Digital Records Forensics Project

Researcher Interview Questions:
Digital Forensics Experts

(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?

Identification

- Do you make any distinction between digital entities that are generated in a computer environment with human intervention and those that are generated in a computer environment without human intervention?
    - If yes,
        - Why and in which way?
        - What do you do to distinguish them?
        - Do you treat them as a separate kind of evidence?
    - If not, do you consider all computer-generated materials as hearsay?
        - If yes, do you at this stage identify the business records exceptions?
- Do you make a distinction between what is a record and what is not and do you treat them in the same way? (How can evidence be submitted as hearsay if it is not acknowledged as a record at the outset?)
- Do you make any distinction between digital entities that are digital evidence and any other documentary evidence?
- How specific should the information be that you receive to determine which entities to extract from the copy?
    - After you have taken an image of the computer, on what grounds do you identify the entities that will be used to further the investigation?

- When you extract useful entities from the copy, do you preserve the documentary context of each entity? (Do you describe through metadata or other means the other entities to which the extracted one is related? For instance, if you extract an email, would you preserve the entire thread or the documents related to the email but not directly concerned with the evidence at hand?)
- What procedures do you follow to protect the authenticity of the digital material at the identification stage?
- Do you declare that the identified digital material is authentic?
    - If yes, is the declaration part of the police process of cataloging evidence?
- How do you assess the relevance to the case of the identified digital material?
    - When and how do you make decisions about relevance of the digital material?
- What techniques do you use to analyze the system to identify the relevant digital material in the system?
    - Do you use keyword searching?
        - If yes, how do you determine search keywords?
    - Do you use other search techniques?
        - If yes, what?
- Do you make determinations about how much identified material is sufficient to fulfill the purposes of the case?
    - If yes,
        - On which criteria do you base your determinations?
        - What do you do when you've found too much?
- How do you establish whether privileged documents are present?
    - If they are, are they removed?
        - If yes,
            - How?
            - How is privilege protected?

Collection

- Do you make explicit the relationship between the records you create about a case and the ones that are collected as evidence?
    - If yes, how?
- How do you protect and verify authenticity when transporting evidence from the crime scene to the DF lab?
- Are you familiar with "live system examination" [need to define]?
    - If yes,
        - Do you think that it is viable?
        - Do you have any experience with it?
        - What is your opinion of the live system examination process?
        - What kind of guarantees do you think need to be in place for a large scale implementation of a live system examination?
- What is the approval process for implementing new collection tools?
    - Have your collection tools ever been challenged?
    - What do you see as the limitations/shortcomings of the collection software/tools you use?
    - How frequently do you need to change your collection tools?
- Have you ever noticed any discrepancies between the image and the original system [define]?
    - If yes,
        - What do you think was the cause of these discrepancies?

        - What sorts of error messages have you experienced?
- What steps do you take to guarantee the integrity of the records during collection?
    - How do you document the collection process?
    - What specific information do you include in the report?
- At the time of collection, are you concerned about the long-term preservation of the extracted evidence?
    - If yes,
        - What special measures do you use to ensure its long-term preservation?
        - Are you concerned with its short-term maintenance for the presentation in court?
        - Or are you only concerned with the form of the evidence?
- Is there or should there be a policy about the long-term preservation of the extracted evidence?

Examination

- During this stage, do you begin by confirming the authenticity of the records?
- What steps are taken to guarantee their authenticity?
- What is your analysis methodology?
    - What tools/strategies do you use?
- Do you generate metadata in the course of your analysis?
    - If yes,
        - What kind/categories of metadata?
        - How are these metadata captured and how are they preserved?
- Do you preserve the original relationship between the records when selected entities are removed from the system?
    - If yes, how?

Presentation

- How do you present the evidence to the relevant parties (e.g., Crown counsel)?
    - How is evidence presented to the court?
    - How is it presented to the other side?
    - Are both sides cooperating?
- What, if any, guidelines for the presentation of evidence do the parties follow (e.g., Sedona Canada, Ontario Bar Guidelines)?
- How is it determined which of the extracted evidence is submitted to the courts?
    - What factors are considered in this determination?
- What, if anything, accompanies the evidence submitted to the courts (e.g., the metadata added during analysis, a report of the analysis, a report of the extraction process)?
- Do requirements for submission and types of information accompanying the submission change depending on the type of material or the collection process?
- Has it ever happened that evidence presented was challenged as a misrepresentation of the defendant's records?
- Has the authenticity of the submitted evidence ever been questioned?
    - What triggers a dispute over the authenticity of the submitted evidence?
    - Do you predict that it will be increasingly questioned or not?
- Are there any obstacles, in addition to the ones already identified, to the submission of evidence?
    - If yes, what?
- Do you retain a copy of what you present?
    - If yes,

        - Where?
        - How?
        - How is it handled?
- Have you been called to court to attest to the authenticity of the evidence you provided?
- Have you been called as an expert in cases for which you have not been responsible for extracting or submitting evidence?
    - If yes, what sorts of questions were you asked?
- If a case is appealed, would you be asked to reproduce or resubmit the evidence?
    - If yes, have you ever had to?
- If a new trial is ordered or a subsequent inquiry is ordered, would you be asked to reproduce or resubmit the evidence?

Management and Preservation [optional]

- 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[1] 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?
    - Where and how is the evidence package kept and for how long?
- If you keep multiple copies of the evidence package, how do you determine which is considered the authoritative version?
    - 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?
- For appeals, retrials and unsolved cases that are revived, how do you connect the old evidence with new evidence?

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?

[1] The evidence presented to 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.

- What qualifications or certifications do you think would convey the existence of such expertise?