Guidelines on Digital Forensic Procedures for OLAF Staff

1 January 2014

Introduction

The OLAF Guidelines on Digital Forensic Procedures are internal rules which are to be followed by OLAF staff with respect to the identification, acquisition, imaging, collection, analysis and preservation of digital evidence. The aim of these Guidelines is to establish rules for conducting digital forensic operations in a manner that ensures the integrity and the chain of custody of potential evidence to be admissible in administrative, disciplinary and judicial procedures. They are designed to implement Article 4(2) of Regulation (EC) 883/2013 and Article 7(1) of Regulation (EC) 2185/96.

The purpose of a digital forensic operation is to secure potential digital evidence by creating a forensic image of digital media relevant for an OLAF investigation. As digital forensic operations often involve the collection of large amounts of data, including personal data, they may be privacy invasive. These Guidelines are therefore also designed to help ensure compliance with data protection provisions in the context of digital forensic operations. They complement the Instructions to Staff on Data Protection (ISDP).

These guidelines take internationally approved standards and good practices into account, such as the ISO Standard 27037 on "Guidelines for identification, collection, acquisition and preservation of digital evidence", adopted in October 2012, and the "Good practice guide for digital evidence" published by the UK Association of Chief Police Officers (APCO) in March 2012.

Article 1. Definitions

The terms defined in this section are used throughout the remainder of this document.

1.1 EU staff: Any official or servant of the EU institution, body, office or agency (IBOA) concerned.

1.2 Digital forensics: The application of digital investigation and analysis techniques to perform a structured examination of a digital storage medium, while maintaining a documented chain of evidence, for the purpose of gathering information admissible in evidence in a court of law or in a disciplinary procedure.

1.3 Digital Evidence Specialist (DES): OLAF staff with specialised technical expertise to perform digital forensic operations and to prepare related reports.

1.4 Digital forensic operation: A technological inspection, acquisition, and examination of digital media and/or their contents, carried out by DES's using forensic equipment and software tools. The objective is to locate, identify, collect and/or acquire data which may be relevant to an investigation, and may be used as evidence in administrative, disciplinary and judicial procedures.

1.5 Preview: A first inspection of a digital medium using an appropriate forensic tool in order to establish whether it may contain data potentially relevant to the investigation.

1.6 Digital forensic collection: The process of gathering the physical devices that contain potential digital evidence.

1.7 Digital forensic acquisition: The acquisition of any data (including deleted data) stored on a digital medium through a forensic imaging process.

1.8 Digital forensic image: The forensic (bitwise) copy of original data contained on a digital storage medium, acquired during a digital forensic operation and stored in binary format with a unique hash value.

1.9 Hash value: A digital fingerprint of the data which helps to verify the integrity of a copy. It is a fixed length computational result generated from a string of data (e.g. files, directories, an entire hard disk) using a specific mathematical algorithm that creates a unique value.

1.10 Digital forensic work file: A copy of the digital forensic image on which all searches and analyses are done in the OLAF forensic laboratory.

1.11 Digital forensic evidence file: A complete set of electronic data created by the DES during the digital forensic operation and the subsequent examination of the data, and linked to a specific CMS case file. This includes files created by the forensic software used, such as log files, index files, recovered files, expanded compound files (e.g. archive files, pst files, database files), files exported from forensic images, bookmarks, handover of digital media notes, and reports.

1.12 Security copy: A copy of the digital forensic image for the purpose of having a backup copy in case of loss, destruction or a compromised original digital forensic image during the transport back to OLAF.

1.13 In-house backup copy: A copy of the digital forensic image stored on tape in the OLAF Archives, which is made by the DES upon return to the office.

1.14 Off-site backup copy: A copy of the digital forensic image stored on tape outside the OLAF premises, which is made by the DES upon return to the office.

1.15 Digital medium/device: A medium/device containing digital data (e.g. a computer hard disk, a CD/DVD, a USB memory stick, a Smartphone, a SIM card, flash memory cards).

1.16 OLAF forensic leaflet: The leaflet explaining the principles of OLAF's digital forensic procedures.

1.17 Cloud Service Provider: A service provider that offers customers storage or software services available for access via the Internet.

1.18 Operational analysis: The collection and evaluation of information, including personal data, the use of specific analytical tools and techniques to establish links between pieces of information, such as persons, economic operators, transactions, and the formulation of observations and hypotheses in support of investigations. Operational analysis reports may be used in judicial proceedings and contribute to anti-fraud policy activities.

Article 2. OLAF's Forensics Laboratory

2.1 The OLAF forensic laboratory is composed of physically isolated and protected offices within OLAF where forensic services are provided. They include the forensic

server rooms, where the digital forensic examination files are stored, and the consultation area for the investigators and operational analysts.

