Ohio Regional Programming Center Digital Forensics Initiatives

The Cincinnati-Dayton Cyber Corridor (Cin-Day Cyber)
Cassie Barlow, PhD
and
University of Akron
Stanley Smith, Professor of Practice

OCRI Digital Forensics Team

Stanley Smith, Professor, The University of Akron

Cassie Barlow, PhD, SOCHE

Ryan Moore, University of Cincinnati

Phu Phung, PhD, University of Dayton

Jaime Carazo, University of Dayton

Scott Belshaw, PhD, University of Dayton

Glenn Goe, Stark State University

Larry Atkinson, Lorain County Community College

Junjie Zhang, PhD, Wright State University

CINCINNATI - DAYTON
CYBER CORRIDOR

Team Accomplishments

- Partnered with Technology First on the Ohio Information Security Conference
- Collected information on existing Digital Forensics curriculum at Colleges/Universities across the State
- Reviewed existing curriculum and mapped to NICE Framework Digital Forensics skills
- Reviewed final rubric for gaps
- Based upon review, Dr Phung and Dr Zhang built new OCRI modules: Binary Analysis & Malicious Web Analysis and Classification
- Collaboration on Digital Forensics Laboratories across State

THE UNIVERSITY OF AKRON
FIAT LUX
1870

CINCINNATI - DAYTON
CYBER CORRIDOR

Statewide Digital Forensics Curriculum

	A	B	D	E	F	G	H
1	**NICE Framework Digital Forensics Skills**	**Priority**	Stark State*	Lorain*	Akron*	UD*	WSU
2		example (1-3; 1=highest)	example: (B - 3; I - 2; A - 1)				
3	**S0032:** Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.	2, to ask Akron	B-1, I-1	B-1, I-2	I-3, A-3	B-4	B-1
4	S0047: Skill in preserving evidence integrity according to standard operating procedures or national standards.	2, to ask Lorain and Stark	B-1, I-1, A-1	B-1, I-1, A-2	B-2, I-3	B-1, I-2	
5	**S0062:** Skill in analyzing memory dumps to extract information.	3, to ask Lorain and Akron	I-2	B-1, I-2, A-1	I-4, A-1	B-3; I-3	
6	**S0065:** Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	3, to ask Lorain and Akron, and Stark	B-2, I-1, A-1	A-3	I-4, A-4	I-2	
7	**S0067: Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).**	3. to ask Lorain and Akron	B-1, I-3, A-3	A-3	B-1, I-2	I-4	
8	**S0068:** Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	3, to ask Lorain and Akron, and UD	B-1	B-2, I-2	I-1, A-1	A-2;B-1	
9	**S0069:** Skill in setting up a forensic workstation.	2, to ask Lorain	B-1	B-1, I-1	I-1, A-1	I-1	B-1
10	**S0071:** Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	3, to ask Lorain and Akron, and UD, and Stark	B-1, A-2	B-1, I-1, A-2	I-1, A-1	A-2	
11	**S0073:** Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	3, no action	B-1, I-1, A-1	B-1, A-1	I-3, A-3	A-3; B-6	B-1
12	**S0074:** Skill in physically disassembling PCs.	1	B-1		I-1	B-1	

Digital Forensics Collaboration

- Complex technology, difficult, and initial start-up expensive
- Funding in the amount of $13,000 for digital forensics
- Strategy to build and Cyber-Digital Forensics ecosystem
- Collaboration on **digital forensics laboratories** across RPC's
- Focus on mobile device forensics chip-off technology
- Focus on cyber-digital forensics training
- Comprehensive digital forensics curriculum with hands-on labs
- Dayton, Akron, Lorain, and Stark State will improve curriculum
- DFAG tasks: mobile device forensics and training
- Demands on the private sector, state, and local government

Mobile Device Forensics

- Chip-reading tools are solutions which support digital forensics
- Digital forensics specialists rely on mobile device forensics

Scope of work requires a lab to provide:

- Cyber and digital forensics process and investigations
- Acquisition procedures for mobile devices
- Provide forensics services and training for the OCRI-RPC's
- Develop digital forensics resources for mobile device forensics
- Set-up lab and equipment to meet requirements for operations

Needs of local law enforcement agencies:

- Authentication, forensic tools, cloud forensics, bitcoin, cryptocurrency, artificial intelligence, and fraud

CINCINNATI - DAYTON
CYBER CORRIDOR

Questions?