Electronic evidence - a basic guide for First Responders

Good practice material for CERT first responders

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Supervisor of the Study: ENISA

Authors of the Study: ENISA and Philip Anderson (Northumbria University, UK)

Contact

For contacting the authors please use cert-relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu

Acknowledgements

The drafting of this report would not have been possible without the feedback and cooperation kindly provided by a number of organisations and individuals. Without endeavouring to be exhaustive, the authors would like to thank all who contributed to and/or reviewed parts of this document. Special thanks go to Andrew Cormack (Janet, UK), Dr. Serge Droz (SWITCH, Switzerland), Andrea Dufkova (ENISA), Lionel Ferette (ENISA), Bruno Halopeau (Europol EC3), Michael Hamm (CIRCL.LU, Luxembourg), Nigel Jones (Centre for Cyberforensics School of Law, UK), Gustavo Neves (CERT.PT, Portugal), Lauri Palkmets (ENISA), Professor Peter Sommer (Visiting Professor, de Montfort University, Visiting Reader, the Open University, Visiting Lecturer, Oxford University Centre for Doctoral Training, Visiting Lecturer, Queen Mary University of London).

Legal notice

Copyright Notice

ISBN 978-92-9204-111-3 doi: 10.2824/068545

Executive summary

Threats to cybersecurity and cyber-attacks respect no boundaries. For that reason ENISA in the last couple of years has helped to bridge the gap between the CERT- and the law enforcement communities. This report is a continuation of the work of ENISA in this field, and aims at providing a guide for first responders in the area of gathering of evidence related to a cybercrime. While the securing of digital evidence is ultimately a task and a responsibility of law enforcement, CERT staff can nevertheless contribute to that work by helping to preserve it during for example the detection of a cybercrime.

This guide does not intend to be exhaustive, nor does it aim to be a full step-by-step guide on how to approach digital evidence as a first responder. Gathering of evidence for example typically involves *ad hoc* decisions that need to be made during the process, based on factors that cannot be determined in advance. Instead, this guide aims at explaining the principles of sound evidence gathering and tries to raise the right questions to be asked by first responders before starting to work.

The document starts with an explanation what is understood by "electronic evidence". Different definitions are presented as well as different sources of electronic evidence (laptops, PDAs, etc.).

Next we discuss the different fundamental principles in the field of evidence gathering. One set of particular interest is the principles described in the *Electronic evidence guide - A basic guide for police officers, prosecutors and judges*[1], developed within the framework of the European Union and the Council of Europe joint project (CyberCrime@IPA project[2]). It identifies five principles that establish a basis for all handling of electronic evidence.

Without trying to be exhaustive we touch then the different phases first responders encounter when performing digital forensics or electronic evidence gathering. We describe how they should act before and while arriving at the (crime) scene, what they should keep in mind when performing memory forensics, etc.

After that we touch upon some important legal topics and questions such as:

- How to determine the applicable law?
- What is the adequacy of the exisiting rules?
- Which jurisdiction applies?

We believe that a key success factor for a CERT first responder deling with gathering of electronic evidence is appropriate communication with law enforcement.

[1] CyberCrime@IPA, EU/COE Joint Project on Regional Cooperation against Cybercrime, *Electronic evidence guide - A basic guide for police officers, prosecutors and judges*,Version 1.0, Authors: Jones, N., George, E., Insa Mérida, F., Rasmussen, U., Völzow, V., http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp [last accessed 10 November 2014]

[2] CyberCrime@IPA, *Electronic evidence guide - A basic guide for police officers, prosecutors and judges*, Op. cit., http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp [last accessed 10 November 2014]

[2] For more information on the Cybercrime@IPA Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime, see: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_IPA_en.asp [last accessed: 10 November 2014]

Table of Contents

1 Introduction

Scope

Threats to cybersecurity and cyber-attacks respect no organisational and territorial boundaries. For that reason, effective cooperation between communities at all levels is required to facilitate the exchange of the information and knowledge needed to reduce vulnerabilities and provide effective responses to cyber incidents. These communities include, among others, Computer Emergency Response Teams (CERTs) within particular business sectors which might be affected by large-scale incidents, other incident responders within a country serving other communities, national/governmental (n/g) CERTs, law enforcement agencies (LEAs) and internationally recognised research and development organisations.

This report is a continuation of the work done by ENISA in the field of of good practices for CERTs and LEAs in the fight against cybercrime. It aims at providing a guide for first responders, with a special emphasis in evidence gathering. It aims at complementing the existing (vast) material on the topic of digital forensics and evidence gathering, as these are in most cases written from the perspective of law enforcement. This guide rather aims at providing guidance for CERTs on how to deal with evidence and the evidence gathering process. For most CERTs this is a limited and (for many of them) relatively new field of operation with a growing importance.

In the last three years, ENISA engaged with the CERT- and law enforcement communities to collect and share good practice, and useful fields of collaboration in the area of fighting cybercrime. From these endeavours stem the following guides:

- A flair for Sharing - Encouraging Information Exchange between CERTs[3]
- The Fight against Cybercrime - Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime - A first collection of practices[4]
- A Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime[5]
- A Good Practice Collection for CERTs on the Directive on attacks against information systems[6]

In addition, ENISA since 2011 organises in collaboration with Europol (and since 2013 with EC3) regular collaboration workshops on topics of common interest:

- 6th CERT workshop (2011, Prague, Czech Republic): Addressing NIS aspects of cybercrime[7]

[3] ENISA, *A flair for sharing - encouraging information exchange between CERTs*. https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing [last accessed 10 November 2014]

[4] ENISA, *Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime - A first collection of practices*. https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/supporting-fight-against-cybercrime [last accessed 10 November 2014]

[5] ENISA, *Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime*. https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime [last accessed 10 November 2014]

[6] ENISA, *A Good Practice Collection for CERTs on the Directive on attacks against information systems*. https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems [last accessed 10 November 2014]

