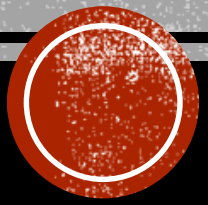
A REMOTELY ACCESSIBLE, CONFIGURABLE, INSTRUMENTED ICS LAB FOR ATTACK, DEFEND, AND FORENSICS RESEARCH AND EDUCATION

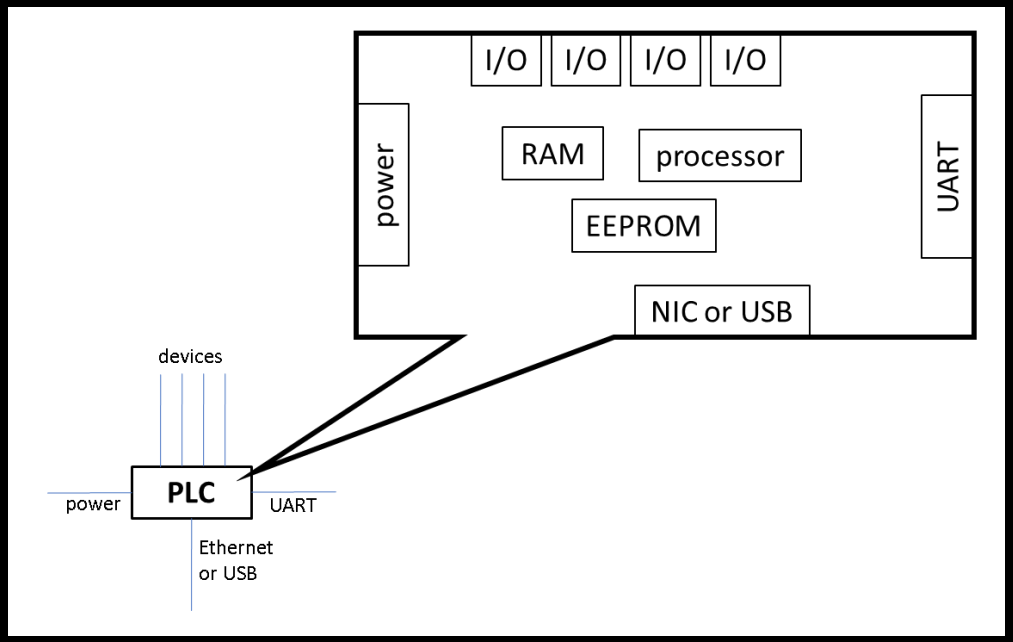


Jim Jones, PhD
Associate Professor, ECE
George Mason University

Peggy Brouse, PhD
Professor, SEOR
George Mason University

BACKGROUND

- **ICS: Industrial Control System**
- **PLC: Programmable Logic Controller**

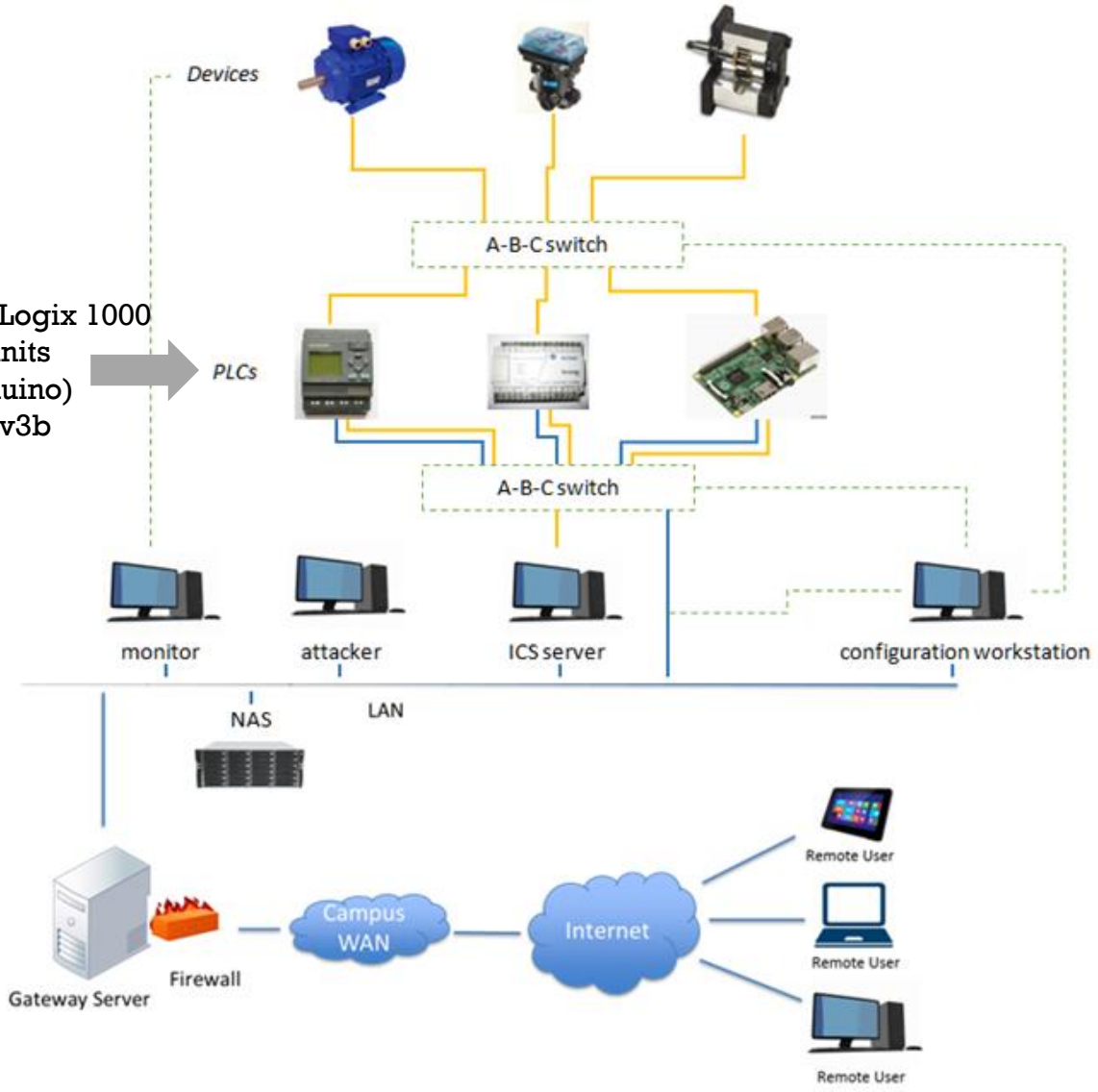


WHY? WHAT'S THE NEED, GAP, PROBLEM?

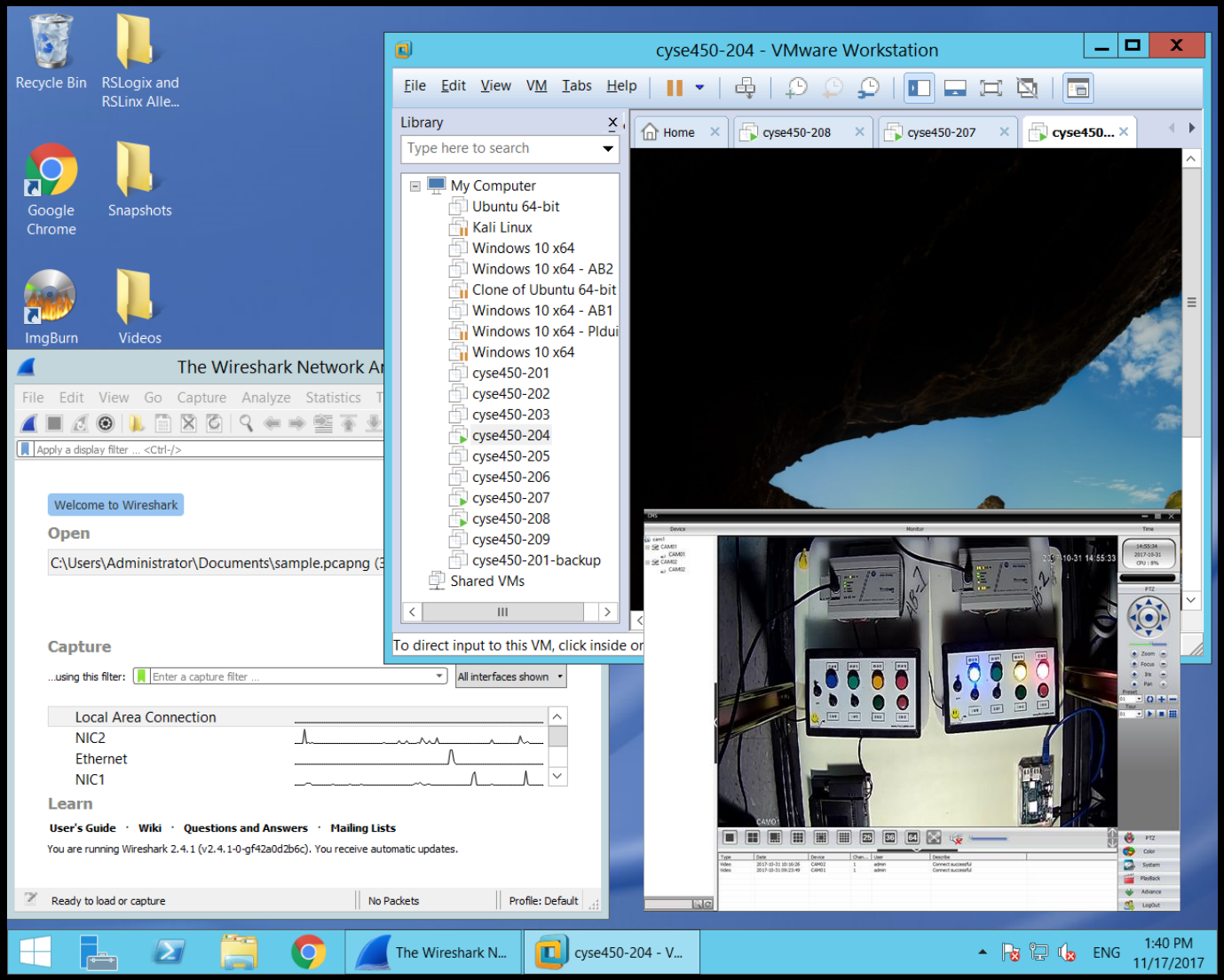
- **Academic programs:**
  - BS Cybersecurity Engineering
  - BS/MS/PhD Computer Engineering
  - PhD Information Technology with concentration in Digital Forensics
- **Research:**
  - Attack and compromise residual digital artifacts
    - persistent storage, volatile memory, and network
- **Need:**
  - Hands-on with realistic devices and environments
- **Problem:** virtual is useful for many cases, but with PLCs…
  - fidelity for deep forensics (e.g., storage behavior)
  - physical effects (e.g., power and other faults, inputs)
- **Goal:**
  - Real, remote environment for testing attack, defense, response, and forensics on ICS components (especially PLCs vs. control workstations)
- **Funding:**
  - NSA/US Army Reserve P3i grant

WHAT WE BUILT...

