Michael K. Mabey

(480) 788–3411 ◇ mmabey@ieee.org ◇ mikemabey.com
github.com/mmabey ◇ bitbucket.org/mmabey
LinkedIn

EDUCATION

Ph.D. Computer Science — Information Assurance *Dec 2017*
Arizona State University Tempe, AZ
Dissertation: Forensic Methods and Tools for Web Environments

M.S. Computer Science — Information Assurance *Aug 2011*
Arizona State University Tempe, AZ
Thesis: Collaborative Digital Forensics: Architecture, Mechanisms, and Case Study

B.S. Computer Science — Information Systems *May 2009*
Utah State University Logan, UT

EXPERIENCE

Computer Scientist (U.S. Army Civilian) *Dec 2017 – Present*
Data Science Directorate, Network Enterprise Technology Command (NETCOM) Phoenix, AZ
Grade: GS-0854-12 Step 1 *Service*: Competitive *Tenure*: Conditional, Full-Time

- Designed, implemented, and deployed analytics for the Army's instance of DISA's **Big Data Platform (BDP)**, including an app for monitoring vulnerability patching compliance and a dashboard for visualizing performance of information technology service management (ITSM) ticket resolution. Analytics were composed of a web interface using **Python**, **Flask**, **Vue**, and **Bootstrap**, with **pandas** for the data analysis, **Plotly** for the visualizations, and **Celery** and **redis** for task management.
- Shortened the development cycle for BDP apps by automating the build, packaging, and deployment process using **Python** and GitLab's **Continuous Integration** utility.
- Acted as technical liaison during fiscal year 2018 for a $3 million contract with Sandia National Laboratories to implement tools such as an anomaly detection ensemble, an emulation model of a notional network, and a WHOIS registrant analyzer. I acquired data samples to inform the implementation and testing of the analytics, ensured the projects stayed focused on operational objectives, held weekly sync meetings, reported to leadership on Sandia's progress, and assessed the value of the delivered products.
- Technical lead for NETCOM Data Science with ASU. Led strategic discussions with ASU's Global Security Initiative (GSI) leadership to collaborate on real-world NETCOM issues. Spearheaded the effort for ASU to gain access to an instance of the Army's BDP for improved technical collaboration. Served as the Army's program lead for the ASU Computer Science Capstone initiative.
- Initiated a culture in the Directorate of using **git**, **GitLab**, and DevOps methods and established internal best practices for collaborating on code development and documenting lessons learned.

Adjunct Professor *Jan 2019 – May 2019*
Arizona State University Tempe, AZ

- Taught CSE 469 Computer and Network Forensics which covered basics and history of digital forensics, proper forensic processes, hard drive geometry, volume analysis, file systems (ext4 in particular), and forensic techniques for email, mobile devices, web environments, and the cloud.
- Designed and taught a senior-level, technically advanced course (CSE 469) with innovate homework, group projects, and in-class labs to apply the processes and principles of digital forensics by writing forensic programs and by using industry-standard software to analyze evidence. Exposed the students to cutting-edge and seminal forensic research papers by a literature review of novel scientific methods and techniques to acquire, store, analyze, and present digital forensic evidence.

Research Assistant *Nov 2009 – Dec 2017*
Security Engineering for Future Computing (SEFCOM) Lab, ASU Tempe, AZ
Lab Directors: Gail-Joon Ahn, Adam Doupé, Ziming Zhao, Yan Shoshitaishvili
Sponsors: Department of Energy, National Science Foundation

- Created a method for identifying extensions installed on **Chrome OS** by analyzing the encrypted files on the hard drive. Wrote an accompanying crawler in **Python** (and using **Ansible**, **Celery**, **MySQL**, **sshfs**, and **OpenStack**) to download all extensions on the Chrome Web Store and analyze them.
- Developed a forensic acquisition approach for web email that reestablishes persistent cookie sessions stored by a browser, and automated the process using **Python** and **Selenium**.
- Maintained fifteen servers for the lab, including a public-facing router, an **OpenVPN** server, a reverse-proxy web server with **TLS** certificate management, an **OpenStack** cloud, switches transmitting **VLAN**-tagged traffic, and a **GitLab** server.

Summer Intern *Jul 2015 – Sep 2015*
Arizona Cyber Threat Response Alliance (ACTRA) Phoenix, AZ

- Designed an operationalized workflow for Arizona Infragard member organizations to share **threat intelligence** through a common **STIX/TAXII** platform.

Graduate Student Summer Intern *May 2011 – Jul 2011*
Sandia National Laboratories Albuquerque, NM

- Helped design a dynamic malware analysis framework built on **OpenStack**, allowing incident responders to define customizable analysis environments and use arbitrary analysis tools for triage or manual analysis.
- Wrote **Python** scripts to automate the setup process for using a SheevaPlug computer as a wireless intrusion detection agent running **Kismet**.

TECHNICAL STRENGTHS & QUALIFICATIONS

Clearance	Active DoD TS/SCI
Programming Languages	Python, Bash, C/C++, HTML, CSS, LaTeX
VCS, Testing, & CI/CD	Git, pytest, Python unittest, GitLab Pipelines, CircleCI, Nexus
Operating Systems	Windows, Linux, Chrome OS
Forensic Tools	FTK, Sleuth Kit & Autopsy, dd, HxD, etc.
Protocols & APIs	JSON, XML, AMQP, REST, STIX, RabbitMQ
Network Administration/Security	Ansible, OpenVPN, ufw, lighttpd, Caddy, Wireshark
Cloud Architectures	OpenStack, Amazon EC2
Databases	MySQL, SQLite

AWARDS AND ACTIVITIES

- Promoted from GS-11 to GS-12 *Dec 2018*
- Individual Cash Award, from NETCOM supervisor *Dec 2018*
- Achievement Medal for Civilian Service *Oct 2018*
- Individual Time-Off Award, from NETCOM supervisor *Sep 2018*
- Individual Cash Award, from NETCOM supervisor *Sep 2018*
- DoD Information Assurance Scholarship Program (IASP) Recipient (5 years) *2012 – 2017*
- Team Leader — ASU team in the UCSB International CTF *2009, 2010, 2014, 2015*
- Inducted into Eta Kappa Nu (HKN) Engineering Honors Society *Nov 2010*
- Eagle Scout, Boy Scouts of America *2002*