State of North Carolina Office of State Personnel Position Description Form (PD-102R-92)	Approved Classification:_____ Effective Date:_____ Analyst:_____ (**This Space for Personnel Department Use Only)**
1. Present Classification Title of Position Forensic Computer Agent	7. Pres. 15 Digit Pos. # /Prop. 15 Digit Pos. # 3613-0000-0002-144
2. Usual Working Title of Position Forensic Computer Agent	8. Dept., University, Commission or Agency Department of Justice
3. Requested Classification of Position Pay Grade 74	9. Institution and Division NC State Bureau of Investigation
4. Name of Supervisor	10. Section and Unit Documents & Digital Evidence Section
5. Supervisor's Position Title & Position #	11. Street Address, City and County 121 E. Tryon Road, Raleigh, Wake
10. Name of Employee	12. Location of Workplace, Bldg. and Room No. SBI Crime Lab, 1st Floor

I. A. PRIMARY PURPOSE OF ORGANIZATIONAL UNIT:

The primary purpose of the Computer Forensics Unit is to assist state and local law enforcement agencies in the analysis of computer-related evidence that may be collected in the investigation of a crime.

B. PRIMARY PURPOSE OF POSITION:

The primary purpose of the Forensic Computer Analyst position is analyze computers and computer related equipment for the evidence of the commission of a crime. This analyst is also required to present and defend the results of the analysis as an expert witness in court.

C. WORK SCHEDULE:

Regular work hours are from 8:00 AM to 5:00 PM; but after hours work is often necessary and is expected. This position is on call 24 hours a day, 7 days a week.

D. CHANGE IN RESPONSIBILITIES OR ORGANIZATIONAL RELATIONSHIP:

None.

II. A. DESCRIPTION OF RESPONSIBILITIES AND DUTIES:

Method used (Check One): Order of Importance: [**X**]
Sequential Order: [ ]

Place an asterisk (*) next to each essential function. (See instructions for complete explanation.) Please note percentage of time for each function.

* **1. CASEWORK 70 %**

This analyst in this position is required to conduct detailed laboratory examinations and analyses of computer evidence involved in criminal cases at the request of state and local authorities. These are very meticulous examinations of very fragile data. Computer forensics cases often involve very large amounts of data and can be stored on several different types of media. During a computer forensics examination an analyst is required to:

1. Conduct forensic examinations of computers and media generated by computers to develop evidence as an expert in the specialty area of forensic computer science.

2 Independently plan, organize and devise the approach necessary to obtain useful forensic information from the evidence submitted, in accordance with agency regulations, state and federal laws.

3. Use experience and knowledge of a wide variety of advanced computer technologies and theories to conduct analysis of submitted evidence and when necessary modify established procedures and develop new techniques, approaches and methods.

4. Evaluate scientific results which may be conflicting or incomplete, to determine their validity and determine whether the information has forensic significance.

5. Coordinate with other forensic disciplines within and outside the laboratory in order to develop optimal information.

A. Prepare formal written reports suitable for legal presentation which state results, interpretation and professional opinions and conclusions, being directly responsible for the accuracy and adequacy of the forensic examinations performed.

6. Travel to provide on-site expert forensic computer support at crime scenes and other areas as required.

7. Appear in state and federal courts of law to provide expert testimony.

8. Maintain state-of-the-art knowledge and technical proficiency in computer science, to include the successful participation in an annual proficiency testing program.

B. Receive, inventory and sign for physical evidence submitted for examination. Detect and resolve any accountability discrepancies according to established procedures. Mark all submitted items of evidence and maintain a chain of custody for said items.

C. Review laboratory requests to determine the type of examination needed. Review evidence and exercise independent judgement to determine the proper approach and sequence of examinations. Determine if any additional information is needed to comply with requests and obtain it by researching technical references, coordinating with other forensic computer examiners, experts, technicians and manufacturers.

9. Determine the most appropriate method of protecting original evidence and recovering deleted, erased, hidden and encrypted data.

10. Use state of the art or developed hardware and software programs to recover data, including fragmented files from damaged or altered storage devices, and when necessary modify systems, hardware, software and diagnostic tools.

11. When appropriate, use education and references to re-construct damaged or non functioning hardware by using off the shelf components or items developed by the analyst to meet original equipment specifications, to include obsolete systems for which components may not be commercially available.

12. Use, as appropriate, a variety of equipment, instruments and aids of the type normally found in a forensic laboratory.

16. Comply with laboratory and analytical practices as required in the Questioned Documents Section Quality Assurance Manual and the Computer Forensics Section Procedure Manual.

