



DIGITAL FORENSICS EXPERT AND DATA RECOVERY ENGINEER

PROFESSIONAL QUALIFICATIONS

Digital Forensics

- Court-seasoned digital forensics expert since 2006 with trial experience in the following courts:
 - Idaho District
 - Texas District
 - Quebec Criminal Div.
 - Washington District
 - California District
 - 6th Cir. Appeals US Dist. OH
 - Oregon Circuit
 - 9th Circuit US Dist. ID
 - Colorado District
- Areas of forensic investigation and expert witness experience include:
 - Embezzlement
 - Fraud
 - Theft of trade secrets
 - Cyberstalking
 - Tax evasion
 - Domestic violence
 - Breach of contract
 - Arson
 - Misappropriation of funds
- Forensic investigations performed across multiple platforms:
 - Servers and desktop computers
 - Laptops, tablets, and cellphones (including JTAG and chip-off)
 - DVRs, industrial and other specialized equipment
 - Social media platforms and cloud accounts
- Analysis and interpretation of geolocation and cell tower data
- Forensic recovery of data from intentionally damaged media:
 - Physical damage: fire, liquid submersion, physical destruction
 - Logical damage: deletion, removal of RAID members
- Conduct research in electronic data storage and retrieval and forensic discovery – collaborating with industry-recognized experts and law enforcement agencies

Data Recovery

- Data recovery engineer since 2005, frequently partnering with industry pioneers to research and develop new data recovery tools and techniques
- Expert-level knowledge of electronic data storage developed through thousands of successful data recoveries performed across multiple media types, providing critical insight for forensic investigations
- Trusted by law enforcement, government agencies, elected officials, and the US military to recover critical and sensitive data

Forensic Tools

- Extensive experience with major data recovery and industry-standard civilian-accessible forensic software, including:
 - EnCase
 - ElcomSoft
 - Magnet Axiom
 - Oxygen
 - X-Ways
 - Wireshark
 - Cellebrite
 - Forensic Explorer
 - PC3000
 - Access Data FTK
 - Autopsy
 - Paladin Pro
 - RECON ITR
 - MailXaminer
 - RuSolut eMMC/NAND

TECHNICAL SKILLS

- Forensic examination
- Live forensic acquisition
- Forensic lab management
- Expert witness testimony
- EnScript programming
- Methodology development
- Mobile/Cellphone forensics
- eDiscovery
- Cloud forensics
- Digital evidence preservation
- Password recovery
- Data recovery
- JTAG and chip-off recovery
- Geolocation analysis
- Video/Audio forensics

PROFESSIONAL EXPERIENCE**Adjunct Faculty – Cyber Operations and Resilience****08/2023**

Boise State University

Present

- Course development and curriculum design
 - Develop and update bachelor- and graduate-level digital forensics courses to reflect current industry advancements and AI integration
 - Design lectures, assignments, and laboratory exercises
 - Lead establishment of new graduate certificate as foundation for standalone digital forensics degree
 - Construct new courses for anticipated forensics program
- Instruction and student engagement
 - Deliver lectures and direct class discussions – ensuring mastery of key concepts
 - Create virtual lab materials and facilitate online laboratory exercises to provide hands-on investigative experience
 - Provide comprehensive feedback on coursework to strengthen student understanding
- Mentor teaching assistants and advise students on course selection and career pathways
- Maintain regular office hours for individualized student support

Digital Forensic Investigator/Chief Executive Officer

01/2021

G2 Research, Inc., Boise, ID

Present

- Expert witness services
 - Provide expert testimony in digital forensics and data storage/recovery as a trial-tested witness across multiple court jurisdictions
 - Prepare exhibits and convey complex technical concepts clearly to judges and juries
- Forensic investigations
 - Conduct comprehensive in-lab and onsite forensic examinations across diverse media, including computers, servers, mobile devices, industrial equipment, cloud accounts, DVRs, and social media platforms
 - Acquire and examine digital evidence using scientifically validated methodologies
 - Review cases and advise clients on optimal investigation strategies that align with case objectives
 - Prepare detailed investigative reports documenting analysis, conclusions, and expert opinions
 - Perform live and remote eDiscovery acquisitions – minimizing business disruption
 - Analyze digital artifacts, including metadata, system logs, unallocated space, and geolocation data to reconstruct user activity and identify evidence
- Specialized forensic services
 - Successfully recover and rebuild data from intentionally damaged or failed media (hard drives, RAID arrays, cellphones, tape drives, solid-state media, DVRs)
 - Perform JTAG and chip-off cellphone recovery from damaged devices
 - Decrypt devices and retrieve/bypass passwords
 - Authenticate electronic documents and locate deleted files
- Laboratory management and development
 - Establish and maintain scientifically sound forensic procedures and methodologies
 - Hire, train, and supervise forensic staff
 - Evaluate, source, and procure cost-effective tools and equipment – ensuring comprehensive service delivery
 - Maintain, test, and validate all forensic tools and equipment
 - Design professional development programs to maintain forensic standards
- Research and continuous improvement
 - Develop custom forensic tools and scripts for specialized forensic applications
 - Maintain current knowledge of forensic procedures through continuing education
 - Sustain proficiency in all major court-vetted forensic tools
 - Continuously evaluate, validate, and update methodologies, procedures, and techniques

Digital Forensic Investigator/Data Recovery Engineer/Chief Executive Officer

Mar 2005

Northwest Data Recovery, Inc., Boise, ID

Present

- Expert witness and forensic investigations
 - Provided comprehensive digital forensics and expert witness services – transitioned forensic operations to G2 Research upon acquisition in 2021 to separate and expand forensic capabilities
 - Provided expert testimony in digital forensics and data storage/recovery, preparing exhibits and conveying complex technical concepts clearly to judges and juries
 - Conducted comprehensive forensic investigations across diverse media
 - Performed eDiscovery acquisitions and analyzed digital artifacts
 - Provided specialized forensic services, including JTAG/chip-off recovery, decryption, and data authentication
- Data recovery expertise
 - Recover and rebuild data from hard drives, RAID arrays, cellphones, tape drives, solid-state media, DVRs, and other electronic media
 - Perform data recovery on intentionally damaged media (physical destruction, fire damage, liquid submersion, deletion, removal of RAID members)
 - Maintain a deep understanding of electronic data storage by performing thousands of successful data recoveries
- Research and development
 - Develop new tools and techniques for data recovery and forensic investigations
 - Frequently partner with industry pioneers to research and advance data recovery methodologies
 - Conduct research in electronic data storage, retrieval, and forensic discovery in collaboration with industry-recognized experts and law enforcement agencies
- Business leadership
 - Establish and manage all business operations for data recovery firm
 - Oversee technical operations, client relationships, and service delivery
 - Source cost-effective tools and equipment while maintaining service standards

Database Administrator/Network Specialist/Computer Repair Technician

Oct 1994

Various companies (most defunct), Duluth, MN and Boise, ID

May 2007

- Provided technical instruction specializing in eDiscovery compliance, Windows, and Linux systems
- Performed data recovery and provided technical support across diverse computing environments
- Developed databases and custom software solutions

EXPERT WITNESS EXPERIENCE

FEDERAL/INTERNATIONAL CASES

United States v William Walls 1:21-CR-00013-BLW-1 **2025**

United States District Court District of Idaho

Charges: Attempted sexual exploitation of a minor child

Summary: I authenticated a cellphone video and determined the video was unaltered and proper procedures were followed.

Minnesota Life Insurance Co. v Pleasants, et al. **2022**

United States District Court District of Idaho

Summary: In a life insurance beneficiary dispute, I attempted to locate relevant digital communications between the decedent and Ms. Pleasants – none were found. The court awarded the death benefit to the named beneficiary.

Banner Life Insurance Co. v Anderson and Eggers 1:20-CV-00036 **2021**

United States District Court Sixth Circuit Court of Appeals Northern Dist. of Ohio

Summary: In a life insurance contract dispute, Ms. Anderson is alleged to have taken possession of the decedent's phone, deleted information from the phone, and traveled to the decedent's property. Analysis of the alleged deletion was inconclusive, but I was able to show the phone's location at the time of possession.

CASE EXAMPLES

Recovery of fire-damaged digital video recorder (DVR)

Summary: I recovered key video evidence from a DVR damaged in an arson fire that led to the successful prosecution of the arsonist.

Violation of non-compete agreement

Summary: In my investigation, I was able to establish the defendant intentionally destroyed electronic evidence.

Lost evidence recovery

Summary: When digital evidence of a regionally infamous murder case stored on a computer was lost, I was able to recover data that was key to successfully prosecuting the murderer.