[7] For more information, see: https://www.enisa.europa.eu/activities/cert/events/6th-workshop-cybercrime [last accessed 10 November 2014]

- 7th CERT workshop part II (2012, The Hague, The Netherlands): Addressing NIS aspects of cybercrime[8]
- 8th CERT workshop part II (2013, The Hague, The Netherlands): ENISA/EC3 Workshop on (automated) information sharing[9]
- 9th CERT workshop part II (2014, The Hague, The Netherlands): ENISA/EC3 Workshop on CERT/LEA collaboration[10]

Aim

One of the returning conclusions of these projects and workshops is that CERTs and law enforcement should cooperate, but that this collaboration is still far from being a "normal and regular activity", and that the collaboration leaves room for improvement on a number of levels. One concrete topic that workshop participants identified as important is guidance to CERTs on how to assist law enforcement in the field of electronic evidence gathering, hence this guide was developed.

The guide has no intentions to be exhaustive, nor does it aim to be a full step-by-step guide on how to approach evidence as a first responder. Digital evidence gathering is typically a science where *ad hoc* decisions need to be made during the process, based on factors that cannot be determined in advance. Instead, this guide aims to explain the principles of sound evidence gathering and tries to raise the right questions to be asked by first responders before engaging in evidence gathering.

Background

In its report 'Baseline capabilities of n/g CERTs - Updated Recommendations 2012,'[11] ENISA delivered an updated set of recommendations on baseline capabilities for n/g CERTs[12] in Europe (ENISA drafted the initial recommendations in 2009/2010). Based on the assessment of deployment of baseline capabilities ENISA identified a number of gaps and shortcomings that still need to be addressed in order for n/g CERTs to fully meet the baseline capabilities.

One of the identified gaps is that n/g CERTs report difficulties in attracting highly specialised personnel, for example in reverse engineering and digital forensics.

Apart from the set of basic services identified in the baseline capabilities, there are other services which can be delivered by a CERT team (the extended services). One of these extended services is digital forensics which covers both computer and network forensics. Both are very practical and can significantly improve the delivery of CERT services.

Digital investigation and forensics are usually provided by CERTs as a service on an on-demand basis. CERT first responders have different priorities than law enforcement, as the primary function of a CERT is normally to ensure that the provision of the service is returned or maintained. Evidence collection

[8] For more information, see: https://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop-partII [last accessed 10 November 2014]
[9] For more information, see: https://www.enisa.europa.eu/activities/cert/events/8th-cert-workshop-part-ii [last accessed 10 November 2014]
[10] For more information, see: https://www.enisa.europa.eu/activities/cert/events/9th-cert-workshop-part-ii [last accessed 10 November 2014]
[11] ENISA, *National/governmental CERTs - Baseline Capabilities.* http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities [last accessed 10 November 2014]
[12] A 'Computer Emergency Response Team' (CERT) is a team of IT security experts whose main business is to respond to computer security incidents. The team provides the necessary services to handle such incidents and to support their constituents (the established term for their customer base) to recover from computer security breaches. In order to mitigate risks and minimise the number of required responses, most CERTs also provide preventative and educational services for their constituency.

is usually only secondary to them, unlike for law enforcement where the sound evidence collection is typically of highest priority. A higher level of mutual understanding and collaboration between CERTs and law enforcement is considered to be the way forward to improve both the quality and the speed of results achieved in the fight against cybercrime.

Currently, digital forensics is mostly used for conventional crime investigations, such as "white-collar crime", organised crimes as drug dealing or others[13]. Therefore many of the forensic services carrying out the investigations of these cases are not assembled by experts on network technologies but rather by experts in conventional investigation techniques.

It should be noted that there are many different use cases where CERTs could act as first responders when it comes to electronic evidence. A first, and perhaps most common use case is confrontation with potential evidence during normal incident handling processes by a CERT, where it detected (or was informed about) a potential compromise of a system in the constituency. A second use case could be the request to a CERT by a law enforcement agency to assist in the electronic evidence gathering or analysis and/or to act as a specialist (for example to cope with the lack of qualified staff in its own ranks).

There might be other potential use cases for this guide where first responders from CERT teams could be required to perform electronic evidence gathering. Although this document focuses on the first two use cases, this does not mean that the principles and the questions this document highlights are not relevant to other cases or situations a CERT could be exposed to.

Target audience

CERTs are responsible for receiving, reviewing, and responding to computer security incidents. An organization will need to define what a computer security incident is: the incident may be an event related to the security of computer systems or computer networks or an employee violating a security policy. The purpose of a CERT must be based on the business goals of the organization and protecting its critical assets.

There are many different CERTs or CSIRTs. Internal CERTs provide incident handling services within an organisation, national ones provide incident handling services to a country while others offer incident handling services to other organisations at a cost.

Planning and fully preparing for the occurrence of security incidents is of vital importance if organisations wish to handle such events efficiently and effectively.

With these extended services, CERTs could act as first responders, for example when asked to preserve evidence when mitigating an incident in their network, for example workstations infected with malware.

Good planning and guidelines for CERT staff can ensure that the different priorities are not mutually exclusive. Often CERTs only consider evidence after remedial action is taken. To put it short, CERTs are incident handlers and their main duty is making attacks stop and putting systems to work again. However, many of the incidents CERTs have to handle have a criminal component and can therefore become subject to a law enforcement investigation. It is therefore important that CERTs have this in mind when handling an incident and dealing with potential evidence.

[13] ACPO (Association of Chief Police Officers), *ACPO Good Practice Guide for Digital Evidence*. http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf [last accessed 10 November 2014]

2 Electronic evidence gathering

2.1 What are electronic evidence and electronic evidence gathering?

There are many different definitions of electronic or digital evidence. The Council of Europe *Convention on Cybercrime*,[14] also called 'Budapest Convention on Cybercrime' or simply 'Budapest Convention' refers to electronic evidence as evidence that can be collected in electronic form of a criminal offence. The United States Department of Justice defines digital evidence as "Information stored or transmitted in binary form that may be relied on in court," as mentioned in the *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*.[15] In general though, most definitions seem to summarise that digital evidence is digital data that can be used to help establish (or refute) whether a crime has been committed.

