Speckin Forensics, LLC
120 N. Washington Square, Suite 300
PMB 5068
Lansing, Michigan 48933
517-349-3528 • Fax 954-839-8219

Please Direct Correspondence & Payment Here:
2450 Hollywood Boulevard, Suite 700
Hollywood, Florida 33020
954-763-6134 • Fax 954-839-8219

www.4N6.com

Leonard A. Speckin
Retired Document Analyst

Dr. George F. Jackson Ph.D.
Forensic Toxicologist

Michael P. Mulderig
Forensic Firearms
Ballistics Specialist

Michael J. Sinke
Retired Latent Print Specialist
Retired Crime Scene Reconstruction
Retired Forensic Document Analyst

Erich J. Speckin
Forensic Document Analyst
Ink Dating Specialist
Crime Scene Reconstruction

Anthony A. Milone
Computer & Graphics Specialist
Forensic Document Specialist

Robert Walker
Crime Scence Analyst
Forensic Firearm Expert

Juan Ruiz
Computer, Mobile Device Specialist

Thomas K. Huard Ph.D.
DNA Analyst & Consultant

Marshaun J. Blake
Arson Investigator
Vehicle Fire Specialist

Dr. Julie A. Howenstine
Serologist
DNA Analyst & Consultant
Crime Scene Reconstruction

CYNTHIA FITCH

SUMMARY STATEMENT

Nearly 20 years of experience working in computer forensics, network security, server management, consulting work, and systems administration for law enforcement and government. Extensive experience testifying and presenting evidence to state and federal court as well as various levels of management. EnCE and CFCE certified.

SKILLS

- Computer Forensics
- Digital Forensics Incident Response
- Network intrusion and Cybersecurity
- Expert witness in state and federal court
- Network security and threat hunting
- Systems and server administration
- Internal investigations
- Policy implementation, procedure overview, change management
- Onsite and field covert forensic imaging
- CFCE, ENCE, SANS, A+, T5R clearance
- Reporting and collaboration with clients, attorneys, and stakeholders
- Education and training background
- EnCase, X-Ways, Axiom, Cellebrite, NIST, OIS

PROFESSIONAL EXPERIENCE

Speckin Forensics, LLC | *Digital Forensic Investigator* 2025 to Present

- Identify, acquire, analyze and conduct forensic imaging and data recovery of digital devices, including computers, hard drives, mobile phones, and cloud-based storage in both criminal and civil investigations.
- Prepare detailed forensic reports, declarations and present testimony in depositions and court proceedings as an expert witness.
- Examination and review of digital data provided in civil cases, corporate investigations, and matters related to criminal offenses

United States Postal Inspection Service | Detroit, MI July 2013 to October 2024
Digital Evidence Unit (Forensic Laboratory Services) | *Computer Forensic Analyst*

- Identify, acquire, and analyze digital media using forensically sound methodology in an accredited ASCLD/LAB computer forensic lab environment in support of criminal investigations.
- Recover data and perform forensic examinations on desktops, laptops, cell phones, and portable devices across multiple platforms (Windows, UNIX, Macintosh).
- Help analyze findings in investigative matters and develop fact-based, technical reports detailing events over specified periods of time.
- Processed cloud storage and takeout packages from Apple and Google.
- Explain technical data from cases for court preparation to local, state, and federal attorneys.
- Maintain chain of custody for evidence submitted to DEU.
- Participate in search site warrants, triaging devices for Inspectors and imaging devices on site when needed.
- Work with law enforcement agents in the field on proper seizure procedures and provide advice about search warrants and evidence retrieval.
- Maintain Laboratory computer equipment, performing necessary upgrades and maintenance as required.
- Investigate a wide variety of cases including child exploitation, drugs, employee misconduct, and identity theft and fraud.
- Developed clear, accessible training materials and course content by translating complex technical and forensic concepts into understandable formats for new and junior employees.
- T5R (Top security clearance) granted by USPIS.
- Received IACIS Certified Forensic Computer Examiner (CFCE) certification.

