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
Committee: Gail-Joon Ahn (Co-Chair), Adam Doupé (Co-Chair), Stephen S. Yau, Jooyung Lee, Ziming Zhao
Dissertation: Forensic Methods and Tools for Web Environments

> The Web is one of the most exciting and dynamic areas of development in today's technology. However, web environments also present a set of new challenges for digital forensic examiners, making their jobs even more difficult. In my dissertation, I present (1) a framework for web environment forensics, which gives examiners a method for how to approach web-based evidence; (2) a method to identify extensions installed on encrypted web thin clients without breaking the encryption; and (3) an approach to reconstructing the timeline of events on encrypted web thin clients by using service provider APIs as a proxy for directly analyzing the device. I also introduce several structured formats that I customized to accommodate the unique features of web-based evidence while also facilitating tool interoperability and information sharing.

M.S. Computer Science — Information Assurance *Aug 2011*
Arizona State University Tempe, AZ
Committee: Gail-Joon Ahn (Chair), Stephen S. Yau, Dijiang Huang
Thesis: Collaborative Digital Forensics: Architecture, Mechanisms, and Case Study

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

EXPERIENCE SUMMARY

Computer Scientist (U.S. Army Civilian) *Dec 2017 – Present*
Data Science Directorate, Network Enterprise Technology Command (NETCOM) Phoenix, AZ

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

Research Assistant *Nov 2009 – Dec 2017*
Security Engineering for Future Computing (SEFCOM) Lab, ASU Tempe, AZ

Civilian Reserve/Intern *May 2016 – Aug 2016*
Arizona Department of Public Safety Phoenix, AZ

Teaching Assistant *Aug 2010 – Dec 2015*
Arizona State University Tempe, AZ

SAT/ACT Instructor *Sep 2015 – Oct 2015*
Minerva Learning, LLC Chandler, AZ

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

Teaching Assistant (Instructor of Record) *Aug 2011 – Dec 2014*
Arizona State University Tempe, AZ

Student Trainee (U.S. Army Civilian) *Jun 2013 – Aug 2013, Jun 2014 – Aug 2014*
Army Cyber Command (ARCYBER) Fort Meade, MD

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

Graduate Student Recruitment Specialist/Webmaster *Jul 2006 – Aug 2009*
Electrical & Computer Engineering Department, USU Logan, UT

Technician Aid *Sep 2006 – Aug 2009*
Electrical & Computer Engineering Department, USU Logan, UT

Store Attendant *Jun 2005 – Sep 2008*
Electrical & Computer Engineering Department, USU Logan, UT

Lab Technician *May 1997 – Aug 2002*
KWM Electronics Co. West Jordan, UT

PROFESSIONAL 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.

Civilian Reserve/Intern *May 2016 – Aug 2016*
Arizona Department of Public Safety Phoenix, AZ

- Updated the content, layout, and topics of the security policy for the Arizona Counter Terrorism Information Center (ACTIC) for clarity and to be in compliance with recommendations from the Department of Homeland Security. Created training slides to accompany the new security policy.

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.

Student Trainee (U.S. Army Civilian) *Jun 2013 – Aug 2013, Jun 2014 – Aug 2014*
Army Cyber Command (ARCYBER) Fort Meade, MD
Grade: GG-0199-09 Step 1 *Service*: Excepted *Tenure*: Permanent, Full-Time

- Summer internships in connection with DoD IASP scholarship.

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**.

Graduate Student Recruitment Specialist/Webmaster *Jul 2006 – Aug 2009*
Electrical & Computer Engineering Department, USU Logan, UT

- Primary responsibilities included maintaining and augmenting the department website using **PHP**, **MySQL**, and other basic web technologies like **CSS**, **JavaScript**, and an **SMTP** server.
- Completed multiple graphic design projects for the department using **GIMP**, **Adobe Photoshop**, and **Adobe Illustrator**.
- Replaced a **MS Access** database by porting the old data to a **MySQL** server and creating a set of **Python** programs with the **Dabo** framework that interfaced with the database.
- Created a testing environment using an **Apache** web server, **PHP**, **MySQL**, and **SVN**.
- Gathered statistics on web visitors, inquiries from students, and applicants' credentials for the purpose of improving the department's graduate student recruitment processes.
- Responded to inquiries from potential domestic and international graduate students.

Technician Aid *Sep 2006 – Aug 2009*
Electrical & Computer Engineering Department, USU Logan, UT

- Built and maintained computers for department faculty and student labs.
- Installed and configured various software on Windows machines for faculty, staff, and students.
- Created and restored backup images of lab computers using **Norton Ghost** and **Acronis TrueImage**.
- Protected lab computers using **Faronics Deep Freeze**.