* **2. TRAINING / PROFESSIONAL DEVELOPMENT 15 %**

The analyst will be required to assist in the on-going development of new forensic procedures, technology and training related to forensic computer analysis. The analyst will also be required to supervise the training of and conduct assessments on Agent Trainees in the Computer Forensics Section. In addition, the analyst will be required to:

1) Attend and participate in relevant schools, seminars, professional societies, and training programs applicable to the position.

2) Keep current with scientific, trade and current event literature as well as other documents designed to enhance professional and personal growth in forensic computer analysis.

3) Continue to enhance the quality control procedures of the Computer Forensics Unit.

4) Conduct seminars and provide information for law enforcement personnel from around the state of the capabilities and submission criteria of the NCSBI Computer Forensics Unit.

*** 3. CALIBRATION AND MAINTENANCE OF SPECIALIZED EQUIPMENT 10%**

Due to the highly technical nature of the evidence examined in this section, this analyst must work extensively with specialized equipment. In regard to the calibration of this equipment, the duties of this analyst include:

1. Validation of any equipment used the Computer Forensics Unit.

2. Studying data generated during each examination to ensure that the equipment is functioning properly during that examination and not giving erroneous results.

3. Keeping abreast with all changes in the computer industry in order to be able to effectively examine a new kind of hardware and software which may be submitted.

4. Keep both the specialized hardware and software used in the computer forensics towers in top working order.

*** 4. COURT TESTIMONY 3%**

As a result of any analyses performed, the analyst may be required to testify as an expert witness and present a competent and unbiased court presentation to explain and defend his or her findings. This involves:

A) Being qualified each time as an expert witness based on knowledge, experience, and current proficiency;

B) Providing direct testimony which, as an expert witness, means providing the courts with an opinion based on the individual=s proven forensic judgement;

C) Securing the credibility of this testimony under cross examination, which may involve the use of opposing Aexperts@;

D) Related travel, preparation of court exhibits, and the review of casework.

*** 5. TECHNICAL FIELD ASSISTANCE 2%**

This analyst may be called upon to help in the serving of search warrants or in conducting computer forensic examinations outside of the Laboratory. The analyst is required to know the proper procedures for seizing computer equipment and examining the equipment on site without damaging the integrity of the evidence.

6. OTHER

As required.

III. A. OTHER POSITION CHARACTERISTICS:

1. ACCURACY REQUIRED IN WORK

The need for precision, accuracy, and exactness are 100% and cannot be over-emphasized. Each case and each examination can determine the fate of an individual or the successful investigation of a serious crime.

2. CONSEQUENCE OF ERROR

Any errors committed during a computer forensic examination may lead to the conviction of an innocent person or set a guilty suspect free. Failing to accurately locate and preserve computer evidence may result in a guilty suspect going undetected and can lead to the commission of additional crimes by that suspect, and, in worst cases, to the loss of life of an additional victim(s).

3. INSTRUCTION PROVIDED TO EMPLOYEE

Employee functions with considerable autonomy, and receives no regular instructions for daily work performed.

4. GUIDES, REGULATIONS, POLICIES AND REFERENCES USED BY EMPLOYEE

Preparation and application guidelines for most technical procedures are outlined in lab manuals. Other guidelines may include instrument handbooks, agency policy, laws and regulations and other reference files. New developments may appear in technical reference materials and journals and can be utilized as a basis for bringing new methods of analysis to the attention of superiors.

5. SUPERVISION RECEIVED BY EMPLOYEE

Employee functions with a considerable degree of autonomy. Technical supervision is provided in only rare cases.

6. VARIETY AND PURPOSE OF PERSONAL CONTACT

The position is routinely in contact with persons both inside and outside of state government. Sources of contact include:

a. Other SBI personnel
b. Other state level law enforcement officers
c. State court officials (including District Attorneys)
d. City and county law enforcement officers
e. Federal court officials
f. Professionals in academic and scientific organizations
g. Defense attorneys/opposing experts
h. Victims/Witnesses
i. Business professionals (vendors, etc.)

7. PHYSICAL EFFORT

With the exception of crime scene activities, physical effort is generally minimal.

8. WORK ENVIRONMENT AND CONDITIONS

Working conditions are usually a laboratory or office setting but will include court rooms and crime scenes of all types.

9. MACHINES, TOOLS, INSTRUMENTS, EQUIPMENT, AND MATERIALS USED

This analyst examines computers, computer media, or other computer-related equipment (example: digital cameras or personal organizers) seized in criminal cases. The use of various hand tools is required to open submitted computers and remove internal components for examination. A knowledge of computer components is required.

10. VISUAL ATTENTION, MENTAL CONCENTRATION AND MANIPULATIVE SKILLS

It is very important that this analyst possess both good visual attention and mental concentration. Computer investigations are often very long and tedious. Finding the information pertinent to the case often requires the examination of large amounts of text and data. Good attention and concentration are important in making sure that important information is not overlooked.

11. SAFETY FOR OTHERS

This analyst must keep the safety of himself and his fellow officers in mind when serving search warrants. Suspects can be combative and uncooperative when confronted with a search warrant. Suspects can also booby trap computer components with the intention of destroying incriminating data and/or injuring officers.

12. DYNAMICS OF WORK

The analyst has no control over the amount of casework submitted and periods of heavy workload and mounting deadlines exist routinely. In addition, the methodology and technology related to the analysis of computer forensic evidence are changing constantly. The analyst must maintain a constant awareness of these changes.

When necessary, specialized instrumentation must be maintained and repairs effected or repair calls must be scheduled. This could occur at any time and require the analyst=s immediate attention.

At times, special projects are assigned that may supersede the analyst=s regular work assignments.

IV. KNOWLEDGE, SKILLS & ABILITIES AND TRAINING & EXPERIENCE REQUIREMENTS

A. KNOWLEDGE, SKILLS AND ABILITIES

5. Mastery of technology and theory related to information systems hardware and software, telecommunication, systems networks and network architecture, and investigative procedures at a level to serve as an expert forensic examiner in identifying the value of computer-related evidence, applying methods for detection of criminal activity, developing proof of criminal activity, and preparing reports of examinations and findings for use in court proceedings.

6. In-depth knowledge of investigative techniques, theory and the ability to adapt methods to information systems environment at a level to provide expert advice and consultation on ongoing criminal investigations and judicial actions.

7. A working knowledge of the methods, procedures and practices used in the investigation of criminal offenses, and of the principles of securing and identifying a variety of crime related evidence, rules of search and seizure and related investigative matters especially as it relates to computer crime.

8. Comprehensive knowledge of computers, computer systems including operating systems such as DOS, Windows 95/98/NT, UNIX, LYNIX, etc, and data recovery from these systems.

9. Understanding of the principles and theories associated with data storage and retrieval, encryption and decryption.

6. The ability to investigate a variety of criminal cases, to interpret and apply criminal laws of North Carolina in investigations, to make arrests, to prepare comprehensive and detailed reports pertaining to individual cases, to present effective court testimony, and to apply the principles, techniques and procedures of modern criminal investigation.

7. The ability to use firearms and tools and equipment involved in evidence collection and preservation effectively.

8. Maintain a physical condition which permits certification by the North Carolina Justice Standards Commission for law enforcement officers.

9. Extensive knowledge of the principles, concepts, theories, reference sources and laboratory practices involved with the forensic examination.

10. Working knowledge of scientific methodology and of laboratory safety practices.

11. Ability to conduct analyses in the more difficult and complex cases.

12. Ability to assist in the administration of specialized technical training to other Forensic Analysts.

13. Ability to conduct routine procedures, analyze results, interpret methodology and to solve theoretical problems.

14. Ability to work productively with laboratory personnel and other law enforcement personnel.

B. 1. REQUIRED MINIMUM TRAINING

Graduation from a four-year college or university, preferably with a major in computer science, forensic science or forensic studies.

2. ADDITIONAL TRAINING/EXPERIENCE

Satisfactory completion of the SBI Academy including state mandated BLET - or equivalent to meet state certification standards.

3. EQUIVALENT TRAINING AND EXPERIENCE

Maybe considered.

C. LICENSE OR CERTIFICATION REQUIRED BY STATUTE OR REGULATION:

Each SBI Agent is a certified law enforcement officer and meets those standards set by the Justice Standards Commission.

V. CERTIFICATION: Signatures indicate agreement with all information provided, including designation of essential functions.

Supervisor's Certification: I certify that:

a. I am the Immediate Supervisor of this position; that
b. I have provided a complete and accurate description of responsibilities and duties; and
c. I have verified (and reconciled as needed) its accuracy and completeness with the employee.

Signature: Title: Date:

Employee's Certification: I certify that I have reviewed this position description and that it is a complete and accurate description of my responsibilities and duties.

Signature: Title: Date:

Section or Division Manager's Certification: I certify that this position description, completed by the above named immediate supervisor, is complete and accurate.

Signature: Title: Date:

Department Head or Authorized Representative's Certification: I certify that this is an authorized, official position description of the subject position.

Signature: Title: Date:
