/notebooks-personales/notebooks-pavilion.html

5 Sitio oficial Intel I5: https://ark.intel.com/content/www/es/es/ark/products/49022/intel-core-i5450m-processor-3m-cache-2-40-ghz.html

6 Sitio oficial PLC Delta: https://www.deltaww.com/en-us/products/PLC-Programmable-Logic-Controllers/ALL/

7 Sitio oficial de switch Cisco: https://www.cisco.com/c/es_es/products/switches/index.html

A la notebook se le instaló un sistema operativo MS-Windows 7 Starter. Sobre éste se instaló el software Wonderware[8] necesario para el desarrollo del escenario SCADA.

III.C Desarrollo del Escenario de Prueba

El escenario desarrollado se corresponde con el de un SCADA que controla una planta de fabricación de botellas de plástico de que contiene una única máquina inyectora. El SCADA posee las siguientes pantallas: Carátula, Menú, Producción, Totales, CNC's, Inyectora 1. La figura 3 presenta la pantalla Menú.

Fig. 3. Pantalla Menú del SCADA del escenario de prueba

El PLC habilita el funcionamiento de la inyectora para cada uno de los turnos. La figura 4 presenta el programa del PLC (en lenguaje Ladder[9]).

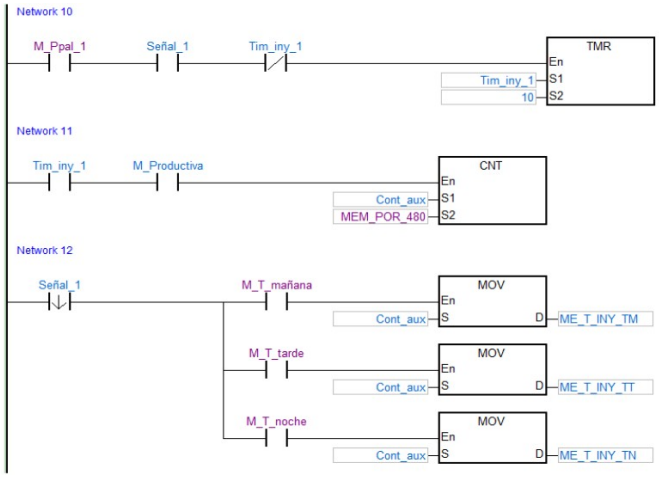

Fig. 4. Programa descargado al PLC

IV Resultados

IV.A Resumen

En esta sección se presentan los resultados de la experiencia. En el laboratorio, la obtención de la información se realizó en vivo (live) tanto al equipo de cómputo como a la red. La adquisición de la información se realizó en vivo de: Características del terminal PC, red y trafico de red, actividades del PLC [11].

IV.B Sistema Operativo y Aplicaciones Instaladas en Terminal SCADA.

La obtención de la información se inicia con un análisis de auditoria del sistema operativo para lo cual se utilizó la aplicación WinAudit, ejecutada desde la herramienta Bento. De la misma se obtiene una completa información del equipo de cómputo. La información obtenida se refiere tanto al Sistema Operativo como otras aplicaciones instaladas, puertos de comunicaciones, entre otros.

Se presentaron los siguientes reportes: Vista General, Sistema Operativo, Grupos Relevantes, Grupos Miembro, Derechos de Usuarios, Usuarios Relevantes, Aplicaciones instaladas Relevantes (COMMGR 1.11, DAServer Runtime Components Upgrade, DCISoft 1.22, HWCONFIG 4.00, ISPSoft 3.10, Modicon MODBUS Plus. Sentinel Protection Installer 7.5.0, SuiteLink, Virtual COM, Wonderware Alarm2U DAServer, Wonderware Common Components, Wonderware Compact Panel DAServer. Wonderware FactorySuite Gateway, Wonderware InTouch, Wonderware Kontron DAServer, Wonderware MBSerial DAServer, Wonderware MBTCP DAServer, Wonderware Modicon MODBUS Ethernet, WonderwareTSInfoTool, WPLSoft 2.49), Dispositivos de Red, Puertos de comunicación, Puertos Abiertos Relevantes, Tabla de Ruteo, Configuración de Seguridad. En la Tabla 1 se presenta el reporte de la aplicación "ISPSoft 3.10".

TABLA I
Reporte de WinAudit de la aplicación ISPSoft 3,10

Item	*Value*
Name	*ISPSoft 3.10*
Vendor	*DELTA ELECTRONICS,INC.*
Version	*3.10*
Product Language	*English*
Install Date	*20200410*
Install Location	
Install Source	*C:\Users\SCADA\AppData\LocalTemp_isE30F*
Install State	*The product is installed for the current user.*
Assignment Type	*Per Machine*
Package Code	*{071AB193-12AA-45A3-A62F-AC8CE890F911}*
Package Name	*ISPSoft 3.10.msi*
Local Package	*C:\Windows\Installer\83fb2.msi*
Product ID	*None*
Registered Owner	*SCADA*
Software ID	*{8E89EEE3-D05E-4C02-B52A-A31FEABAEE9C}*

IV.C Análisis de la Red

Para lectura del tráfico de red y captura de paquetes se utilizaron las aplicaciones NetworkTrafficViewer y SmartSnif, ejecutadas desde Bento. Para el tráfico de red, la aplicación NetworkTrafficViewer, la misma captura las direcciones IP de los dispositivos conectados a la red, al momento de ejecutar la aplicación. Para la captura de paquetes, la aplicación SmartSnif, al momento de ejecutar la aplicación, captura el paquete de información que se transmite desde el equipo de cómputo al PLC y viceversa.

La lectura del tráfico de red, a través de la aplicación NetworkTrafficViewer, arrojó resultados satisfactorios de comunicación recíproca entre el equipo de cómputo y el PLC. Las direcciones IP del equipo de cómputo es 192.168.1.2 y el

8 Sitio de Wonderware: https://www.wonderware.es/hmi-scada/productos/
9 Acerca del lenguaje Ladder: https://www.educacionurbana.com/apuntes/ladder.pdf

PLC es 192.168.1.5. Los reportes presentados por la aplicación son: Visualización de comunicación entre el equipo de cómputo y el PLC, Captura de paquetes de datos en modo Automático, Captura de paquetes de datos en modo Ascii (notar que los datos viajan en claro), Captura de paquetes de datos en modo Hex Dump,

En la figura 5 se presenta la pantalla Captura de paquetes de datos en modo Ascii de NetworkTrafficViewer.

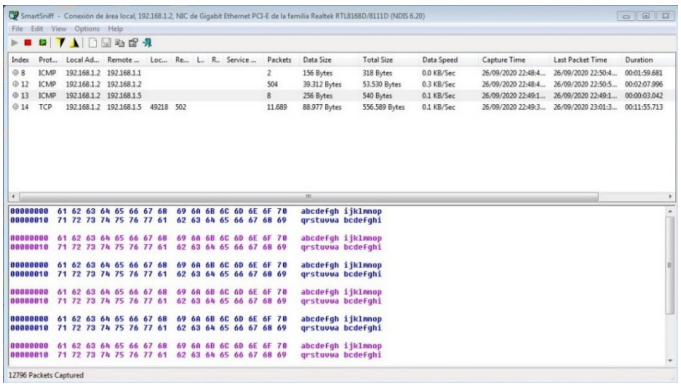

Fig. 5. Pantalla Captura de paquetes de datos en modo Ascii del módulo NetworkTrafficViewer,

Observar que el mensaje “abcdefghijklmnop” viaja en claro (sin encriptar) en la red desde el SCADA hacia el PLC.

IV.D Huellas de los Dispositivos de Control Industrial

Para leer la trazabilidad de actividades realizadas por el PLC se utilizó la aplicación SMC (Archestra System Management Console), Log Viewer de la herramienta Wonderware InTouch.

Para leer la trazabilidad de actividades realizadas por el PLC se utilizó la aplicación SMC de la herramienta Wonderware InTouch. En dicha aplicación se visualizan los eventos satisfactorios y no satisfactorios que ocurren en el PLC.

Las pantallas obtenidas son: Visor de Eventos de actividad del software Intouch Wonderware – Licenciamiento, Visor de Eventos de actividad del software Intouch Wonderware – Conexión.

En la figura 6 se presenta el Visor de Eventos de actividad del software Intouch Wonderware – Conexión.

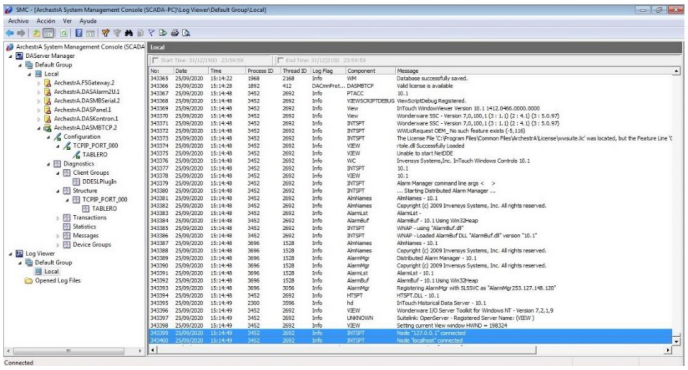

Fig. 6. Visor de Eventos de actividad del software Intouch Wonderware – Conexión.,

IV.E Análisis de los Resultados

Del análisis del Sistema Operativo y Aplicaciones Instaladas en el Terminal SCADA, la herramienta Bento ejecutó la aplicación WinAudit. De la misma se obtuvieron reportes con información detallada de las características del equipo, aplicaciones instaladas, usuarios y configuraciones de seguridad.

Para el caso del tráfico de red se verificó que existe comunicación recíproca entre el equipo de cómputo y el PLC, en el mismo proceso se visualizaron las direcciones IP de ambos dispositivos.

En el caso de las actividades registradas en el PLC, se puede verificar actividades que se realizaron en el PLC y se registran en el software Intouch Wonderware.

Para información detallada de los reportes se recomienda obtenerlos del trabajo de Romero [11] donde originalmente se presentaron los resultados de esta experiencia.

V Conclusiones

Con la herramienta Bento realizó una adquisición en vivo del funcionamiento de un ICS / SCADA en funcionamiento, sin detenerlo. De la imagen adquirida pudo obtenerse evidencias forenses tanto el terminal SCADA, en la red de comunicaciones entre el PLC y la PC con el SCADA y actividades del PLC registradas en la PC.

Una primer conclusión de esto, es que el método de adquisición forense en vivo puede ser adecuado para adquirir evidencias de un ICS / SCADA sin necesidad de detener el funcionamiento de la planta.

Una segunda conclusión se refiere al detalle de la evidencia: si bien podría decirse que el análisis del terminal SCADA brinda información equivalente a un análisis de una adquisición fría, el resultado de los demás análisis (tráfico de red y actividad del PLC) brindan información adicional muy relevante.

VI Agradecimientos

Los autores queremos agradecer la ayuda brindada por la empresa Trend Ingeniería[10], para lograr realizar exitosamente la implementación del experimento.

VII Referencias

[1] Montagut E. “La transición demográfica en la revolución industrial”. Los ojos de hipatía. ISSN: 2341-0612, (2017). En línea: https://cadiznoticias.es/la-transicion-demografica-la-revolucion-industrial/. Consultado el: 16/07/2022.

[2] Divyanshi Wadhwa. “The number of extremely poor people continues to rise in Sub-Saharan Africa, while falling rapidly in all other regions”. Wold bank blogs, (2018).

[3] Kamlofsky J, Trigo S, Gonzalez G. “Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales”. WICC, (2021).

[4] Henning, K. “Recommendations for implementing the strategic initiative INDUSTRIE 4.0”, (2013).

[5] P. Binnar, A. Dalvi, S. Bhirud and F. Kazi, "Cyber Forensic Case Study of Waste Water Treatment Plant". 2021 IEEE

10 Trend Ingeniería SRL: http://www.trendingenieria.com.ar/

Bombay Section Signature Conference (IBSSC), (2021), pp. 1-5, doi: https://doi.org/10.1109/IBSSC53889.2021.9673346.
[6] Karabiyik, Umit, et al. "Forensic analysis of scada/ics system with security and vulnerability assessment." 2018 ASEE Annual Conference & Exposition, (2018).
[7] Di Iorio, Ana Haydée, et al. "El rastro digital del delito: Aspectos técnicos, legales y estratégicos de la informática forense." (2017).
[8] Mahesh Kolhe et al. “Live Vs Dead Computer Forensic Image Acquisition”. International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 8 (3), (2017), 455-457.
[9] R.M. Van der Knijff. “Control systems/SCADA forensics, what's the difference?”. Digital Investigation Volume 11, Issue 3, Elsevier, September 2014, Pages 160-174. https://doi.org/10.1016/j.diin.2014.06.007
[10] Abdullah, Haris Iskandar Mohd, et al. "Digital Forensics Investigation Procedures of Smart Grid Environment." International Journal of Computing and Digital System. Vol 11, No.1, (2021). DOI: https://dx.doi.org/10.12785/ijcds/110186
[11] Romero Raul Oscar. “Informática Forense, Seguridad y Estándares en Sistemas Industriales e Infraestructuras Críticas”, (2021).
[12] Murray, Glenn, Michael N. Johnstone, and Craig Valli. "The convergence of IT and OT in critical infrastructure." (2017).
[13] Cai, N., Wang, J., & Yu, X. (2008, July). SCADA system security: Complexity, history and new developments. In 2008 6th IEEE International Conference on Industrial Informatics (pp. 569-574). IEEE.
[14] Control para la Industria S.A. “¿Porqué 4 – 20 mA?”. En línea: https://www.cpi.com.ar/notas/por-que-4-20-ma/. Consultado 01/07/2022.
[15] Copa Roman. “Entradas digitales en equipo de control industrial”. Blog Coparoman, (2019). En línea: https://coparoman.blogspot.com/2019/08/entradas-digitales-en-equipo-de-control.html. Consultado: 01/07/2022.
[16] Blog Enerxia. “Automatismos: Partes de un PLC - Salidas digitales”. En linea: https://www.enerxia.net/portal/index.php/i-auto/941-automatismos-partes-de-un-plc-salidas-digitales. Consultado: 09/07/2022.
[17] Industrias GSL. “Qué es un PLC y cómo funciona”, (2021). En línea: https://industriasgsl.com/blogs/automatizacion/que-es-un-plc-y-como-funciona. Consultado: 09/07/2022.
[18] Bernard Cubizolles. “Everything You Need to Know about HMI / SCADA”, (2020). En línea: https://www.ge.com/digital/blog/everything-you-need-know-about-hmi-scada. Consultado: 10/07/2022.
[19] Modbus Organization. “Modbus News”, (2022). En línea: https://modbus.org/. Consultado: 01/08/2022.
[20] Nexus Integra. “MES vs SCADA en la Industria 4.0”. En línea: https://nexusintegra.io/es/mes-vs-scada/. Consultado el 01/08/2022.
[21] Kamlofsky, J., Colombo, H., Sliafertas, M., & Pedernera, J. Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas. In *III Congreso Nacional de Ingeniería Informática/Sistemas de Información,* pp. 2346-9927 (2015).
[22] Iso Org. “ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary”. En línea: https://www.iso.org/standard/73906.html. Consultado el: 10/08/2022.
[23] Arnold Johnson et al. “NIST Special Publication 800-128. Guide for Security-Focused Configuration Management of Information Systems”, National Institute of Standards and Technology, U.S. Department of Commerce, (2011). En línea: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf. Consultado el: 10/08/2022.
[24] International Society of Automation. “ISA/IEC 62443 standard specifies security capabilities for control system components”. (2018). En línea: https://www.isa.org/intech/201810standards/. Consultado el: 10/08/2022.
[25] Keith Stouffer et al. “NIST Special Publication 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security”. National Institute of Standards and Technology, U.S. Department of Commerce, (2015). En línea: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf. Consultado el: 10/08/2022.
[26] McKemmish, Rodney. “What is forensic computing?”. Canberra: Australian Institute of Criminology, 1999.
[27] CPCI, Perito Informático Forense. “Adquisiciones Forenses y Extracciones de Datos”, (2019).