Electronic evidence gathering is a process that involves the assessment of a given situation and the identification and recovery of relevant sources of data that could be of evidential value to the investigation. However, there are a number of key issues that need to be addressed during the assessment: a thorough understanding of the situation, the potential business impact of an investigation, and the identification of the business infrastructure.

2.2 Different sources of evidence

There are numerous sources of digital evidence and each requires a different process for gathering that evidence as well as different tools and methods for capturing it. It is not just the personal computer, laptop, mobile phone or Internet that provide sources of digital evidence, any piece of digital technology that processes or stores digital data could be used to commit a crime. The device and information it contains may store relevant digital evidence for proving or disproving a suspected offence.

It is vital that responders are able to identify and correctly seize potential sources of digital evidence. An example of the types of digital devices encountered by a digital forensic practitioner include, but are not limited to the following:

- Computers – such as Personal Computers (PC's), laptops, servers or even game consoles
- Storage devices – Compact Discs, Digitally Verstaile Discs, removeable data storage drives (USB thumb drives) and memory cards
- Handheld devices - mobile (smart) phones, digital cameras, satelite navigation systems
- Network devices like hubs, switches, routers and wireless access points

There is an important difference between volatile and non-volatile data. Volatile data is data that is lost when the device is not powered on. A typical example of this would be the random-access memory (RAM) storage in a PC. Nowadays personal computers have gigabytes of volatile storage so the data in the RAM is becoming more and more important. When gathering evidence, this should be taken into account as just simply disconnecting a system from power might destroy evidence stored in volatile storage. Doing a memory dump is necessary at this stage in many cases.

[14] Council of Europe, *Convention on Cybercrime,* CETS N. 185, Budapest, 23 November 2001. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG [last accessed 10 November 2014]

[15] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*,(2004). 1st ed, p. 46. https://www.ncjrs.gov/pdffiles1/nij/199408.pdf [last accessed 10 November 2014]

3 Principles of electronic evidence gathering

When gathering any form of evidence, including digital evidence, it is of vital importance that appropriate procedures and guidelines are strictly followed and adhered to. There are numerous guidelines avaiable to digital forensic practitioners and all these guidelines focus on a number of key issues, including some main principles that establish a basis for all dealings with electronic evidence.

While laws regarding admissibility of evidence differ between countries, using these more practical principles is considered to be a good basic guideline as they are accepted internationally. This does not mean that by applying only these guidelines the evidence gathered will be admissible in court.

The *Electronic evidence guide - A basic guide for police officers, prosecutors and judges*,[16] developed within the framework of the European Union and the Council of Europe joint project (CyberCrime@IPA project[17]), for example, identifies five principles that establish a basis for all dealings with electronic evidence.

- Principle 1 – Data Integrity
- Principle 2 – Audit Trail
- Principle 3 – Specialist Support
- Principle 4 – Appropriate Training
- Principle 5 – Legality

A brief explanation of these five principles is given below. A more detailed explanation can be found in the full guide published by the Council of Europe. The guide is free of charge, however access to the file must be asked directly from the Council of Europe. ENISA has also developped training material based on these principles, namely the *Digital Forensics Training Handbook*[18] .

Another set of guidelines that could (and should) be considered when dealing with digital evidence and electronic evidence gathering in general is the *Good Practice Guide for Computer-Based Electronic Evidence*[19] published by the Association of Chief Police Officers (ACPO) in the United Kingdom for the authentication and integrity of evidence. Although principally aimed at law enforcement personnel it is relevant to the collection and examination of digital evidence. These guidelines have been used as a reference for other guidelines in the field. For instance, together with the *ISO Standard 27037* on

[16] CyberCrime@IPA, EU/COE Joint Project on Regional Cooperation against Cybercrime, *Electronic evidence guide - A basic guide for police officers, prosecutors and judges*,Version 1.0, Authors: Jones, N., George, E., Insa Mérida, F., Rasmussen, U., Völzow, V. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp [last accessed 10 November 2014]

[17] CyberCrime@IPA, *Electronic evidence guide - A basic guide for police officers, prosecutors and judges*, Op. cit. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp [last accessed 10 November 2014]

[17] For more information on the Cybercrime@IPA Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime, see: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_IPA_en.asp [last accessed: 10 November 2014]

[18] ENISA, *Digital forensics Handbook, Document for teachers*, http://www.enisa.europa.eu/activities/cert/support/exercise/files/digital-forensics-handbook [last accessed 10 November 2014]

[18] ACPO (Association of Chief Police Officers), *ACPO Good Practice Guide for Digital Evidence*. http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf [last accessed 10 November 2014]

Guidelines for identification, collection, acquisition and preservation of digital evidence[20], adopted in October 2012, these guidelines served, amongst others, as input for example to the *Guidelines on Digital Forensics for OLAF Staff*[21].

Other guidelines aimed at law enforcement that might be worthwile to look at are the *Guidelines for Best Practice in the Forensic Examination of Digital Technology*[22] from the Forensic Information Technology (FIT) Working group interest of the European Network of Forensic Science Institutes (ENFSI). The guidelines already date back to 2009 but an updated version is currently being worked on.

As a first responder it is important to find out which principles or rules are applicable to you. It is advisable that CERTS get in touch with law enforcement representatives prior to engaging in evidence gathering activities and to familiarize themselves with the applicable rules. In most cases these will be very similar to the principles mentioned above. There may be specific legal requirements, depending on the jurisidiction of the proposed activity.

Integrity

The integrity of digital evidence must be maintained at all stages. "No action taken […] should change data which may subsequently be relied upon in court."[23] From all the principles this is probably the most important one. As the integrity of the evidence is of extreme importance, it is vital that the integrity requirement of the evidence is the main driver and should be the most important factor in deciding what to do (and what not do).