2.2 The file server and the forensic workstations are on a dedicated forensic network, with no Internet connection and totally separated from the Commission network.

2.3 Access to this laboratory is restricted to staff that have a need to know via electronic access control and logged by badge readers. Entrance to the laboratory is monitored by a video surveillance system.

2.4 All data transfers from the forensic laboratory to an investigator or an operational analyst must be recorded in the CMS Intelligence Request Module in order to protect the chain of evidence.

Article 3. Preparation of a digital forensic operation

3.1 When planning a Digital Forensic Operation the investigator assisted by the DES should go through the "Checklist for the Preparation of a Digital Forensic Operation" and provide the information requested as complete as possible.

3.2 The investigator assisted by the DES, shall complete the work form "Request for Authorisation to carry out a Digital Forensic Operation", which should provide, if known in advance, the names or functions of persons and/or the names of economic operators holding digital media which shall be subject to the digital forensic operation.

3.3 The "Request for Authorisation to carry out a Digital Forensic Operation" shall be presented to the Investigation Selection & Review Unit together with a draft of the "Authority to carry out a Digital Forensic Operation". This latter document should specify that the digital forensic operation may be extended to further digital devices found at the premises which may contain data held by the institution. Where appropriate, it should also specify that contact may be made with a relevant Cloud Service Provider and/or Internet Service Provider.

3.4 The Head of the Investigation Unit and the Head of the Operational Analysis and Digital Forensics Unit shall ensure that the DES(s) and/or the operational analyst(s) have access to the relevant case file in the Case Management System.

Article 4. Conducting a digital forensic operation – general procedure

4.1 Digital forensic operations may only be conducted by OLAF DES's to ensure admissibility of the evidence obtained in subsequent legal proceedings. The digital forensic operation shall be conducted under the coordination of an OLAF investigator, who should normally be present at the start of the operation, but does not need to remain present throughout. The DES should remain present for the duration of the digital forensic operation.

4.2 At the beginning of the digital forensic operation, the investigator shall hand the person or the economic operator holding media which are subject to the digital forensic operation a copy of the "OLAF Digital Forensic Operations Information Leaflet". The DES shall assist the investigator in answering any questions related to the digital forensic operation.

4.3 At the start of the digital forensic operation, the DES shall: (1) document and take photographs of all digital media which shall be subject to the forensic operation, as well as the physical surroundings and layout; (2) make an inventory of the digital media. The inventory should be included in the "Digital Forensic Operation Report", and the photographs attached to it.

4.4 The DES shall create a digital forensic image of the original data. If, for technical reasons, it is not possible to make a full digital forensic image, the DES may instead conduct a partial digital forensic acquisition of the data. A short description of the contents and the case reference number added by the DES shall be recorded during the acquisition of the digital forensic image.

4.5 The DES shall create a security copy of the acquired data on site, if possible and if time permits, store it on a separate digital medium, and verify that it functions properly.

4.6 In order to protect the chain of evidence, the investigator shall not accept digital devices from any person at any time during the digital forensic operation. Only the DES shall accept such digital device where appropriate and conduct a digital forensic acquisition of the device obtained.

4.7 At the premises, the DES shall draw up a "Digital Forensic Operation Report" recording all activities relating to the access, acquisition, collection and storage of the data. All digital forensic copies created and their respective hash values shall be listed. Any error, damage or other incident and any remedial steps taken shall be specified and documented. If the digital medium was not acquired forensically, this shall be recorded. Any objections made during the digital forensic operation shall be recorded in the report.

4.8 All persons present at the digital forensic operation, including officials of national authorities, shall be listed and when possible asked to sign the report. If a person declines to sign, the DES shall note this in the report. The DES shall sign the report and give it to the investigator. The investigator shall register the report immediately upon return to the office.

4.9 The DES shall provide a copy of the "Digital Forensic Operation Report" to the person (economic operator) whose digital media have been acquired, unless the person has not been informed about the investigation in accordance with Article 9(3) of Regulation (EC) 883/2013.

4.10 All devices containing information gathered during digital forensic operations shall be transported in a secure manner (e.g. anti-static plastic bags sealed with security seals, protective carrying bags to avoid damaging the device(s)), which remain under the physical control of OLAF staff (e.g. on the body or in hand luggage during air travel) at all times during the transport, in order to guarantee the integrity of the chain of evidence. If a digital forensic image and a security copy have been made, they should be carried by different members of staff. If this is not possible, they should be sent by diplomatic bag.

Article 5. Conducting a digital forensic operation – internal investigations

5.1 The investigator shall explain that the EU staff or member is under a duty to cooperate with OLAF in accordance with Article 4(7) of Regulation (EC) 883/2013 and the decision adopted by the institution concerned.