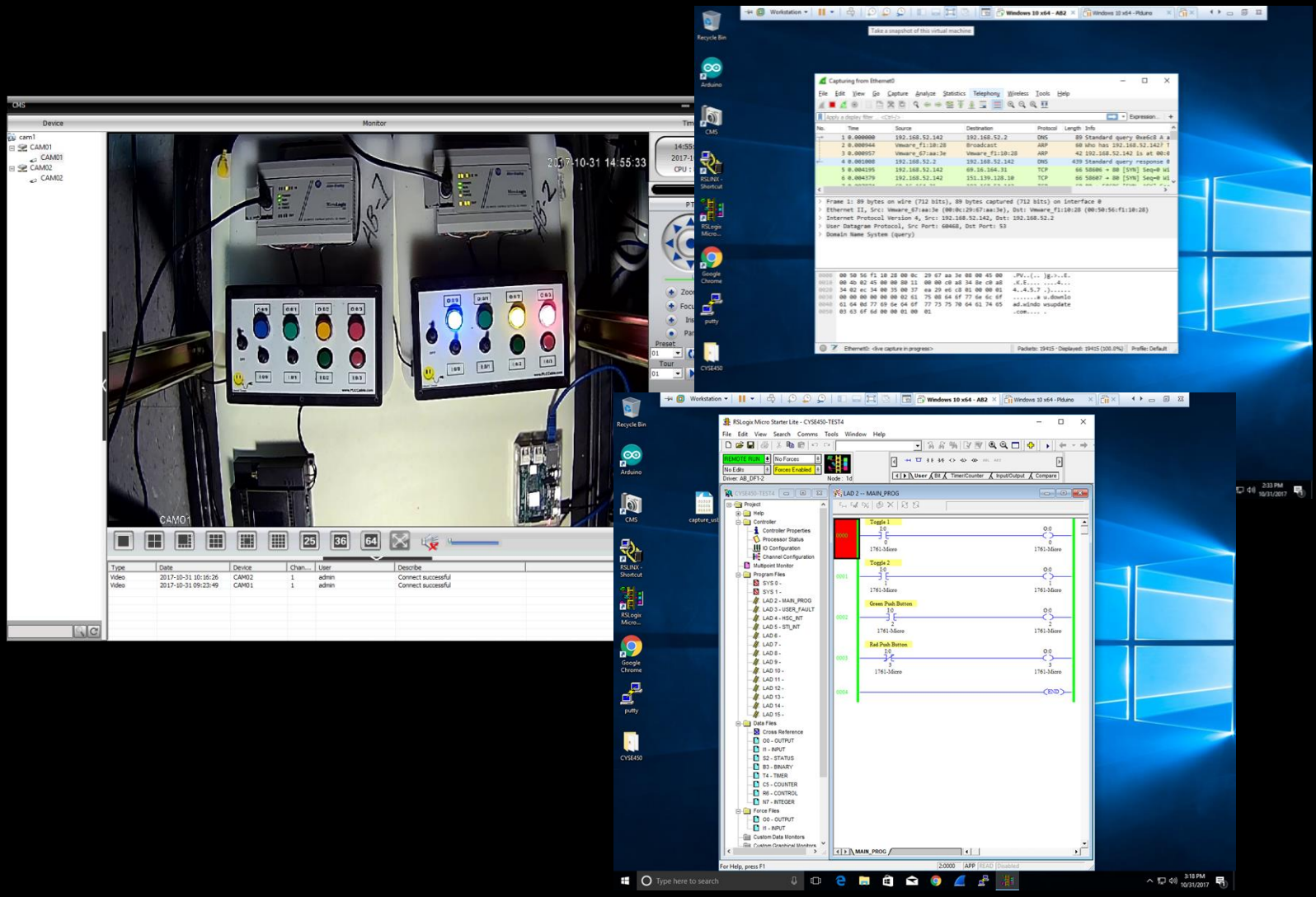
2 Allen-Bradley MicroLogix 1000
2 Siemens S7 units
1 OpenPLC (Arduino)
2 RaspberryPi v3b



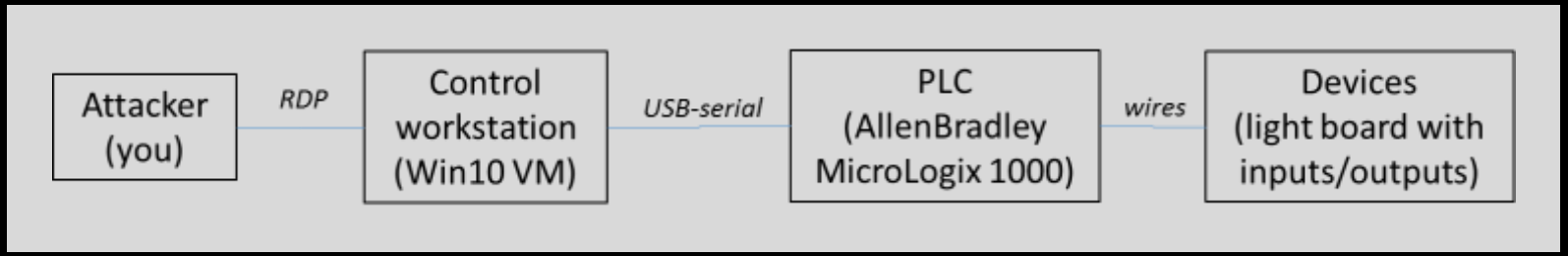
THE ADMINISTRATOR SEES...



THE STUDENT SEES…



STUDENT EXERCISE (CYSE 450)



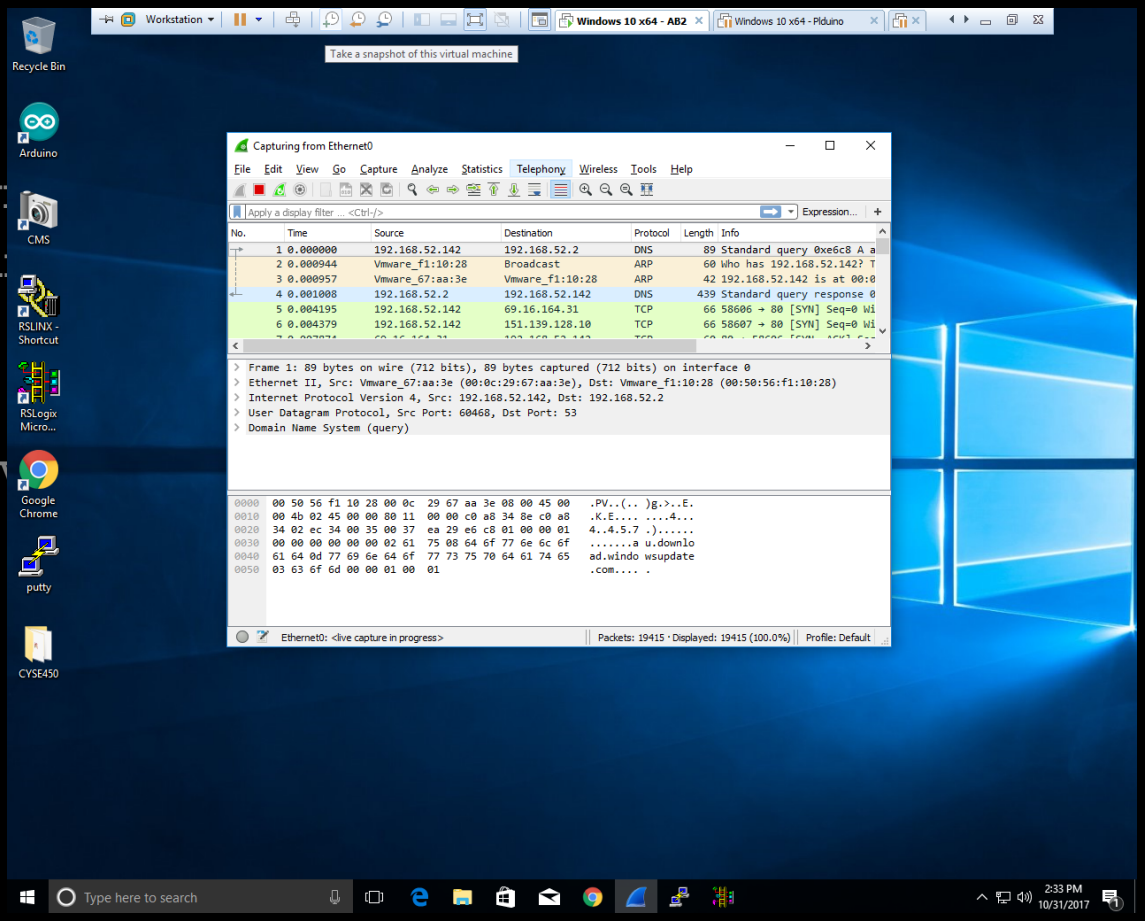
Exercise Activities:

- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- Capture running program
- Modify and load running program
- Analyze firmware
- Analyze memory
- Offensive and defensive considerations

STUDENT EXERCISE (CYSE 450)

Exercise Activities:

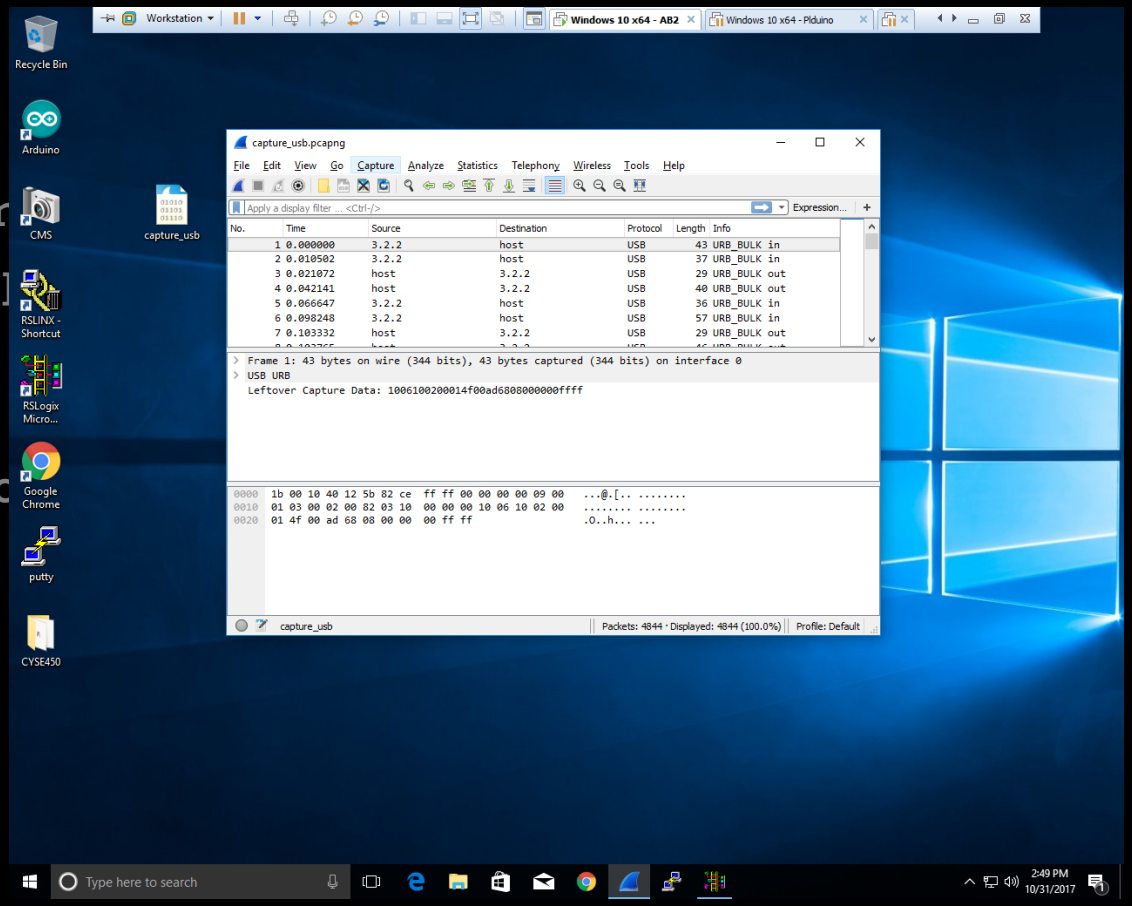
- **Access VM (control workstation)**
- **Sniff Ethernet side**
- Sniff USB/serial side
- Alter PLC states
- Capture running prog
- Modify and load runni
- Analyze firmware
- Analyze memory
- Offensive and defensi



STUDENT EXERCISE (CYSE 450)

Exercise Activities:

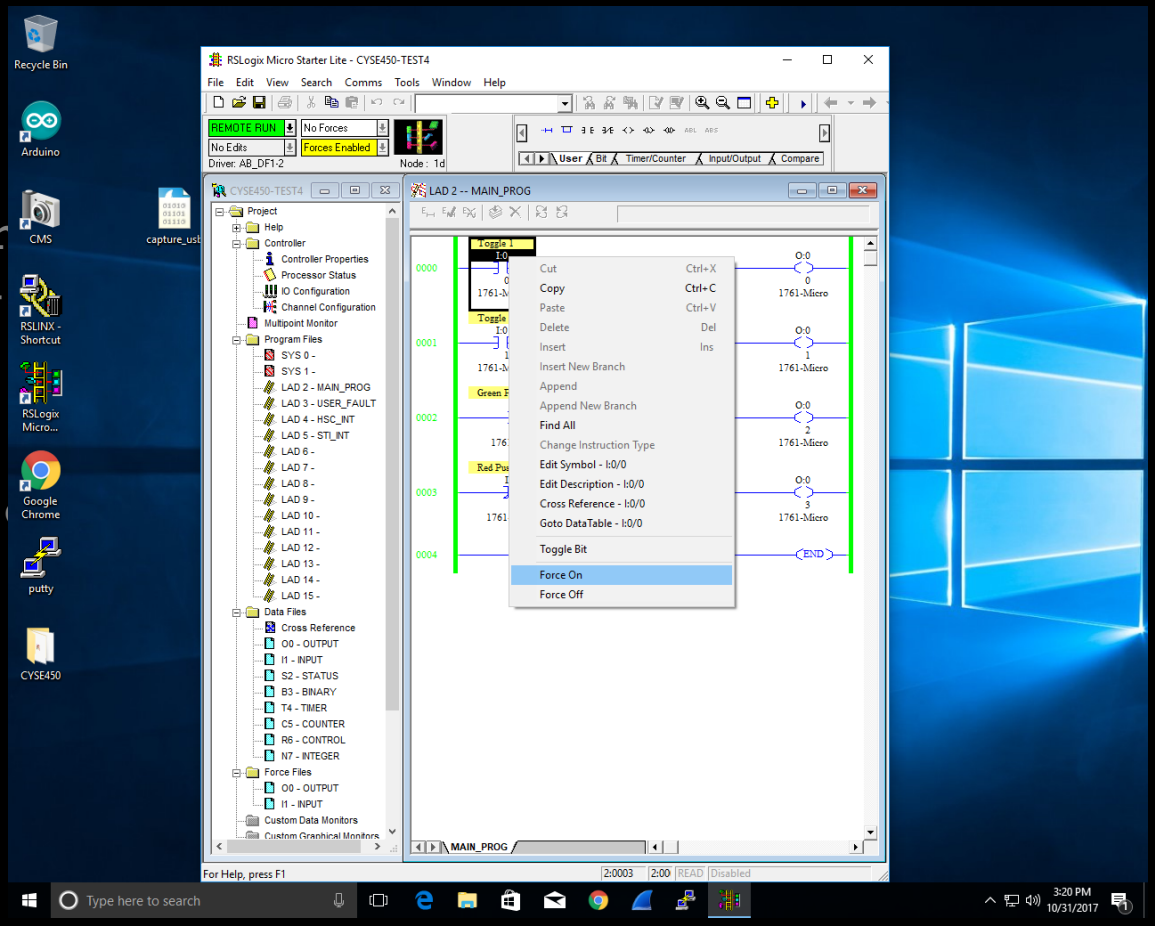
- Access VM (control workstation)
- Sniff Ethernet side
- **Sniff USB/serial side**
- Alter PLC states
- Capture running program
- Modify and load running
- Analyze firmware
- Analyze memory
- Offensive and defensive