Recovery of cellphone information

Summary: When a local law enforcement agency was unable to gain access to a murder victim's cellphone, I successfully decrypted the phone and recovered texts, e-mails, location information, contacts, and deleted files that led to the identification and eventual conviction of the murderer.

Validity of in-house forensic application

I was able to obtain a look at redacted documentation of a forensic application developed in-house by the Royal Canadian Mounted Police (RCMP). Despite the redactions, I was able to determine that due to several flaws, the application did not meet forensically sound scientific standards of reproducibility and verifiable authenticity. I was also able to demonstrate the RCMP witness made false statements regarding the application. Though a closer look at the application was warranted and court approved, the case moved in another direction and I was unable to obtain permission to review the actual application to ascertain its forensic viability through error testing and other validation procedures.

CERTIFICATIONS AND MEMBERSHIPS

ACE Labs Technical Certificate	Jun 2018
ACE Labs	
Oxygen Forensic Expert (OFE)	Apr 2018
Cybercrime Forensics Training Center	
Member	Jan 2016
The International Association of Computer Investigative Specialists (IACIS)	
EnCase Certified Examiner (EnCE)	May 2016
Certification Number 15-0316-7018	
Guidance Software	
Certified Data Recovery Specialist, Level III	Jan 2010
Capital Data Recovery	
Microsoft Certified Professional (MCP)	Mar 2007
Certification Number A719-1785	
Microsoft	
Certified Computer Examiner (CCE)	Jun 2006
Certification Number 513	
The International Society of Forensic Computer Examiners	
Windows NT 4.0 Certification	Dec 2000
Lake Superior College, Duluth, MN	
A+ Certification	Dec 1994
CompTIA	

EDUCATION

Master of Science: Digital Forensic Science	May 2022
Champlain College, Burlington, VT GPA: 4.0	
Bachelor of Science: Computer Forensics & Digital Investigations	May 2017
Champlain College, Burlington, VT GPA: 3.957 - Summa Cum Laude	

RESEARCH PROJECTS

RAID 5 rebuild (unpublished)	2016
I was presented with a four-member RAID 5 system that had been tampered with in an attempt to hide documents required for litigation disclosure. Two members of the RAID were replaced with non-member drives and the RAID was rebuilt across the two original and two replaced drives. In consultation with other data recovery colleagues, I was able to rebuild the original RAID and retrieve all documents under 512 kilobytes in size.	
Beta test forensic software (unpublished)	2018
I was tasked with locating flaws in a new forensic software title. During beta testing, I discovered several problems that affected the forensic soundness of images created by the software and offered suggestions on how to address the problems.	

PRESENTATIONS

What is computer forensics and when should I call an expert?	Jan 2019
Idaho State Bar Association Luncheon, Pocatello, ID	
Decrypting self-encrypted Western Digital hard drives	Oct 2017
Project 7, Boise, ID	
How to preserve evidence when responding to an incident	Aug 2021
Project 7, Boise, ID	
Social Media Evidence as an Investigative Tool	Jun 2026
Public Defender 2026, Boise, ID	

LECTURES

Guest Lecturer: CS 332 Ethical Hacking**Apr 2020**

Boise State University

Demonstrated how to identify and preserve cellphone and network anomalies that might indicate illicit access. Discussed the ethics of hacking in digital forensics and the potential legal ramifications.

RECENT PROFESSIONAL DEVELOPMENT

- ACE Labs Tech Conference: Exploring the Latest Data Recovery Trends & Developments
- EnFuse Security and Digital Investigations Conference 2017, 2019, 2021
- Access Data Boot Camp Computer Forensics Training
- DefCon 23 Hacker Conference
- New Technology Advances in SSD and HDD Data Recovery conference, Ace Laboratory
- New Techniques in Data Recovery, Capital Data Recovery
- Chip-Off Data Recovery and Digital Forensics Training, Basic and Advanced, RuSolut
- SaintCon 2023 Cybersecurity Conference
- Oxygen Forensics Training: AI workflows that streamline mobile investigations
- Oxygen Forensics Training: Google Takeout, Facebook Account, and Snapchat My Data
- Oxygen Forensics Training: In case you missed it – KeyScout
- Oxygen Forensic Advanced Analysis (OFAA)
- Oxygen Forensic SQLite Analysis
- Oxygen Forensic Boot Camp