5.2 The DES shall take copies of any document held by the institution or acquire the contents of any data medium held by the institutions relevant for the investigation.

5.3 Where it is not possible to establish whether the data is held by the institution or the data medium found at the premises contains data held by the institution, the DES should acquire the data and place the forensic image in a sealed envelope. OLAF will invite the person whose data was forensically acquired for a meeting to decide on this issue.

5.4 OLAF shall follow the procedure in Article 5.3 also in situations where the digital forensic operation is conducted while the EU staff or the member is absent.

5.5 The fact that an EU staff or a member or an institution, body, office or agency has marked certain e-mails, folders, drives or other data as private does not prevent the DES from conducting a digital forensic acquisition.

Article 6. Conducting a digital forensic operation – external investigations

6.1 OLAF must prepare and conduct such digital forensic operations in close cooperation with competent authorities of the Member State concerned and, in accordance with the cooperation and mutual assistance agreements and any other legal instrument in force with competent authorities of the third country concerned.

6.2 Subject to the European Union law applicable, OLAF shall comply with the rules of procedure laid down by the law of the Member State or third country concerned.

6.3 If during an "On-the-spot check" of an economic operator, it claims that the device subject of the digital forensic operation contains data of a legally privileged nature, the data shall be acquired and placed in a sealed envelope. The economic operator shall be told that it will be invited for a meeting to resolve the issue before OLAF opens the sealed envelope, where it may be assisted by a person of its choice. The DES shall seal the envelope with a unique reference number and assume custody of it until such a meeting occurs. This must be reported in the "Digital Forensic Operation Report". Should the economic operator raise objections to this procedure, OLAF should consider requesting the competent national authorities of the Member State or third country to take the appropriate precautionary measures under national law in order to safeguard evidence as authorised under Article 7(2) of Regulation (EC) 2185/96.

Article 7. Collection of data stored with a Cloud Service Provider

7.1 The DES may find that data of potential relevance for the investigation are stored remotely with a Cloud Service Provider. In such a case, the investigator shall ask the person or the economic operator concerned to download the data using his/her/its credentials. OLAF may also request the Cloud Service Provider to hand over the potentially relevant data to the investigator as authorised under Article 5 of Regulation (EC) 2185/96. OLAF may also request information relevant for the investigation from the national Internet Service Provider.

Article 8. Examination of data gathered during a digital forensic operation

8.1 Immediately after the return from the digital forensic operation, the DES shall transfer the digital forensic image to the forensic file server in the forensic laboratory. The file thus transferred becomes the forensic work file.

8.2 The DES shall create two back-up copies of the digital forensic image on tape, and place them in sealed envelopes with unique identification numbers. One of these is the in-house backup copy, which shall be stored in the OLAF Archives, protected by electronic access control. The other is the off-site backup copy, which shall be stored in a protected area outside the OLAF premises, protected by biometric access control. The DES should inform the investigator as soon as the forensic work file is ready.

8.3 Following the creation of the forensic work file and the two back-up files, the original digital forensic image and security copy are wiped from the devices on which those copies were made (e.g. laptops, portable hard disks).

8.4 When the forensic work file is available, the investigator shall promptly launch a written request for analysis to the Operational Analysis and Digital Forensics Unit through the CMS Intelligence Request Module. The request should describe the aim of the search and what type of evidence and/or proof the investigator is searching for. The process could include looking for traces of deleted data in unallocated space, specifying keywords to be searched, or making more complex searches such as special expression or timeline searches.

8.5 In response to the investigator's written request for analysis, the DES shall extract data matching the search criteria from the digital forensic work file for read-only access by the investigator. The investigator may also request the DES or operational analyst to print or make an electronic copy of relevant files.

8.6 The investigator shall bookmark potentially relevant information using the facilities of the forensics laboratory. He/she shall request the DES to back up these bookmarks at regular intervals. The DES shall do so automatically when the Intelligence Request is closed in the CMS Intelligence Request Module.

8.7 The investigator may request, via the CMS Intelligence Request Module, the assistance of the operational analyst in designing the search criteria and analysing the results. Upon completion of the analysis, the operational analyst shall prepare a "Operational Analysis Report" of the data contained in the digital forensic work file and the results obtained, which must be attached to the relevant CMS case file.

