FREDERICK HAGGERTY

DIGITAL FORENSICS AND CYBERSECURITY EXPERT

44330 Mercure Circle, Suite 274, Sterling, VA 20166
Email: fhaggerty@datigent.com
Cell Phone: 571.663.4545

PROFILE

Frederick Haggerty is an experienced Information Technology (IT) expert witness with 28 years in the Cybersecurity field, specializing in digital forensics, malware analysis, email investigations, and network intrusion responses. With a strong background in software development, Mr. Haggerty has deep technical expertise in examining computer systems, servers, and digital media. His graduate studies at Albany Law School have enhanced his understanding of laws affecting privacy and cybersecurity. Mr. Haggerty has collaborated with legal counsel on cases involving business email compromises, extortion, trade secret theft, and other complex cybersecurity matters.

EDUCATION

M.S. Legal Studies (MSLS), Cybersecurity and Data Privacy, Albany Law School, 2020

B.S. Computer Information Systems (Computer Forensics Management), Strayer University, 2016

Certificate, Computer Information Systems, Strayer University, 1996

CERTIFICATIONS

IACRB's Certified Expert Reverse Engineering Analyst (CEREA) | August 2017

GIAC Reverse Engineering Malware (GREM) | May 2017
Certified Data Recovery Expert (CDRE) | October 2016

Certified Data Recovery Professional (CDRP) | May 2016

GIAC Certified Forensic Analyst (GCFA) | March 2016

Certified Information Systems Security Professional (CISSP®) | Member ID: 497591 | September 2014

Qualified/Forensic Expert (Q/FE) | November 2013

Facility Security Officer (FSO) | November 2001

PROFESSIONAL EXPERIENCE

Digital Forensics and Incident Response Consultant
Datigent, LLC

January 2014 – Present

Conduct sound computer forensic analysis and maintain strict media chain of custody using protocols and procedures in line with established state and federal guidelines and company policies. Acquire and preserve computer media in either a lab setting or through onsite data capture or seizure. Create bit-by-bit forensic copies of original media for legal and investigative purposes. Perform data recovery, including both file and email recovery, on electronic media to be analyzed during the course of a computer forensic investigation.

Conduct investigations involving analysis of electronic media. Example analyses include but are not limited to:

- Examination of a computer memory image that was infected with malicious software. Findings were provided in a detailed report to client.
- Examination of a camera MicroSD card. Recovered images that were deleted from the MicroSD card related to the client request.
- Imaged and analyzed a compromised web server with a RAID 5 configuration to detect hacking methods and to properly extract evidence. Findings were provided in a detailed report to client.

- Performing forensic analysis in support of intrusion and allegations of misuse cases.
- Documenting and presenting investigative findings via detailed analysis reports.
- Regularly use tools such as X-Ways Forensics, Magnet Axiom, Cellebrite (UFED & Physical Analyzer), Intella, Autopsy, Cyber Triage, and other forensic tools. I also use cloud-based tools such as Azure, Sentinel, and Splunk for log acquisition and analysis.
- Supported and conducted forensic analysis on several Business Email Compromise (BECs) investigations.
- Performed several HR\Legal investigations using a variety of forensic and eDiscovery tools.
- Develop tools to support incident response and forensic work.

IR Forensic Engineer
Levi, Ray & Shoup, Inc. (LRS)

January 2020 – February 2020

A member of the LRS cybersecurity incident response (IR) team providing incident response and digital forensic support to LRS and its clients. Primary responsibilities include:

- Preserving and forensically imaging data from computer and mobile device systems using accepted forensic protocols.
- Creating and maintaining chain of custody.
- Collecting and analyzing host- and network-based data in support of incident response investigations.
- Interpreting, analyzing, and reporting on events and anomalous activity discovered through incident response investigations.
- Performing ransomware remediation and data recovery.
- Correlating and analyzing data between disparate sources to assess threat actor techniques, tactics, and procedures.
- Identifying and enhancing processes where automation has the potential to improve efficiency.
- Developing custom scripts (Batch, Python, Encase EnScripts) as needed to support IR engagements.
- Leveraging tools such as FTK Imager, Paladin, X-Ways, Encase, MacQuisition, Magnet Axiom, Volatility, and SIFT Workstation to perform incident response and digital forensic duties.