STUDENT EXERCISE (CYSE 450)

Exercise Activities:

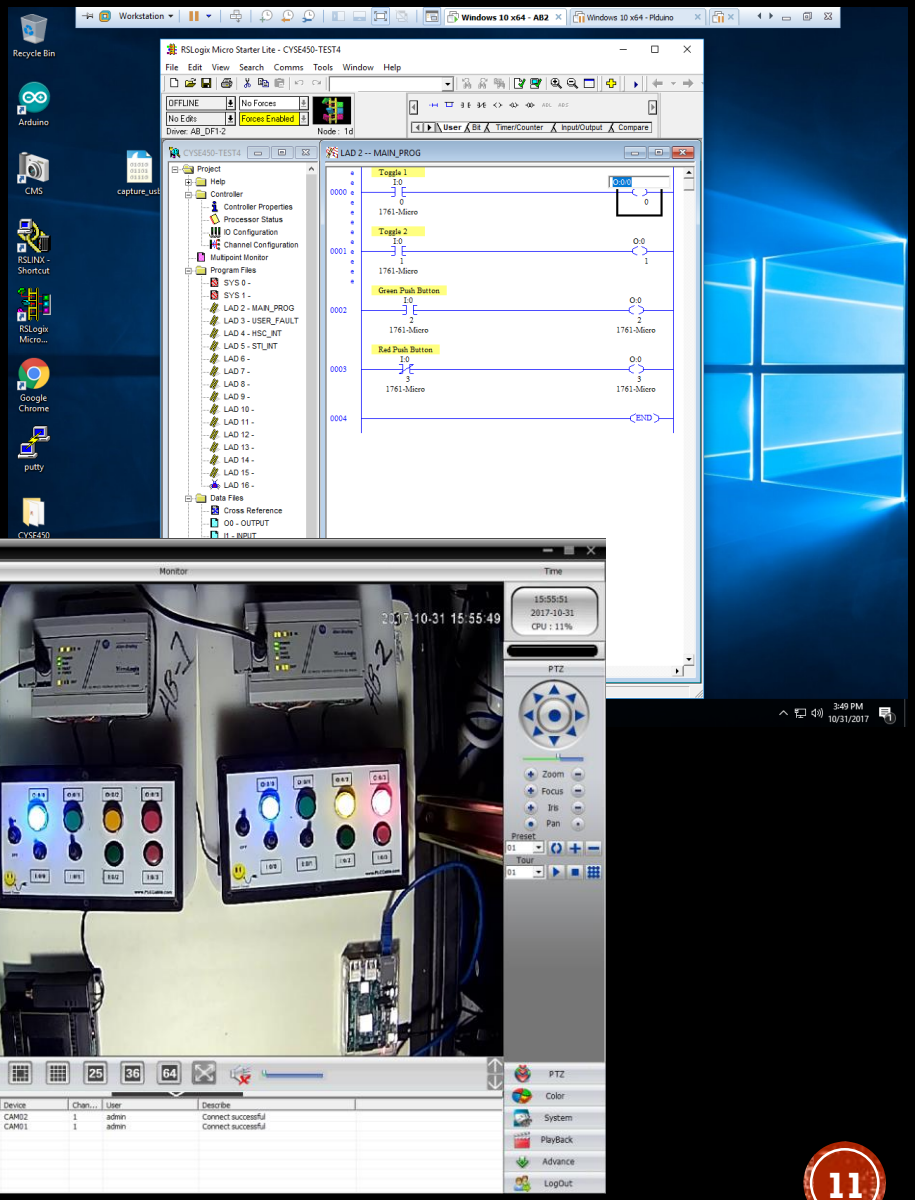
- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- **Alter PLC states**
- Capture running prograr
- Modify and load running
- Analyze firmware
- Analyze memory
- Offensive and defensive



STUDENT EXERCISE (CYSE 450)

Exercise Activities:

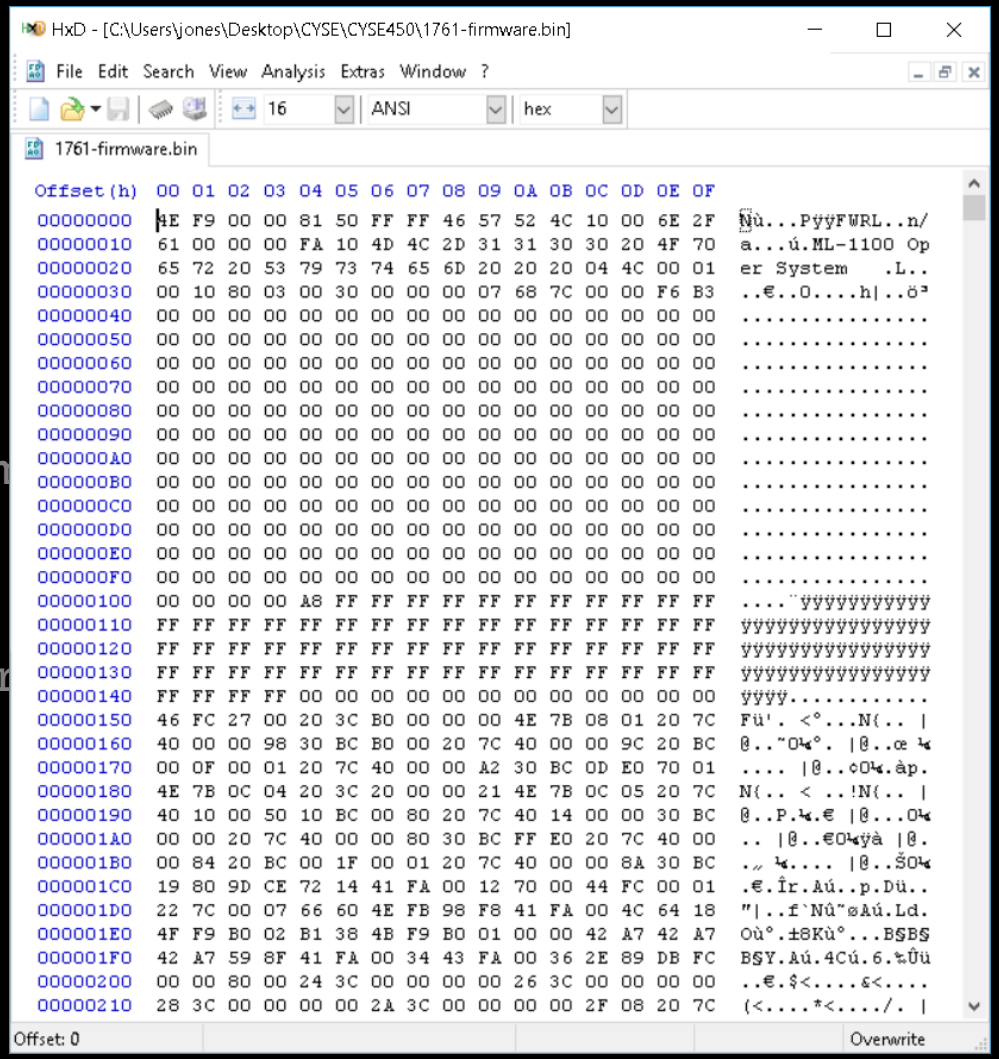
- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- **Capture running program**
- **Modify and load running program**
- Analyze firmware
- Analyze memory
- Offensive and defensive c



STUDENT EXERCISE (CYSE 450)

Exercise Activities:

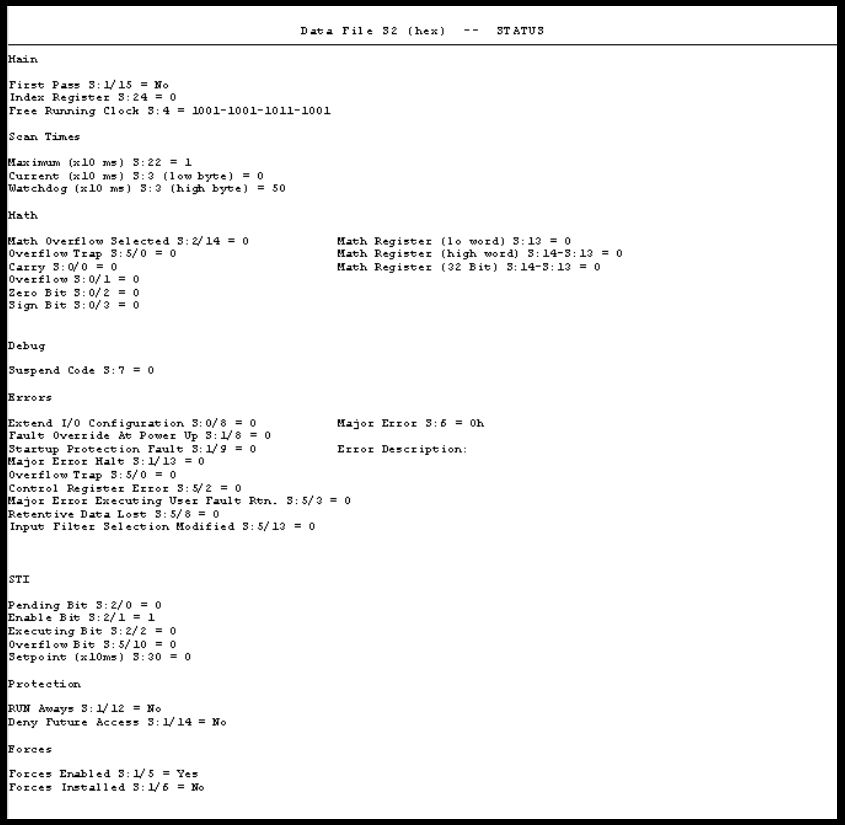
- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- Capture running program
- Modify and load running program
- **Analyze firmware**
- Analyze memory
- Offensive and defensive considerations