Digital data is volatile, and the ease with which digital media can be modified implies that documenting a chain of custody is extremely important to establish the authenticity of evidence. In addition, all examination processes must be documented so that if needed, they can be replicated. The evidential integrity and authenticity of digital evidence can be demonstrated by using hash checksum or Cyclic Redundancy Check (CRC)[24], which is used during the acquisition stage as a method of checking for errors in the evidence file. However, nowadays we can consider that those methods are not sufficient anymore. Therefore it is considered better to use a one-way hash algorithm such as MD5 or SHA-1. This way it is possible to determine if changes have occured to digital evidence at any point of an investigation. As both MD5 and SHA-1 algorithms are now considered to be relatively weak it is recommended to use stronger algorithms such as SHA-2[25].

---

[20] *ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*.
http://www.iso27001security.com/html/27037.html [last accessed 10 November 2014]

[21] http://ec.europa.eu/anti_fraud/documents/forensics/guidelines_en.pdf [last accessed 10 November 2014]

[22] OLAF (European Commission Anti-Fraud Office), *Guidelines on Digital Forensic Procedures for OLAF Staff*, Ref. Ares(2013)3769761 - 19/12/2013, 1 Juanuary 2014.
http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf [last accessed 10 November 2014]

[23] ACPO, *ACPO Good Practice Guide for Digital Evidence*, Op. cit.,
http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf [last accessed 10 November 2014]

[24] A 'cyclic redundancy check' or CRC is a code to detect errors in raw data. This code is mainly used in electronic networks and storage devices to detect (accidental) changes to data. This code can also be used to prove the integrity of the data.

[25] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/recommended-cryptographic-measures-securing-personal-data [last accessed 28 November 2014]

In some circumstances it is necessary that data on a computer that is still running has to be accessed. Special precautions should be taken to minimise the impact on the data and this should be done, as said, only exceptionally and only by competent personel to perform this operation and able to "explain the relevance and the implications of their actions"[26].

When the evidence cannot be collected without altering it, gathering steps must be very well documented and you have to be able to tell exactly what tools were used, what they did to the system and which changes they produced. This is for example important when performing a memory dump[27]. Such a memory dump cannot be done without incurring at least some modification of the memory. But in many cases it is much more valuable to have the data from volatile memory even if altered than not have it at all. The first responder must however be able to testify later which steps he/she took and to explain any alteration to the evidence that was not avoidable.

Audit trail

An audit trail (often refered to as chain of custody or chain of evidence) is the process of preserving the integrity of the digital evidence. "Documentation permeates all steps of investigative process but is particularly imporant in the digital evidence seizure step. It is necessary to record details of each piece of seized evidence to help to establish its authenticity and initiate the chain of custody."[28] Indeed, an "audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those actions and achieve the same result."[29]

It is of vital importance that any digital exhibit can be tracked from the moment when it was seized at the crime scene all the way to the courtroom, as well as anywhere else in between such as laboratories or storages. To demonstrate that a robust chain of custody or audit log was maintained details of the evidence and how it was handled, by whom as well as everything that has happened to it needs to be recorded at every step of the investigation.

It is important to stress how such details can be crucial. It is better to note down too many details than recording too few details about the actions taken. It is, for example, advisable to note down which keystrokes were entered and which mouse movements have been made rather than just to write down in generic terms that "a forensic backup has been performed."

Specialist support

Specialist support needs to be requested as soon as possible when evidence gathering raises some specific (technical issues) and the first responders in charge of the evidence collection is not familiar with the issue or its implications.

As there exist so many different systems and technical situations, it is almost impossible for a digital forensics expert to have the specific know-how on how to deal with all these sorts of electronic evidence. This is why it is so crucial to call in the right specialists – either internal from the team or

[26] ACPO, *ACPO Good Practice Guide for Digital Evidence*, Op. cit., p. 6. http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf [last accessed 10 November 2014]
[27] A recorded state of the volatile memory in a system, for example of the RAM memory.
[28] Casey, E. *Digital Evidence and Computer Crime*, 2004, 2nd Ed. Elsevier, p. 106.
[29] ACPO, *ACPO Good Practice Guide for Digital Evidence*, Op. cit., p. 6. http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf [last accessed 10 November 2014]

from external - when necessary and to have the right equipment ready for them to perform their tasks.

Appropriate training

Proper training is a very important prerequisite for the success of the search and seizure of electronic evidence. Appropriate and constant training should be provided to all first responders dealing with digital forensic, especially when they are expectedto deal specifically with 'live' computer and access original data.

Legality

"The person in charge of the investigation has overall responsibility for ensuring that the law and these principles [the principles of digital evidence] are adhered to.[30]"

Legal guidance for the practitioner varies depending on the jurisdiction in which they reside. Further, a distinction must be made between legislative documents and guidance and principles provided by relevant governing bodies within the forensic industry. Examples of such guidance documents include the above-mentioned *Electronic evidence guide - A basic guide for police officers, prosecutors and judges* developed within the framework of the European Union and the Council of Europe joint project (CyberCrime@IPA project) and the UK *ACPO Good Practice Guide for Digital Evidence*.

[30] ACPO, *ACPO Good Practice Guide for Digital Evidence*, Op. cit., p. 6. http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf [last accessed 10 November 2014]

4 Before arriving at the crime scene

The first responders to an incident are in a unique and important position. Regardless of the case, they should have an appropriate toolkit and follow a predetermined plan.

The very first step the CERT first responder should take is to get a clear understanding of what is requested. Does the constituent actually plan to take the case to court? Or does the constituent only want to confirm or refute a certain suspicion (e.g. Malware X was present on the system, or data of type X has been exfiltrated)? Or maybe the constituent just wants the system up and running as quickly as possible? First responders should clear this up before preparing their tools. Sometimes it may even be necessary for the CERT to recommend a certain goal to the constituent.