Senior Forensic Analyst
Blue Ally, LLC

August 2017 – December 2019

Provide digital forensic support to the National Rural Electric Cooperative Association (NRECA). Primary responsibilities include:

- Spearheading the establishment of a forensic capability that allows the organization to properly collect, preserve, protect and analyze digital evidence so the evidence can be effectively used in legal and disciplinary matters and in a court of law.
- Collecting and developing intelligence to detect and investigate high-confidence threats to the brand, service infrastructure, and enterprise users and systems.
- Incorporating a risk management approach to guide the organization in proactively gathering digital evidence to support investigations.
- Performing digital forensic investigations when directed by Human Resources.
- Documenting and presenting investigative findings via detailed analysis reports.
- Providing proactive (threat hunting) and reactive computer security defense to the NRECA critical infrastructure.
- Performing computer security incident response duties including the monitoring of multiple operating systems (Windows, Linux, and Mac OS X).
- Supporting the Security Intelligence & Operations Center (SIOC) by performing live forensic analysis on NRECA systems.
- Managing the day-to-day operations of Carbon Black (Cb) Response to continuously monitor all activity on NRECA endpoints and servers.

Adjunct Professor
University of Baltimore, Forensic Science – High Technology Crime

February 2017– May 2019

Effectively communicate course material to facilitate a successful understanding of the principles, mechanisms and implementation of data security. Guide students through an examination of data/information loss by theft, intrusion, and natural disaster, while assessing vulnerabilities and their remediation. Thoroughly evaluate government and commercial incident response plans and strategies.

Cyber Forensic Specialist (Forensics and Malware Analyst)
Northrop Grumman

September 2015 – January 2019

A member of the Malware and Forensic Analysis Team (MFAT) within the Cyber Division of the Marine Corps Cyber Operations Group (MCCOG), providing cyber security solutions to the Marine Corps. Perform digital forensic analysis in support of incident response; both dead and live forensics of compromised or suspect hosts; and static and dynamic analysis of suspected malware and other files that are identified with the MCEN. Document and present investigative findings via detailed analysis reports.

Senior Java/Application Integrator
NES Associates, LLC

June 2014 – August 2015

Provide support to Defense Information Systems Agency (DISA) Support Services as a member of the software development team. Responsible for the design and development of a content driven web portal that will be used for the sharing of network management information for DISA Support Services. Perform enterprise strategic systems planning, and enterprise information planning, as well as performing process and data modeling in support of the planning and analysis efforts. Responsible for creating user interfaces, business logic and communications services for the OSS-Central and related systems.

Senior Applications Developer
Alta IT Services

November 2012 – July 2014

Provided support as a technical expert in the continued development of the Consolidated Law Enforcement Operations Center (CLEOC) — a Web-based system for managing investigations and storing information on law enforcement, command, judicial, and corrections response to criminal activity within the Department of the Navy for NCIS. Assisted in the development, delivery, and maintenance of CLEOC, as well as the identification, definition and vetting of application requirements. Developed new modules as assigned and make recommendations for improving the functionality and performance of the system.

Senior Java Developer
Apex Systems

March 2012 – October 2012

Provided support to the Product Director-Transportation Information Systems (PD-TIS) as a member of the development team that was converting a large legacy Power Builder transportation application to a modern Web-based system for the Army using JSF/Primefaces (a rich set of JSF components) and JPA. Deployed on a JBoss AS 7 platform, the new Web-based application uses JSF Facelets to layout the application and is backed by JSF Managed Beans, EJB 3.x (Session and Entity), and Java DAOs. The application also uses jQuery to update the user interface and dynamic PDF reports are created using Jasper Reports and iReport Designer. Assisted in the implementation of a Java role-based security model (RBAC), using Java Authentication and Authorization Service (JAAS), to improve code reliability, make enhancement and maintenance easy, and increase system security. This implementation used Tomcat 6.0 and MySQL 5.0 as a datastore.

Senior Systems Analyst
Atechra, Inc. (Lewis Technologies)

December 2010 – March 2012

Provided support for multiple projects for the Bureau of Land Management (BLM). Responsible for gathering requirements and analyzing representative data to help develop business cases and system requirements. Worked with the Information Resources Management Directorate to develop a Department System Lifecycle Management (SLM) process for the systems development lifecycle (SDLC). Worked with BLM IT Security, to ensure overarching Federal, DOI, and BLM policies and requirements are fully integrated throughout the SLM Process. Offered advice and provided guidance to the team and management, helping to prioritize work on activities and projects. Also provided analytical and problem-solving skills to help maximize the services provided by the BLM Information Resources Management (IRM) Directorate.

Previous positions include Web Services Engineer for Tower Technologies, Inc., Senior Java Developer for Mindbank Consulting, J2EE Developer for K&M Softech, Inc., J2EE Consultant for DFI International, Government Services Division, Lead Engineer for Calnet, Inc., Lead Engineer for BAE Systems Enterprise Systems, Inc., Facility Security Officer (FSO) for

Visionarie Corporation, Counterintelligence Information Program Manager for Kajax Engineering, Inc., Senior Software Engineer for Wang Global (Getronics), Sr. Systems Engineer for J.G. Van Dyke & Associates, Inc., Software Developer for Presearch, Inc., and Sergeant for the United States Marine Corps.

TRAINING

- Workshop: Investigating Ransomware, Sleuth Kit Labs | April 2024
- Workshop: Investigating Insider Threats, Sleuth Kit Labs | April 2024
- Into to DFIR: The Divide and Conquer Process, Sleuth Kit Labs | April 2024
- Cyber Triage Basics, Sleuth Kit Labs | April 2024
- Intella Foundation Course, Vound Software | April 2024
- AI Prompt Engineering, AI Advantage | January 2024
- X-Ways Forensics I, X-Ways | August 2023
- X-Ways Forensics: X-Ways Forensics (Computer Forensics Course) | December 2021
- Spider Forensics: Advanced (sUAS) Drone Forensic Analysis Course | May 2019
- Rupprecht Drones.com: Airspace & Chart Reading Course | May 2019
- Rupprecht Drones.com: Part 107 Drone Regulations Course | May 2019
- LinkedIn: Cert Prep: FAA Part 107 Commercial Drone License | May 2019
- Magnet Forensics: AX200 – Axiom Examinations | November 2018
- International Association of Privacy Professionals (IAPP): U.S. Private-Sector Privacy Online Training | September 2018
- PI Education, Georgia Private Detective Pre-License Training Class | June 2018
- Carbon Black: Cb Response Advanced Analyst Training | May 2018
- Surviving Digital Forensics (Sumuri): Windows Shimcache Forensics, sumuri.com | September 2017
- Applied Network Defense: Effective Information Security Writing | August 2017
- Advance Reverse Engineering On-line Training, InfoSec Institute | May 2017
- Reverse-Engineering Malware: Malware Analysis Tools and Techniques (FOR610), SANS | March 2017
- 5-Day Hard Drive Data Recovery Course, My Hard Drive Died | October 2016
- RSA Malware Analysis Course, RSA University | August 2016
- Intro to Malware Analysis and Reverse Engineering, Cybrary.it | August 2016
- Data Recovery Boot Camp, InfoSec Institute | May 2016
- Advanced Computer Forensic Analysis and Incident Response (FOR508), SANS | December 2015
- Malware Analysis Course, MCNOSC | December 2015
- Incident Response Training, MCNOSC | October 2015
- DCOS Intrusion Detection Analyst Training, MCNOSC | October 2015
- HBSS 201 Admin ePOS5.1 (v2014), DISA | September 2015
- Surviving Encryption (Sumuri): Memory Analysis 1, udemy.com | September 2015
- Surviving Encryption (Sumuri): Cryptanalysis, udemy.com | July 2015
- Surviving Encryption (Sumuri): Essentials, udemy.com | July 2015
- Surviving Digital Forensics (Sumuri): Link Files, udemy.com | June 2015
- Surviving Digital Forensics (Sumuri): Resolving Attached USBs, udemy.com | June 2015
- Surviving Digital Forensics (Sumuri): RAM Extraction Fundamentals, udemy.com | June 2015
- Surviving Digital Forensics (Sumuri): Windows Shellbags, udemy.com | June 2015
- X-Ways Forensics Practitioner's Guide Online Course I, dfironlinetraining.com | May 2015
- IFCI Expert Cybercrime Investigator's Course, udemy.com | March 2015
- IFCI's Studies in Cybercrime: The Great Sony Hack of 2014, udemy.com | February 2015
- Wireshark Crash Course, udemy.com | February 2015
- Surviving Digital Forensics (Sumuri): Understanding OS X Time Stamps, udemy.com | January 2015
- Surviving Digital Forensics (Sumuri): Paladin Virtual Machine, udemy.com | January 2015
- Surviving Digital Forensics (Sumuri): Providing File Knowledge (Windows Explorer), udemy.com | January 2015
- Surviving Digital Forensics (Sumuri): Providing File Knowledge (Windows Prefetch), udemy.com | January 2015
- Surviving Digital Forensics (Sumuri): Volume Shadow Copy, udemy.com | January 2015
- Maintaining Cyber Security, DeVry University | January 2015
- Introduction to Forensic Science, udemy.com | January 2015
- Health Insurance Portability and Accountability Act (HIPAA) Compliance, udemy.com | December 2014
- Techno Security & Forensics Investigations Training Conference, Myrtle Beach, SC | June 2014

- Expert Witness Training Course, SEAK, Inc., Orlando, FL | May 2014
- Certified Information Systems Security Professional 2012, uCertify | March 2014
- Computer Hacking Forensic Investigator, uCertify | January 2014
- Qualified/Forensic Expert, Security University, Herndon, VA | November 2013
- Certified Ethical Hacking and Countermeasures v8, EC-Council | August 2013
- Adobe Flash Builder 4.6 (Flex), Adobe online training (one week) | January 2012
- Horizontal Fusion (KMINCE) Architecture Overview | January 2005
- Hyperwave Advance Document Classes | October 2003
- Hyperwave Document Classes, Hyperwave IS/6 Administration, Hyperwave IS/6 Fundamentals | 2002
- Hyperwave IS/6 Template Programming, Hyperwave Development Basics | 2002
- Understanding Verity K2 Infrastructure v4.5x, Developing Verity K2 Applications v4.5x | August 2002
- Deploying Verity K2 Infrastructure - Part 1 v4.5x | August 2002
- Essentials of Industrial Security Management (EISM), Defense Security Service | November 2001
- Introduction to ArcView GIS, Environmental Systems Research Institute (ESRI), Inc. | 1998
- Programming ArcView GIS w/Avenue, ESRI, Vienna, VA | 1998
- Oracle Developer 2000\Forms I v4.5, Oracle Corporation, Vienna, VA | 1998

TECHNICAL EXPERIENCE

Forensic Tools

EnCase 7.10.x, X-Ways Forensics v18.2, WinHex v18.2, Autopsy v3.x, SleuthKit v4.1.x, AccessData FTK Imager v3.1.x, Registry Ripper v2.x, SANS Investigative Forensic Toolkit (SIFT) v2.14, Volatility Framework v2.2, Foremost v1.5.x, Paladin v5.02, Helix3 Pro, BackTrack v5R3, Kali v1, MAGNET AXIOM (Examine & Process), F-Response Consultant + Covert Edition, Carbon Black (Cb) Response, SIFT Workstation, Symantec Bluecoat (Security Analytics), Anomali ThreatStream, LANDESK Management Console, and other digital forensics and malware analysis tools

Operating Systems

UNIX, SUN SOLARIS, SUN OS, IRIX, Linux (CentOs, Fedora, Red Hat), Windows (NT, 2000, XP)

Programming Languages

Java, C, C++, X Windows, MOTIF, SQL, PL/SQL, AVENUE (ArcView), JavaScript, PHP 3.0/4.0/5, Cold Fusion, HTML, Unix C, Bourne Shells

Developer Tools

Struts, Exadel Struts Studio, XDoclet, Ant, Axis 1.1, Eclipse 3.x, Cocoon 2.1.x, Jakarta Slide, Jakarta Slide Webdavclient, Verisign Payflow Pro API, Jboss Developer Studio, Jasper Reports, iReport Designer, PrimeFaces 3.x, JSF 2.x, JPA, Flex 4, ActionScript 3.0

Applications

NES 3.51, Jrun 2.3, Arcview GIS, Arcview IMS, Oracle 7.3 – 9I, Oracle Forms v4.5, Oracle Web Application Server 3.0, HomeSite 4.5.1, Cold Fusion Server 4.5, Cold Fusion Studio 4.5, MySQL, Apache, make, JDeveloper, Hyperwave, Verity K2 Infrastructure v4.5.x/5.0, Verity Intelligent Classifier (VIC) v4.5.x/5.0, JBOSS 3.x/4.0/5.x, Tomcat, Xselerator (XSLT IDE), EJB3, Drools, Smooks, Libvirt Virtualization API, Xen linux hypervisor, KVM linux hypervisor, Jboss ESB, Altova XMLSpy, Adobe Flash Builder 4.6, SoapUI

ASSOCIATION MEMBERSHIPS

- Security University's Federation of Q/FE (Qualified/Forensic Experts & Examiners)
- (ISC)^2 – International Information Systems Security Certification Consortium
- InfraGard, Washington, D.C. – National Capital Region Members Alliance

PREVIOUS INDUSTRY PARTICIPATION

Malware Analysis Course Instructor, Marine Corps Cyber Operations Group (MCCOG), Quantico, VA

Primary instructor for the MCCOG's five-day Malware Analysis course, providing students with an introduction to the tools and methodologies used to perform malware analysis on all major file types, using a practical, hands-on approach. Students are taught how to extract host and network-based indicators of compromise (IOCs) from a malicious program using both static and dynamic analysis techniques. Important computing principles and techniques are also taught to help students determine how to best analyze a file, de-obfuscate code, and determine the functionality of a program.

Presentation, Community Business Partnership, Springfield, VA
Protecting Your Business: An IT Perspective
As a business owner, it's your responsibility to protect your business, limit risk, and keep the business running as smoothly as possible. But how do you limit the possibility of security incidents and lawsuits to ensure business continuity? In this session, you will learn some of the core security principles and practices that you can implement today to protect your business for tomorrow.

Forensics Advisor/Instructor, Security University, Herndon, VA
Support Security University's Qualified/Forensic Expert training courses by providing recommendations for course material and developing hands-on training labs.

Envision National Youth Leadership Forum (NYLF): National Security, Falls Church, VA
A regular participant on the NYLF cyber security panel. Discuss cyber security issues, opportunities, latest intelligence strategies, and opportunities in public service.

PUBLICATIONS

PenTest Magazine (pentestmag.com), February 2017 Edition, Article (p. 34), Don't Waste Your Time and Money If You're Not Going to Test It!
https://pentestmag.com/product/pentest-brothers-in-arms/

ShariGloverSpeaks.com, Protect Your Business With An Incident Response Plan
https://shariglovers peaks.com/protect-your-business-with-an-incident-response-plan/

EXPERT TESTIMONY

Depositions

- RoyaltyStat LLC v. IntangibleSpring, January 16, 2019

Testimonies

- RoyaltyStat LLC v. IntangibleSpring, July 1, 2021
- Commonwealth v. French - Matter No. 1568, March 14, 2019