Digital Records Forensics Project

Researcher Interview Questions: Records Managers[1]

(v1.0, May 7, 2009)

General

- What do you consider to be digital records?
- Please outline the role that you have in one or more of the following activities:
    - creation, collection, maintenance, use and/or preservation of digital records
- When would you consider digital records to be trustworthy?
- When would you consider a digital record to be authentic?
    - Therefore, what for you are the characteristics of an authentic digital record?
    - When would you consider digital records to be admissible evidence with respect to authenticity?
    - Do you have any written regulations or policies with respect to the above?
- Are there specific types of digital records/digital environments that constitute a special challenge with respect to authenticity?
- Do you think that there are specific challenges to the maintenance of digital records as authentic evidence?
    - Can you describe instances in which digital records became inaccessible for evidence purposes?
    - Can you describe instances in which digital records lost their trustworthiness as evidence over time?
    - What is the longest time span that you are aware of in which digital records used as authentic evidence needed to be maintained?

Management and Preservation

- Do you have a policy or follow guidelines, rules or procedures related to the maintenance and preservation of evidence packages?
- How aware are you of the importance of maintaining authenticity over the long term?
    - Are there any explicit rules about maintaining authenticity over the long term?
- What is your procedure for the maintenance of the evidence package[2] before submission to court and for its preservation after the trial?
    - What about for the original?
    - What about for the copy?
- After trial and possible appeal, who is responsible for the preservation of the evidence package?
    - If you are responsible, where and how is the evidence package kept and for how long?
- If multiple copies of the evidence package are kept, how is it determined which is considered the authoritative version?

[1] Those involved in the administration of justice (i.e., associated with the police and/or the courts).

[2] The evidence presented to/received by the court (essentially, the exhibits to be used/used in the trial with the documentation of the entire investigatory process); includes the extracted documents, metadata, reports of the analysis, etc.

  - Who keeps it?
- Are you aware that the maintenance of live system acquisitions requires different measures?
- Do you generate management and preservation metadata?
  - Do you keep audit trails of management and preservation measures?
  - How is access to the material regulated and controlled (access privileges, passwords, encryption, etc.)?
- How do you deal with technological obsolescence, possible loss of accessibility and interoperability?
- What do you do with extracted digital material that is not included in an evidence package?
- What evidence is destroyed?
  - What evidence is retained?
  - Do you follow ARCS/ORCS in relation to digital records?
- For appeals, retrials and unsolved cases that are revived, how do you connect the old evidence with new evidence?
- How is the evidence (e.g., transcripts, proceedings, etc.) generated during the court processes; how is it managed and how is it connected to the exhibits for the purposes of:
  - the trial;
  - a possible appeal; and
  - on into the future?

Conclusive Questions

- Do you think that there is a specific knowledge necessary for anybody who has to assess the authenticity of digital records?
- What knowledge and expertise would be desirable for DRF professionals?
  - How would you assess the quality of digital forensics expertise?
  - What qualifications or certifications do you think would convey the existence of such expertise?