DUTY STATEMENT
DEPARTMENT OF JUSTICE
DIVISION OF MEDI-CAL FRAUD AND ELDER ABUSE
INVESTIGATIONS SECTION
DIGITAL FORENSICS

NAME:
CLASSIFICATION: Information Technology Specialist II
WORKING TITLE: Digital Forensic Investigator

PRIMARY DOMAIN: Information Security Engineering: The security aspects of the initiation, design, development, testing, operation, and defense of information technology data and environments.

SECONDARY DOMAIN(S): N/A

STATEMENT OF DUTIES: Under the general direction of the Information Technology Manager (ITM) I, the Information Technology Specialist (ITS) II demonstrates leadership and ingenuity in the Information Security Engineering domain, serving as a subject matter expert (SME) and skilled practitioner of advanced digital investigations and forensic examinations. The incumbent serves as a member of a team of Digital Forensic Investigators providing digital investigative and forensic services to attorneys and law enforcement officers. Focuses may include digital forensics, big data, cloud, internet of things, electronic information systems, and social media forensics. The position performs a variety of technical tasks in connection with the collection and analysis of the most complex electronic information processing systems in support of the Division of Medi-Cal Fraud and Elder Abuse (DMFEA) digital forensic work. The position is primarily responsible for conducting advanced level forensic examination, analysis, reconstruction of computing environments and research specific to the collection and preservation of digital evidence in a forensically sound manner. The ITS II identifies, documents, collects, processes, presents and preserves evidence in criminal and civil investigations, pre-litigation, and litigation matters. Examples of digital evidence and electronic media include, but are not limited to: computer hard drives, external/thumb drives, servers, cellular phones, network devices, information systems, and any other devices or media that stores and/or process digital information. The ITS II acts as part a team of law enforcement personnel.

The ITS II must exercise a high degree of initiative, independence, and confidentiality during the performance of critical and routine assignments and will provide technical expertise and project management on a wide variety of complex information technology solutions. The ITS II serves as a SME and demonstrates a high level of knowledge as it pertains to digital forensic analysis; forensic best practices; data storage and management and information security, as it relates to ensuring the integrity of the forensic process. The incumbent will make optimal recommendations for management's consideration in order to establish or improve organizational wide policies and procedures. Other duties will include but are not limited to: preparing standard forensic reports; maintaining files, peer review of casework and appearing in court in order to provide expert testimony as a SME or witness.

This position requires a high level of confidentiality as information that the ITS II will have access to may be very private, privileged or sensitive in nature. In-state and occasional out-of-state travel is required.

SUPERVISION RECEIVED: Under the general direction of the ITM I.

SUPERVISION EXERCISED: None.

TYPICAL PHYSICAL DEMANDS: Ability to work at a computer terminal for extended periods of time and to lift, carry, and move up to 20 pounds.

DUTY STATEMENT
DEPARTMENT OF JUSTICE
DIVISION OF MEDI-CAL FRAUD AND ELDER ABUSE
INVESTIGATIONS SECTION
DIGITAL FORENSICS

TYPICAL WORKING CONDITIONS: Modular workstation or laboratory setting in a smoke-free environment. Travel will be required to the DMFEA regional offices and throughout California, sometimes without advanced notice. Travel may be required out of state.

ESSENTIAL FUNCTIONS:

50% Work, as part of the investigative team, with Special Agents, Deputy Attorneys General, and technical staff to perform specialized digital forensic examinations in a lab and on-site during the service of court-ordered searches of locations. Provide forensic analysis of digital information obtained; this includes travel throughout the state for the removal and installation of electronic media, hard drives, copying of hard drives from stand alone and network computers, mapping computer systems to preserve electronic evidence, and computer forensic examination of electronic data to discover, document, collect and preserve computer-based evidence for investigations and potential prosecution.

20% Responsible for comprehensive documentation of all work performed, including, but not limited to, writing reports and applicable documentation of systems, as well as quality assurance review of case reports and documentation prepared by other digital forensic staff.

10% Collaborate and engage in on-the-job training with digital forensics staff to enhance the unit's expertise. Ensure compliance to standards, procedures, and methodologies pertaining to digital forensics. Performs "intelligence" type of activities to assist attorneys in litigations, such as social media captures and other investigative activities.

10% Coordinate communication between and conduct meetings with clients, management, supervisory, analytical and vendor/consultant staff regarding conceptual design, technical specifications, system testing and implementation, as well as policy, procedures, timelines, funding and training concerns.

5% Research software, including proprietary software, communicate with vendors and act as liaison between digital forensic staff and trusted vendors necessary for the retrieval of digital evidence.

5% Testify in criminal, civil, and administrative court proceedings as necessary.

I have read and understand the essential functions and typical physical demands required of this job (please check one of the boxes below regarding a Reasonable Accommodation):

☐ I am able to complete the essential functions and typical physical demands of the job without a need for a reasonable accommodation.
☐ I am able to complete the essential functions and typical physical demands of the job, but will require a reasonable accommodation. I will discuss my reasonable accommodation request with my supervisor.
☐ I am unable to perform one or more of the essential functions and typical physical demands of the job, even with a reasonable accommodation.
☐ I am not sure that I will be able to perform one or more of the essential functions and typical physical demands of the job, and will discuss the functional limitations I have with my supervisor.