8.8 Any special categories of personal data, as defined in Article 10(1) of Regulation (EC) 45/2001, gathered during a digital forensic operation may only be further processed following a specific assessment of the applicability of one of the exceptions listed in Article 10(2) of Regulation 45/2001. Furthermore, Article 4.5 of the ISDP states that "marital status" and "children" categories of data can only be included in case files if relevant to the matter under investigation. Article 4.3 of the ISDP provides that "the investigation unit shall record the processing of any such data in the OLAF Data Protection Module. If any such data have been exported to the case file but is later deemed not relevant, the investigator shall remove such data from the case file. However, the data will remain on the digital forensic evidence file and cannot be physically erased.

Article 9. Re-acquisition of a digital forensic image acquired in the context of different investigation

9.1 The investigation unit may submit a request for the Director General's authorisation to carry out a re-acquisition and examination of a forensic image taken in the context of a different investigation.

9.2 The investigator shall inform the person or the economic operator from whom the forensic image was acquired, of the decision to re-acquire and examine the forensic image for the purpose of a different investigation. The person or the economic operator will be informed of the date and place of the re-acquisition and will be provided with a copy of the "OLAF Digital Forensic Operations Information Leaflet".

9.3 The investigator shall inform the person concerned of the decision to re-acquire and examine a forensic image taken in the context of a different investigation. The person concerned will be informed of the date and place of the re-acquisition and will be provided with a copy of the "OLAF Digital Forensic Operations Information Leaflet".

9.4 In case of an internal investigation, OLAF will inform also the institution concerned of the decision to re-acquire and examine a forensic image for the purpose of a different investigation.

9.5 The provision of this information may be deferred in accordance of Article 9(3) of Regulation 883/2013 and Article 20 of Regulation 45/2001.

9.6 The DES shall draw up a "Digital Forensic Operation Report" recording the re-acquisition in accordance with the general procedure foreseen in Article 4 above. Any objections made during the forensic re-acquisition shall be recorded and included in the report.

Article 10. Final back-up of results

10.1 When no more requests for digital forensic examination or operational analysis are to be expected or at the latest when the investigation is closed, the DES shall make two backup copies of the digital forensic evidence files. They should be placed in sealed envelopes with unique identification numbers, and processed in accordance with Article 8.2.

10.2 The DES shall hand over one backup copy to the OLAF Archives completing the work form "Transfer of digital evidence to the OLAF Archives / Off-site Storage" where it shall receive a unique electronically registered identification number. The tape(s) shall be listed as annexes to this work form. The second back-up copy shall be transferred to the off-site storage.

10.3 All copies shall be removed from the forensic file server.

Article 11. Digital forensic assistance to OLAF's partners

11.1 An EU institution, body, office or agency, a competent Member State or third country judicial or administrative authority, or an international organisation may request the assistance of OLAF to conduct a digital forensic operation. Such assistance may be provided in the framework of an OLAF investigation, and where providing the assistance is compatible with OLAF's own planning and allocation of resources.

11.2 After consulting with the Operational Analysis and Digital Forensics Unit, the investigator shall prepare a response to the requesting authority specifying whether OLAF will provide digital forensic assistance for the signature of the Director General.

11.3 When OLAF agrees to assist a national authority with a digital forensic operation, the DES(s) and/or the operational analysts operate with the express and written authorisation of the relevant national authorities. OLAF shall conduct only investigative activities which are authorised under EU law and may not conduct any such activity established only under national law. Upon completion the DES shall prepare a "Digital Forensic Operation Report".

11.4 The DES shall hand over all digital forensic images and reports prepared by OLAF staff to the national authorities. OLAF may keep a copy and make use of the digital forensic images and/or reports only with the authorisation of the competent national authorities to the extent necessary for the conduct of its investigation. This must be reported in the "Digital Forensic Operation Report".

11.5 The investigator will take steps to ensure that the national authority will authorise OLAF's use of the information gathered in this way within a reasonable time and without prejudice to any ongoing administrative, disciplinary or judicial procedures.

Article 12. Use of digital forensic evidence file in court proceedings

12.1 Any request from a national court for the digital forensic evidence file shall be placed in the relevant case file. Upon receipt, the investigator shall request, through the CMS Intelligence Request Module, a copy of the digital forensic evidence file on a data medium (hard disk drive, tape, or other, depending on the volume of data), which shall be sent to the requestor in a secure way.

Article 13. Destruction of the digital forensic images

13.1 At the end of the case file's retention period, the Operational Analysis and Digital Forensic Unit shall wipe all copies of the digital forensic evidence files, unless the Director General decides to transfer the case documents to the Commission's Historical Archives as provided for by ISDP Article 13.3.

Article 14. Entry into Effect and Publication

14.1 These Guidelines will take effect from 1 January 2014 and replace the "Operating Procedures for Conducting Computer Forensic Operations and Examinations" from 4 July 2011.

14.2 These Guidelines will be published at http://ec.europa.eu/anti_fraud.

Giovanni KESSLER
Director General