**Controlling Contamination - Chain of custody-**

**Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases. Each step in the chain is essential as if broke, the evidence may be rendered inadmissible. Thus we can say that preserving the chain of custody is about following the correct and consistent procedure and hence ensuring the quality of evidence.**

**Importance of maintaining Chain of Custody-**

* **Importance to Examiner:**
* **To preserve the integrity of the evidence.**
* **To prevent the evidence from contamination, which can alter the state of the evidence.**
* **In case you obtained metadata for a piece of evidence but unable to extract any meaningful information from the metadata. In such a case, the chain of custody helps to show where possible evidence might lie, where it came from, who created it, and the type of equipment used. This will help you to generate an exemplar and compare it to the evidence to confirm the evidence properties.**
* **Importance to the Court: If not preserved, the evidence submitted in the court might be challenged and ruled inadmissible.**
* **Chain of Custody Process**
* **In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.**
* **Data Collection: This is where chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.**
* **Examination: During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.**
* **Analysis: This stage is the result of the examination stage. In the Analysis stage, legally justifiable methods and techniques are used to derive useful information to address questions posed in the particular case.**
* **Reporting: This is the documentation phase of the Examination and Analysis stage. Reporting includes the following:**
* **Statement regarding Chain of Custody.**
* **Explanation of the various tools used.**
* **A description of the analysis of various data sources.**
* **Issues identified.**
* **Vulnerabilities identified.**
* **Recommendation for additional forensics measures that can be taken.**
* **The Chain of Custody Form**

**In order to prove a chain of custody, you’ll need a form that lists out the details of how the evidence was handled every step of the way. The form should answer the following questions:**

**What is the evidence?**

**For example- digital information includes the filename, md5 hash, and Hardware information includes serial number, asset ID, hostname, photos, description.**

**How did you get it?**

**For example- Bagged, tagged or pulled from the desktop.**

**When it was collected?**

**Date, Time**

**Who has handle it?**

**Why did that person handled it?**

**Where was it stored?**

**This includes the information about the physical location in which proof is stored or information of the storage used to store the forensic image.**

**How you transported it?**

**For example- in a sealed static-free bag, or in a secure storage container.**

**How it was tracked?**

**How it was stored?**

**For example- in a secure storage container.**

**Who has access to the evidence?**

**This involves developing a check-in/ check-out process.**

**The CoC form must be kept up-to-date. This means every time the best evidence is handled off, the chain of custody form needs to be updated.**

**Procedure to establish the Chain of Custody-**

**In order to assure the authenticity of the chain of custody, a series of steps must be followed. It is important to note that the more information Forensic expert obtains concerning the evidence, the more authentic is the created chain of custody. You should ensure that the following procedure is followed according to the chain of custody for electronic devices:**

* **Save the original material**
* **Take photos of the physical evidence**
* **Take screenshots of the digital evidence.**
* **Document date, time, and any other information on the receipt of the evidence.**
* **Inject a bit-for-bit clone of digital evidence content into forensic computers.**
* **Perform a hash test analysis to authenticate the working clone.**

**How can the Chain of Custody be assured?**

**A couple of considerations are involved when dealing with digital evidence and Chain of Custody. We shall discuss the most common and globally accepted and practiced best practices.**

**Never ever work with the Original Evidence: The biggest consideration that needs to be taken care of while dealing with digital evidence is that the forensic expert has to make a full copy of the evidence for forensic analysis. This cannot be overlooked as when errors are made to working copies or comparisons need to be done, then, in that case, we need an original copy.**

**Ensuring storage media is sterilized: It is important to ensure that the examiner’s storage device is forensically clean when acquiring the evidence. Suppose if the examiner’s storage media is infected with malware, in that case, malware can escape into the machine being examined and all of the evidence will eventually get compromised.**

**Document any extra scope: During the process of examination, it is important to document all such information that is beyond the scope of current legal authority and later brought to the attention of the case agent. A comprehensive report must contain following sections:**

* **Identity of the reporting agency.**
* **Case identifier.**
* **Case investigator.**
* **Identity of the submitter.**
* **Date of receipt.**
* **Date of report.**
* **Descriptive list of items submitted for examination: This includes the serial number, make, and model.**
* **Identity and signature of the examiner**

**Brief description of steps taken during the examination: For example- string searches, graphics image searches, and recovering erased files.**

**Results-**

**Consider the safety of the personnel at the scene: It is very important to ensure that the crime scene is fully secure before and during the search. In some cases, the examiner may only be able to do the following while onsite:**

* **Identify the number and type of computers.**
* **Interview the system administrator and users.**
* **Identify and document the types and volume of media: This includes removable media also.**
* **Determine if a network is present.**
* **Document the information about the location from which the media was removed.**
* **Identify offsite storage areas and/or remote computing locations.**
* **Identify proprietary software.**

**Determine the operating system in question.**

**The Digital evidence and Digital Chain of Custody are the backbones of any action taken by digital forensic specialists. In this article, we have examined the seriousness of the digital evidence and what it entails and how slight tampering with the digital evidence can change the course of the forensic expert’s investigation.**

**References: – https://en.wikipedia.org/wiki/Chain\_of\_custody**