DUTY STATEMENT
DEPARTMENT OF JUSTICE
DIVISION OF MEDI-CAL FRAUD AND ELDER ABUSE
INVESTIGATIONS SECTION
DIGITAL FORENSICS

Employee Signature	Date	Supervisor Signature	Date
Employee Name		Supervisor Name	

DEPARTMENT OF JUSTICE
DIVISION OF MEDI-CAL FRAUD AND ELDER ABUSE
INVESTIGATIONS SECTION
DIGITAL FORENSICS
DUTY STATEMENT

NAME:
CLASSIFICATION: Information Technology Specialist I
WORKING TITLE: Information Technology Specialist I

PRIMARY DOMAINS: Information Security Engineering: The security aspects of the initiation, design, development, testing, operation, and defense of information technology data and environments. Client Services: The full lifecycle of end-user device solutions, including evaluation, configuration, provisioning, training, security, tracking, and support for an end-user computing environment.

SECONDARY DOMAINS: Business Technology Management: The management of information technology resources according to an organization's priorities and needs.

STATEMENT OF DUTIES: As a full journey level analyst, performs a variety of tasks in connection with the analysis of electronic information processing systems in support of the Computer Forensics Lab. Applies a knowledge of network computer systems, including RAID technology, common communication software, including Outlook and Exchange, and familiarity with electronic e-mail systems; knowledge of different operating systems, including Windows, DOS, variations of Unix, including Linux, and Mac OS; the Internet; hardware in standalone computers; various electronic storage media including internal and external hard drives, optical technology, tape devices, large capacity cartridges, and multimedia card/flash memory; PDA and alike personal scheduling/address book/e-mail devices; data archiving technology; USB/Firewire technology; and computer and mobile forensic acquisition and analysis tools.

SUPERVISION RECEIVED: Under the general supervision of an Information Technology Supervisor II.

SUPERVISION EXERCISED: None.

TYPICAL PHYSICAL DEMANDS: Ability to move up to 25 pounds. Ability to sit and enter key strokes for up to eight hours. Ability to work extended and flexible hours within a 24-hour period. Ability to travel throughout the state at short notice.

TYPICAL WORKING CONDITIONS: Open-space office in a smoke-free environment.

ESSENTIAL FUNCTIONS:

35% Responsible for the management, maintenance, and security of computer forensic labs. Works closely with Attorneys, Special Agents and Auditors, in both lead and supporting roles, in computer examinations both in a lab and on-site during service of court-ordered searches of locations in question. This includes traveling throughout the state for the removal and installation of hard drives, copying of hard drives from standalone and network computers, mapping computer systems to determine the location of evidence, perform mobile device image acquisition and analysis, and computer forensic examination of electronic data to discover, document, collect, and preserve computer-based evidence for the prosecution and defense.

30% Applies relevant laws, penal codes, government codes, and procedures and the handling, transporting, processing, and storage of criminal evidence. Educates, trains, and assists staff on the use of specialized forensic tools, changes in technology, the law and best practices, ensuring restored evidence is forensically sound, and ensuring digital evidence for client examination is provided in a

manner not requiring this level of expertise.

20% Serves as a search warrant computer forensic lead, resolves complex problems with encryption; protects and avoids tripping defensive security devices designed to prevent law enforcement access; rebuilds suspect systems within a virtual environment and troubleshoot access issues; restores complex vendor-specific healthcare related software in order to gain access to evidence. Recovers purposely hidden data in unallocated space; understands the complex world of file headers and how they can be used to recover data; deals with and understands complex cloud based services in the performance of their functions and develops strategies for cloud access within and outside jurisdiction; serves as the advanced technical specialist, and performs ethical hacking on standalone and network systems. Responsible for the development of computer forensic network systems.

10 % Researches and validates software, including proprietary software, communicates with vendors, and obtains information from vendors necessary for the retrieval of evidence. Submits recommendations related to proposed changes in processes or programs to the Information Technology Supervisor II.

5 % Serves as an expert witness in court proceedings; renders expert opinions; testifies in criminal, civil, and administrative court proceedings as necessary. Responsible for the operation of a state-owned vehicle.

I have read and understand the essential functions and typical physical demands required of this job (please check one of the boxes below regarding a Reasonable Accommodation):

☐ I am able to complete the essential functions and typical physical demands of the job without a need for a reasonable accommodation.

☐ I am able to complete the essential functions and typical physical demands of the job, but will require a reasonable accommodation. I will discuss my reasonable accommodation request with my supervisor.

☐ I am unable to perform one or more of the essential functions and typical physical demands of the job, even with a reasonable accommodation.

☐ I am not sure that I will be able to perform one or more of the essential functions and typical physical demands of the job, and will discuss the functional limitations I have with my supervisor.

Employee Signature Date	Supervisor Signature Date
Employee Name	Supervisor Name