

STATE OF OHIO (DAS) CLASSIFICATION SPECIFICATION	<b>CLASSIFICATION SERIES:</b> Forensic Computer Specialist	<b>SERIES NO.:</b> 6716AG
	<b>MAJOR AGENCIES:</b> Attorney General Only	<b>EFFECTIVE DATE:</b> 10/07/01

**SERIES PURPOSE:**

The purpose of the forensic computer specialist occupation is to perform highly specialized forensic analysis of seized evidence and generate reports of findings for use in the prosecution of criminal offenses.

At the first level, incumbents utilize specialized tools and procedures to collect, preserve and examine computer related evidence and assist higher-level forensic computer specialists as assigned. At the second level, incumbents independently develop and utilize specialized tools and procedures to collect, preserve and forensically examine computer related evidence and assist investigators in field investigations as assigned.

Note: Class developed exclusively for use by Office of Attorney General.

**CLASS TITLE:**

Forensic Computer Specialist 1

**CLASS NUMBER:**

67161AG

**EFFECTIVE DATE:**

10/07/01

**CLASS CONCEPT:**

The full-performance level class works under general supervision & requires considerable knowledge of information technologies & computer hardware & software specifications in order to utilize specialized tools & procedures to collect, preserve & examine computer related evidence.

**CLASS TITLE:**

Forensic Computer Specialist 2

**CLASS NUMBER:**

67162AG

**EFFECTIVE DATE:**

10/07/01

**CLASS CONCEPT:**

The advanced level class works under direction & requires thorough knowledge of information technologies & computer hardware & software in order to independently develop & utilize specialized tools & procedures to collect, preserve & forensically examine computer related evidence.

<b>CLASS TITLE:</b> Forensic Computer Specialist 1	<b>CLASS NUMBER:</b> 67161AG	<b>BARGAINING UNIT:</b> 47
---	---------------------------------	-------------------------------

**EFFECTIVE DATE:**

10/07/01

**JOB DUTIES IN ORDER OF IMPORTANCE: (These duties are illustrative only. Incumbents may perform some or all of these duties or other job-related duties as assigned.)**

Utilizes specialized tools (e.g., evidence acquisition devices; automated floppy diskette reader) & procedures to collect, preserve & examine (e.g., prepares duplicate images backup copies; recovers deleted &/or corrupted files, password protected &/or encrypted files; recovers hidden data; traces internet & network communications) computer evidence of criminal offenses (e.g., homicides & assaults, rape, gross sexual imposition, corruption of minor, disseminating matter harmful to juveniles, pandering sexually oriented matter involving minor(s) & illegal use of minor in nudity-oriented material or performance, aggravated arson, burglary cases, illegal access to hospital files, wire tapping of citizens by law enforcement personnel, illegal traffic/access into military establishments, money laundering, theft & fraud & counterfeiting) in accordance with established & validated forensic principles, develops & implements policies & procedures relating to seizure & examination of evidence from computer systems, reviews & updates policies & procedures on regular basis in order to ensure policies support new computer technology, makes procedural suggestions to & reviews procedural suggestions received from other law enforcement jurisdictions statewide, researches & implements tools which image drives (i.e., of original computer evidence) prior to examination & provides training to law enforcement agencies statewide, prepares reports of findings for presentation in criminal case proceedings & testifies as required, confers with higher-level forensic computer specialist to determine appropriateness of procedures &/or products, receives, maintains & releases evidence in accordance with evidence handling procedures, maintains electronic & hard copies of evidence transfers & assists higher-level forensic computer specialists as assigned.

Tests computer program according to procedural specifications; designs, configures & maintains computer hardware for use in case work & program development; resolves technical issues involving equipment connectivity & communication; drafts & follows up on purchase order requests; executes verification tests of forensic software & methods to independently validate functionality; collects information from investigators &/or prosecutors & confers with higher-level forensic computer specialist to determine best forensic analysis strategy.

Attends seminars & classes for training in specialized forensic software applications, forensic analysis techniques & other specialized areas; participates in professional networking forums.

**MAJOR WORKER CHARACTERISTICS:**

Knowledge of computer systems & technology (e.g., systems administration; network security; internet protocol); interviewing\*; human relations\*. Skill in operation & configuration of personal computer systems & peripheral equipment. Ability to deal with many variables & determine specific action; resolve technical issues involving many variables; gather, collate & classify information; handle sensitive inquiries from & contacts with other law enforcement agencies & general public; demonstrate dexterity to move fingers & limbs to easily perform manual functions repeatedly.

(\*) Developed after employment.

**MINIMUM CLASS QUALIFICATIONS FOR EMPLOYMENT:**

Completion of associate core program in computer forensics (e.g., information technology or related scientific discipline systems administration; network security; internet protocol).

-Or 24 mos. exp. in computer forensic processing or related specialty area (e.g., systems administration; network security; internet protocol).

-Or equivalent of minimum class qualifications for employment noted above.

**TRAINING AND DEVELOPMENT REQUIRED TO REMAIN IN THE CLASSIFICATION AFTER EMPLOYMENT:**

Not applicable.

**UNUSUAL WORKING CONDITIONS:**

May require travel.

<b>CLASS TITLE:</b> Forensic Computer Specialist 2	<b>CLASS NUMBER:</b> 67162AG	<b>BARGAINING UNIT:</b> 47
---	---------------------------------	-------------------------------

**EFFECTIVE DATE:**

10/07/01

**JOB DUTIES IN ORDER OF IMPORTANCE: (These duties are illustrative only. Incumbents may perform some or all of these duties or other job-related duties as assigned.)**

Independently develops & utilizes specialized tools (e.g., portable forensic workstations; first responder imaging & examination disks; evidence acquisition devices; automated floppy diskette reader & procedures to collect, preserve & forensically examine (e.g., prepares duplicate images backup copies; recovers deleted &/or corrupted files; recovers password protected &/or encrypted files; recovers hidden data; traces internet & network communications), computer related evidence of criminal offenses (e.g., homicides & assaults, rape, gross sexual imposition, corruption of minor, disseminating matter harmful to juveniles, pandering sexually oriented matter involving minor(s) & illegal use of minor in nudity-oriented material or performance, aggravated arson, burglary cases, illegal access to hospital files, wire tapping of citizens by law enforcement personnel, illegal traffic/access into military establishments, money laundering, theft & fraud & counterfeiting) in accordance with established & validated forensic principles, develops & implements policies & procedures relating to seizure & examination of evidence from computer systems, reviews & updates policies & procedures on regular basis in order to ensure policies support new computer technology, makes procedural suggestions to & reviews procedural suggestions received from other law enforcement jurisdictions statewide, researches & implements tools which image drives (i.e., of original computer evidence) prior to examination & provides training to law enforcement agencies statewide, assists investigators in preparation for seizure of computer evidence related to criminal activity, accompanies & assists investigators in field investigations as assigned, conducts interviews with investigators, victims & other informed persons to ascertain facts pertinent to criminal case, determines best forensic analysis strategy, prepares reports of findings for presentation in criminal case proceedings & testifies as required, confers with prosecuting attorneys, receives, maintains & releases evidence in accordance with agency handling procedures & assures security of seized evidence.

Designs, configures & maintains complex computer hardware for use during evidence acquisition & analysis; resolves complex technical issues involving equipment connectivity & communications between suspect system & forensic equipment; identifies, researches & evaluates computer equipment & software; drafts & follows up on purchase order requests; provides assistance to federal, state & local law enforcement agencies in matters involving computer related crime & forensics.

Attends seminars & classes for training in specialized forensic software applications, forensic analysis techniques & other specialized areas; participates in professional networking forums; executes verification tests of forensic software & methods to independently validate functionality; trains investigators, law enforcement officials & lower-level forensic computer specialists in specialty areas of computer related crime & forensic techniques.

**MAJOR WORKER CHARACTERISTICS:**

Knowledge of computer systems & technology; interviewing\*; human relations\*. Skill in operation & configuration of personal computer systems & peripheral equipment. Ability to analyze, collate & classify information; resolve technical issues involving many variables; handle sensitive inquires from & contacts with other law enforcement agencies & general public; demonstrate dexterity to move fingers & limbs to easily perform manual functions repeatedly.

(\*)Developed after employment.

**MINIMUM CLASS QUALIFICATIONS FOR EMPLOYMENT:**

Completion of undergraduate core program in computer information sciences, information systems, computer science or related technology discipline (e.g., systems administration; network security; internet protocol); 160 hours trg. specific to computer forensic science &/or security.

-Or 36 mos. exp. in computer forensic processing or related specialty area (e.g., systems administration; network security; internet protocol).

-Or 12 mos. exp. as Forensic Computer Specialist 1, 67161AG.

-Or equivalent of minimum class qualifications for employment noted above.

**TRAINING AND DEVELOPMENT REQUIRED TO REMAIN IN THE CLASSIFICATION AFTER EMPLOYMENT:**

Not applicable.

**UNUSUAL WORKING CONDITIONS:**

May require travel.