Kentucky State Police | Frankfort, KY February 2007 to June 2013
Electronic Crime Section (Division of Technical Services) | *Forensic Examiner II*

- Performed forensic investigations utilizing EnCase, FTK, Cellebrite, and XRY.
- Certified in multiple cell phone forensic programs (XRY and Cellebrite).
- Recovered data and performed forensic investigations on desktops, laptops, and portable devices across multiple platforms (Windows, UNIX, Macintosh).
- Court preparation with federal attorneys on cases, explaining technical data for court presentation.
- Maintained chain of custody for evidence submitted to Electronic Crime Branch.
- Crafted policies and procedures for the entire branch, focusing on best practices and industry standards.
- Presented “lunch and learn” seminars to various computing groups and businesses on topical subjects like cell phone app security.
- Maintained electronic databases as well as physical evidence logs.
- Provided in-field training and guidance to law enforcement personnel on proper digital evidence seizure procedures, translating legal and technical requirements into clear, actionable instructions to support effective learning and compliance.
- Maintain Laboratory computer equipment, performing necessary upgrades and maintenance as required.
- Received Encase Certified Examiner certification in February of 2010.
- Recognized for having an excellent ability to describe complex technical concepts and ideas in non-technical terms.

Kentucky State Police | Frankfort, KY February 2007 to June 2013
Electronic Crime Section (Division of Technical Services) | *Forensic Examiner II*

- Performed forensic investigations utilizing EnCase, FTK, Cellebrite, and XRY.

- Certified in multiple cell phone forensic programs (XRY and Cellebrite).
- Recovered data and performed forensic investigations on desktops, laptops, and portable devices across multiple platforms (Windows, UNIX, Macintosh).
- Court preparation with federal attorneys on cases, explaining technical data for court presentation.
- Maintained chain of custody for evidence submitted to Electronic Crime Branch.
- Crafted policies and procedures for the entire branch, focusing on best practices and industry standards.
- Presented "lunch and learn" seminars to various computing groups and businesses on topical subjects like cell phone app security.
- Maintained electronic databases as well as physical evidence logs.
- Provided in-field training and guidance to law enforcement personnel on proper digital evidence seizure procedures, translating legal and technical requirements into clear, actionable instructions to support effective learning and compliance.
- Maintain Laboratory computer equipment, performing necessary upgrades and maintenance as required.
- Received Encase Certified Examiner certification in February of 2010.
- Recognized for having an excellent ability to describe complex technical concepts and ideas in non-technical terms.

Commonwealth Office of Technology (NOC) | Frankfort, KY July 2001 to February 2007

Security Team | *Forensic Examiner* August 2004 – February 2007

- Performed forensics examinations utilizing EnCase, FTK, Paraben, Axiom, X-ways, LinEn, and Linux boot CDs such as Knoppix, STD, and Helix.
- Conducted data forensic investigations for enterprise computer security incidents including internal intellectual property theft, attacks/intrusions, computer abuse, and insider threats investigation.
- Recovered data and performed forensic investigations on servers, RAID, desktops, laptops, and portable devices.
- Testified in front of a Grand Jury in an 18-month investigation of state government officials that resulted in 23 indictments.
- Provided testimony in state court related to personnel disputes.
- Performed covert data recovery at remote locations across the state.
- Participated in a major investigation which involved the imaging and analysis of over 40 PCs/servers on a court-ordered deadline, following court-ordered procedures.
- Prepared reports on investigation results for multiple audiences, including top management, non-technical supervisors and attorneys, explaining the scope of the data recovered, the process used to recover it, and analysis of the facts around the data recovered.
- Managed a secure forensics lab, including the network and 2 secure servers, with safeguards in place to ensure the integrity of sensitive data.
- Followed standard rules of evidence collection, with particular emphasis on data recovery and storage.
- Maintained highly sensitive data and used circumspection in daily correspondence regarding sensitive matters.
- Worked closely with lawyers to write personnel actions against employees, making sure that technical forensic findings were correctly explained and outlined to the appropriate audience.
- Worked security incidences as part of the state's incident response team, including virus outbreaks and data breaches in the Network Operation Center.
- Collaborate with IT and other stakeholders to implement security controls and best practices to prevent future incidents.
- Conduct post-incident reviews to identify lessons learned and improve incident response processes.
- Training and awareness for all stakeholders regarding best practices and improved security policies.

Security Auditing Team | *Team Leader* May 2004 – August 2004

- Managed 4 employees and was responsible for collecting and analyzing log files for a server farm of over 300 servers.
- Performed correlation of log activity and identified servers with security vulnerabilities.
- Maintained close communication with the server and WAN/Firewall teams to work on issues regarding network traffic and the state's server farm.
- Penetration tested the state network and subnets utilizing tools such as Ethereal (Wireshark), Netcat, Nmap, and *Nessus* to analyze packets, network traffic, and potential vulnerabilities.
- Mapped potential wireless security risks via war driving, utilizing such tools as Netstumbler, Kismet, and Wellenreiter.
- Conducted password cracking using Cain and Abel, John the Ripper and L0pthcrack.