All members of the first responder team should be familiar with the relevant legislation within the jurisdiction they are operating in advance of responding to any incident. It is vital that first responders have the appropriate knowledge and training to enable them to deal with the incident and secure the evidence in a sound way.

First responders must also have a thorough understanding of the IT equipment likely to be used during the investigation. A comprehensive checklist should be created to assist in determining the 'items of interest' including any technical and business related information. A first responder should plan for the types of digital media they will encounter (CD/DVD, USB memory stick, memory card, external hard drive, etc.). In large organisations a detailed planning is extremely important as computer systems can contain a large number of individual systems and drives, in addition to the possible combinations of laptops, desktop or tower workstations used by employees.

Prior to arriving at the (potential) crime scene it is important that the first responder ascertains as much information about the suspected offence and the crime scene itself as possible. The type of crime investigated may influence preparation for arrival at the scene.

Nowadays the amount of data stored in systems is enormous. It is hence important that the scope of the investigation is well-defined. Not doing so could result in getting lost in an overload of data.

The roles and responsibilities of all individuals involved in performing or assisting in a digital forensic investigation need to be clearly defined. To ensure that an investigation is carried out correctly there needs to be a designated coordinator who will lead the investigation. This coordinator is responsible for ensuring that all persons involved in an investigation are communicating appropriately to ensure that everyone involved can carry out their tasks successfully.

As well as the digital forensic experts any other specialist resources that could be needed during the investigation need to be identified. Additional expertise needed could be for example database experts, networking experts accountants or legal support.

4.1 First responders toolkit

The first responder should assemble a toolkit, which enables them to arrive at the scene and collect all available evidence, ensuring its integrity for later investigation. Such a toolkit should include but is not limited to the following:

- **Cameras (photo and video)**: used to capture images of the scene and record the state of digital exhibits
- **A digital clock**: to be put on the pictures taken, so the timestamps are visible as image, not just as meta data

- **Cardboard boxes** or **secure evidence bags**: for collecting evidence for transportation to the laboratory
- **Writing equipment**: prepared log forms to document steps taken. They should include a column for time/date, action taken, picture reference, person doing the proceedings, pens and pencils for recording contemporaneous notes at the scene
- A **flow chart** on how to proceed in different cases, e.g. when the computer is running, when the computer is networked, etc.
- **Gloves**: to protect against contaminants present at the scene
- **Evidence inventory logs, evidence tape, bags, stickers, labels, or tags**: crucial to ensure the integrity and continuity of the evidence found at the scene
- **Antistatic bags and equipment** and **non-magnetic toolkit**: to allow for the safe collection of evidence, protecting its integrity
- **A check list of possible relevant legal issues to consider and a list of relevant contacts for getting legal advice where appropriate**: this check list of relevant legal issues is not intended to help first respondents actually resolve those issues, but merely to ensure that they spot (all of) the relevant issues; the list of relevant contacts for getting legal advice is to help ensure that first respondents will contact someone with legal expertise in an effort to comply with the law

If on-scene acquisition is required or if there is a high probability that such an acquisition will take place on site some additional equipment needs to be part of the toolkit, namely:

- **Forensic Laptop** to allow on-scene acquisition (see for more detail Sub-section 4.2)
- Forensic **write protection device** to protect evidential exhibits
- Devices (e.g. Firewire) to get a memory dump. To intercept network traffic a **hub** (rather than a switch) may be necessary
- All needed **cables** should be in the kit
- **Sanitised media** to store image of any digital exhibits

A first responders' toolkit should be influenced by the types of media which may be present at a crime scene. In general, such a toolkit should consist of equipment capable of collecting digital evidence from standard PC/laptop devices, mobile phones, tablet PCs, smart TVs, game consoles and all other modern devices containing digital storage media. When dealing with mobile phones it should be considered to use Faraday bags[31] in order to prevent changes to the device.

4.2 First responder forensic laptop

The following is a description of the basic hardware and software specifications required for a first responder forensic laptop. There are a number of keys issues that need to be taken into consideration when purchasing a suitable laptop. Firstly it should contain a fast processor combined with sufficient amount of RAM to allow fast processing of the case at hand. Second, a number of USB (3.0 at the time of writing) ports will be needed to support the use of multiple peripheral devices such as portable hard disk drives (alternatively a small USB hub with additional connectors works as well). A large

[31] A 'Faraday bag' is a bag that acts as a Faraday shield. This way electronic equipment can be protected from for example lightning strikes and electrostatic discharges.

capacity, fast hard drive or an SSD (Solid State Disk) should be included, to allow disk images to be stored locally (additional external USB hard drives might be useful as well)..

Hardware Recommendations (at the time of writing of this document):

- Processor – Intel i7, i9 or AMD equivalent
- RAM – 8GB+
- Motherboard
  - USB ports – 4 minimum and USB 3 if possible
  - Firewire port – for device compatibility and creating memory dumps for example from digital cameras with firewire
- Large enough hard drive – Solid State Drive
- Spare disks

Besides the hardware, the operating system that is running on the forensic laptop is very important. The operating system should be forensically sound [32]and the first responder must be aware of how the system works.

An alternative to a forensic laptop for creating disk to disk or disk to image duplication is a forensic disk duplicator.

4.3 First responder tools and commands

The mainstream tools used by law enforcement and the private sector to carry out digital forensic investigations are often close-sourced and expensive commercial packages. During the 1980s and the beginning of the 1990s, most digital forensic investigations were carried out using non-specialist tools. From then on, specialised software (sometimes open-source) and hardware was created that allowed digital forensics investigations to take place without modifying data and media. The move from 'live analysis' to the use of these tools boosted the capabilities of digital forensics enormously. We opted not to provide a list of tools. Instead we rather list a couple of commands (and their functionality) that can be useful for first responders. We recommend that first responders that deal with evidence gathering have a look at this list and look themselves into tools that provide the required functionality.. Many of these commands are quite powerful when used correctly and to their maximum capability. Reading through the help sections of these commands and experimenting with these tools in a test environment and on test data is a very good way for getting to know the strength of the respective tools. This should be part of any good training and preparation for (potential) first responders!. Various disk images and memory dumps that can be used to train and experiment can be found online[33]. It is important that first responders have good command of their tools and that they have the functionalities of these commands always in the back of their minds.

