309 Stove Pipe Rd
Voorheesville, NY 12186
(518) 380-8956
JFarley248@gmail.com
FarleyForensics.com

Jack Farley

SKILLS

- JTAG/ISP/Chip Off Extractions
- Basic x86 & x86_64
- Python & C++
- Basic Malware Analysis
- Cellebrite
- Magnet Axiom
- EnCase
- Filesystem Forensics
- Public Speaking
- Incident Response
- X-Ways
- Research & Development

ACTIVITIES

- Presenter at the 2019 Magnet User Summit
- Created forensics tools that are now taught in SANS 585
- Owns JTAG/ISP/Chip Off equipment and practices on broken androids in free time
- Champlain College Digital Forensics Association Vice President
- Github.com/jfarley248?tab=repositories
- Published author in eForensicsMag

EXPERIENCE

Blackstone Discovery, Palo Alto, CA — *Associate Cyber Investigator & Tool Developer*

September 2019 - Present

- Performs research and development on new forensics artifacts.
- Assists in incident response and forensics cases.

Champlain College, Burlington, VT — *Teacher's Assistant*

January 2019 - Present

- TA for the following classes
  - FOR-430 Malware Analysis & IR
  - FOR-310 Mobile Forensics
  - FOR-240 Intro to Digital Forensics

Stroz Friedberg, Dallas, TX — *Summer Cyber Associate*

June 2019 - August 2019

- Performed research on windows mini crash dumps and event trace log parsing and presented to all offices at the end of the summer.
- Assisted in incident response investigations.

Leahy Center for Digital Investigation, Burlington, VT — *Research Assistant II*

January 2017 - Present

- IoT Forensics Mentor - Fall 2019
  - Mentor for the new team of IoT Forensics. Helps team members with research and project goals.
- IoT Forensics - Spring 2019
  - Tasked with data generation and forensic examination of various IoT devices such as the Facebook Portal, Amazon Echo family, and more. This research was presented by Jonathan Rajewski at the 2019 Magnet User Conference.
- Malware Analysis - Fall 2018
  - Team Lead, tasked with creating a high-end lab environment to safely analyze malware in multiple Windows environments. Created Cuckoo sandbox, as well as 2 other machines with FLARE equipped VM's to dynamically and statically analyze malware with BRO and Elk Stack monitoring network data.
- Bluetooth Tracking Project - Fall 2017 & Spring 2018
  - Tasked with creating Python scripts paired with Ubertooths and Raspberry Pis to triangulate Bluetooth devices throughout a building.
- Application Analysis - Spring 2017
  - Investigated forensic artifacts left behind by Android Applications.
  - Maintained a chain of custody with superiors for our test device.
  - Performed extractions via ADB and Cellebrite.

Sony, Herndon, VA — *Computer Forensics Intern*

June 2018 - August 2018

- Worked on two Capstone projects as well as other research.
- Capstone 1: ISP/JTAG
  - Learned how to successfully perform both JTAG and ISP extractions on multiple Android devices.
- Capstone 2: Global Threat Emulation - GTE
  - Worked with Sony's Red Team to find forensic artifacts left behind by their custom tools.
- Other research
  - Assisted with casework when cases came in.
  - Taught myself basic x86 assembly using Xeno Kovah's 12-hour online x86 class to prepare for GTE capstone.
  - Completed x86 practice labs created by Sony's Red Team.
  - Started Corey Kallenberg's online intro to software exploits class.
  - Attended coworker led malware/reverse engineering classes based off of the *Practical Malware Analysis* textbook.

Leahy Center for Digital Investigation, Burlington, VT — *Technical Intern*

August 2016 - December 2016

- Semester-long group project called Forensic Tool Evaluation
  - Generated test data on HDD.
  - Tested various forensic tools to compare performance between them.

- Created a finalized report to present to our superiors.

EDUCATION

Champlain College, Burlington, VT — *B.S. Digital Forensics, Minor Computer Science*

August 2016 - May 2020

Classes Taken:

- File System Forensics
- Operating System Forensics
- Python Forensics
- Intro x86 Assembly
- Advanced Programming
- Incident Response
- Mobile Forensics
- E-Discovery
- Malware Analysis & IR