Store Attendant *Jun 2005 – Sep 2008*
Electrical & Computer Engineering Department, USU Logan, UT

- Maintained equipment and instruments in the labs for electrical engineering students.
- Performed store duties including maintaining inventory, serving customers, cleaning rooms, and running errands.

Lab Technician *May 1997 – Aug 2002*
KWM Electronics Co. West Jordan, UT

- Worked closely with CEO/Head Engineer to build prototypes of electronic devices.
- Used various soldering techniques on both through-hole and surface-mount parts.

HONORS AND AWARDS

- Promoted from GS-11 to GS-12 *Dec 2018*
- Individual Cash Award, from NETCOM supervisor *Dec 2018*
  - For exceeding performance expectations.

- Achievement Medal for Civilian Service *Oct 2018*
  - "For outstanding performance while assigned to the Performance Standards Benchmarking (PSB) Fire Team. . . . Mr. Mabey's superb contributions played an instrumental part in the team's successful overall development of the benchmarking methodology. . . . His unparalleled commitment to excellence ensured the overall success of the PSB Fire Team and reflects great credit upon himself, the Network Enterprise Technology Command, and the U.S. Army."
- Individual Time-Off Award, from NETCOM supervisor *Sep 2018*
  - For exceeding performance expectations.
- Individual Cash Award, from NETCOM supervisor *Sep 2018*
  - For exceeding performance expectations.
- DoD Information Assurance Scholarship Program (IASP) Recipient (5 years) *2012 – 2017*
- Inducted into Eta Kappa Nu (HKN) Engineering Honors Society *Nov 2010*
- Eagle Scout, Boy Scouts of America *2002*

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

RESEARCH EXPERIENCE

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

- Projects:
  - Designed a framework for conducting forensics on web environments that addresses the unique challenges forensic examiners face in this domain.
    Publications: [C1]
  - Implemented a forensic tool in **Python** that uses the G Suite APIs as a proxy for analyzing encrypted **Chromebooks** to reconstruct the timeline of events of an incident.
  - 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.
    Publications: [J1, P2, BL2, BL3]
  - Helped design and implement a cloud-based version of the International Capture the Flag (iCTF) competition, allowing educators to more easily host their own CTF competitions. Used **Ansible**, **Vagrant**, **Amazon EC2**, and **Python** for the implementation and deployment.
    Publications: [C2]
  - 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**.
    Publications: [C3]
  - Designed and implemented the core components of a modular, highly scalable, collaboration-centric digital forensic framework built on the **OpenStack** cloud architecture. Functions of the components included distributed job scheduling, storage management, and concise evidence representation and

transmission.
Publications: [C5, BC1, P4]

- Other experience:
  - 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.
- Sponsors:
  - Department of Defense Information Assurance Scholarship Program (IASP)
  - Department of Energy
  - National Science Foundation

RESEARCH INTERESTS

- Digital Forensics
  - Web and Email Forensics
  - Evidence Representation Formats
  - Forensics on Non-Traditional Devices
- Cyber Security
  - Threat Intelligence Sharing
  - Web Security

PUBLICATIONS

Peer–Reviewed Conference Proceedings

[C1] **Mike Mabey**, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. "Challenges, Opportunities, and a Framework for Web Environment Forensics". In: *Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, January 3-5, 2018, Revised Selected Papers*. Springer International Publishing, 2018, pp. 11–33. ISBN: 978-3-319-99277-8. DOI: 10.1007/978-3-319-99277-8_2.

[C2] Erik Trickel, Francesco Disperati, Eric Gustafson, Faezeh Kalantari, **Mike Mabey**, Naveen Tiwari, Yeganeh Safaei, Adam Doupé, and Giovanni Vigna. "Shell We Play A Game? CTF-as-a-service for Security Education". In: *2017 USENIX Workshop on Advances in Security Education (ASE 17)*. USENIX Association, August 2017.

[C3] Justin Paglierani, **Mike Mabey**, and Gail-Joon Ahn. "Towards Comprehensive and Collaborative Forensics on Email Evidence". In: *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*. October 2013, pp. 11–20. DOI: 10.4108/icst.collaboratecom.2013.254125.

[C4] Wonkyu Han, **Mike Mabey**, and Gail-Joon Ahn. "Simulation-based validation for smart grid environments". In: *2013 IEEE 14th International Conference on Information Reuse & Integration (IRI)*. IEEE, August 2013, pp. 14–21. ISBN: 978-1-4799-1050-2. DOI: 10.1109/IRI.2013.6642448.

[C5] **Mike Mabey** and Gail-Joon Ahn. "Towards Collaborative Forensics: Preliminary Framework". In: *Information Reuse and Integration (IRI), 2011 IEEE International Conference on*. August 2011, pp. 94–99. DOI: 10.1109/IRI.2011.6009527.