4.3.1 Windows commands

1. cmd.exe
2. ipconfig /all
3. netstat
4. Tasklist | sort
5. Tasklist /v
6. Tasklist /svc

[32] A system that is proven not to change the data of the evidence.

[33] One example of this can be the "Test Images and Forensic Challenges" from Forensic Focus which can be found on http://www.forensicfocus.com/images-and-challenges [last accessed 12 November 2014].

7. Ftype
8. Taskkill
9. Sc query
10. Openfiles
11. SystemInfo
12. ver
13. Driverquery /v
14. Driverquery /si
15. Netstat –ano
16. netstat –anb
17. Netstat –ab –proto
18. Netstat -r
19. Netstat –s.
20. Netstat –f
21. netstat –p
22. netstat -nao
23. date /t & time /t
24. ipconfig /all
25. net use
26. net start
27. net share
28. net session
29. nbtstat –n
30. nbtstat -c
31. nbtstat -s
32. arp –a
33. schtasks
34. at
35. chkntfs c:

4.3.2 Linux commands

1. Pwd
2. whoami
3. Ps
4. Top
5. Ifconfig
6. uptime
7. df –h
8. lostat
9. sar
10. netstat
11. iptraf
12. tcpdump

13. strings
14. grep
15. xxd
16. File
17. Mount
18. less /mnt/etc/fstab
19. uname –a
20. route
21. arp –an
22. cp
23. date
24. time
25. Last
26. w
27. who
28. ls
29. ps
30. lsof
31. find
32. md5deep –r
33. dmesg
34. fdisk –l
35. shutdown –h now

5 Arriving at the scene

Upon arrival at a (potential) crime scene, it is vital that the first responder establishes his surroundings, identifying key evidential areas of the scene and any individuals who are involved in the suspected offence. If the first responder is not the first person at the scene, they should seek to establish contact with those persons who attended the crime scene first. Upon doing so, they can establish the potential location of digital devices and any interaction which has occurred between suspects at the scene.

Prior to entering the scene, health and safety requirements should be established. It is crucial to identify threats which remain, either in the form of personnel still present at the scene, along with environmental factors. The safety of the first responder and other officials at the scene is paramount and steps should be taken to ensure they are not placed in danger.

It also is best practice to never go alone to unknown locations (like home user appartments, a customers offices, etc.). When doing this as support for a client like for example a bank, someone from the client institution should accompany the first responder. In some cases it might be necessary to explain to the representative of the constituent or client what exactly will be done (e.g. trying to confirm that there is malware on the system) and, even more importantly, what will not be done. It can be useful to ask this person what (s)he has been doing and if he (s)he has noticed strange behaviour of the system. This information can lead to clues on the necessary next steps.

Upon entering the scene the first responder should maintain contemporaneous notes of their actions. The first responder should have access to guidelines from his/her employer or from the body that requested the evidence gathering on how to do this. Two examples of such guidelines are the above-mentioned UK's ACPO *Good Practice Guide for Computer-Based Electronic Evidence* [34] and the *Guidelines on Digital Forensic Procedures for OLAF Staff*.[35]

To supplement written notes, a first responder should utilise a digital camera or video recording device in order to create accurate depictions of the scene.

Records should include but are not limited to:

- Time and date which the scene was entered
- Floor plan of the scene documenting the location of devices and surrounding objects
- Personnel present in the scene
- Photographs of the scene upon entering
- Photographs of all digital exhibits *in situ*

All digital evidence should be identified and secured and no unauthorised individuals should interact with the devices. First responders should also attempt to ascertain as much information from the constituent. Password login information, network topology (both physical and virtual), users of the computer systems, Internet connections and security provisions could all provide useful guidance during an examination of the exhibit. It is important to note that first responders should not deal with suspects.

[34] ACPO, *ACPO Good Practice Guide for Digital Evidence*, Op. cit., http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf [last accessed 10 November 2014]

[35] OLAF, *Guidelines on Digital Forensic Procedures for OLAF Staff*, Op. cit., http://ec.europa.eu/anti_fraud/documents/forensics/guidelines_en.pdf [last accessed 10 November 2014]

6 Seizure

As mentioned, in many cases the first responder might be required to collect evidence in the premises of a client (e.g. a bank, company or a private individual's home). As analysing this data is in most cases quite time-consuming, it often will make sense to produce a mirror of the systems and analyse the images in the lab and not on site.

It is recommended that the first responder has a flow chart at hand on how to proceed in different cases. It is vital that this flow chart covers almost all possible cases. Important questions in this tree would be:

- Is the computer running?
- Is the computer networked?
- Do you want to preserve volatile data?
- Is there full-disk encryption applied?
- Is the console unlocked?

