WYOMING LEGISLATIVE SERVICE OFFICE

Research Memorandum

QUALIFICATIONS AND DUTIES OF DIGITAL FORENSIC ANALYSTS IN WYOMING AND OTHER STATES

September 2023

by

Pierre Chesnais, Associate Research Analyst

SUMMARY: This memorandum surveys digital forensic analysts' qualifications, duties, and law enforcement licensing requirements in Wyoming and nine other states: Colorado, Idaho, Kansas, Montana, Nebraska, North Dakota, Oklahoma, South Dakota, and Utah.

Wyoming and four other states surveyed here (Colorado, Kansas, Oklahoma, and South Dakota) require applicants for digital forensic analyst positions to possess at least a bachelor's degree. While Wyoming favors applicants with a degree in criminal justice, some states requiring a four-year degree do not specify preferred fields of study. The other states surveyed in this memorandum either do not specify educational requirements or have lower requirements than a bachelor's degree.

Four states surveyed here (Colorado, Kansas, Nebraska, and Oklahoma) mention that they require or favor applicants that have completed digital forensic certifications. The most common certification types are the Computer Forensic Certified Examiner[1] and the EnCase Certified Examiner.[2]

Regarding the professional duties of digital forensic analysts, limited variance appears to exist across the surveyed states. Duties performed by analysts in Wyoming are representative of those conducted by analysts in other states. These standard duties include:

[1] The Certified Forensic Computer Examiner (CFCE) certification program, offered by the International Association of Computer Investigative Specialists (IACIS), is based on a series of core competencies in the field of computer and digital forensics.

[2] EnCE certification acknowledges that professionals have mastered computer investigation methodology as well as the use of EnCase software during complex computer examinations.

23RM019 • LSO RESEARCH AND EVALUATION DIVISION • 200 W. 24th Street • Cheyenne, Wyoming 82002
TELEPHONE 307-777-7881 • EMAIL lso@wyoleg.gov • WEBSITE www.wyoleg.gov

- Performing computer forensic analysis by identifying, preserving, and analyzing data and technical items for evidence;
- Acting as part of search warrant teams to search for, identify, and seize evidence;
- Providing testimony as a qualified expert in the areas of computer forensics; and
- Implementing highly specialized equipment for recovering data from damaged or secured cell phones.

Three states (Montana, North Dakota, and South Dakota) have law enforcement licensing requirements. Montana requires applicants to hold a Public Officer Standards and Training certificate. North Dakota requires that applicants to digital forensic analyst positions have been sworn police officers for five years. The South Dakota Division of Criminal Investigation only has sworn police officers performing as digital forensic analysts. Other states rely on and allow civilians to work as digital forensic analysts. In Wyoming, the Division of Criminal Investigation does not require applicants to be licensed police officers.

Appendix A provides a table that compares the different states' educational, certification, and law enforcement licensing requirements.

DISCUSSION:

WYOMING[3]

In Wyoming, computer forensic investigators are assigned to the Internet Crimes Against Children (ICAC) team within the Division of Criminal Investigation.[4]

Qualifications:

The Division of Criminal Investigation requires that applicants for computer forensic investigator positions have at least a bachelor's degree, typically in criminal justice, and up to three years of progressive work experience in investigative work. A candidate may substitute the requirement for the bachelor's degree by having four to six years of investigative work experience.

[3] All information provided in this section was received from Matt Waldock, Commander of the Wyoming Division of Criminal Investigation.

[4] The United States Department of Justice's Internet Crimes Against Children Task Force Program (ICAC program) helps state and local law enforcement agencies develop an effective response to technology-facilitated child sexual exploitation and Internet crimes against children. This help encompasses forensic and investigative components, training and technical assistance, victim services, and community education.

Professional Duties:

Duties that Computer Forensic Investigators perform within the Division include:

- Performing computer forensic analysis by identifying, preserving, and analyzing data and technical items for evidence;
- Acting as part of search warrant teams to search for, identify, and seize evidence;
- Employing forensically sound methods to preserve digital evidence and interpreting the results in a meaningful and presentable manner in court;
- Providing testimony as a qualified expert in the areas of computer forensics, digital media analysis, evidence seizure, and crime scene processing for computers, cellular phones, digital storage devices, wired networks, and wireless networks;
- Implementing highly specialized equipment for recovering data from damaged or secured cell phones; and
- Maintaining and supporting hardware, software, wired and wireless network equipment, forensic equipment, and other network infrastructure**.**

Law Enforcement Licensing Requirement:

The Division of Criminal Investigation does not require computer-forensic-investigator applicants to hold a current and valid Public Officer Standards and Training (POST) certification.