STUDENT EXERCISE (CYSE 450)

Exercise Activities:

- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- Capture running program
- Modify and load running program
- Analyze firmware
- **Analyze memory**
- Offensive and defensive considerations



Data File S2 (hex) -- STATUS

Main

First Pass S:1/15 = No
Index Register S:24 = 0
Free Running Clock S:4 = 1001-1001-1011-1001

Scan Times

Maximum (x10 ms) S:22 = 1
Current (x10 ms) S:3 (low byte) = 0
Watchdog (x10 ms) S:3 (high byte) = 50

Math

Math Overflow Selected S:2/14 = 0
Overflow Trap S:5/0 = 0
Carry S:0/0 = 0
Overflow S:0/1 = 0
Zero Bit S:0/2 = 0
Sign Bit S:0/3 = 0
Math Register (lo word) S:13 = 0
Math Register (high word) S:14-S:13 = 0
Math Register (32 Bit) S:14-S:13 = 0

Debug

Suspend Code S:7 = 0

Errors

Extend I/O Configuration S:0/8 = 0
Fault Override At Power Up S:1/8 = 0
Startup Protection Fault S:1/9 = 0
Major Error Halt S:1/13 = 0
Overflow Trap S:5/0 = 0
Control Register Error S:5/2 = 0
Major Error Executing User Fault Rtn. S:5/3 = 0
Retentive Data Lost S:5/8 = 0
Input Filter Selection Modified S:5/13 = 0
Major Error S:6 = 0h
Error Description:

STI

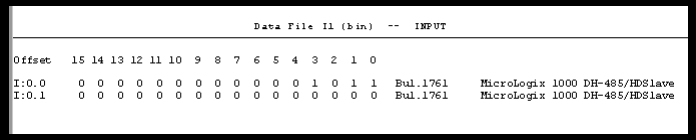
Pending Bit S:2/0 = 0
Enable Bit S:2/1 = 1
Executing Bit S:2/2 = 0
Overflow Bit S:5/10 = 0
Setpoint (x10ms) S:30 = 0

Protection

RUN Aways S:1/12 = No
Deny Future Access S:1/14 = No

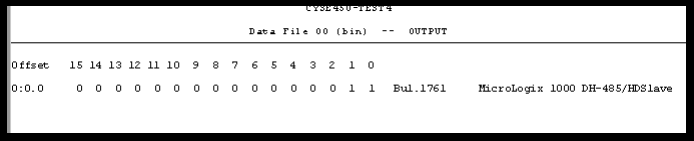
Forces

Forces Enabled S:1/5 = Yes
Forces Installed S:1/6 = No



Data File I1 (bin) -- INPUT

Offset	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		
I:0.0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	Bul.1761	MicroLogix 1000 DH-485/HDSlave
I:0.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Bul.1761	MicroLogix 1000 DH-485/HDSlave



CYSE450-TEST4

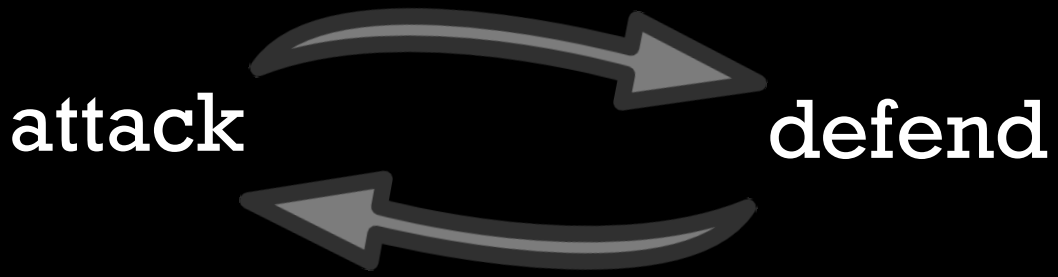
Data File O0 (bin) -- OUTPUT

Offset	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		
O:0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	Bul.1761	MicroLogix 1000 DH-485/HDSlave

STUDENT EXERCISE (CYSE 450)

Exercise Activities:

- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- Capture running program
- Modify and load running program
- Analyze firmware
- Analyze memory
- **Offensive and defensive considerations**



RESULTS AND NEXT STEPS

RESULTS:

- Minimal problems walking through guided portion of lab
  - Exposure to PLCs, ladder logic
- Applied existing skills analyzing network, code, firmware, memory
- Offense and defense:
  - ideas from lab and open sources
  - applied iterative security assessment model

NEXT STEPS:

- Additional hardware (more PLCs)
- Additional exercises (attack and manipulation; forensics)
- More instrumentation
- Sequential memory snapshot analysis under adversarial activity

QUESTIONS?

Jim Jones, PhD
Associate Professor, ECE
Digital Forensics and Cyber Analysis
Nguyen Engineering Bldg., Room 3241
George Mason University, MS 2B5
Fairfax, VA 22030
(o) 703-993-5599
(c) 703-955-1033
(e) jjonesu@gmu.edu
(w) http://ece.gmu.edu/
(w) http://cfrs.gmu.edu/
(w) http://dfdarg.wordpress.com