



The Hague, 15 March 2013

Reg. n°: Europol/2013/TA/AD7/121

VACANCY NOTICE

Name of the post: Senior Specialist - Forensic investigator in the EC3 Forensic Laboratory (AD7)

Reporting to: Manager of the Research and Development team in the European Cybercrime Centre (Operations)

1. About Europol and the European Cybercrime Centre (EC3)

Applications are invited for this position at the European Police Office (Europol).¹

Europol is located in The Hague, The Netherlands, and its main tasks are the following:

- a) to collect, store, process, analyse and exchange information and intelligence;
- b) to aid investigations in the Member States, in particular by forwarding all relevant information to the national units;
- c) to ask the competent authorities of the Member States concerned to initiate, conduct or coordinate investigations and to suggest the setting up of joint investigation teams in specific cases;
- d) to provide intelligence and analytical support to Member States in connection with major international events;
- e) to prepare threat assessments, strategic analyses and general situation reports relating to its objective, including organised crime threat assessments.

Following the Commission's communication "*Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*" (8543/12), the Council endorsed on 6 June 2012 the setting-up of such a centre at Europol. The European Cybercrime Centre (EC3) will be part of Europol's existing structure to facilitate cross-working with other crime areas.

The EC3 started activities in January 2013 to 'serve as the European cybercrime information focal point' in the fight against cybercrime in the European Union, and deliver operational and investigative support to the Member States on cybercrime. One of the facilities providing support will be the forensic laboratory, for which this senior specialist is recruited.

For more information please visit Europol's website www.europol.europa.eu.

Europol applies a policy of equal opportunity for men and women and accepts applications without distinction on ground of sex, race colour, ethnic or social origin, genetic characteristics, and language, religious, political or other convictions and opinions, financial situation, disability, age sexual orientation, marital status or family situation. Applications from female candidates are particularly encouraged. Employment at Europol is open to nationals of the EU Member States. There is no national quota system in operation but Europol is required to strive for a broad range of nationalities in order to keep a well balanced geographical distribution among its staff members.

¹ Europol has been established under the Council Decision (EC) No. 2009/371 of 6 April 2009.

2. Background and purpose of the post

The European Cybercrime Centre (EC3) is one of four business areas in the Europol Operations Department (OD), which is responsible for delivering operational and investigative support to the services in the Member States competent to fight organised crime and terrorism.

EC3 is a multi-disciplinary and multi-purpose centre integrated by 2 groups: the first group is Operations, fighting on-line criminal activities in the fields of child sexual exploitation, fraud and cyber intrusion.

The second group is in charge of Strategy and Development. The Strategy and Development group is composed by two teams, the first one in charge of Strategy, Outreach and Communication and the second one in charge of Research and Development.

The forensic laboratory is part of the second team. In the implementation process of EC3, during 2013 new forensic facilities and equipment will be added to the existing resources. The forensic expert to be recruited will be a member of the new EC3 laboratory.

Under the supervision of the Team Leader, the successful candidate will be responsible for forensic analysis, delivery of digital forensic reports and support.

In addition to the recruited person, the process can establish a reserve list for future appointment of successful candidates to future vacancies with the same profile.

3. Tasks and responsibilities

The successful candidate(s) will have to carry out the following duties:

- Advise operational investigators on the availability and reliability of digital evidence;
- Carry out specialised forensic examination to acquire digital evidence from computers and other data storage devices;
- Deliver cyber forensic reports;
- Perform on-the-spot technical support to investigations;
- Ensure the availability of up-to-date information for the operational areas of the EC3;
- Participate in specialised forensic networks with Europol-EC3 Partners;
- Provide training to cyber investigators;
- Liaise with the relevant competent authorities in the Member States and third parties involved as appropriate;
- Perform any other tasks in the area of competence as assigned by the management of the EC3.

4. Requirements

4.1 Eligibility criteria:

a. Candidates must:

- Be a national of one of the Member States of the European Union and enjoy full rights as a citizen;

Europol Public Information

- Have fulfilled any obligations imposed by the applicable laws on military service;
- Produce appropriate character references as to his or her suitability for the performance of the duties;
- Be physically fit to perform the duties pertaining to the position;²
- Produce evidence of a thorough knowledge of one of the languages of the Union and a satisfactory knowledge of another language of the Union to the extent necessary for the performance of the duties.

b. Candidates must have:

- A level of education which corresponds to completed university studies, preferably in the area of Computer Science or Information Technology, attested by a diploma when the normal period of university education is 4 years or more;

OR

A level of education which corresponds to completed university studies, preferably in the area of Computer Science or Information Technology attested by a diploma and appropriate professional experience of at least 1 year when the normal period of university education is 3 years.

OR

Professional training of an equivalent level in a relevant area (e.g. certification in computer forensics or cyber security training) and -after having completed the training- at least the number of years of relevant professional experience as indicated in the table below:

Duration of professional training	Professional experience
Up to 1 year	4 years
More than 1 year and up to 2 years	3 years
More than 2 years and up to 3 years	2 years
More than 3 years	1 years

- **In addition** to the above, at least **6** years of relevant professional work experience gained after the award of the diploma/certification.

4.2 Selection criteria:

a. Professional experience:

Essential:

- Hands-on support for at least 4 years in cyber security investigations;
- Broad case work experience employing digital forensics; "post mortem" and live forensic situations.

Desirable:

- Experience with international cooperation;
- Experience working in a computer laboratory environment;
- Forensic instructor/trainer experience;
- Membership of a forensic association;

² Prior to appointment the successful candidate will be medically examined by one of the institution's medical officers in order that the institution may be satisfied that the candidate fulfils the requirements of Article 12(2)(d) Conditions of Employment of Other Servants of the European Union (CEOS)

Europol Public Information

- Law enforcement knowledge or background.

b. Professional knowledge:

Essential:

- Deep knowledge of the newest digital forensic techniques (acquisition and analysis) applied to hard drives, networking and encryption;
- Knowledge of the principles and techniques of cyber security investigation;
- Updated knowledge of the latest trends and technical developments accredited by recent certifications.

Desirable:

- University degree relevant for the tasks and responsibilities of the post (Computer Engineering, Computer Science, Software Engineering or related field).

c. Technical skills and competencies:

Essential:

- Deep knowledge on common file systems, operating internal systems and application level services/implementation artefacts;
- Knowledge on computer system intrusion, network fundamentals and database technologies;
- Knowledge on hex dump analysis and volatile memory analysis;
- Knowledge of programming/scripting e.g. Python, Bash, Perl.

Desirable:

- Knowledge of cloud computing – Big data and data mining.

c. Organisation and communication skills:

Essential:

- Good communication skills in English, both verbally and in writing;
- Good reporting skills on technical matters;
- Good organisational skills including the ability to establish clear priorities, exercise initiative and work in a team;

Desirable:

- Good presentation skills;
- Ability to manage projects.

d. Social skills and competencies:

Essential:

- Excellent interpersonal skills with the ability to work well under pressure;
- High passion for IT security;
- Ability to work effectively in an international and multi-cultural environment;
- Stress resistance;
- High degree of commitment and flexibility.

5. Selection procedure

The Contracting Authority sets up a Selection Committee which consists of at least three members, one from the Human Resources Unit of Europol, one from the concerned Unit or Department and one designated by the Staff Committee.

For **non-restricted** posts the Contracting Authority may designate up to two additional members to the Selection Committee on a proposal from the Management Board, either from another service of Europol, from outside Europol or from outside the community institutions including Member States.

The Selection Committee determines candidates' suitability for the position by assessing their skills, experience and qualifications against the established job profile and makes an initial selection from the applications received.

Shortlisted applicants are invited to participate in a post-related selection procedure, generally consisting of written and/or practical tests and competency-based interviews.

The Contracting Authority makes a decision of appointment on the basis of advice from the Selection Committee. He will inform the Committee of his decision. All candidates who attend the selection procedure will be informed of the outcome.

Candidates who attended a selection procedure may request feedback on their performance of the written test and interview within three months after the selection procedure. Europol will not be in a position to respond to feedback inquiries received outside this time frame.

The Selection Committee's work and deliberations are confidential. It is forbidden for candidates to make direct or indirect contact with the members of the Selection Committee or for anyone to do so on their behalf. All enquiries or requests for information or documentation in relation to the competition should be addressed to the Europol Recruitment Office.

6. Salary

Scale: AD7

The basic monthly salary is EUR **5 568, 11** (step 1) or EUR **5 802, 09** (step 2).

The step in grade is determined on the basis of professional experience gained after the education required for the position and in line with applicable implementing rules.

In addition, if applicable, allowances such as expatriation allowance, household allowance, dependent child and education allowance may be granted.

Europol offers a comprehensive welfare package comprising additional benefits such as medical insurance, unemployment and invalidity allowance as well as a pension scheme.

Salaries are subject to a community tax but exempt from national taxation.

7. Terms and conditions

7.1 Probation period

Engagement for this position is subject to the successful completion of a probationary period of 6 months.

Europol reserves the right to terminate the contract of employment during or at the end of the probation period in accordance with Article 14 of CEOS.

7.2 Security screening and certificate of good conduct

The successful candidate(s) shall obtain a Personal Security Clearance Certificate (PSCC) at the level indicated in the Vacancy Notice. Europol will support all candidates who successfully passed the selection procedure. A PSCC is a certificate issued by a competent authority establishing that an individual is security cleared. It contains: the level of clearance; the date of issuance and the date of expiry. **The PSCC must be provided to Europol prior the signature of the employment contract.**

The requested level of Security Clearance for this post is: CONFIDENTIEL UE / EU CONFIDENTIAL.

7.3 Contract of employment

The successful candidate will be recruited as Temporary Agent AD 7 pursuant to Article 2 (a) of CEOS, for a period of 5 years³ (full-time – 40 hours a week).

The contract may be renewed. The place of employment will be The Hague, The Netherlands.

For further information on terms and conditions please consult the EC Staff Regulations which are available on Europol's website www.europol.europa.eu.

8. Data protection

The data submitted is processed in order to assess the suitability of candidates for a position at Europol. All personal data collected for the purpose of the selection procedure will only be used within this specific context and will not be disclosed to any third party, except for restricted posts in which the application may be transmitted to the National Unit and the respective Liaison Bureau.

Any data provided will be treated in strict confidence and in full compliance with all applicable data protection rules. The legal basis for the processing of personal data are the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union (Title III Chapter 1) and their implementing rules.

All documents provided to Europol will be kept in Europol's files and will not be returned to the candidate. Applications of non-recruited candidates will be kept for a maximum of two years. Data of non-recruited applicants on the reserve list for appointment will be kept for a maximum of two years after the expiry of the reserve list. Data of recruited candidates will be transferred to their personal file.

The Head of the Administration Business Area is responsible for the data processing operation. Candidates have the right to access, rectify, block and erase their personal data in accordance with the applicable data protection rules.

Candidates have the right of recourse to the Europol Data Protection Office (Data Protection Office - PO Box 90850, 2509 LW The Hague, The Netherlands) and the Joint Supervisory Body (www.europoljsb.consilium.europa.eu). Applications sent to the DPO or JSB will not be processed and will be deleted.

³ For the internal candidates the duration of the current contract will be taken into account in the total duration of the contract

9. Additional information

9.1 Main dates

Deadline for application: **24 April 2013**
Recruitment procedure: **May/June 2013**

9.2 Application process and selection procedure

Please refer to the EUROPOL RECRUITMENT GUIDELINES available on Europol's website www.europol.europa.eu for further details on the application process and the selection procedure.

9.3 Contact details

For further details on the application process please call +31 (0) 70 353 1583 or +31 (0) 70 353 1679.