Daniel Haggerty

(PhD, MCFE, OSCP)

Houston, TX, USA. 832-279-5505

I have an investigative and questioning mindset. I am hard-working, have a tenacious character and am a continuous learner. I changed careers from cutting-edge neuroscientific research to cyber investigations to find new and different challenges.

Experience

[2018 - Present] – Senior Consultant Cyber Investigations

PNG Cyber, LLC (ProNet Group, Inc). Sugar Land, TX

- Conduct data forensic investigations for enterprise computer security incidents: ransomware, attacks/intrusions, business-email compromises, cloud-based forensics and intellectual property theft.
- Preservation and collection of digital evidence, knowledge of policies and procedures regarding chain of custody.Development of custom scripts to parse, classify and display digital evidence.
- Develop fact-based technical reports detailing events over specified periods of time.
- Flexibility to adjust to multiple demands, shifting priorities, ambiguity, and rapid change.
- Maintain clear and efficient communications with management and clients.
- Provide interactive discussion and guidance to peers.
- Discuss technical subject matter for a variety of audiences.

[2009 - 2017] – Post-Doctoral Research Associate

Baylor College of Medicine Houston, TX.

- Extensive investigation of the neuronal networks underlying the relationship between memory and consciousness.
- Acquisition, analysis, and interpretation of complex neurophysiological data using MATLAB and Python.
- Mathematical understanding of probability, statistics, data-scientific methods, correlation, regression, Bayesian Inference, image classification and their analysis using computer programs.
- Presented work at international conferences and a history of publications in top-tier scientific journals.

Skills

DIGITAL FORENSICS INCIDENT RESPONSE

- Knowledge of the full cyber investigation process from evidence acquisition to report writing.
- A deep understanding of Windows, Mac, and Linux operating systems and their respective forensic artifacts.
- Experience in on-site and remote acquisition of forensic artifacts and images: *Cybereason, Velociraptor, CyLR, FTKImager, Magnet Acquire, KAPE*.
- Deep knowledge of a multitude of tools used to carry out forensic analysis: *Magnet Axiom* (Certified), *EnCase, Splun*k and *Elasticsearch*.
- Developing *ad hoc Python* scripts/programs to perform a variety of forensic and artifact parsing functions.
- *Office 365* Business Email Compromise investigations with customized *PowerShell, Python* scripts, IP geolocation (*MaxMind* API), *Microsoft* Admin console, Message Trace, Search Content and persistent inbox rules.
- Data Mining PII and PHI within various file formats (pst, E01, archives) with *Canopy*.
- Mobile phone forensic analysis and Cell Phone Data Record analysis (incoming/outgoing connections to cell phone towers) with *Oxygen Forensics*.
- Endpoint Detection and Response (*Cybereason*, *SentinelOne)*
- Block-chain analytics with *Elliptic*.
- Providing continuous and professional conversations and reports to keep clients, legal counsel, and insurance carriers updated regarding the status of the investigation process.
- Experience performing due diligence reviews of cyber insurance claims: Liaise with Insured, Carriers, and Vendors regarding invoices submitted to insurance carriers.

- Certified penetration tester (OSCP). *Kali Linux, Metasploit, BurpSuite, nmap*, password attacks, directory traversal, cross-site scripting, SQL injection, *PowerShell Empire*, privilege escalation techniques.
- A vast experience in understanding and communicating complex technical material in verbal and written reports spanning two disciplines (cyber investigations and neuroscience).

SOFTWARE ENGINEERING/DEVOPS

I am an experienced software engineer primarily with the *Python, PowerShell, Bash, JavaScript, node.js, C#*, git versioning, *Docker* and cloud platform hosting solutions, *AWS, Microsoft Azure, Google Cloud Platform*. I have developed a large number of scripts and programs built to solve interesting problems particularly related to ingesting, parsing, filtering and presenting data.

