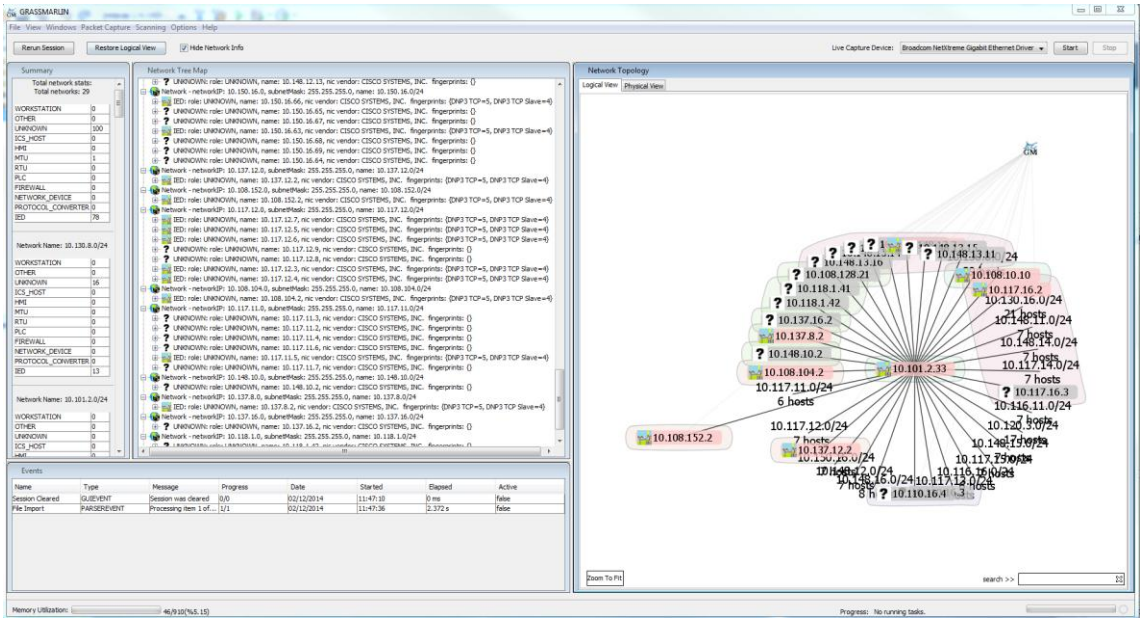
# GRASSMARLIN:

## Situational Awareness for ICS/SCADA Network Security Assessments



**Objective:** Provide IP network situational awareness of industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks to support network security. Passively map, and visually display, an ICS/SCADA network topology while safely conducting device discovery, accounting, and reporting on these critical cyber-physical systems.

**Background:** The cyber risk to ICS/SCADA systems which control our US Critical Infrastructure and Key Resources (CI/KR) is significant and growing daily. There is an increasing possibility of cyber attacks with disruptive or physically destructive consequences. The vulnerable state of ICS/SCADA systems and devices (e.g. PLC, HMI) has been publicly documented in vulnerability reports on the Internet and discussed at multiple conferences. To understand the related risk, we must understand what we're trying to protect. That starts with good situational awareness.

**Plan:** To establish passive ICS/SCADA network situational awareness capabilities and support ICS/SCADA device and communications identification. Expand the identification Knowledge Base through collaboration with the user community.

**Benefits:**

- Lightweight framework designed to provide safe unobtrusive network situational awareness
- Intuitive graphical view of control system network topology
- Device and communication data enhancements via ICS/SCADA Knowledge Base