Appendix B provides a complete description of the position's educational, knowledge, and ability requirements and a complete listing of duties.[5]

COLORADO

The Colorado Bureau of Investigation does not provide computer forensic analysis but partners with the Northern Colorado Regional Forensic Laboratory (NCRFL), a division within the Weld County Sheriff's Office.[6] The Northern Colorado Regional Forensic Laboratory (NCRFL) provides forensic science services to six local and statewide agencies: the Weld County Sheriff's

[5] Email from Matt Waldock, Commander of the Wyoming Division of Criminal Investigation, to Pierre Chesnais, Associate Research Analyst, Wyoming Legislative Service Office (May. 25, 2023).
[6] Email from Lance Allen, Deputy Director – Forensic Services, Colorado Bureau of Investigation, to Pierre Chesnais, Associate Research Analyst, Wyoming Legislative Service Office (Jul. 14, 2023).

Office, Larimer County Sheriff's Office, the Greeley Police Department, Fort Collins Police Services, the Loveland Police Department, and the Colorado Bureau of Investigation.[7]

Staff from the six agencies provide staff to the NCRFL to work in six different disciplines, including digital and multimedia evidence.[8]

Qualifications:[9]

The Weld County Sheriff's Office, which provides digital forensic staff to NCRFL, requires senior digital forensic analysts to have completed at least a four-year college degree and have three years of experience in:

- Computer forensics;
- Computer operations;
- Computer systems analysis;
- Criminal investigations; or
- Intelligence analysis.

The Northern Colorado Regional Forensic Laboratory also requires incoming staff to obtain a Computer Forensic Certified Examiner Certification through the International Association of Computer Investigative Services.

Professional Duties:[10]

The Weld County Sheriff's Office lists the following duties for digital forensic analysts:

- Performing computer and network forensic examinations and investigations in support of internal investigations and intrusion incidents;
- Conducting examinations of all digital media, including but not limited to computers, handheld devices, flash or thumb drives, networking devices, and other digital media;
- Creating and maintaining forensic processes and procedures based on industry best practices;

[7] Weld County Sheriff's Office. Division - Northern Colorado Regional Forensic Lab. **https://www.weldsheriff.com/Divisions/Patrol/Regional-Crime-Lab**. (Last Accessed Jul. 20, 2023).
[8] *Id.*
[9] All information included in this subsection was received from Daren Ford, Director of the Northern Colorado Regional Forensic Laboratory.
[10] All information included in this subsection was received from Daren Ford, Director of the Northern Colorado Regional Forensic Laboratory.

- Developing and maintaining the necessary documentation to support the forensic and investigative processes and procedures;
- Using experience and knowledge of advanced computer technologies and theories to conduct investigations, collection of, and analysis of digital evidence;
- Installing and maintaining forensic hardware and software;
- Determining the most appropriate method of collecting, protecting, analyzing, and retaining original evidence; and
- Coordinating with internal support organizations to develop additional evidence-collection methods, technologies, and processes that support detecting and responding to unauthorized or unintentional activities.

Law Enforcement Licensing Requirement:[11]

The Northern Colorado Regional Forensic Laboratory does not require forensic analysts to be licensed or sworn police officers and reports that all current analysts are civilians.

IDAHO[12]

The Cyber Crime Unit, a unit within the Idaho State Police, provides all Idaho law enforcement agencies with forensic imaging and analysis of digital evidence.[13] The Cyber Crime Unit and the Idaho Criminal Intelligence Center operate under one administrator.[14] The Idaho Criminal Intelligence Center receives requests for investigation assistance from law enforcement agencies across the State. As most local Idaho law enforcement agencies lack the funding and expertise to conduct computer forensics, Computer Forensic Examiners (CFE) within the Cyber Crime Unit perform those duties for local agencies.

Qualifications:

The Cyber Crime Unit does not have specific educational requirements for CFEs. Most applicants, however, have professional or educational backgrounds in information technology. The Cyber

[11] All information included in this subsection was received from Daren Ford, Director of the Northern Colorado Regional Forensic Laboratory.
[12] All information provided in this section, unless otherwise noted, was received from Bret Kessinger, administration of the Idaho Criminal Intelligence Center and the Cyber Crime Unit within the Idaho State Police.
[13] Idaho State Police. Cyber Crime Unit. **https://isp.idaho.gov/cybercrime/** (Last Accessed Jul. 20, 2023).
[14] The Idaho Criminal Intelligence Center is responsible for integrating, analyzing, producing, and disseminating actionable criminal intelligence in combating criminal activity and terrorism.

Crime Unit favors applicants with past forensic experience and who can demonstrate knowledge of computer forensics concepts.

Professional Duties:

Computer forensic analysts perform forensics on digital devices that law enforcement agencies confiscate or obtain when investigating criminal matters. In addition, CFEs develop and prepare for presentation in court digital files of evidentiary value extracted from digital devices, including:

- Computers;
- Cellular devices;
- Memory devices;
- Surveillance recording equipment; and
- Action cameras.[15]

Other duties that CFEs perform include:

- Providing on-scene forensic analysis;
- Testifying in courts across the State regarding forensic processes and findings; and
- Supporting a variety of investigations, including homicide, robbery, theft, distribution and creation of child pornography, embezzlement, and vehicle crash investigations.

Law Enforcement Licensing Requirement:

Currently, only one CFE is a sworn-in law enforcement officer. Although the other CFEs are non-sworn staff, they directly support law enforcement agencies and must successfully complete an in-depth background check and polygraph test before commencing employment.

KANSAS

The Kansas Bureau of Investigation includes a Forensic Science Laboratory, which provides examinations and services in various areas, including digital evidence. The Digital Evidence Section is responsible for collecting, processing, examining, and analyzing digital media stored on electronic devices, including:

- Computer systems;
- Mobile devices;

[15] Idaho State Police. Cyber Crime Unit. **https://isp.idaho.gov/cybercrime/** (Last Accessed July 20, 2023).

- External storage devices; and
- Removable media.[16]

The Digital Evidence Section conducts the following types of testing:

- Computer Forensics: Application of methods and techniques for acquiring and examining data contained within computers, external drives, hard drives, drive images, and other media storage;
- Mobile Forensics: Application of methods and techniques for acquiring and examining data contained within a mobile device and associated components.
- Advanced Methods: Preserve and recover digital evidence on mobile devices when standard methods are unsuccessful. These techniques allow the examiner to overcome challenges such as passcode locks, damaged devices, and new technology not yet supported by forensic tools.[17]

Qualifications:[18]

The Kansas Bureau of Investigation provided information for the Forensic Analyst II position, which requires applicants to have the following qualifications:

- At least a bachelor's degree relevant to the field of forensic analysis;
- Two years of experience as a digital forensic examiner; and
- Experience in testifying in a court of law as a digital forensic examiner.

The Kansas Bureau of Investigation favors applicants that have received the following certifications:

- Certified Forensic Computer Examiner Program through the International Association of Computer Investigative Specialists;
- EnCase Certified Examiner through Guidance Software; and
- Crime Scene Certification through the International Association of Identification.

[16] Kansas Bureau of Investigation. Digital Evidence Section. **https://www.kansas.gov/kbi/about/about_lab_digitalevidence.shtml** (Last Accessed Jul. 20, 2023).
[17] *Id.*
[18] All information included in this subsection was received from Danielle Brady, SHRM-CP, Recruiting Supervisor at the Kansas Bureau of Investigation.

Professional Duties:[19]

Forensic analysts perform the following duties for state-related cases and to assist local law enforcement agencies:

- Performing examinations on digital evidence, which includes recovering, preserving, and analyzing data from electronic sources, including desktop and laptop computers, mobile devices, and removable media;
- Preparing examination notes documenting the recovery, preservation, and analysis performed and laboratory reports explaining examination results;
- Testifying in court as to qualifications to be an expert witness and presenting laboratory findings in court;
- Performing general maintenance of digital evidence instrumentation and software; and
- Reviewing forensic scientific literature and information related to the field of digital evidence.

Law Enforcement Licensing Requirement:[20]

The Kansas Bureau of Investigation does not require forensic analysts within the Digital Evidence Section to be certified (or sworn) law enforcement personnel.

MONTANA[21]

Digital forensic examiners work for the Crime Information Bureau within the Montana Department of Justice's Division of Criminal Investigation.

Qualifications:

The Division of Criminal Investigation requires that applicants for digital forensic examiners have, at a minimum, a high school diploma. The Division of Criminal Investigation, however, favors applicants with a bachelor's degree in public administration, criminal justice, sociology, and psychology.

[19] All information included in this subsection was received from Danielle Brady, SHRM-CP, Recruiting Supervisor at the Kansas Bureau of Investigation.
[20] All information included in this subsection was received from Danielle Brady, SHRM-CP, Recruiting Supervisor at the Kansas Bureau of Investigation.
[21] All information provided in this section was received from Anne Dormady, Chief of the Crime Information Bureau, Division of Criminal Investigation.

The Division of Criminal Investigation also considers applicants without a completed degree but who have had college coursework closely related to criminal justice.

Regarding professional experience, applicants for digital forensic examiner positions must have at least three years of criminal, investigative, or law enforcement experience. The Division of Criminal Investigation recommends that applicants have at least five years of investigative experience and a minimum of two years as a full-time investigator handling a variety of felony investigations.

Professional Duties:

Digital forensic examiners investigate all crimes within the Division of Criminal Investigation's jurisdiction where computers are the vehicle for the commission of criminal acts, sources of evidence, or the object of attack. Specific duties that digital forensic examiners perform include:

- Conducting forensic data recovery and analysis of all computer systems seized by DCI and any other Montana law enforcement agency requesting technical or investigative services;
- Conducting undercover operations to identify, arrest, and convict suspects involved in computer and high technology crimes;
- Cooperating with computer forensics associations to provide information, education, and training to law enforcement and the public;
- Investigating computer manipulation crimes, which involves changing data or creating data in a computer system to advance criminal activities; and
- Investigating illegal online activities by monitoring and investigating illicit online activities, including distributing child pornography, credit card and telephone fraud, copyright violations, gambling operations, money laundering, and narcotics trafficking.

Digital Forensic Examiners also serve on the United States Department of Justice's Internet Crime Against Children Task Force. As part of serving on the ICAC task force, digital forensic examiners support in-state agencies for equipment, training, and ICAC investigations. The Montana Department of Justice also reports that many ICAC investigations have connections to other states, which leads examiners to work with other states' agencies.

Law Enforcement Licensing Requirement:

The Division of Criminal Investigation requires all forensic-examiner applicants to hold a current and valid Public Officer Standards and Training (POST) Law Enforcement Basic Certificate. Applicants must also meet eligibility requirements for the POST Law Enforcement Intermediate Certificate. In addition, applicants must have received firearms training, which is mandatory for all peace officers.

NEBRASKA

The Technical Crimes Division within the Nebraska State Police handles forensic analyses of digital evidence performed by digital forensic examiners.[22] The Division consists of the following five units:

- Cyber Unit;
- Child Exploitation Unit;
- Forensic Unit;
- Technical Services Unit; and
- Intel/Public Information Unit.[23]

Qualifications:[24]

The Nebraska State Patrol requires applicants to have at least an associate degree in computer science plus three years of related technical and business experience or post-high-school coursework in computer science plus four years of related experience.

The Nebraska State Patrol, however, prefers that applicants have the following qualifications:

- Certified Forensic Computer Analyst (CFCE) through the International Association of Computer Investigative Specialists (IACIS) or EnCase Certified Examiner (ENCE) through Guidance Software;
- Bachelor's degree in computer science or a closely related field supplemented by specialized training in microcomputers, computer forensics, and data recovery; and
- Experience with information technologies, including hardware and software specifications to utilize specialized tools and procedures, to collect, preserve, and examine computer-related evidence.

[22] Nebraska State Patrol. Technical Crimes Division. **https://statepatrol.nebraska.gov/divisions/investigative-services/technical-crimes-division**. (Last Accessed Jul. 20, 2023).

[23] *Id.*

[24] All information included in this subsection was either provided by Chris Peters, Human Resources Specialist, Nebraska State Patrol, or on the State's job portal. (Available at **https://www.governmentjobs.com/careers/nebraska/jobs/2732960/digital-forensic-examiner**)

Professional Duties:[25]

Digital examiners conduct the following duties:

- Conducting forensic examinations of computer systems and analyzing electronic evidence using acceptable forensic methods for the Nebraska State Patrol, allied law enforcement agencies, and the Internet Crimes Against Children (ICAC) task force;
- Examining cases involving the sexual exploitation of children, fraud, forgery, theft, homicide, and drug violations.
- Analyzing submitted evidence by following acceptable forensic methods in evidence analysis;
- Writing reports on the analysis results;
- Testifying in court hearings and providing depositions on analysis results and reports;
- Assisting with in-service training to law enforcement agencies and county attorneys;
- Obtaining data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer;
- Assisting with search warrants and the seizure of evidence from crime scenes; and
- Performing routine instrument upkeep.

Law Enforcement Licensing Requirement:

Digital Evidence Examiners do not have to be licensed law enforcement officers.[26]

NORTH DAKOTA[27]

In North Dakota, forensic analysts work for the Bureau of Criminal Investigation within the State's attorney general's office.

[25] Job Opportunities – Digital Forensic Examiner. Nebraska State Jobs. **https://www.governmentjobs.com/careers/nebraska/jobs/2732960/digital-forensic-examiner** (Last Accessed Jul. 24, 2023)

[26] Email from Chris Peters, Human Resources Specialist, Nebraska State Patrol, to Pierre Chesnais, Associate Research Analyst, Wyoming Legislative Service Office (Jul. 14, 2023).

[27] All information included in this subsection was provided by Ashley Eisenbeis, Human Resources Officer at the North Dakota Office of Attorney General.

Qualifications:

The North Dakota Bureau of Criminal Investigation does not have specific educational requirements, but applicants for forensic analyst positions must have been sworn or certified law enforcement officers for at least five years.

Professional Duties:

Duties that Forensic Analysts perform in North Dakota include:

- Assisting all law enforcement agencies within the state with digital forensics on devices related to criminal cases or used as vehicles for the commission of criminal acts;
- Conducting proactive investigations of ICAC cases (i.e., corresponding with suspects using mobile applications or messaging services); and
- Investigating National Center for Missing and Exploited Children cyber tips.

Law Enforcement Licensing Requirement:

All forensic analysts are currently sworn law enforcement officers. In addition, all applicants for forensic analyst positions must have been sworn officers for at least five years.

OKLAHOMA

Digital examiners work within the Oklahoma State Bureau of Investigation's Digital Evidence Unit, which is attached to the Oklahoma Internet Crime Against Children Task Force.[28] The Digital Evidence Unit specializes in the preservation, acquisition, processing, and analysis of evidence in a digital format.[29] The Unit also provide local and state law enforcement agencies with the recovery and analysis of digital evidence, especially in crimes involving children.[30]

Qualifications:[31]

The digital evidence unit has four levels of digital examiners and provides the following minimum qualifications:

[28] Oklahoma State Bureau of Investigation. Digital Evidence. **https://osbi.ok.gov/investigative-services/digital-evidence**. (Last Accessed Jul. 20, 2023).
[29] *Id.*
[30] *Id.*
[31] All information included in this subsection was received from Rachel Ross, Supervision Lieutenant of the Digital Evidence Unit, Oklahoma State Bureau of Investigation.

- Applicants applying for the entry-level position must have a completed bachelor's degree in any field;
- Applicants applying for the second level of digital examiners must have a bachelor's degree plus one year of experience working as a full-time criminalist in which the candidate performed full-time forensic analyses in digital work directly related to criminal prosecutions;
- Applicants applying for the third level must have a bachelor's degree plus two years of full-time professional experience in forensic analysis in digital work; and
- Applicants applying for the fourth level must meet the requirements identified for the third level and be proficient in supervision and management of budgeting and planning.

The Digital Evidence Unit favors applicants for the third level and up to have received certification from the International Association of Computer Investigative Specialists (IACIS).

Professional Duties:[32]

Digital examiners in Oklahoma conduct the following duties:

- Performing forensic examinations and analysis of computers and other items of digital evidence in criminal investigations;
- Issuing reports of findings and testifying in court as an expert witness;
- Receiving, managing, and returning evidence associated with cases submitted for forensic analysts;
- Ensuring that the integrity of the evidence is protected by following standard procedures and evidence handling;
- Ensuring that work performed complies with OSBI standards and policies.
- Assisting in updating protocols, procedures, and manuals for all aspects of the Digital Evidence Unit; and
- Training law enforcement officers, district attorneys, and other requestors on issues related to digital and computer evidence.

Law Enforcement Licensing Requirement:[33]

Digital Evidence Examiners do not have to be licensed law enforcement officers.

[32] All information included in this subsection was received from Rachel Ross, Supervision Lieutenant of the Digital Evidence Unit, Oklahoma State Bureau of Investigation.
[33] All information included in this subsection was received from Rachel Ross, Supervision Lieutenant of the Digital Evidence Unit, Oklahoma State Bureau of Investigation.

SOUTH DAKOTA[34]

The Division of Criminal Investigation within the South Dakota Office of the Attorney General includes an Internet Crime Against Children Task Force, a Digital Evidence Unit, and a digital evidence laboratory. The digital evidence laboratory conducts forensic examinations of computer systems and analyzes electronic evidence using acceptable forensic methods. Cases referred to the digital evidence laboratory include sexual exploitation of children, fraud, forgery, theft, homicide, and drug violations.

Qualifications:

All computer forensic examiners and investigators are sworn law enforcement officers. The Division of Criminal Investigation requires its agents to possess at least a four-year college degree, which does not have to be in computer forensics or other related fields.

The Department of Criminal Investigation also subjects applicants to a psychological evaluation to assess the applicants' ability to cope with child sexual exploitation.

Professional Duties:

Computer forensic examiners perform the following duties:

- Analyzing submitted evidence;
- Following acceptable forensic methods in evidence analysis**;**
- Writing lab reports on the analysis results;
- Testifying in court hearings;
- Providing depositions on analysis results and reports;
- Obtaining data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer; and
- Assisting with search warrants and the seizure of evidence from crime scenes.

In addition to the duties listed above, computer forensic investigators conduct criminal investigations, perform computer forensic examinations, and provide digital evidence support for investigations conducted by the Internet Crimes Against Children Task Force and all other crimes investigated by the Division of Criminal Investigation.

[34] All information included in this section was received from Toby Russell, ICAC Task Force Commander, South Dakota Division of Criminal Investigation.

Law Enforcement Licensing Requirement:

The Division of Criminal Investigation currently does not employ any civilian computer forensic examiners. As a result, all computer forensic examiners are sworn law enforcement officers. The Division of Criminal Investigation is, however, considering creating civilian forensic examiner positions to meet the growing demand for computer forensic analysis.

UTAH[35]

The Utah Department of Public Safety includes a Bureau of Forensic Services Laboratory System (State Crime Laboratory), which analyzes evidence from crime scenes and crime-related incidents submitted by federal, state, county, and municipal criminal justice agencies.[36]

Qualifications:

The State Crime Laboratory does not have specific educational preferences for digital forensic scientist positions but reports that the best-qualified applicants have a bachelor's degree in criminal justice, computer science, or related fields.

Professional Duties:

Duties that digital forensic analysts perform include:

- Performing examinations and analyses of digital evidence according to procedures and all required quality guidelines and policies;
- Extracting, collecting, and preserving data from digital media;
- Acquiring and utilizing suitable hardware and software interfaces to handle specific data situations;
- Identifying, diagnosing, and correcting errors and problem conditions encountered in the acquisition and examination of evidence;
- Producing technical reports based on forensic investigation findings; and
- Acting as an expert witness in courts.

[35] All information included in this section, unless otherwise noted, was received from Sherry Saracino, Manager at the Utah Division of Human Resource Management. The Utah Division of Human Resource Management received information from the Bureau of Forensic Services' Chief Forensic Scientist within the Utah Department of Public Safety.

[36] Utah Department of Public Safety. Forensic Services. **https://forensicservices.utah.gov/** (Last Accessed Jul. 20, 2023).

Law Enforcement Licensing Requirement:

Digital forensics analysts working for the State Crime Laboratory are civilian employees and not law enforcement officers.

If you have any further questions, please do not hesitate to contact LSO Research and Evaluation Division at 777-7881.

Appendix A:

State-by-State Comparison Table

State	Educational Requirements	Certifications	Law Enforcement Licensing Requirements
Wyoming	At least a bachelor's degree, typically in criminal justice plus three years of experience in investigative work. An applicant may substitute the requirement for the bachelor's degree by having four to six years of investigative experience.	Not specified.	No law enforcement licensing requirement.
Colorado	At least a four-year college degree and three years of work experience in forensic-related fields.	Requires incoming staff to obtain the Computer Forensic Certified Examiner Certification through the International Association of Computer Investigative Services.	No law enforcement licensing requirement.
Idaho	No specific educational requirements. Favors applicants with past forensic experience and can demonstrate knowledge of computer forensics concepts.	Not specified.	No law enforcement licensing requirement.
Kansas	At least a bachelor's degree relevant to the field of forensic analysis plus two years of experience as a digital forensic examiner.	Favors applicants with the following certifications: Certified Forensic Computer Examiner Program, EnCase Certified Examiner, or Crime Scene Certification.	No law enforcement licensing requirement.
Montana	At least a high school diploma but favors applicants with bachelor's degrees. Requires three years of investigative, criminal, or law enforcement experience but recommends five years of experience.	Not specified.	Applicants must hold a current and valid Public Officer Standards (POST) and Training Law Enforcement Basic Certificate.
Nebraska	At least an associate degree in computer science plus three years of related experience or post-high-school coursework in computer science plus four years of experience	Favors applicants with the following certifications: Certified Forensic Computer Examiner Program or EnCase Certified Examiner.	No law enforcement licensing requirement.

North Dakota	No specific educational requirements.	Not specified.	All applicants for forensic analyst positions must have been sworn officers for at least five years.
Oklahoma	Entry level: At least a bachelor's degree in any field. Second level: At least a bachelor's degree in any field plus one year of experience working as a full-time criminalist with experience in forensic analysis in digital work. Third level: At least a bachelor's degree in any field plus two years of experience working as a full-time criminalist with experience in forensic analysis in digital work. Fourth level: Same requirements identified for the third level plus proficiency in supervision and management of budgeting and planning.	Favors applications for the third level and up to have received certification from the International Association of Computer Investigative Specialists.	No law enforcement licensing requirement.
South Dakota	At least a four-year college degree	Not specified.	All current computer forensic examiners are currently sworn law enforcement officers. The South Dakota Division of Criminal Investigation is considering opening examiner positions to civilians to meet the growing demand for digital forensics.
Utah	No specific educational requirements but reports that best-qualified applicants have a bachelor's degree in criminal justice, computer, science, or related fields.	Not specified.	No law enforcement licensing requirement.

Source: LSO Staff

Appendix B:

Qualifications and Functions of Computer Forensic Investigators in Wyoming

Computer Forensic Investigator

Minimum Qualifications

Education:

Bachelor's Degree (typically in Criminal Justice)

Experience:

0-3 years of progressive work experience in investigation.

OR

Education & Experience Substitution:

4-6 years of progressive work experience in investigation.

Essential functions

- Perform computer forensic analysis by identifying, preserving, and analyzing data and technical items for evidence involving breaking encryption, recovering and analyzing files from hard drives, examining computers and data storage media, etc.
- Employ forensically sound methods to preserve digital evidence, including computer hard drives, flash media, solid-state drives, and cellular phones, process it, and interpret the results in a meaningful and presentable manner in court.
- Act as part of search warrant teams to search for, identify, and seize evidence according to established policies, procedures, and laws.
- Serve as a subject matter expert in performing onsite previews, processing live systems, wired networks, and wireless networks.
- Provide testimony as a qualified expert in the areas of computer forensics, digital media analysis, evidence seizure, and crime scene processing for computers, cellular phones, digital storage devices, wired networks, and wireless networks.
- Support and scale infrastructures of networks to meet the Task Force needs pertaining to the maintenance and configuration of undercover and classroom networks and equipment such as firewalls, switches, and routers.
- Provide direct support, maintenance, and configuration of systems used for investigative de-confliction queries, geolocation of IP addresses, images and image hash queries, forensic analysis request services, and activity tracking as required by the Office of Juvenile Justice Delinquency Prevention Program for ICAC grant reporting.
- Manage such server technical aspects including, but not limited to, DNS, DHCP, IP addressing, firewall configuration, remote access, core OS setup/configuration, backup/restore, security groups, trust relationships, user/group administration, admin delegation, security certificates, and web services.

- Provide direct support, operation, and maintenance of a lab that utilizes Mac and Windows desktop environments and requires maintenance of the software applications used in each environment.
- Maintain the training environment through system and software updates and maintenance of the wired and wireless network equipment.
- Operate as a liaison with the ICAC De-confliction System (IDS) operators and establish and maintain communication protocols between the Wyoming de-confliction system and IDS to naturally provide de-confliction services.
- Provide direct hardware and software support of Apple computers implemented to run desktop versions of Mac OS X and Windows to ensure that investigators perform their duties.
- Responsible for maintaining software and hardware licenses, facilitating repairs when needed, providing input and detailed specifications of the software and hardware to be used, and assisting the Task Force team leader in establishing the budget for equipment, training, and software.
- Responsible for the maintenance of the mobile forensic laboratory, operating and maintaining the interview equipment, forensic equipment, internal wired and wireless network and equipment, undercover Internet connection via a cellular carrier, evidence storage equipment, printer/copier equipment, file server, and search warrant supplies.
- The Task Force implements highly specialized equipment for recovering data from damaged or secured cell phones.

Knowledge

- Forensic knowledge of Windows, Mac, and Linux operating systems as well as forensic knowledge of common applications used in these operating systems that can contain evidence of criminal activity.
- Knowledge of the use of that equipment for performing the JTAG method to acquire data from locked cell phones.
- Knowledge and ability to perform soldering to repair and/or replace cell phone components using this equipment.
- Knowledge and understanding of Bootcamp and virtual machine environments for these functions.
- Knowledge and experience in the use of the Wyoming de-confliction systems for performing lookups of images, videos, and files related to child pornography investigations.
- Knowledge of onsite preview tools, as well as the implementation of hardware, write-blockers.
- Knowledge of capturing volatile data, such as RAM contents, from a running system.
- Knowledge and experience of Ubuntu Linux server, PHP programming, HTML coding, XML coding, SQL scripting, bash scripting, MySQL database administration, VPN server operations, and making data backups.

- Knowledge of virtual machine software, software used for conducting distributed network attacks in order to crack encrypted data, software for distributing processing of high volume data, masking system identities, restoring systems to their baseline configuration, and conducting in-depth forensic analysis of recovered data when necessary.
- Knowledge and understanding of Bootcamp and virtual machine environments.
- Knowledge of the use of highly specialized equipment for performing the JTAG method to acquire data from locked cell phones.
- Knowledge and ability to perform soldering to repair and/or replace cell phone components.
- Knowledge of data entry and collection and data reporting systems.
- Knowledge of the criminal justice system.
- Knowledge of the various criminal justice and counter-terrorism systems, programs, networks, and agencies.
- Skill in conducting subject and telephone interviews.
- Skill in computer-aided searches and database management.
- Skill in oral and written communication.
- Skill in collection, analysis, utilization, and interpretation of data pertaining to records management.
- Skill in decision-making in regard to the value of specific records.
- Ability to interpret and clearly communicate policies and procedures and statutory mandates to various criminal justice agencies.
- Ability to produce written documents with clearly organized thoughts using proper sentence construction, punctuation, and grammar.
- Ability to communicate in English by phone or in-person in a group or one-to-one setting.
- Ability to think analytically and interpret data in a variety of records systems.
- Ability to read, analyze, interpret and evaluate research findings and recommendations.
- Ability to work cooperatively with employees from other law enforcement agencies.
- Ability to organize and present accurate information in a logical sequence.