Forensics applications/scripting:

- Developed custom *Python* scripts for uploading *Microsoft O365* audit logs to ElasticSearch and enhancing the IP address data during upload with *Maxmind API* ip-geolocation and further IP information. Developed further *Python* scripts that can be used for subsequent downloading of significant results from *ElasticSearch* in *Microsoft Excel* formatted files (*Python* Libraries: *Elasticsearch, Openpyxl*).
- Developed a *Python* program that ingests cell phone data records from *csv* files (*Verizon, ATT*, etc) and produces, for each phone call made/received, a map of the cell phone tower location and the sector/face of the cell-phone tower that communicated the call with the Azimuth (direction) of the cell tower sector (*Google Maps* API).
- Developed a *Python* script to take in any *.csv* file with an IP Address column and query the *Maxmind API* and return the input csv data enriched with columns of the equivalent IP lookup from *MaxMind API* data. The geolocations and accuracy radii of these data are also saved to a mapping html file for viewing IP geolocations in a browser.
- Developed a *Python* script to search and return all files of a certain extension (e.g., *.evtx, .csv* etc…) from nested subdirectories (for example from a *CyLR* triage collection) and copy them all to another directory, labeled with their origin/parent folder name. These collections can then all be pushed into other forensics tools such as *Event Log Explorer.*

Non-forensics applications:

- Development of a web application that returns a formatted *Microsoft Word* document with boilerplate text and a host of case-specific information (Insured/Client/Company addresses, names, people, dates). The data is pulled from two data sources (MSSQL database, PostgreSQL database) embedded as a starter template for report writing into *Microsoft Word* (*Python* Libraries: *Flask*), *Docker*, deployed as a *Web App* via *Azure Container Registry*.
- Development of a web application to query data from an *MSSQL* database and a directory of nested directories full of *Microsoft Excel* files and extract specific company data regarding engineers hours, travel time, expenses and display and export the data to formatted *Microsoft Excel* reports (*Python* Libraries: *Dash,* a heavy use of *Pandas, Openpyxl*, *Google Maps* API).
- *Windows Forms C#/.NET* desktop application for assembling, viewing, annotating photographs and exporting to a *Microsoft Word* document.

Professional Education

Magnet Certified Forensic Examiner (MCFE) [SEPTEMBER 2020]

Completed following Magnet Courses [All 32 hours]:

- AX100 Forensic Fundamentals
- AX200 Axiom Examinations
- AX250 Axiom Advanced Computer Forensics
- AX300 Axiom Advanced Mobile Forensics
- AX310 Axiom Incident Response
- AX320 Axiom Internet & Cloud Investigations
- AX350 macOS Examinations

Offensive Security Certified Professional (OSCP) [JULY 2019]

- The OSCP teaches ethical hacking methodologies: use of the tools included with the *Kali Linux* distribution to successfully attack and penetrate various live machines in a safe lab environment

Web-Development

Digital-Crafts, Houston, TX. [16 WEEKS IMMERSIVE]

- Full-stack web-development program based upon *Python, JavaScript, node.js, HTML, CSS.*

Academic Education

[2005 - 2009] – Doctoral Research

PhD Neuroscience Newcastle University, United Kingdom

[2002 - 2005]

BSc Neuroscience Leeds University, United Kingdom

[1997 - 2000]

BSc Sport Science Leeds Beckett University, United Kingdom

Publications

Domenico C, **Haggerty DC**, Mou X, Ji D. (2021) LSD degrades hippocampal spatial representations and suppresses hippocampal-visual cortical interactions. Sep 14; 36(11) 109714. DOI: 10.1016/j.celrep.2021.109714

Wu CT, **Haggerty DC**, Kemere C, Ji D. (2017) Hippocampal awake replay in fear memory retrieval. *Nature Neuroscience* Apr 20(4):571-580. DOI: 10.1038/nn.4507

Haggerty DC, Ji D. (2015) Activities of visual cortical and hippocampal neurons co-fluctuate in freely moving rats during spatial navigation. *eLife* Sep 8; 4: 2015; DOI: 10.7554/eLife.08902

Haggerty DC, Ji D. Coordinated sequence replays between the visual cortex and hippocampus. In: Analysis and Modeling of Coordinated Multi-neuronal Activity. (Editor: Masami Tatsuno). Springer, 2015.

Haggerty DC, Ji D. (2014) Initiation of sleep-dependent cortical-hippocampal correlations at wakefulness-sleep transition. *Journal of Neurophysiology*, Oct 1; 112(7):1763-74. DOI: 10.1152/jn.00783.2013

Haggerty DC, Glykos V, Adams NE, LeBeau FE. (2013) Bidirectional modulation of hippocampal gamma (20-80Hz) frequency activity in vitro via alpha(α)- and beta(β)-adrenergic receptors (AR). *Neuroscience*. Dec 3; 253:142-54. DOI: 10.1016/j.neuroscience.2013.08.028