Peer–Reviewed Journal Papers

[J1] **Mike Mabey**, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. "dbling: Identifying extensions installed on encrypted web thin clients". In: *Digital Investigation* 18 (August 2016). The Proceedings of the Sixteenth Annual DFRWS Conference, S55–S65. ISSN: 17422876. DOI: 10.1016/j.diin.2016.04.007.

[J2] Wonkyu Han, **Mike Mabey**, Gail-Joon Ahn, and Tae Sung Kim. "Simulation-Based Validation for Smart Grid Environments: Framework and Experimental Results". In: *Integration of Reusable Systems*. Ed. by Thouraya Bouabana-Tebibel and Stuart H Rubin. Vol. 263. Advances in Intelligent Systems and Computing. (Extended version of [C4]). Springer International Publishing, February 2014, pp. 27–44. ISBN: 978-3-319-04716-4. DOI: 10.1007/978-3-319-04717-1_2.

Peer-Reviewed Book Chapters

[BC1] **Mike Mabey** and Gail-Joon Ahn. "Towards Collaborative Forensics". In: *Information Reuse and Integration in Academia and Industry*. Ed. by Tansel Özyer, Keivan Kianmehr, Mehmet Tan, and Jia Zeng. (Extended version of [C5]). Springer Vienna, 2013, pp. 237–260. ISBN: 978-3-7091-1537-4. DOI: 10.1007/978-3-7091-1538-1_12.

Invited Talks

[T1] **Mike Mabey**. "dbling: Identifying Extensions Installed on Encrypted Web Thin Clients". Presentation given at the Sixteenth Annual DFRWS Conference on paper [J1]. August 2016.

Poster Presentations

[P1] Erik Trickel, Faezeh Kalantari, Yeganeh Safaei, Lakshmi Srinivas, Naveen Tiwari, **Mike Mabey**, Sukwha Kyung, and Wonkyu Han. *Capture the Flag in the Cloud*. *Symposium on Information Assurance Research and Education, ASU*. October 2016.

[P2] **Mike Mabey**, Jeremy Whitaker, Gail-Joon Ahn, and Adam Doupé. *Towards Forensics for Web Thin Clients*. *Symposium on Information Assurance Research and Education, ASU*. November 2015.

[P3] Jeremy Whitaker, **Mike Mabey**, Gail-Joon Ahn, and Adam Doupé. *Forensic Analysis on Mobile Devices*. *Symposium on Information Assurance Research and Education, ASU*. October 2014.

[P4] **Mike Mabey**, Justin Paglierani, and Gail-Joon Ahn. *Towards Collaborative Forensics*. *Workshop on Information Assurance Research and Education, ASU*. April 2012.

[P5] James Bridges, Kasimir Gabert, and **Michael Mabey**. *Cyber Tracer*. *University Day, Sandia National Laboratories*. July 2011.

TEACHING EXPERIENCE

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.

Invited Lectures

- *Lecture Title:* "Digital Forensics and the Internet of Things" *Feb 2017*
  Class: CSE 469 Computer and Network Forensics, Arizona State University *Invited by:* Dr. Ziming Zhao
- *Lecture Title:* "IoT Security" *Nov 2016*
  Class: CSE 465 Information Assurance, Arizona State University *Invited by:* Dr. Stephen S. Yau
- *Lecture Title:* "Introduction to Cryptography" *Sep 2016*
  Class: CSE 465 Information Assurance, Arizona State University *Invited by:* Dr. Stephen S. Yau

Teaching Assistant *Aug 2010 – Dec 2015*
Arizona State University Tempe, AZ

- CSE 465 Information Assurance with Dr. Gail-Joon Ahn: Fall 2010, Fall 2015.
- CSE 469 Computer and Network Forensics with Dr. Gail-Joon Ahn: Spring 2015.
- FSE 100 Introduction to Engineering with Dr. Ryan Meuth: Spring 2014.
- CSE 423/424 Capstone I and CSE 485/486 Capstone II with Dr. Debra Calliss: Spring 2014.
- CSE 467 Data & Information Security with Dr. Gail-Joon Ahn: Spring 2011.

SAT/ACT Instructor *Sep 2015 – Oct 2015*
Minerva Learning, LLC Chandler, AZ

· Individual tutor for a high school student preparing for the PSAT.

Teaching Assistant (Instructor of Record) *Aug 2011 – Dec 2014*
Arizona State University Tempe, AZ

· CSE 465 Information Assurance: Fall 2014.
· FSE 100 Introduction to Engineering: Fall 2011 – Fall 2013 (5 semesters).

TEACHING INTERESTS

· Computer and Network Forensics
· Advanced Topics in Digital Forensics
· Information Assurance
· Security Toolkit Programming with Python
· Cryptography
· Software Security

ACADEMIC ACTIVITIES

Fulton Undergraduate Research Initiative (FURI) Mentor
· Adric Rukkila B.S. in Computer Science at ASU *Sep 2016 – May 2017*
Topic: Leveraging Cloud Service APIs for Forensic Data Collection

Undergraduate Honors Thesis Mentor
· Samantha Juntiff B.S. in Computer Science at ASU *Spring 2015*
Thesis: Squeegee: Integrating Forensic Tools for Collaborative Forensic Analysis

SERVICE

Department
· Admin Team: UCSB International Capture the Flag (iCTF) *2017*
Publications: [C2]
· Team Leader: ASU team in the UCSB iCTF *2009, 2010, 2014, 2015*
· Panelist: PhD Open House Student Panel *Feb 2014, Feb 2015*

Profession
· Conference Proceedings Subreviewer:
  ◦ ACM CODASPY *2013, 2014, 2015, 2016, 2017*
  ◦ SACMAT *2014*
  ◦ ASIACCS *2014*
· Student Volunteer:
  ◦ ACM CODASPY *2017*
  ◦ ACM CCS *2014*
· Student Program Committee Member:
  ◦ IEEE Security & Privacy *2016*

Technical Blog Posts

[BL1] **Mike Mabey**. *How eCryptfs Affects Filename Lengths*. https://mikemabey.com/blog/2017/08/ecryptfs_filenames.html. August 2017.

[BL2] **Mike Mabey**. *How to check out an old version of Chromium OS*. https://mikemabey.com/blog/2016/02/check_out_old_chromium.html. February 2016.

[BL3] **Mike Mabey**. *Fixing repo init to check out Chromium OS code*. https://mikemabey.com/blog/2015/01/fixing_repo_init_chromium_os.html. January 2015.

[BL4] **Mike Mabey**. *Getting into Developer Mode on the HP Pavilion 14 Chromebook*. https://mikemabey.com/blog/2013/05/getting_into_developer_mode.html. May 2013.

[BL5] **Mike Mabey**. *Debian on Android and my quest for a full-fledged terminal Python IDE*. https://mikemabey.com/blog/2012/06/debian_on_android.html. June 2012.

[BL6] **Mike Mabey**. *OpenVPN Update: Fixed!* https://mikemabey.com/blog/2012/06/openvpn-update-fixed.html. June 2012.

PROFESSIONAL MEMBERSHIPS

- IEEE
  - Cybersecurity Community
  - Internet of Things Community
- IEEE Computer Society
- Python Software Foundation (Basic Member)

PROFESSIONAL DEVELOPMENT

- Applied Data Science with Python from University of Michigan on Coursera
  - Applied Plotting, Charting & Data Representation in Python *(Ongoing)*
  - Introduction to Data Science in Python *Apr 2019*
- Data Science Specialization from Johns Hopkins University on Coursera
  - Getting and Cleaning Data *Nov 2018*
  - R Programming *Oct 2018*
  - The Data Scientist's Toolbox *Aug 2018*
- Preparing Future Faculty (GRD 791 at ASU) *Aug 2015 – May 2016*

  The Preparing Future Faculty (PFF) program is a year-long series of seminars, discussions, and activities designed to expose graduate students and postdocs more fully to the realities of teaching, research, and service in higher education.

REFERENCES

Please feel free to contact any of my references.

Jerrie Core
Division Chief, NETCOM Data Science Directorate — Phoenix Branch
6201 E Oak Street
Phoenix, AZ 85008
Phone: (719) 317-3108
jerrie.l.core.civ@mail.mil

Gail-Joon Ahn
Director, Center for Cybersecurity and Digital Forensics
Professor of Computer Science and Engineering
Fulton Entrepreneurial Professor
School of Computing, Informatics and Decision Systems Engineering
Ira A. Fulton Schools of Engineering, Arizona State University
Brickyard Engineering (BYENG) Bldg, Room 486
699 S. Mill Avenue
Tempe, AZ 85281
Phone: (480) 965-9007
Fax: (480) 965-2751
http://www.public.asu.edu/~gahn1/
gahn@asu.edu

Adam Doupé
Associate Director, Center for Cybersecurity and Digital Forensics
Assistant Professor of Computer Science and Engineering
School of Computing, Informatics and Decision Systems Engineering
Ira A. Fulton Schools of Engineering, Arizona State University
Brickyard Engineering (BYENG) Bldg, Room 472
699 S. Mill Avenue
Tempe, AZ 85281
Fax: (480) 965-2751
http://adamdoupe.com
doupe@asu.edu

Frank J. Grimmelmann
President & CEO/Intelligence Liaison Officer
Arizona Cyber Threat Response Alliance (ACTRA)
Phone: (623) 551-1526
Fax: (623) 551-4221
fgrimmelmann@actraaz.org