Career Opportunities: Cyber Forensics Investigator (P-3) (22499)

Requisition ID **22499** - Posted **02/11/2022** - **Professional - Information Technology / Computer Science - The Hague - NL**

Job Description Print Preview

Apply | Save Job | Email Job to Friend | Return to List

22499 | OTP

Deadline for applications:	30/11/2022
Position title and level	Cyber Forensics Investigator (P-3)
Organisational unit	Cyber Unit, IKEMS, Integrated Services Division, Office of the Prosecutor
Duty station	The Hague - NL
Type of appointment	Fixed-term
Post number	Established post (S-9144)
Minimum net annual salary	€87,213.00
Contract duration	For initial appointments, the Court offers a two-year appointment with the possibility of extension (six months probationary period).

A roster of suitable candidates may be established for this post as a result of this selection process for both fixed-term established and general temporary assistance posts.

Organisational Context
The Information, Knowledge and Evidence Management Section (IKEMS), headed by an Information Management Coordinator, reports directly to the Prosecutor, and combines the Office of the Prosecutor's (OTP) information, knowledge and evidence management operations into one consolidated section. IKEMS aims to maintain a coordinated, flexible and operationally responsive IKEM support capacity throughout the OTP, in order to support the full spectrum of OTP information and evidence operations.

The position of Cyber Forensics Investigator is part of the Cyber Unit (CU) of the Information, Knowledge and Evidence Management Section (IKEMS) which:

(a) Provides user and information management support to OTP core businesses and systems such as investigations and witness management;
(b) Conducts comprehensive business analyses, process mapping, requirements gathering, as well as business needs assessment exercises on behalf of the Prosecutor for all OTP business streams and leads a balanced and transparent approach toward OTP business development and innovation;
(c) Supports OTP business development initiatives by ensuring continuous and recurring in-house program and project evaluation, as well as intra and inter-Organ sharing of lessons learnt in relation to IKEM;
(d) Drafts and maintains the OTP's IKEM strategic plan, as well as forecast assessments of IKEM-related developments which may impact OTP core business or operations;
(e) Supports existing knowledge- and information-management systems, business processes and eLearning needs within the Office by acting as the primary OTP knowledge broker in the IKEM area.

Duties and Responsibilities
Under the direct supervision of the Head of Cyber Unit and the overall management of the Information Management Coordinator, the incumbent will perform the following tasks:

- Advise operational investigators on the safest way to conduct online investigations, as well as on the availability and reliability of digital evidence;
- Carry out specialized digital forensic examination to acquire digital evidence from computers and other storage devices, including mobile phones or tablet devices, perform specialized digital forensic analysis and deliver digital forensic reports and support; to manage, supervise, monitor, assist or participate in required field activities;
- Reinforce the leading position of the Cyber Unit as the main provider of digital forensics and associated disciplines to the ICC/OTP, and as a cyber forensic adviser for external clients;
- Provide training to first responders/operational investigators;
- Participate in the creation of operational forensic capabilities regarding cyber forensic methodologies, digital forensic equipment, digital forensic networks, cyber forensic support to investigation/prosecution teams in compliance with international quality standards;
- Advise and assist the Head of the Cyber Unit on all digital forensics-related matters, procedures and techniques. Participate in specialized cyber forensic international network;
- Perform any other duties as required.

Essential Qualifications
Education:
Advanced university degree in information and communication technology in the field of digital, cyber or security forensics. A first level university degree in combination with two additional years of qualifying experience is accepted in lieu of an advanced university degree.

Professional certifications in digital, cyber or security forensics, would be considered an advantage.

Experience:
At least 5 years of experience (7 years with a first-level university degree) in cyber forensic investigations/examinations, with a special focus on complex, large-scale cases and operations, working in a governmental or inter-governmental agency, scientific police institute, ad hoc international tribunals, international fact finding commissions, criminal sciences school or as a private expert, is required.

In addition,
Experience in the execution and/or coordination of vast specialized cyber forensic operations is preferred.

Knowledge, skills and abilities:
- Extensive knowledge of the newest digital forensic techniques (acquisition and analysis) applied to hard drives, networking and encryption, principles and techniques of cyber security investigation, etc. is required;

- Excellent ability to organize complex and voluminous sets of records and facts as well as the ability to execute various forensic tasks is required;
- Excellent ability to communicate effectively with police, forensic, academic or other relevant networks;
- Ability to work under stressful conditions and in a volatile environment;
- Ability to work in a non-discriminatory manner, with respect for diversity;
- Professional and personal integrity.

Knowledge of Languages:
Proficiency in one of the working language of the Court, English or French, is essential. Working knowledge of the other is desirable. Knowledge of another official language of the Court (Arabic, Chinese, Russian and Spanish) would be considered an asset.

ICC Leadership Competencies
Purpose
Collaboration
People
Results
ICC Core Competencies
Dedication to the mission and values
Professionalism
Teamwork
Learning and developing
Handling uncertain situations
Interaction
Realising objectives

Learn more about ICC leadership and core competencies.

General Information
- The selected candidate will be subject to a Personnel Security Clearance (PSC) process in accordance with ICC policy. The PSC process will include but will not be limited to, verification of the information provided in the personal history form and a criminal record check.

- Applicants may check the status of vacancies on ICC E-Recruitment web-site.
- Post to be filled preferably by a national of a State Party to the ICC Statute, or of a State which has signed and is engaged in the ratification process or which is engaged in the accession process, but nationals from non-state parties may also be considered.
- In accordance with the Rome Statute, the ICC aims to achieve fair representation of women and men for all positions, representation of the principal legal systems of the world for legal positions, and equitable geographical representation for positions in the professional category.
- Applications from female candidates are particularly encouraged.
- The Court reserves the right not to make any appointment to the vacancy, to make an appointment at a lower grade, or to make an appointment with a modified job description.