



UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH

OFFICE OF PROBATION AND PRETRIAL SERVICES

VACANCY ANNOUNCEMENT

FORENSIC EXAMINER

12-UTP-26

OPEN DATE: SEPTEMBER 1, 2026

CLOSE DATE: OPEN UNTIL FILLED

PREFERRED APPLICATION DATE: SEPTEMBER 10, 2026

The Office of Probation and Pretrial Services is accepting applications for the position of full-time Forensic Examiner. The position is a Court Personnel System classification level 27/28. This position will be located in the Salt Lake City office, with a work schedule Monday through Friday days. This position will report to the Cyber Investigation Lab Manager.

POSITION OVERVIEW:

A Forensic Examiner performs digital forensic examinations and provides technical and investigative support in cases involving defendants and persons under supervision who utilize computers, mobile devices, digital storage media, or other electronic technology as an instrument or tool for criminal activity. Such cases may involve computer fraud, hacking, stalking, credit card fraud, money laundering, counterfeiting, child sexual exploitation, identity theft, and other criminal conduct involving digital evidence.

A Forensic Examiner conducts forensic examinations of digital evidence, collects and preserves electronic evidence, prepares reports of examination findings, assists with the district's computer and internet monitoring program, and provides technical assistance and training to probation and pretrial services officers. The Forensic Examiner works closely with and assists the Cybercrime Investigation Lab Manager in the operation, development, and maintenance of the district's cybercrime investigation and digital forensics program.

REPRESENTATIVE DUTIES AND RESPONSIBILITIES:

- Conduct forensic examinations of digital evidence using established policies, procedures, forensic methodologies, and accepted techniques. Examinations may involve computers, mobile phones, tablets, digital storage devices, GPS devices, Internet of Things (IoT) devices, gaming systems, and other electronic equipment.
- Collect, preserve, image, process, and analyze digital evidence in a forensically sound manner while maintaining proper evidence handling procedures and chain of custody.
- Ensure cases are properly updated within applicable case management and tracking systems, including entries in SIRS and PACTS.
- Conduct investigations and examinations involving digital evidence associated with criminal activity, violations of conditions of release or supervision, and other matters within the responsibilities of the Office of Probation and Pretrial Services.
- Develop, prepare, and present clear and comprehensive reports detailing the procedures used, evidence examined, analytical methods employed, and findings of forensic examinations.
- Testify as necessary in court proceedings regarding the collection, preservation, examination, and analysis of digital evidence, including the procedures and methods used to obtain and analyze data and the findings of the examination.

- Assist probation and pretrial services officers with the identification, collection, preservation, and evaluation of digital evidence and provide technical guidance regarding computer- and internet-related investigations.
- Train employees within the district and, as requested, employees from other districts regarding digital forensics, evidence collection, evidence handling, chain of custody, forensic procedures, and related technical matters. Training may be provided in person or through video or teleconference.
- Assist with the district's computer and internet monitoring program, including the initial examination of electronic devices, installation and configuration of monitoring software, troubleshooting technical issues, and providing technical assistance to officers and persons under supervision.
- Perform validation and verification of forensic tools and assist in ensuring that forensic hardware and software are properly maintained, tested, updated, and suitable for use.
- Coordinate routine maintenance and troubleshooting of forensic hardware, software, workstations, and related technical equipment. Identify, diagnose, and correct technical errors and operational problems.
- Prepare and maintain technical documentation, standard operating procedures, checklists, examination protocols, and other written guidance for forensic laboratory personnel, officers, and other end users.
- Conduct periodic inventories of evidence maintained by the cybercrime investigation lab. Track evidence to determine whether continued retention is necessary and assist with the proper disposition and documentation of evidence that is no longer required.
- Ensure evidence tracking records accurately reflect the receipt, custody, transfer, retention, and disposition of digital evidence.
- Maintain knowledge of current developments in digital forensics, computer technology, cybersecurity, forensic examination techniques, investigative methods, hardware, software, and emerging technologies.
- Recommend forensic hardware, software, equipment, training, and technical resources needed to maintain effective cybercrime investigation and forensic operations.
- Assist the Cybercrime Investigation Lab Manager in researching, testing, and evaluating new forensic tools, monitoring technologies, software applications, and equipment.
- Assist the Cybercrime Investigation Lab Manager in developing, reviewing, and updating policies, procedures, protocols, and proposals related to digital evidence, forensic examinations, computer monitoring, and cybercrime investigations.
- Assist the Cybercrime Investigation Lab Manager in identifying technical and operational needs of the cybercrime investigation program and coordinating with Information Technology staff to maintain necessary technical resources.
- Assist in providing forensic services to other districts pursuant to established agreements and procedures, including receiving evidence, conducting examinations, maintaining appropriate records, and communicating regarding the status and results of examinations.
- Develop and maintain cooperative working relationships with federal, state, and local law enforcement agencies, forensic laboratories, technical professionals, vendors, and other members of the digital forensic community.
- Serve as a technical resource to probation and pretrial services officers and staff regarding digital evidence, forensic technology, cybercrime investigations, and computer and internet monitoring.
- Interpret and apply policies and procedures, statutes, Federal Rules of Criminal Procedure, the U.S. Sentencing Guidelines, the Guide to Judiciary Policy, and relevant case law in the area of specialization.

- Perform other related duties as assigned by the Cybercrime Investigation Lab Manager, Deputy Chief U.S. Probation Officer, and/or Chief U.S. Probation Officer.

QUALIFICATIONS & REQUIREMENTS:

To qualify for the position candidates must have a minimum of five years' progressively responsible experience in a related field, including a minimum of three years of specialized experience.

The successful candidate must possess a broad knowledge of the criminal justice system; knowledge of investigative techniques; strong analytical and problem-solving abilities; superior verbal and written communication skills; the ability to organize work and meet deadlines; the ability to exercise sound judgment and determine appropriate solutions to technical and investigative problems; the ability to maintain confidentiality; the ability to interact tactfully and professionally with a wide variety of individuals; and the ability to work effectively both independently and as part of a team. The successful candidate must be able to reach, bend, kneel, use a step ladder, and walk a substantial amount. Lift heavy items (up to 50 lbs.) and equipment is also required.

The successful candidate must be capable of documenting forensic processes and findings in sufficient detail to explain and support the results of an examination and, when necessary, provide testimony regarding those processes and findings.

SPECIALIZED EXPERIENCE:

Extensive experience in digital forensics, computer technology, or closely related investigative work that has provided the candidate with the knowledge, skills, and abilities necessary to successfully perform the duties of the position, including substantial knowledge and practical experience in digital forensic examination and computer technology. The following are indicative of preferred qualifications:

- Thorough knowledge of current digital forensic examination techniques, methodologies, hardware, software, and forensic tools.
- Knowledge of computers, operating systems, computer networks, mobile devices, wireless technologies, digital storage media, and other electronic systems.
- Skill in examining a variety of digital technologies, including computers, mobile phones, tablets, digital storage devices, GPS devices, IoT devices, and gaming systems.
- Ability to perform routine disassembly of desktop and laptop computers, mobile phones, tablets, and similar electronic devices when necessary for forensic acquisition or examination.
- Ability to acquire and image digital devices and storage media in a forensically sound manner.
- Ability to conduct thorough investigations and examinations involving potential criminal conduct or violations of conditions of release or supervision and accurately document investigative and forensic findings.
- Experience using industry-standard forensic software and tools, such as Magnet Forensics AXIOM, Cellebrite, or comparable forensic platforms.
- Knowledge of evidence preservation, chain-of-custody requirements, forensic documentation, and evidence retention and disposition practices.
- Ability to evaluate, validate, troubleshoot, and maintain forensic hardware and software.
- Ability to clearly document each stage of a forensic examination and prepare detailed reports explaining analytical findings.

PREFERRED QUALIFICATIONS:

Bachelor's degree from an accredited college or university in digital forensics, computer science, cybersecurity, criminal justice, information technology, or another related field that demonstrates the capacity to understand and apply the legal, technical, and investigative requirements of the position. Five years of work experience as a certified digital forensic examiner may be substituted in lieu of a bachelor's degree. Apart from education, the following are indicative of preferred qualifications:

- Prior professional experience conducting digital forensic examinations.
- Digital forensic experience within a law enforcement, court, corrections, probation, pretrial services, or other criminal justice environment.
- Completion of recognized digital forensic training or certifications, such as SCERS, MFTP, CNITP, FBI CART training, National White Collar Crime Center training, U.S. Secret Service training, U.S. Postal Inspection Service training, or equivalent programs.
- Industry certifications in cybersecurity, networking, computer systems, or related disciplines, such as CompTIA Security+, CySA+, Network+, or equivalent certifications.
- Experience providing technical or digital forensic training to law enforcement officers, investigators, probation or pretrial services officers, or other professionals.
- Experience providing testimony regarding digital forensic examinations and/or technical findings.

PERSONAL CHARACTERISTICS:

A successful candidate must be mature, responsible, poised, organized, and meticulous. Must also possess tact, good judgment, initiative and the ability to work with a wide variety of people with diverse backgrounds.

SALARY AND BENEFITS:

The salary for this position is a CL 27 (\$59,732 - \$97,098) or a CL 28 (\$71,583 - \$116,394) depending on length and relevance of experience. The position falls within the Judicial Branch of the U.S. Government and the benefits include participation in the FERS_FRAE retirement system, health, dental, vision and life insurance programs, holiday and leave accrual, tax deferred saving plan and periodic salary increases. This position is subject to mandatory direct deposit participation.

CONDITIONS OF EMPLOYMENT:

All application information is subject to verification. Appointment to this position is contingent upon a background investigation including an FBI fingerprint check. The Forensic Examiner is an excepted service position, serves at the pleasure of the court, and is an 'at will' employee who can be terminated with or without cause. All judiciary employees are required to adhere to the Judicial Code of Conduct. Applicants must be United States citizens or be eligible to work in the United States, under 8 U.S.C. § 1324b(a)(3)(B).

APPLICATION PROCEDURES:

Qualified candidates and/or transfers are invited to submit:

1. Letter of interest outlining your experience in computer technology, cybersecurity and investigations
2. Detailed resume including education, previous employment, and key career accomplishments
3. Application for Judicial Branch Employment ([AO78](#))

The application form ([AO78](#)) is available on the court's website <https://www.utp.uscourts.gov/> or at the address listed below from 9:00 a.m. to 4:30 p.m. Monday - Friday. Application packages are preferred by September 10, 2026. Incomplete applications will not be considered. Applications will be screened for qualifications and only the most qualified applicants will be contacted and selected for a personal interview. Applicants selected for interviews must travel at their own expense, and relocation expenses will not be

reimbursed. Applicants who are invited to interview may advise the Human Resources Office if an accommodation is necessary.

Please email application packages in PDF format to UTD_HumanResources@utd.uscourts.gov

Or mail or hand deliver to:

**United States District Court
Attention: HR – Forensic Examiner
351 South West Temple, Suite 2.117
Salt Lake City, UT 84101**

THE UNITED STATES DISTRICT COURT IS AN EQUAL OPPORTUNITY EMPLOYER