## 6. Chain of Custody and Evidence Topics (V2)

(The author is NOT a lawyer!) Chain of Custody[1] refers to the physical, demonstrable, chronological documentation (paper) history, or trail, of the capture or seizure, custody, control points and methods, transfer, storage, check in/out, analysis, and eventual disposition of a piece of "evidence", whether it is digital or physical. CoC is most often accomplished (in the author's experience) by noting the time of evidence acquisition, the details of that acquisition, and the actual piece of evidence itself on a standard form used throughout the organization. CoC is maintained by the paper trail, log, form updates, and storage in at least a tamper evident "locker", which is then behind a locked door. A primary issue in CoC is that if the evidence can be "changed". The opposing side will be able to challenge the validity of the evidence item and the process used to acquire and store the evidence, thus it is likely to be inadmissible.

### Suggestions for Evidence Data

*Be self-documenting!* Develop a "case" directory and data structure, follow it, and make the naming convention intelligent enough to be useful. For example, name directories YYYYMMDD_CASETYPE_SUBJECTNAME. The case types would be for your organization. For example, "AV" for antivirus, "HR" for a Human Resources case, "ABUSE" from the abuse@ email handle, "EXTATTACK" for external cyber-attack, "AUP" for Acceptable Use Policy Issues (a subset of HR cases where Security identified the issue first), etc.

As you capture data in your case directory, organize it in "Box##" folders. Box folder names can be data sources, user names and then data sources, and other organizational support structures. What is important is that your case notes describe what is in a "Box", you keep "Boxes" clean, and you avoid mixing data types in "Boxes".

Name data collection files using a self-documenting standard. For example YYYYMMDD_HHMM_SOURCE_TYPE_USER. The SOURCE can be a server name, an application, a workstation name – basically the proper name of the data source. The TYPE is used to explain the type of data captured. For example: 20140202_1244_WEBSENSE_

[1] Adapted from legal dictionaries, forensic courses, and CoC Wikipedia article.

BLOCKLOG_JSMITH.csv, would be Websense block activity for a particular user called J. Smith collected on 2/2/14 at 12:44 PM.

Incident responders should read the Federal Rules of Evidence, particularly the article posted below. It is much better to be informed ahead of time.

http://federalevidence.com/rules-of-evidence#Rule901

IR : Identification : Capture and Preserve case information