

ELECTRONIC EVIDENCE MANAGEMENT

LUBIENIECKI JR, GENE

Program Coordinator, United States Environmental Protection Agency, Office of Enforcement and Compliance Assurance (OECA), National Enforcement Investigations Center (NEIC), Bldg 25 DFC, PO Box 25227, Denver, Colorado 80227 USA, (lubieniecki.gene@epa.gov)

SUMMARY

Evidence management is a process designed to protect the integrity of evidence and defend against allegations that evidence was tampered with or otherwise compromised. The integrity of evidence is maintained through proper handling and is supported through documentation.

Environmental enforcement personnel may collect computerized electronic information as evidence during criminal search warrants or civil compliance monitoring investigations. This paper introduces some standard procedures to protect and document the integrity of electronic evidence.

1 PROCEDURE

The integrity of electronic evidence is maintained by proper handling and appropriate documentation. The custody of this type of evidence is tracked from collection through analysis and final disposition. The following are some procedures used to protect electronic evidence and document custody while being collected and shipped.

- The project logbook (to record actions and observations relating to the evidence).
- A label or tag, with the project number and a unique identifier (to be placed on the evidence to uniquely identify that evidence).
- Tamper-evident material, e.g., tape, seal, bag (to seal the evidence itself, or the outer shipping container for the evidence).
- A chain of custody record (to document the transport and receipt of the evidence and identify the persons and carriers involved). This record contains two copies: the original to accompany the evidence during transport, and the carbonless copy for the team leader's project files.
- Locked shipping containers (to secure samples during shipping, using re-settleable combination locks if available).

- Shipping records (to document the transport of the evidence by commercial carriers. These can include freight bills, bills of lading, Federal Express air bills, etc.).

When transferring the possession of electronic evidence, the person relinquishing the evidence, as well as the person accepting the evidence, will sign, date, and note the time of transfer on the chain of custody record. Custody documentation and shipping records will be retained as part of the project file. Employees of commercial carriers do not have access to the evidence (through the use of locked shipping containers) and therefore do not sign the chain of custody record.

Once the evidence arrives at the receiving facility, receipt is documented and any abnormalities are recorded on the chain of custody record. The sealed electronic evidence is stored in fire-resistant locked cabinets within the receiving facility. When analyses are to be performed, the electronic evidence is removed from the locked cabinet and restored to a hard drive on a designated computer forensics work station. Once the data has been restored, the original evidence is returned to the locked cabinet. Actual computer forensics analysis is performed on the copies restored from the original electronic evidence, not the original evidence. To document the restoration process and maintain the link between the electronic copies to the original evidence, information concerning the restoration process (such as the person restoring, date, time, media stored on, etc.) is recorded in a bound project logbook or on bench sheets that become part of the permanent project file.

2 ELECTRONIC EVIDENCE LONG-TERM STORAGE AND FINAL DISPOSITION

After the restoration process and analyses are complete, the electronic evidence (both original and restored), including hard drives, tapes, and other electronic media will be re-sealed with a custody seal or stored in evidence bags. The evidence will be transferred to long-term secure storage. The evidence will remain sealed until a formal request is made for either further analysis or final disposition (in accordance with any particular organization's specific procedures).

When the case is closed, a copy of the original electronic evidence is copied on alternative media (currently DVDs) and retained in the permanent case file. Other copies of electronic evidence may also be transferred after receipt of a request, (verbal or written). The request for transfer of the electronic evidence must contain the date, name of requestor, and title of requestor. The request becomes part of the project file. If the electronic data is released, a custody record must be completed by the relinquisher and the receiver of the electronic evidence. A copy of the custody record for the release must be kept in the project file.

3 BIBLIOGRAPHY

Information in this paper adopted from; US Environmental Protection Agency, Office of Enforcement and Compliance Assurance, National Enforcement Investigations Center, *Evidence Management Procedure, NEICPROC/00-059R2*

Excerpt from the Proceedings of the International Network for Environmental Compliance and Enforcement's (INECE) Eighth International Conference, Linking Concepts to Actions: Successful Strategies for Environmental Compliance and Enforcement, held 5-11 April 2008, in Cape Town, South Africa.

Reproduction of this document in whole or in part and in any form for educational or non-profit purposes may be made without special permission from the INECE Secretariat, provided acknowledgement of the source is included.

The INECE Secretariat would appreciate receiving copies of any materials that use this publication as a source.

Opinions expressed are those of the authors and do not represent the views of their governments or organizations, the INECE Secretariat, or Cameron May.

Please access <http://www.inece.org/conference/8/> for the full Proceedings.

INECE Secretariat
2300 Wisconsin Ave, NW Suite 300B
Washington, DC 20007
inece@inece.org
<http://www.inece.org>