Server Team | *Team Member* July 2001 – May 2004

- Built, configured, and maintained a server farm of 1300+ servers.
- Maintained a database that collected script information about all servers in the network, their components, patch levels, installed software packages, and a dynamic account of their SAN usage.
- Documented processes and procedures for multiple projects regarding server management and disaster recovery scenarios.
- Managed trouble tickets via the Remedy interface regarding software, hardware, and network issues.
- Worked with end users statewide on server and application issues related to the state network.
- Created a process to automatically collect and offload log files via scripts, resulting in a database used in security log file auditing.
- Created on demand reports in Crystal Reports for server usage, security events, and database information.
- Managed roll out of LanDesk, and daily use of DumpSec, LanDesk, Remedy, Patrol.
-

EDUCATION

University of Louisville | *Louisville, KY*
Master of Education, Educational Counseling Psychology

University of Louisville | *Louisville, KY*
Bachelor of Arts, History

CERTIFICATIONS

- CFCE- Certified Forensic Computer Examiner, IACIS 2016, 2019, 2022, 2025
- ENCE- EnCase Certified Examiner, Guidance Software 2010 (recertified 2013, 2016, 2019)
- Cellebrite UFED- UFED Mobile Device Examiner 2012
- Cellebrite UFED- UFED Physical Examiner 2012
- XRY - XRY Certification of training 2012
- A+- CompTIA 2010 (Lifetime)
- GSEC GIAC- SANS 2008 (expired)

PROFESSIONAL TRAINING

- 2023 - IACIS Mobile Digital Forensics MDF202307
- 2022 - SANS 585 Smartphone Forensics (50 hours)
- 2021 - IACIS Windows Forensic Examiner (36 hours)
- 2020 - USPIS Digital Evidence, Axiom, Sumuri Mac and Courtroom Training (9 Hours)
- 2019 - SANS 508: Advanced Incident Response, Threat Hunting and Digital Forensics (49 Hours)
- 2019 - USPIS Digital Evidence, Macintosh Forensic Essentials (16 Hours)
- 2018 - USPIS Cryptocurrency/Dark Web (16 Hours)
- 2017 - Encase v7 Computer Forensics II (32 Hours)
- 2017 - Recon for MAC OS forensic training (24 Hours)
- 2016 - X-Ways computer forensics (24 Hours)
- 2015 - IACIS Basic Forensic Computer Examiner (80 Hours)
- 2015 - USPIS Digital Evidence, Triage Responder, OSTriage, RAM & EnCase v7 Ent. (24 Hours)
- 2013 - Handheld Devices and Crimes: Online Training (40 Hours)
- 2013 - USPIS Digital Evidence, Mobile Device Training (40 Hours)
- 2013 - The Computer and Enterprise Investigations Conference
- 2012 - Cellebrite UFED/Physical Certification
- 2012 - Techno Security and Forensic Investigations and Mobile Forensics World Conference
- 2012 - The Computer and Enterprise Investigations Conference
- 2012 - Peer Marshal / Mac Marshal Train
- 2012 - XRY Cell Phone Training and Certification 2010 Comptia A+ (Certification)
- 2010 - EnCase Network Intrusion
- 2010 - NW3C Linux Forensics
- 2009 - EnCase EnCE Prep Class
- 2009 - EnCase Computer Forensics II
- 2009 - EnCase Computer Forensics I
- 2009 - AccessData's FTK Windows Forensics Vista
- 2008 - AccessData's FTK Windows Vista Forensics
- 2007 - Computer Forensics with FRED
- 2007 - 6th Annual ICAC National Conference
- 2007 - AccessData's FTK Internet Forensics
- 2007 - Investigating Computer Facilitated Crimes Against Children
- 2007 - Cell Phone Forensics 101, Presented by BK Forensics
- 2007 - AccessData's FTK Windows Forensics
- 2007 - AccessData's FTK Boot Camp
- 2006 - EnCase Intermediate Training
- 2004 - GIAC Security Essentials Certification (GSEC)

EXPERT TESTIMONY

- State of Florida v. Almando Marquez | *Fort Lauderdale, FL* | *September 2025*
- United States v. Anthony Roy Milligan, Jr. | *Detroit, MI* | *November 2024*
- United States v. Alexis Young | *Hammond, IN* | *January 2016*
- Commonwealth v. Michael Brandon Thompson | *Owensboro, KY* | *January 2014*
- Commonwealth v. Samuel Crabtree | *Richmond, KY* | *January 2011*
- Commonwealth v. Brittany Miller | *Liberty, KY* | *November 2010*