To give an initial idea of how such a flow chart could look like we provide an example of a part of such chart in Figure 1 below. The excerpt in Figure 1 is part of the flow chart 'Computer Forensic Hard Drive Imaging Process Tree with Volatile Data collection' by Lance Mueller.[36]

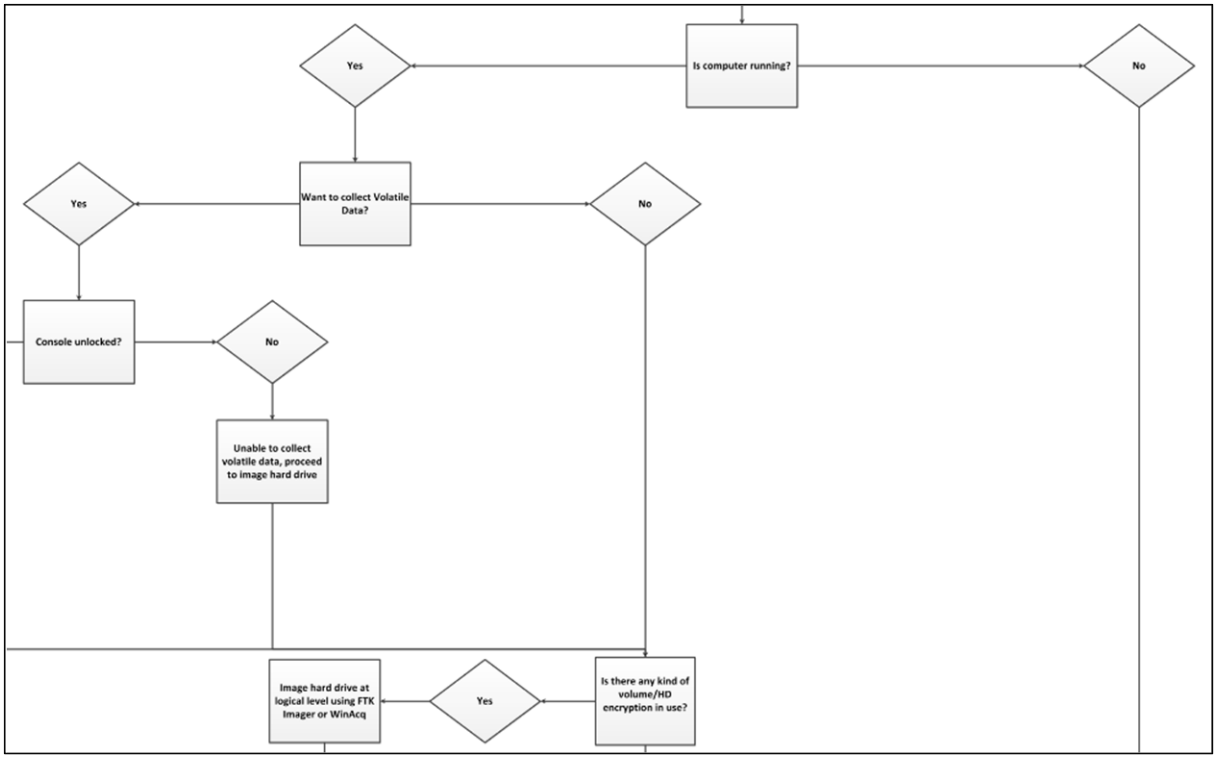

Figure 1: Example of a flow chart on e-evidence gathering

Source: Excerpt from 'Computer Forensic Hard Drive Imaging Process Tree with Volatile Data collection' by Lance Mueller

[36] Mueller, L.,'Computer Forensic Hard Drive Imaging Process Tree with Volatile Data Collection', 11 December 2010. http://www.forensickb.com/2010/12/computer-forensic-hard-drive-imaging_11.html [last accessed 11 November 2014]

7 Memory forensics

Although forensic analysis of volatile memory is out of the scope of this document as it is quite complex, it is important for the first responder to understand that sometimes the data or evidence you're looking for is only in the physical memory. In such cases a shutdown to create a forensic image of the discs will cause that data to be lost or changed. Data within physical memory that might be evidentially relevant could among other things be application processes, open files and registry handles, network information, passwords and cryptographic keys, unencrypted content, hidden data and possibly malicious code.

Data within physical memory is constantly changing and is not structured in the same way that in file systems of for example hard drives and is therefore much more difficult to predict and parse into meaningful data as a result. Hard disks have a strict pre-defined structure where analysts know where to look for certain structures and data types on a specific kind of file system. Memory can be allocated and de-allocated to different areas depending on what memory is already being used.

In many occasions passwords and configuration files reside (in decrypted form) in the memory, but can only be found on disk in encrypted form. When investigating for example a possible malware infection it might be useful to know which network connections were made. Removing a computer system from the network will terminate these connections which could possibly be very important to know.

As storage becomes cheaper and cheaper we often encounter cases where the hard drive space would take weeks to analyse as the amount of data is enormous. In these cases an appropriate and targeted memory search could give the desired results fairly quickly.

There are a number of tools that can be used to dump physical memory for different platforms and where possible the tool should be run from an external device such as a USB thumbdrive, and the memory dump itself should be saved to an external harddrive as well. A note worth remembering is that when a USB device is inserted into a PC it will leave information behind and unavoidably alter the system. In a Windows for example this would be creating entries in the Registry for the USB device being used.

8 Evidence examination

The investigation process itself involves the interpretation of the raw data and the reconstruction of events. This examination should be conducted on the data acquired and not on the original evidence. Although this examination is in most cases out of the scope for most CERTs, it is important that first responders have a good knowledge of what could be done with the evidence. Also, in some cases it could be that law enforcement asks for assistance to CERTs with regards to the examination.

8.1 Extraction

The examination and identification of evidence is dependent upon the type of crime which is being analysed. Evidential files can come in many forms, ranging from proprietary operating systems files to Internet browser artefacts. There are many techniques used to target this evidence which include but are not limited to:

- Hashing
  - Hashes are a unique string used to identify a file and ensure it has not been tampered with since its gathering.

- Keyword searching
  - Keyword searching is the process of location strings of information.
  - Often utilised in forensics to highlight files which may contain particular text which would indicate that they are evidential.
  - Can significantly cut down the time it takes to complete an investigation.

- File signatures
  - Each type of file mains a series of bytes at the beginning which identifies its type. This must be queried against the extension it has - if they match then the file is what it says it is.

