Paul Skare for

Lori Ross O’Neil, Theora Rice, Penny McKenzie

PNNL

EDS Forensics

Assessing Energy Systems Using Live Analysis, A Toolkit Approach

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

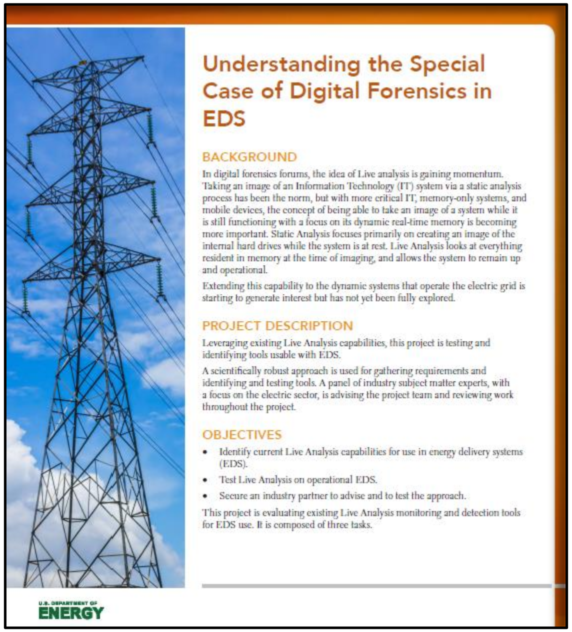
Summary: EDS Monitoring and Live Analysis

Objective

- To research and evaluate existing tools for live data capture and extraction from active energy delivery systems for analysis and response.

Schedule

- January 2015-January 2017
- 3 reports and several presentations have been completed. Two reports remaining.
- Industry will have a list of vetted and tested EDS live capture software for use on live EDS networks and systems along with a QA approach for their own future testing.



Understanding the Special Case of Digital Forensics in EDS

BACKGROUND

In digital forensics forums, the idea of Live analysis is gaining momentum. Taking an image of an Information Technology (IT) system via a static analysis process has been the norm, but with more critical IT, memory-only systems, and mobile devices, the concept of being able to take an image of a system while it is still functioning with a focus on its dynamic real-time memory is becoming more important. Static Analysis focuses primarily on creating an image of the internal hard drives while the system is at rest. Live Analysis looks at everything resident in memory at the time of imaging, and allows the system to remain up and operational.

Extending this capability to the dynamic systems that operate the electric grid is starting to generate interest but has not yet been fully explored.

PROJECT DESCRIPTION

Leveraging existing Live Analysis capabilities, this project is testing and identifying tools usable with EDS.

A scientifically robust approach is used for gathering requirements and identifying and testing tools. A panel of industry subject matter experts, with a focus on the electric sector, is advising the project team and reviewing work throughout the project.

OBJECTIVES

- Identify current Live Analysis capabilities for use in energy delivery systems (EDS).
- Test Live Analysis on operational EDS.
- Secure an industry partner to advise and to test the approach.

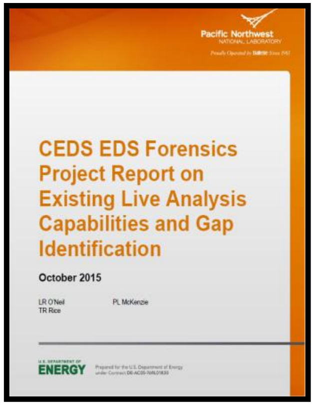
This project is evaluating existing Live Analysis monitoring and detection tools for EDS use. It is composed of three tasks.

U.S. DEPARTMENT OF ENERGY

Performer:	Pacific Northwest National Laboratory
Partners:	None
Federal Cost:	$425k
Cost Share:	0
Total Value of Award:	$425k
Funds Expended to Date:	80%

Advancing the State of the Art (SOA)

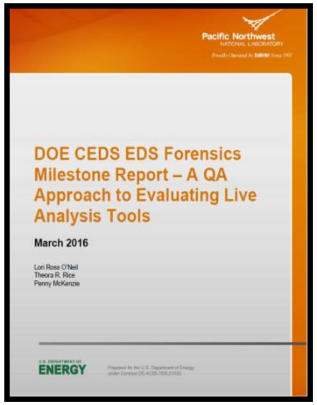
- Currently there is not a single comprehensive tool that exists to holistically address live analysis of all EDS devices.
- Our project developed an easily implemented software QA testing approach which provides a way to methodically evaluate the many tools that could be used in this field. This flexible QA framework can be applied to a variety of cyber security needs in EDS, and can also address the rapid development of software in this area.
- Our research has also highlighted functionality in current software that could be enhanced for future applicability to data extraction from a running EDS system.



CEDS EDS Forensics Project Report on Existing Live Analysis Capabilities and Gap Identification

October 2015

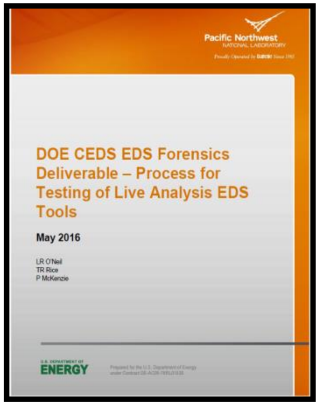
LR O'Neil
TR Rice
PL McKenzie



DOE CEDS EDS Forensics Milestone Report – A QA Approach to Evaluating Live Analysis Tools

March 2016

Lori Ross O'Neil
Theora R. Rice
Penny McKenzie



DOE CEDS EDS Forensics Deliverable – Process for Testing of Live Analysis EDS Tools

May 2016

LR O'Neil
TR Rice
P McKenzie

Challenges to Success

Test Design

- Based on industry requirements, we developed an EDS-centric QA plan for software review and testing of live analysis tools.

Identifying Initial Software To Test

- We formed an IAB and a technical advisory board, and consulted with them on industry SOA to understand the foundational software used in the field and identify software to test to meet those needs.

Tool Adaptation

- Due to the diverse nature of EDS, we found no opensource or commercial tools currently available to meet all requirements. We did find several that met the majority of the IAB's requirements, but as each environment is unique, each utility will need to determine how these tools can enhance their incident management approach.

Progress to Date

Major Accomplishments

- Presented at the Industrial Control System Joint Working Group (ICSJWG) 2016 fall meeting
- Presented at CEDS CREDC All Hands with Carol Hawk
- Completion of 3 reports for use by industry
- Attendance at BlackHat ICS training 2015
- Engaged DOE IARC (Information Assurance Resource Center) expert in PNNL testbed for interactive learning opportunity
- Formed IAB with additional parties continuing to express interest.

FY16 Status	
M2: Stand up powerNET with EDS Live Analysis tools	Complete
G/NG3: Does Panel and utility partner agree that approach adds substantial value and is the utility partner willing to actively participate	Complete
M3: Use a Quality Assurance (QA) approach to test event and capture scenarios	Complete
D3: Report on process for testing of Live Analysis EDS tools	Complete
M4: Test enhancements identified by IAB	Complete

Collaboration/Technology Transfer

Our targeted end user is Asset Owners, with interest from vendors

- Our project has used industry driven software requirements to
  - Identify software tools for live field capture by non-cyber professionals for later analysis by cyber analysts.
- Project outreach will help gain industry acceptance:
  - Industry Advisory Board: Our IAB has directed the progress of our efforts throughout the project to ensure our products are useful to industry.
  - ICSJWG Fall 2016 meeting: Lori Ross O'Neil and Theora Rice presented at this meeting and networked with industry members which generated interest in our project.
  - Presented to Chelan and Grant County PUDs, September 2016. Interest was generated and future collaboration is planned.

SEL SCHWEITZER ENGINEERING LABORATORIES

Digital Energy

AVISTA

Grant PUD

P.U.D. CHELAN COUNTY

Next Steps for this Project

- Submit Final Project Report due January 2017.
- Submit IAB reviewed no-cost extension for use with remaining funds.
- Continue to evaluate software tools recommended by industry in time remaining.

FY17 Status	
D4: Report on enhancements identified by industry for future capabilities	11/8/16
D5: Final Report	Due 1/8/17