- Known evidential locations
  - Specific areas of a system can be analysed to identify known relevant files.
    - Registry for MRU lists, Typed URLs etc.
    - Recent folder for records of recently accessed files.
    - Often specific Malware samples can be identified by specific files or other changes visible to the analyst

- File carving
  - Files have a file signature or string of bytes at the beginning which identifies the starting point of the file - often this is termed as the file header
  - Files often also maintain a ‘file footer’. Similar to the header, this is a unique set of bytes at the end of the file.
  - All data between the header and footer is relevant to that particular file and the process of collection of this data from unallocated areas of the disk is known file carving.

- Mounting of compound files
  - Files with an internal file structure or set of files storage within it.
  - Examples include, .zip, .rar

- Filesystem containers
    - Often interesting data is stored in filesystem containers or images which may require a password to mount. If a system is shut down access to mounted devices may no longer be possible due to missing passwords. Some filecontainers cannot be recognized as such. Thus due care is needed analysing a live system

8.2 Analysis

Once the data is extracted it can be analysed. Although the analysis of evidence is out of scope of this report, we quickly want to touch upon this topic.

One example of this analysis is the evidence from the Internet-based activities. This can take multiple forms depending on the user's choice of application for accessing Internet-based content.

Typically a user will browse the Internet using an Internet browser application, like Chrome, Internet Explorer, and FireFox.

A user visits a website by either typing in the URL (universal resource locator) for the webpage or searching for it via a search engine (e.g. Google). These actions leave behind traces known as Internet History (IH). IH is often stored in system files belonging to the web browser, however each browser maintains its own unique structure for maintaining its IH. Internet Explorer maintains IH in index.dat files, Firefox maintains SQLite database files. An analysis of IH can often reveal where a user has been whilst browsing the Internet, the time and date these actions were carried out and how often a user visits a particular site. Many browsers have the ability to delete their IH, however, even after this action has been carried out it is often possible to recover these recovered from deleted portions of the hard drive.

Another important source of information depicting Internet usage is the Internet cache and temporary Internet Files (TIF). The Internet cache is a feature of most browsers, designed to improve the user's experience whilst browsing the website by speeding up the process of rendering webpages. Every time a user visits a webpage it is downloaded to the local machine. The next time the user visits this website, the webpage can be re-built quicker by using the locally downloaded elements as opposed to downloading the website content again. This provides significant benefit to the forensic analyst as the cache maintains a record of webpages, which the user has visited which could include pictures and videos hosted on the webpage itself.

Furthermore browsers store cookies containing a plethora of information. It also should be noted, that many browsers create backups of history files which may be recovered.

Modern web browsers can operate in so called 'incognito' or 'private' mode. No information is saved then. In most of these cases preserving live evidence is the only way to go.

During the analysis it is extremely important to have the overall timeline (a list with timestamps, sources, names and descriptions of the findings). Timelines are for identifying at what point in time a certain activity has occurred on a system. They are mostly used for data reduction as well as for the identification of changes that have occurred on a certain system over time. Many forensic tools now have integrated options for timeline searches. Timelines are very powerful in the field of digital forensics but they also bring a lot of complexity with them. There can be a mismatch between BIOS and System Clock settings, settings from multiple users or even systems, etc.

One point that can lead to confusion and must be considered by the analyst is the time on the system. What time zone the system was running in. How much time was the system off from the real time? The time of some evidence is recorded in local system time. Other time stamps are recorded in UTC time. All time stamps must hence be 'normalized' to get an accurate picture.

9 Evaluating and presenting the evidence

A report must be written in a way that is suitable for a non-technical audience and digital evidence needs to be presented in a clear and accurate manner, which clearly identifies the significance of the actual evidence to the investigation. The report should focus on and verify that the evidence being presented is authentic, reliable and admissible and it should be sufficiently detailed so that an independent third party could replicate the conclusions. To support the report writing process a forensic examination requires detailed notes to be taken contemporaneously. The investigator should clearly state what forensic tools were used in the investigation to assist any reviewer in understanding the results and conclusions being made.

Casey describes reporting as "To provide a transparent view of the investigative process, final reports should contain important details from each step, including reference to protocols followed and methods used, to seize, document, collect, preserve, recover, reconstruct, organize and search key evidence."[37]

Before formally submitting a written report or presenting any results from an investigation, the investigator should validate these results. It is considered best practice to verify the evidence and the best way to verify your results is by running a second reliable forensic tool, or by manually checking the evidences original location and confirming it matches the original results.

When a digital forensic investigator presents the findings it is often beneficial to state clearly in the report how the evidence was handled and analysed to demonstrate and verify the chain of custody and also all of the investigative processes that were carried out on the evidence.

An interesting read for how to properly write such a report is the *Intro to Report Writing for Digital Forensics*[38] and the *Report Writing Guidelines.*[39] Of course the format of the report depends on the initial requirements on the investigation. It should, if possible, be agreed on beforehand.

[37] Casey, E., *Digital Evidence and Computer Crime,* Op. cit., p. 219.
[38] Garnett, B., *Intro to Report Writing for Digital Forensics*, http://digital-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics# [last accessed 10 November 2014]
[39] Kelley, M., *Report Writing Guidelines,* http://www.dfinews.com/articles/2012/05/report-writing-guidelines [last accessed 10 November 2014]

10 Final remarks

In this guide we tried to summarize some of the topics CERT first responders might encounter when engaging in activities such as electronic evidence gathering and digital forensics. This topic is so broad that it is impossible to be exhaustive, moreover it really depends very much on the case or on how to 'properly' act.

It is difficult to make comprehensive charts with what to do in specific situations, but we do recommend to try to cover as many scenarios as possible beforehand. This makes it afterwards easier to justify why a first responder those a certain course of action.

It cannot be stressed enough that the cooperation with law enforcement prior to be confronted with a real case is of utmost importance. The main recommendation of this guide is that the CERT should seek to have a discussion with law enforcement in their Member State prior to engaging in these kind of activities. It is vital that possible scenarios are presented where CERT first responders can be required to gather electronic digital evidence and what the exact roles are in those scenarios for those first responders.

TP-05-14-116-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN 978-92-9204-111-3
doi: 10.2824/068545

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu